National Defence University
Series 1: Research Publications No. 40

Digital Soviet Union

The Russian national segment of the Internet as a closed national network shaped by strategic cultural ideas

Juha Kukkola

JUHA KUKKOLA

DIGITAL SOVIET UNION

The Russian national segment of the Internet as a closed
national network shaped by strategic cultural ideas

ACADEMIC DISSERTATION

To be presented, with the permission of the Research Council of National Defence University, for public criticism for the degree of Doctor of Military Sciences in auditorium Itälinnake at the Finnish National Defence University, Santahamina, Helsinki, on May 27th 2020 at 12:00.

NATIONAL DEFENCE UNIVERSITY
HELSINKI 2020

MAANPUOLUSTUSKORKEAKOULU
JULKAISUSARJA 1: TUTKIMUKSIA NRO 40

NATIONAL DEFENCE UNIVERSITY
SERIES 1: RESEARCH PUBLICATIONS NO. 40

DIGITAL SOVIET UNION

The Russian national segment of the Internet as a closed
national network shaped by strategic cultural ideas

JUHA KUKKOLA

NATIONAL DEFENCE UNIVERSITY
HELSINKI 2020

Juha Kukkola: *Digital Soviet Union: The Russian national segment of the Internet as a closed national network shaped by strategic cultural ideas*

Maanpuolustuskorkeakoulu
Julkaisusarja 1: Tutkimuksia nro 40
Väitöskirja /
National Defence University
Series 1: Research Publications No. 40
Doctoral dissertation

Author:	Capt. Juha Kukkola
Supervising professor:	Professor Pekka Sivonen National Defence University
Preliminary examiners:	Professor of Practice Jarno Limnéll, Aalto University
	Dr. Olli-Matti Mikkola, Finnish Defence Forces
Official opponents:	DScMil, docent, Lt Col (ret.), Petteri Lalu
	Professor of Practice Jarno Limnéll, Aalto University

Recent publications in PDF format: *http://www.doria.fi/handle/10024/73990*

Cover by: Benjamin Vanha-Majamaa & Mari Ristolainen

ISBN 978-951-25-3131-8 (pbk.)
ISBN 978-951-25-3132-5 (PDF)
ISSN 2342-9992 (print)
ISSN 2343-0001 (web)

Maanpuolustuskorkeakoulu
National Defence University

PunaMusta Oy
Tampere 2020

ABSTRACT

The Russian Federation has declared that it will develop a Russian national segment of Internet which can be disconnected from the global Internet if need be. This project is related to the wider phenomenon of militarization and fragmentation of the Internet. The Russian national segment of Internet may not only be used a tool of political control, but as a closed national network it can be used to gain a strategic advantage in cyberspace. The aim of this thesis is to understand why Russia is creating a national segment of the Internet and how this segment, operating as a closed national network, could function.

This thesis uses a modified neoclassical realist theoretical framework to argue that strategic cultural ideas give Russian military and security elites reason to pursue certain policies when confronted by an unpredictable and threatening new environment. States are able to control and shape cyberspace to their advantage using cyber power and the result of this strategy will be affected by strategic cultural ideas carried by the epistemic communities. Therefore, these ideas must be analysed in order to understand how and why national segments of the Internet are being developed as real representations of a theoretical closed national network.

This thesis argues that the ideas of an interstate struggle, digital sovereignty, strategic deterrence, asymmetric response, information superiority, unified information space, information-technological warfare, and automated command and control systems make the policies of the Russian elites reasonable and understandable. The need for political control of the Internet after 2011 and the definite change of the strategic environment in 2014 required a new strategy and, thus, new ideas were fitted to old ones to provide that strategy. The result has been a project to develop a national system of systems of information security and defence to defend Russia from information-technological and psychological threats and to possibly gain an advantage over more technologically advanced adversaries. This system of systems offers flexible, centralised and hierarchical control of the national segment of the Internet in all the phases of interstate relations. In the information era, it offers a centralized and all-seeing way to control the geographically vast Russian state, its society and economy.

The Russian national segment of the Internet is also a manifestation of old Soviet ideas in a new context and, thus, demonstrates the continuity of historical ideas in Russian security thinking. Moreover, the system of systems is a Russian version of a closed national network, which can be used for further studying the strategic-level phenomena in cyberspace. Finally, this thesis argues for a critical re-evaluation of some of the premises of the Western research on Russian cyber strategy.

Keywords: Russian Federation, national segment of the Internet, cyber warfare, strategic culture, neoclassical realism

TIIVISTELMÄ

Digitaalinen Neuvostoliitto - Venäjän kansallinen internetsegmentti suljetun kansallisen verkon strategiskulttuuristen ideoiden muokkaamana ilmentymänä

Venäjän federaatio on ilmoittanut kehittävänsä Venäjän kansallisen internetsegmentin, joka voidaan tarvittaessa irrottaa globaalista internetistä. Tämä projekti liittyy laajempaan internetin militarisoitumiseen ja fragmentaatioon. Venäjän kansallinen internetsegmentti ei ole pelkästään sisäinen poliittisen kontrollin väline. Suljettuna kansallisena verkkona sen avulla voidaan saavuttaa strateginen etu kybertilassa. Tämän väitöskirjan tavoitteena on ymmärtää, miksi Venäjä rakentaa kansallista internetsegmenttiä ja miten tämä segmentti ymmärrettynä teoreettisena suljettuna kansallisena verkkona voisi toimia.

Modifioidun neoklassisen realismin teoriakehyksen perustalta voidaan väittää, että strategiskulttuuriset ideat antavat järjellisen perusteen Venäjän sotilas- ja turvallisuuseliiteille noudattaa määrättyä politiikkaa kohdatessaan ennalta-arvaamattoman ja uhkaavan uuden ympäristön. Teorian mukaan valtiot kykenevät kontrolloimaan ja muokkaamaan kybertilaa omaksi edukseen käyttämällä kybervoimaa. Tämän strategian lopputulokseen vaikuttavat strategiskulttuuriset ideat, joita kantavat episteemiset yhteisöt. Näin ollen strategiskulttuurisia ideoita pitää tutkia, jotta ymmärretään, miten ja miksi kansallisia internetsegmenttejä kehitetään teoreettisten suljettujen kansallisten verkkojen ilmentyminä.

Tämä väitöskirja väittää, että valtioiden välisen kamppailun, digitaalisen suvereniteetin, strategisen pidäkkeen, asymmetrisen vasteen, informaatioylivoiman, yhtenäisen informaatiotilan, informaatioteknologisen sodankäynnin ja automatisoitujen johtamisjärjestelmien ideat tekevät Venäjän eliittien politiikan järkeenkäyväksi ja ymmärrettäväksi. Tarve kontrolloida internettiä vuoden 2011 jälkeen ja selkeä muutos Venäjän strategisessa ympäristössä vuonna 2014 edellyttivät uutta strategiaa ja näin ollen uusia ideoita sovitettiin vanhoihin sopivan strategian laatimiseksi. Tuloksena oli projekti kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmien järjestelmän kehittämiseksi Venäjän puolustamiseksi informaatioteknologisilta ja -psykologisilta uhilta sekä etuaseman hankkimiseksi teknologisesti kehittyneempiin vastustajiin nähden. Järjestelmien järjestelmä tarjoaa joustavan, keskitetyn ja hierarkkisen kontrollin kansallisesta internetsegmentistä kaikissa valtioiden välisten suhteiden vaiheissa. Informaatioaikakaudella se tarjoaa myös keinon kontrolloida Venäjän laajaa valtakuntaa, yhteiskuntaa ja taloutta keskitetysti ja kaikkinäkevästi. Venäjän kansallinen internetsegmentti on vanhojen neuvostoaikaisten ideoiden ilmentymä uudessa kontekstissa ja todistaa historiallisten ideoiden jatkuvuutta venäläisessä turvallisuusajattelussa. Lisäksi järjestelmien järjestelmästä tehtyjä havaintoja voidaan käyttää kybertilan strategisen tason ilmiöiden jatkotutkimukseen ja läntisen Venäjään kohdistuvan kybertutkimuksen taustaoletusten kriittiseen uudelleen arviointiin.

Avainsanat: Venäjän federaatio, internetin kansallinen segmentti, kybersodankäynti, strateginen kulttuuri, neoklassinen realismi

Note on transliteration and translation:

With the exception of some commonly occurring names, Russian words are transliterated according to the Library of Congress system. The titles of documents and specific noteworthy concepts are given in translated form with transliterations. Unless otherwise indicated all translations are by the author.

LIST OF ABBREVIATIONS

A2/AD	Anti-Access/Area-Denial
AI	Artificial Intelligence
AS	Autonomous System
ASU	Automated System of Command and Control/Management
ASAT	Anti-Satellite
BGP	Border Gateway Protocol
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CERT	Computer Emergency Response Teams
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIS	Commonwealth of Independent States
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CSIRT	Computer Security Incident Response Teams
CSTO	Collective Security Treaty Organization
DCO	Defensive Cyber Operations
DIKW	Data-Information-Knowledge-Wisdom hierarchy
DDoS	Distributed Denial of Service attack
DNS	Domain Name System
DODIN	Department of Defence (of the U.S.) Information Networks
EEU	Eurasian Economic Union
EIP	Unified Information Space
ESPD	Unified Data Network
EU	European Union
FPE	Foreign Policy Elites
FSB	The Federal Security Service of the Russian Federation
FSO	The Federal Protective Service of the Russian Federation
FSTEK	The Federal Service for Technical and Export Control of the Russian Federation
GosSOPKA	Government System for Detecting, Preventing and Eliminating the Effects of Computer Attacks
GRU (G.U.)	Main Directorate of the General Staff of the Armed Forced of the Russian Federation
GS	The General Staff of the Russian Armed Forces
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information Communication Technology
IESG	Internet Engineering Steering Group
IETF	The Internet Engineering Task Force
IO	Information Operation
IR	International Relations (a school of)
IRR	Internet Routing Registry

IoT	Internet of Things
IXP	Internet Exchange Point
ISOC	Internet Society
ISP	Internet Service Provider
ITU	International Telecommunications Union
IW	Information Warfare
KGB	Committee for State Security
LEO	Low-Earth Orbit
LPWAN	Low Power Wide Area Networks
MFA	The Ministry of Foreign Affairs of the Russian Federation
MGU	Moscow State University
MGIMO	Moscow State Institute of International Relations
Minkomsviaz’	Ministry of Digital Development, Communications and Mass Media of Russian Federation
MPLS	Multiprotocol Label Switching
MOD	The Ministry of Defence of the Russian Federation
MTSS	Multiservice Transport Network
MVD	The Ministry of Interior of the Russian Federation
NATO	North Atlantic Treaty Organization
NDMC	National Defence Management Centre
NGO	Non-Governmental Organization
NCR	Neoclassical Realism
NCW	Network Centric Warfare
NKTsKI	National Coordination Centre of Computer Incidents
NOC	Network Operation Centre
NSUD	National System of Information Management
NTIA	National Telecommunications and Information Administration
OATsSS	Integrated Automated Digital Communication System
OCO	Offensive Cyber Operations
OPK	The Defence-Industrial Complex
ORI	Register of Information Dissemination Organizers
OSCE	Organization for Security and Cooperation in Europe
PLC	Programmable Logic Controllers
POTS	Plain Old Telephone Networks
RFC	Request for Comments
RFP	Russian Foreign Policy
RIR	Regional Internet registries
RKTsKI	Regional Coordination Centres of Computer Incidents
RMA	Revolution in Military Affairs
Roskomnadzor	Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications of the Russian Federation
SCADA	Supervisory control and data acquisition systems
SCO	Shanghai Cooperation Organization
SDN	Software Defined Network
SOC	Security Operation Centre
SORM	System (of technical means) for Operative Investigative Activities

SIW	Strategic Information Warfare
SVR	Foreign Intelligence Service
TCP/IP	Transmission Control Protocol/Internet Protocol
TLD	Top-Level Domain
TsMUSSOP	Centre for Monitoring and Managing Public Communication Networks
TTsI	Technical Centre Internet
UN GGE	UN Group of Governmental Experts on Information Security
WCIT	World Conference on International Telecommunications
WTO	World Trade Organization

KEY CONCEPTS

The key concepts used in this thesis are presented and briefly explained below to assist the readability of the thesis. The formulations given below are necessarily brief and explicit. The contested nature of some of the concepts is acknowledged and thus the references given below indicate the Chapter where the concepts are introduced from previous studies, defined or derived.

Closed national network. A state-controlled segment of the Internet that can be technically disconnected from the global Internet. Chapter 3.

Cybernetics or kibernetika. A science based on studying control and communication in complex systems, i.e. goal-directed machines, living organisms, and society. Chapters 3 & 4.

Cyberspace. A man-made and governed global domain within the information environment whose distinct and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies. The Russian concept of information space includes the information infrastructure, systems, information as well as the users and their interaction. Chapter 3 & 5.

Cyber power. An ability that empowers an actor to influence others in or through cyberspace and to control and shape cyberspace to its advantage according to its preferences. The Russian concept of cyber power is an abstract idea based on control of systems and information, effectiveness, efficiency and resilience, and measurable material and human potential. Chapter 3 & 5.

Cyber resilience. The ability to anticipate, withstand, recover from, and adapt to adverse internal and external conditions of systems that include cyber resources. The Russian concept consists of the ability of communication systems and networks to operate according to specifications under internal and external disturbances and to return to their initial state. Chapter 3 & 6.

Cyber security and defence. The former refers to measures to protect computer systems, networks, and information from intentional or unintentional harm. The latter refers either to protective systems or functions explicitly designed against malicious attacks or to defensive military actions in cyberspace. Chapter 3.

Cyber warfare. The use of force based on cyber power in or through cyberspace with a coercive intent to make political gains in the context of the continuum of interstate relations. The Russian concept of information-technological warfare includes cyber or computer warfare. Chapter 3 & 5.

Cyber strategy. Ways to use means based on power to produce effects in or through cyberspace for some end. These ends, ways, means and power derive their characteristics from cyberspace but might have effects outside it. The Russian understanding of issues related to cyber strategy are incorporated in the wider concept of strategic planning and information security. Chapter 3 & 5.

Cyber asymmetry. A disproportional and exploitable offensive and defensive advantage of a nation closing its networks over a nation that has kept its national networks open. A related concept is structural cyber asymmetry which is a property of cyberspace produced by shaping it through technology, governance, norms, and politics. Chapter 3.

Defence and security elites. A group of people making decisions on state policy and use of force and responses to perceived threats. Chapter 2.

Digital territory. An analytical concept which refers to the material, functional, normative, and political elements of cyberspace. It enables the visualization and mapping of hardware, software, infrastructure, interconnections, information, human resources, protocols, services, policies and norms. Chapter 3.

Epistemic community. A network of individuals or groups sharing values, and principled and causal beliefs with an authoritative claim to policy-relevant knowledge within their domain of expertise and a common policy project. Chapter 2.

Information warfare. Actions aimed at destroying, degrading, and exploiting the information systems and information of adversaries while protecting own systems and information. This includes both kinetic and non-kinetic means. The Russian concept of information warfare has technological and psychological aspects. The latter consists of computer attacks, electronic warfare, electromagnetic attacks, guided kinetic weapons and exotic weapons. It has a geopolitical, systemic, and operational variations. Chapter 3 & 5.

Internet. A global network of interconnected networks sharing compatible protocols of communication and enabling the sharing of information and services. Part of cyberspace. Chapter 3.

Internet governance. Policies and administration related to the technology which are necessary to keep the Internet operational and the norm-building and regulation related to the relationships and interaction of the users of the Internet. Chapter 3.

National segment of the Internet. A portion of the Internet infrastructure and services which resides on a state's territory and under its sovereign jurisdiction. A real representation of a theoretical closed national network. Chapter 5.

Power ministries. A number of federal ministries, services, agencies and directorates that have armed personnel and militarized formations under their command or are authorized to use violence to respond to threats to national security. Chapter 4.

RuNet. RuNet refers to a relatively closed, online environment that is based on the Russian language but also includes a social aspect. It is the sociocultural basis of the Russian segment of the Internet. Chapter 5.

Siloviki. Group of active duty or retired but still influential officers of the 'power ministries'. Chapter 4.

Sovereignty. A state's autonomous and exclusive authority over its territory and a recognized position by other states in the international system. The Russian concept of sovereignty includes different spheres of sovereignty, for example, economic, technological and information. Chapter 2 & 5.

Strategic cultural ideas. Causal beliefs and sometimes principled beliefs held by people representing epistemic communities and, consequently, defence and security elites about the threat and use of force, and about how the means and ends fit together in issues concerning state security interests. In this thesis these include the concepts of interstate struggle, digital sovereignty, strategic deterrence, asymmetric response, unified information space, information superiority, information-technological warfare, and automated command and control systems. Chapter 2.

Strategic effect. The effects of a military use of force that have a direct relationship with policy goals or have political consequences. Conversely, an enabling effect does not directly achieve the objectives of war. The concept of enabling is sometimes used interchangeably with 'force multiplier'. Chapter 3.

System of systems. A complex system composed of multiple interconnected subsystems able to achieve results beyond the capabilities of the individual subsystems. The subsystems have their own functions are capable of operating on their own. Chapter 3.

West/Western. 'The West' denotes the United States of America and its political and military allies which were opposed by the Soviet Union and its allies during the Cold War from the late 1940s until 1989/1991. In the period after the Cold War the West and Western refer to the United States of America, Canada, Western Europe, Australia and New Zealand, including collective institutions of NATO and the European Union. It also refers to academic circles writing in English-language journals published by institutions located in the above mentioned countries. Chapter 3.

TABLE OF CONTENTS

1

INTRODUCTION

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. […] We will create a civilization of the Mind in Cyberspace. May it be more humane and fair than the world your governments have made before.

– John Perry Barlow (1947–2018), *Declaration of the Independence of Cyberspace, February 8, 1996*[1]

You should simply always bear in mind that such is the reality created by the Americans. They are the ones who did it. You know that it all began initially, when the Internet first appeared, as a special CIA project. And this is the way it is developing.

– Vladimir Vladimirovich Putin (1952–), *Media Forum of Independent Local and Regional Media, April 24th, 2014*[2]

We are engaged in a long-term strategic competition with China and Russia. These States have expanded that competition to include persistent campaigns in and through cyberspace that pose long-term strategic risk to the Nation as well as to our allies and partners.

– The United States Department of Defence, *Cyber Strategy – Summary 2018*[3]

1.1 Background and previous research

The dream of a free, or even anarchical, Internet has passed as some states, great powers among them, are carving out sovereign-territory-based blocks of cyberspace, and international IT firms are creating ecosystems centred around their proprietary systems, platforms and 'terms of service'.[4] The multi-stakeholder governance model of the Internet is increasingly being challenged by a model based on multilateral state control. The digital markets are being divided by monopolistic companies as data itself is being localized, based on the concepts of citizenship and state jurisdiction. This process has been referred to as the 'splintering', 'fragmentation' or 'balkanization' of the Internet.[5]

[1] Barlow, John Perry. A Declaration of the Independence of Cyberspace. Davos, Switzerland February 8, 1996 [Online]. Available: https://www.eff.org/cyberspace-independence [Accessed: 6th August 2018].

[2] Kremlin.ru. Media Forum of Independent Local and Regional Media, President of Russia's Official Web Portal, April 24, 2014 [English] [Online]. Available: http://en.kremlin.ru/events/president/news/20858 [Accessed: 13th July 2019].

[3] The United States Department of Defence. Cyber Strategy – Summary 2018 [Online]. Available: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF [Accessed: 3rd May 2019].

[4] DeNardis, Laura. The Global War for Internet Governance. New Haven: Yale University Press, 2014; Musiani, Francesca, Cogburn, Derrick L., DeNardis, Laura and Levinson, Nanette S. (Eds.) The Turn to Infrastructure in Internet Governance. New York: Palgrave Macmillan, 2016; Milton Mueller. Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace, Cambridge, UK: Polity, 2017.

[5] Drake, William J., Cerf, Vinton G. and Kleinwächter, Wolfgang. Future of the Internet Initiative White Paper.

The reason for the changing character of cyberspace is that it is a domain of human activity. Human beings create it and act in and through it. Cyberspace is a man-made and malleable environment.[6] For example, Nazli Choucri and David Clark have described it as "a new arena of human interaction"[7] and Jan-Frederik Kramer and Benedict Müller have used the term "cyberization of international relations [IR]" to refer to the way cyberspace has become an indistinguishable part of international politics.[8] According to scholars such as Martin Libicki and Joseph Nye Jr., states are increasingly interested and required to consider cyberspace as a domain of politics and warfare.[9] The regulation and governance of the Internet are thus becoming an issue of great power politics.[10] Consequently, what can be controlled and shaped can be converted to power through human action guided by historical ideas.

Already in 2011 Chris Demchak and Peter Dombrowski proposed a concept of 'Cyber Westphalia' for understanding how states delineated borders and reaffirmed state sovereignty in cyberspace. They foretold that states succeeding in this project could wield military cyber power more effectively than those that fail to create necessary laws and organizations. Demchak and Dombrowski were optimistic in that they saw Western nations having a material and technological advantage in this competition.[11] However, there is no reason why the advantage might not go to those states who are willing to tightly delimit and control their national networks and restrict the flow of information irrespective of technological challenges or economic difficulties.[12] Moreover, Patricia Vargas-Leon has argued that the 'shut-down' practices of some states, i.e. the disconnection of mobile and Internet networks in times of domestic

Internet Fragmentation: An Overview. World Economic Forum, January 2016. [Online] Available: http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf [Accessed: 9th August 2018].

[6] Libicki, Martin. Cyberdeterrence and Cyberwar. Santa Monica: RAND, 2009; Sheldon, John B. The Rise of Cyberpower. In Baylis, John, Wirtz, James J. and Gray, Colin S. Strategy in the Contemporary World (4th ed.) Oxford: Oxford University Press, 2013, 301-319; Bryant, William D. International Conflict and Cyberspace Superiority: Theory and Practice. New York: Routledge, 2016.

[7] Choucri, Nazli and Clark, David D. Who controls cyberspace? Bulletin of the Atomic Scientists, Vol. 69, No. 5 (2013), 21-31, 22. More precisely a domain of politics and interaction. Cf. Choucri, Nazli. Cyberpolitics in International Relations. Cambridge: The MIT Press, 2012.

[8] Kremer, Jan-Fredrik and Müller, Benedikt (eds.) Cyberspace and International Relations: Theory, Prospects and Challenges. Heidelberg: Springer, 2016, xi.

[9] Libicki, Martin C. Cyberspace in Peace and War. Annapolis: Naval Institute Press, 2016; Nye, Joseph. The Future of Power. New York: Public Affairs, 2011. Cf. also Perry, Jake and Costigan, Sean S. (eds.) Cyberspaces and Global Affairs. Surrey: Ashgate, 2012.

[10] Tikk, Eneken and Kerttunen, Mika. Parabasis. Cyber-diplomacy in Stalemate. Norwegian Institute of International Affairs, 2018 [Online]. Available: https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2569401/NUPI_Report_5_18_Tikk_Kerttunen.pdf?sequence=1&isAllowed=y [Accessed: 6th May 2019].

[11] Demchak, Chris and Dombrowski, Peter. Rise of the Cybered Westphalian Age. Strategic Studies Quarterly, Vol. 5, No. 1 (Spring 2011), 32-61.

[12] Kukkola, Juha. Russian Cyber Power and Structural Asymmetry, 13th International Conference on Cyber Warfare and Security (ICCWS), 8-9 March 2018, Washington DC, USA. Cf. also Kukkola, Juha. Cyber asymmetry – Towards new strategic thinking? In Kukkola, Juha, Ristolainen, Mari and Nikkarila, Juha-Pekka. Game Changer: Structural Transformation of Cyberspace. Riihimäki: Finnish Defence Research Agency, 2017, 131-188.

disorder, demonstrate that the control over the flow of information is a beneficial tool in the hands of authoritarian regimes.[13]

The theoretical musings of Demchak, Dombrovski, Vargas-Leon and others are currently being put into reality by the Russian Federation. It has tried to achieve comprehensive state control over the Internet from the beginning of the third term (2012–2018) of President Vladimir Putin. In 2014 the Russian Security Council declared that Russia would seek to create the ability to disconnect the Russian Internet from the global Internet.[14] This declaration was followed by the Information Security Doctrine in 2016, which stated that Russia would protect its sovereignty in the information space and develop a national system for the management of the Russian segment of the Internet.[15] In 2017 Russia adopted the Law on Critical Information Infrastructure which made it mandatory for public and private actors to protect certain critical objects of the Internet residing on Russian territory and to connect these systems to a cyber security system controlled by the Federal Security Service of the Russian Federation (FSB).[16] The National Program of Digital Economy adopted and complemented in 2017–2018 declared that Russia would achieve 'digital sovereignty' in 2020. Finally, in 2019 president Putin signed the so-called Law on Sovereign Internet, which will, if fully implemented, create a truly unified, resilient, and secure Russian segment of the Internet which can be disconnected from the global Internet by the order of the government.[17] The Digital Economy Program and related laws could, in principle, great a state-led and controlled digitalized Russian economy and society. As will be shown, this was something already dreamed of by the Soviet era scholars of cybernetics.

In previous research the above described Russian process of taking control of the national segment of the Internet has been mainly interpreted as a domestic affair and an attempt to ensure authoritarian political control over the Internet. This is the emancipatory view taken by many human rights organizations such as Russian Agora and Western Freedom House.[18] However, there are other views. Andrei Soldatov and Irina Borogan have researched the birth of the Russian Internet and emphasised the

[13] Vargas-Leon, Patricia. Tracking Internet Shutdown Practices: Democracies and Hybrid Regimes. In Musiani, Francesca, Cogburn, Derrick L., DeNardis, Laura & Levinson, Nanette S. (Eds.) The Turn to Infrastructure in Internet Governance. New York: Palgrave Macmillan, 2016, 167-188.

[14] Совет Безопасности РФ. Заседание Совета Безопасности Российской Федерации по вопросу «О противодействии угрозам национальной безопасности Российской Федерации в информационной сфере» 1 октября 2014 года [Online]. Available: http://www.scrf.gov.ru/news/allnews/831/ [Accessed: 16th May 2019].

[15] Указ Президента РФ от 5 декабря 2016 г. N 646 "Об утверждении доктриныинформационной безопасности Российской Федерации" [Online]. Available: http://rulaws.ru/president/Ukaz-Prezidenta-RF-ot-05.12.2016-N-646/ [Accessed: 21st March 2019].

[16] Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_220885/ [Accessed: 21st March 2019].

[17] Распоряжение Правительства РФ от 28.07.2017 N 1632-р "Об утверждении программы "Цифровая экономика Российской Федерации" [Online]. Available: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf [Accessed: 16th May 2019]; Федеральный закон от 01.05.2019 № 90-ФЗ "О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_323815/ [Accessed: 8th May 2019].

[18] Агора. Свобода интернета 2018: делегирование репрессий [Online]. Available: https://meduza.io/static/0001/Свобода-интернета-2018.pdf [Accessed: 1st March 2019]; Freedom House. Freedom in the

role of the security services and the KGB mentality in 'the taming of the Internet' and thus the historical continuity in the Russian approach to security issues.[19] Another, historical-cultural view is offered by Julian Nocetti who has argued that the idea of state sovereignty has influenced the Russian understanding of the Internet. In this view, Russia is thus trying to build virtual borders in cyberspace through internal policies and external norm-building diplomacy.[20] According to Nocetti, the Russian policy is in principle defensive and considers the Internet as a soft power tool.[21] The importance of the concept of sovereignty was already pointed out by Margarita Jaitner and Jari Rantapelkonen in 2013 when they argued that "the Russian information policies follow a distinct line of thought and focus, namely on sovereignty and independence in every possible aspect…"[22] Moreover, Nocetti's views on the norm-building aspect are confirmed by Eneken Tikk and Mika Kerttunen who have traced Russia's efforts to push through its version of global Internet governance in the context of the United Nations Group of Government Experts on information security (UN GGE).[23]

Russian policies have also been studied from the viewpoint of the economy and internal security. Carolina Vendil Pallin has described how state control over the independently developed Russian Internet has been achieved through the direct or indirect control of Internet companies by the state since Russian authoritarianism reasserted itself in 2012.[24] She has also provided an up-to-date overview of the Russian state policies related to the Internet.[25] Moreover, Katri Pynnöniemi has tracked the development of the Russian concept of critical infrastructure from the concept of emergency situations, through critical objects to infrastructure. In her work Pynnöniemi notes that recent development of the concept has focused on cyber vulnerabilities.[26] Thus Russia's policies are not entirely isolated from current Western trends concerning the protection of 'critical information infrastructure', however this is defined.

The above presented research is largely based on the view that the Russian Internet policy is largely a political, cultural and governance issue. However, since the annex-

World 2018 – Russia. [Online]. Available: https://freedomhouse.org/report/freedom-world/2018/russia [Accessed: 25th March 2019].

[19] Soldatov, Andrei and Borogan, Irina. The Red Web. The Struggle Between Russia's Digital Dictators and The New Online Revolutionaries. New York: Public Affairs, 2015; Soldatov, Andrei. The Taming of the Internet. Russian Social Science Review, Vol. 58, No. 1 (January–February 2017), 39-59; Soldatov, Andrei and Borogan, Irina. The New Nobility: The Restoration of Russia's Security State and the Legacy of the KGB. New York: Public Affairs, 2010.

[20] Nocetti, Julian. Contest and conquest: Russia and global internet governance. International Affairs, Vol. 91, No. 1 (2015), 111-130.

[21] Nocetti, Julian. Cyber Power. In Tsyganov, Andrei P. Routledge Handbook of Russian Foreign Policy. London and New York: Routledge, 2018, 182-198.

[22] Jaitner, Margarita and Rantapelkonen, Jari. Russian Struggle for Sovereignty in Cyberspace. Tiede ja Ase, Vol. 71 (2013), 64-89, 83.

[23] Tikk & Kerttunen 2018.

[24] Vendil Pallin, Carolina. Internet control through ownership: the case of Russia. Post-Soviet Affairs, Vol. 33, No. 1 (2017), 16-33.

[25] Vendil Pallin, Carolina. Russian information security and warfare. In Kanet, Roger E. Routledge Handbook of Russian Security. London and New York: Routledge, 2019, 203-213.

[26] Pynnöniemi, Katri (ed.) Russia´s Critical Infrastructures - Vulnerabilities and Possibilities, FIIA Report 35, 2012.

ation of Crimea in 2014, the alleged Russian offensive cyber and information operations have produced vast amounts of Western research on Russian views and techniques of information warfare.[27] As will be argued in Chapter 4 of this thesis, these interpretations are largely based on the works of Mary Fitzgerald and Timothy L. Thomas. Especially Timothy Thomas has provided the English-speaking audience with a window into the Russian military strategic thinking through multiple accounts based on primary sources starting from the 1990s. In his latest text, Thomas argues that "Russia is motivated by dangers and threats to its information space, whether they be political, economic, military, diplomatic, or other" and that it continues to search for asymmetric means to counter its enemies.[28] Dmitry Adamsky has also analysed Russian strategic thinking on information warfare and argued that the information struggle is central to the Russian doctrine and that it is holistic, unified, and uninterrupted in its nature.[29] Kier Giles is perhaps one of the most well-known current scholars on Russian information warfare although his ideas are largely based on Thomas.[30] Giles has especially warned about using Western concepts in analysing Russian thinking. He argues that Russian thinking diverges decidedly from the Western ideas on cyber and information warfare.

The main premise around which Western theories about Russian information warfare coalesced in 2016–2018 was that the Russians did not use the concept of cyber but instead differentiated between technological and psychological information warfare. Moreover, they had somehow devised a holistic, integrated, continuous and centrally controlled method of strategic-level information warfare to destabilize their opponents, i.e. the West.[31] Thus, Vendil Pallin states that Russia "sees information warfare as an integrated entity, where propaganda, electronic warfare and IT operations are all used simultaneously."[32] More recently, Katri Pynnöniemi has argued that Russia is actively defending itself through an asymmetric approach which includes a wide spectrum of information means to prevent and neutralize threats.[33] It could thus be argued that the Russian 'information offensive' is seen by Western scholars as a part of the strategic defence by an actor which is distinctly different from the West. The problem is that this line of thought has led to serious misconceptions, for example, during the Cold War.[34] Moreover, 'holists' and those emphasizing culturally and ethnically pri-

[27] For example, Google Scholar produced 40 hits on "Russian information warfare" between the time range 2000–2013 and 790 between 2014–2019 in 17th November 2019. Cf. Also NATO library guides (http://www.natolibguides.info/library/find/library_pubs).

[28] Thomas, Timothy. Russia's Expanding Cyber Activities: Exerting Civilian Control While Enhancing Military Reform. In Blank, Stephen J. (ed.) The Russian Military in Contemporary Perspective. Carlisle Barracks, PA., U.S. Army War College Press, 2019, 491-574.

[29] Adamsky, Dmitry (Dima). From Moscow with coercion: Russian deterrence theory and strategic culture, Journal of Strategic Studies, Vol. 41, No. 1-2 (2018), 33-60.

[30] This is apparent in Giles, Keir. Handbook of Russian Information Warfare. Fellowship monograph 9. Rome: NATO Defence College, 2016.

[31] Giles 2016a; Adamsky 2018; Nocetti 2018; Thomas 2019, Jonsson 2019.

[32] Vendil Pallin 2019, 211.

[33] Pynnöniemi, Katri. The Asymmetric Approach in Russian Security Strategy: Implications for the Nordic Countries, Terrorism and Political Violence, Vol 31, No. 1 (2019), 154-167.

[34] Cf. Garthoff, Raymond L. Deterrence and the Revolution in Soviet Military Doctrine. Washington D.C.: The Brookings Institution, 1990; Gray, Colin, S. War, Peace and International Relations: An Introduction to Strategic History. New York: Routledge, 2007.

mordial distinctive features of Russian thinking disregard the fact that Western military theories have adopted holistic 'complex adaptive systems' as their primary building block since the early 2000s.[35]

The importance the Russians put on information as a military strategic issue is reflected in the works by Roger N. Dermott, Jakob W. Kipp and Tor Bukkvoll.[36] They and others have argued that Russia is deeply interested in Western models of Network Centric Warfare (NCW) and is constructing its own version of this doctrine. Moreover, Julian Cooper and Andrew Monaghan have pointed out the role of strategic planning in Russian strategy.[37] Following their logic, Russia's Internet policy should be incorporated in its national economic and military planning, which aims to produce security, economic prosperity, and power. This top-down, centrally state controlled comprehensive approach to information and technology issues has its roots in the Soviet era political culture, which has been researched by Ilmari Susiluoto, Slava Gerovich and Benjamin Peters. One of their main arguments has been that the Soviet version of the science of cybernetics heavily influenced the way in which the Soviet Union tried to build its national networks.[38] They implicitly argue that it is possible for a state to construct its networks according to historical and cultural ideas, and thus the future of the Internet might not be homogenous. Moreover, in a recent study, Valeriano, Jensen and Maness have proposed that the United States, Russia and China have differing cyber strategies and understandings of the use of cyber power, which might be the result of differing strategic cultures.[39] Thus, cyberspace is what we as encultured human beings make of it. This logic is compatible with the idea that Russia, like the Soviet Union before it, is trying to find a culturally and historically bound way into something called modernity.[40]

The issues of defence and threat are also present in Martti J. Kari's doctoral thesis "Russian Strategic Culture in Cyberspace", written in parallel to this study, in which

[35] Cf. Joint Chiefs of Staff, the U.S. Department of Defence. Planner's Handbook for Operational Design, January 2011 [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pams_hands/opdesign_hbk.pdf [Accessed: 24th January 2020].

[36] McDermott, Roger N. The Transformation of Russia's Armed Forces. Twenty Lost Years. New York: Routledge, 2015; Kipp, Jacob W. 'Smart' Defense. From New Threats: Future War from a Russian Perspective: Back to the Future after the War on Terror, The Journal of Slavic Military Studies, Vol. 27, No. 1 (2014), 36-62; Bukkvoll, Tor. Iron Cannot Fight – The Role of Technology in Current Russian Military Theory, Journal of Strategic Studies, Vol. 34, No. 5 (2011), 681-706.

[37] Cooper, Julian. What If War Comes Tomorrow: Who Russia Prepares for Possible Armed Aggression, RUSI, Whitehall Report 4-16, 2016; Monaghan, Andrew. Power in Modern Russia. Manchester: Manchester University Press, 2017.

[38] Susiluoto, Ilmari. Suuruuden laskuoppi: Venäläisen tietoyhteiskunnan synty ja kehitys [Arithmetic of greatness: The birth and development of the Russian information society]. Juva: WSOY, 2006; Gerovitch, Slava. From Newspeak to Cyberspeak: A History of Soviet Cybernetics. Cambridge: The MIT Press, 2002; Peters, Benjamin. How Not to Network a Nation: The Uneasy History of the Soviet Internet. MIT Press: Cambridge, 2016.

[39] Valeriano, Brandon, Jensen, Benjamin and Maness, Ryan C. Cyber Strategy: The Evolving Character of Power and Coercion. New York: Oxford University Press, 2018.

[40] Sakwa, Richard. The Soviet collapse: Contradictions and neo-modernisation. Journal of Eurasian Studies, Vol. 4, No. 1 (2013), 65-77; Kivinen, Markku Kivinen and Cox, Terry Cox. Russian Modernisation—A New Paradigm. Europe-Asia Studies, Vol. 68, No. 1 (2016), 1-19.

Kari uses the concept of strategic culture to explain the Russian cyber threat perception and Russia's response to cyber threats.[41] Kari uses a content-analysis-based grounded theory to create a "model of Russian cyber threat perception and response to that threat". This model is based on computerized analysis of 140 official Russian government documents. He then argues that central elements of Russian strategic culture, i.e. "a sense of vulnerability, the concept of permanent war and the narrative of the besieged fortress, a Clausewitzian belief in the use of force, and a fear of external and internal enemies" can be identified as a list of preferences which guide the Russian cyber threat perception and responses to threats.[42] However, Kari's coding of Russian cyber threat perceptions is based only on official published government documents, which is a limited view. Moreover, his view of the central paradigm of Russian strategic culture is based on previous, mainly Western, studies. Additionally, he does not explain how he has come to choose the elements of the paradigm. This leads him to argue that the Russian strategic culture in cyberspace revolves around the concept of a 'besieged fortress' even though he does not critically analyse the concept and its historical and contextual roots. Additionally, as Kari conflates strategic preferences with behaviour, i.e. responses to cyber threats, his claim of 'explaining' observed behaviour can be considered suspect. Interestingly, although Kari does not state that he explores the development of threat perceptions and responses, he nevertheless offers such a summary in his conclusions. Here he differs from those such as Andrei Soldatov, who have placed the start of the Russian 'taming of the Internet' around 2012 and attributed it to reasons connected to internal policies.[43]

A more 'unorthodox' and intriguing interpretation of Russian motives has been offered by Mari Ristolainen and Juha-Pekka Nikkarila from the Finnish Defence Research Agency who proposed in a conference paper written in December 2016 that, instead of political objectives, the Russian regime might be, in fact, aiming at achieving a military advantage in cyberspace.[44] They referred to Russia with its disconnected Internet as a 'closed network nation', and argued that when its relationship to open network nations was analysed through the basic elements of combat power, the closed network nation would indeed have an upper hand. As a research officer from the National Defence University, I was invited to comment on the paper by Ristolainen and Nikkarila, after which, during the period of 2017–2019, we have written over a dozen articles together, individually or with other contributors on the subject of the Russian national segment of the Internet and its military implications. This multidisciplinary, interdepartmental academic research project has produced two published collections of conference papers titled: Game Changer: Structural Transformation of Cyberspace, and Game Player: Facing the Structural Transformation of Cyberspace and is still producing further research.[45]

[41] Kari, Martti J. Russian Strategic Culture in Cyberspace Theory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats. JYU Dissertations 122. Jyväskylä, Jyväskylän yliopisto, 2019.

[42] Kari 2019, 89.

[43] Soldatov 2017.

[44] Nikkarila, Juha-Pekka and Ristolainen, Mari. 'RuNet 2020' – Deploying traditional elements of combat power in cyberspace. Presented in the International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, May 15.-16., 2017.

[45] Kukkola, Ristolainen & Nikkarila 2017a; Kukkola, Juha, Ristolainen, Mari and Nikkarila, Juha-Pekka. Game Player. Facing the structural transformation of cyberspace. Finnish Defence Research Agency Publications 11. Riihimäki: Finnish Defence Research Agency, 2019.

In the conference papers we examined Russian policies, laws and the writings of the Russian information security theorists and concluded that Russia was shaping the strategic-level cyber battlefield to gain an asymmetric advantage through a closed national network. By disconnecting its national segment of the Internet Russia would gain a disproportionate and exploitable advantage in situational awareness, decision-making, and freedom of action.[46] As the asymmetry was based on the properties of cyberspace, I decided to call it structural cyber asymmetry.[47] Furthermore, by pursuing a cyber security policy related to an authoritarian state control over the Internet, Ristolainen, Nikkarila and I argued that Russia was shaping the entire nature of the Internet in a way that challenged the way it was governed and perhaps even the whole value base of the so-called Western world-order[48]. We continued our studies by further examining the nature of the Russian segment of the Internet and digital sovereignty, the nature of structural cyber asymmetry, and the ideas behind it, by conducting a mathematical analysis of cyber asymmetry, and even examining how wargaming could be used to understand how closed national networks worked.[49]

This thesis and its research aims and objectives are inherently tied to my research with Ristolainen and Nikkarila. I first started this work as an attempt to solve the riddle of how the Russian state viewed and used cyber power as a tool of military strategy, but as time has passed, knowledge has been accumulated, and realities have been established, I decided to concentrate on the phenomena of the closed national network. We had argued that this kind of state controlled, and disconnected segment of the Internet would provide an asymmetric advantage, but we had not truly asked *why Russia was pursuing this kind of network and how it would function*. I felt that it was important to understand what the reasons behind the policies of the Russian regime were, what has made the Russian regime to choose those policies, and how a theoretical concept of a closed national network corresponded to real-life phenomena.

Moreover, throughout our research, Ristolainen, Nikkarila and I have argued that there has been something elementary missing in the current Western cyber and military strategic research on Russia.[50] We mostly based our arguments on the regrettably scarce use of primary, Russian language sources in that research.[51] Additionally, the view of Russia as an aggressive, revisionist troublemaker and antagonist to Western

[46] For more on the theoretical background cf. Chapter 3.

[47] Kukkola 2017a & 2018a.

[48] Cf. Definitions. More precisely the term refers to a contested and admittedly political concept of the post II World War international political and economic system based on the power of the United States and its allies and some supposedly universal and modern values such as democracy, human rights, domestic and international rule of law and liberal economics. (Gill, Stephen. Power and Resistance in the New World Order (2nd ed.) New York: Palgrave Macmillan, 2008; Kundnani, Hans. What is the Liberal International Order? GMF, Policy Essay No. 17 (2017) [Online]. Available: http://www.gmfus.org/publications/what-liberal-international-order [Accessed: 15th July 2019]; Stuenkel, Oliver. Post-Western World: How Emerging Powers Are Remaking Global Order. Cambridge: Polity Press, 2016).

[49] Kukkola, Ristolainen & Nikkarila 2017 & 2019.

[50] This was first claimed by Mari Ristolainen (Ristolainen, Mari. Should 'RuNet 2020' be taken seriously? Contradictory views about cyber security between Russia and the West. In Scanlon, Mark and Le-Khac, Nhien-An (eds.) Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS), Dublin, Ireland, June 29.-30., 2017, 370-379).

[51] A noteworthy exception is Oscar Jonsson whose book on the Russian understanding of war was published in November 2019 when this thesis was already under review (Jonsson, Oscar. The Understanding of War. Blurring the Lines between War and Peace. Washington, D.C.: Georgetown University Press, 2019, 33-34).

states and values did not really contribute to a scientifically neutral discussion.[52] Furthermore, it seemed that Cold War era mirror-imaging of the enemy did little to further the understanding of how the Russians truly view cyberspace, cyber power, cyber warfare or strategy.[53] There was also the question of the interaction of Western and Russian ideas, that is, who had learned from whom and did it matter?[54] Thus, I decided to complement the research on Russian policies with a strategic cultural approach. More precisely, *I wanted to investigate what kind of strategic cultural ideas made Russian policies reasonable and how they affected the shaping and control of the Russian national segment of the Internet in the case of creating a closed national network*. I explicitly wanted to concentrate on individual ideas, not culture, as culture is quite a contested and amorphous concept.[55] I especially wanted to analyse as wide as possible a range of primary Russian sources myself, avoiding the 'idolatry' and authority-bound approach, which only repeats 'self-evident' truths and offers them as new research. Thus, I also made the decision to include original sources in this report for others to use and reflect upon, even though the manuscript may at times be demanding to read and somewhat lengthy.

I also felt that our previous research and my thesis required a robust theoretical basis. The mere listing of Internet laws, programs and projects was not enough. *I wanted to offer a theoretical explanation for why states choose to shape cyberspace in certain ways and what the role and essence of cyber power is in all of this.* Clearly, states are approaching cyberspace more and more as a sphere of action, interest and security. Cyberspace to me seemed to be a material and objective reality that state elites understand through various ideas and shape them accordingly. Thus, the basic theoretical argument is that the strategic environment in which state elites operate motivates them to behave and legitimize their actions according to strategic cultural ideas offered by groups of professionals and specialists, i.e. epistemic communities. By examining these ideas, it is possible to interpret the reasons for the policies promoted by the state defence and security elites. Because these understandings and ideas have long roots, it is necessary to examine how the legacy of the Soviet Union might still be felt in the way the Russian state approaches the Internet. Moreover, the Russian state policy is so multifaceted and multidimensional that some kind of systematic synthesis is required to make sense of it.

Against this background, I have chosen to examine the closed national network, cyberspace, power, warfare, and strategy as theoretical cross-cultural phenomena largely

[52] Cf. Chapter 4 and also Jonsson 2019.

[53] During the Cold War the Soviet views on the possibility of a nuclear war was a source of confusion and debate between game-theorists and 'culturalists'. The Russian and Chinese views on cyber warfare have reignited this discussion and whether there are or are not grounds to claim that the military strategic culture affects the making of strategy. (Gray, Colin. Soviet nuclear strategy and new military thinking. In Leebaert, Derek and Dickinson, Timothy (eds.) Soviet Strategy and the New Military Thinking. Cambridge: Cambridge University Press 1992, 28-54; Lindsay, Jon R., Cheung, Tai Ming and Reveron, Derek S. China and Cybersecurity. Espionage, Strategy, and Politics in the Digital Domain. Oxford: Oxford University Press, 2015; Mizokami, Kyle. How the Pentagon Exaggerated Russia's Cold War Super Weapons. The National Interest, June 5, 2016 [Online]. Available: https://nationalinterest.org/blog/the-buzz/how-the-pentagon-exaggerated-russias-cold-war-super-weapons-16468?page=2 [Accessed: 14th July 2019].)

[54] As shall be argued in the following chapters, whereas Western scholars have usually kept quiet about their borrowing of Russian ideas, Russians have, to the contrary, developed their ideas in open discussion with Western ideas, although, arguably in the spirit of 'creative plagiarism'.

[55] Cf. Chapter 2.

based on Western theorizing to be able to offer some comparable and generalizable knowledge. I then investigate a particular Russian understanding of these concepts to offer a more inclusive, comparable, and comprehensive interpretation of them. This approach provides an understanding on how Russian culture and history guide its approach to warfare and modernity. Furthermore, I want to take a critical look at how the Russian cyber policies have been interpreted in the West. Ultimately, I hope to provide an explanation of why the dream of late John Perry Barlow never materialized and humankind has yet again managed to transform one sphere of life into a domain of state control and ultimately, war.

1.2 Research purpose and objectives

The aim of this thesis is to understand why Russia is creating a national segment of the Internet and how this segment, operating as a closed national network could, function. My research problem has two parts, theoretical and analytical. The theoretical part examines the role of ideas in strategy making, and the related concepts of cyberspace, cyber power, cyber warfare, cyber strategy, and a closed national network. The analytical part examines the Russian strategy to control and shape a part of cyberspace into 'a national segment of the Internet' as a real case of a state creating a closed national network. In a question form the research problem is presented as: *How do strategic cultural ideas give reason to the Russian Federation's strategy to control and shape a part of cyberspace into 'a national segment of the Internet', how does this segment function in a context of conflict and what does it say about closed national networks?* By answering this problem, I aim to provide an increased understanding of Russian strategic thinking on cyber issues and its current policies and provide a case study of a closed national segment that can be adopted for comparative research on other networks and nations.

I intend to find answers to my research problem's theoretical and analytical part by answering six auxiliary research questions or subproblems, which also provide the structure of the thesis. These are:

A. What is a strategic culture and a strategic environment and how do strategic cultural ideas come to affect strategic state behaviour?
B. What is cyberspace, cyber power, cyber warfare and cyber strategy and how do states use cyber power to achieve military ends and political objectives?
C. How is cyberspace shaped by utilizing cyber power and what is a closed national network?
D. What are the Russian strategic cultural ideas of: interstate struggle, digital sovereignty, strategic deterrence, asymmetric response, information superiority, unified information space, information-technological warfare, and automated command and control systems and how they have developed?
E. How do the strategic environment and strategic cultural ideas provide reasons for the Russian strategy of shaping and controlling a part of cyberspace into a national segment of the Internet?
F. What is the Russian national segment of the Internet and how does it function?

These subproblems are informed by four theory-based premises, which are comprehensively explained in Chapters 2 and 3. The first is that the changes in a state's strategic environment and strategic cultural ideas affect the way state elites develop strategies by making some actions reasonable. The second is that cyber power enables states to shape cyberspace into a closed national network and control it. The third is that Russia is shaping cyberspace to control a part of it as a national segment of the Internet through a strategy which is reasonable in the context of strategic cultural ideas. The fourth premise is that the Russian national segment of the Internet corresponds to the theoretical concept of a closed national network and thus could provide a strategic advantage. The research purpose and objectives of this thesis are admittedly informed by a critical view of the current state of Western cyber research on Russia.[56] Moreover, they are directed towards building an interpretive understanding and no causal, positivist explanations are offered in this study. The analytical part of the research problem of this study thus forms a case study of a closed national network. The case being the Russian national segment of the Internet.[57]

This thesis' treatment of the theoretical part of the research problem is based on earlier Western or English-language scholarship. For example, the ideas of Laura DeNardis, Chris Demchak, Martin Libicki, Joseph Nye Jr., Daniel Khuel and David Betz and Tim Stevens on cyber governance and power are crucial to my own theorizing.[58] I hope to add to their knowledge by using their ideas to analyse contemporary and real manifestations of the Russian thinking on the Internet and its consequences. This is justifiable as my research strives to study the same objective and material reality that Russian officials and scholars are facing.[59] Moreover, this thesis is based on earlier research conducted by myself, Ristolainen and Nikkarila. That research is not duplicated here but it is updated and refined where necessary. When using material from earlier research I will refer to either *Game Changer* or *Game Player* books.[60] The theoretical part is therefore an attempt to adapt existing IR theory and cyber security concepts to the study of a new phenomenon, i.e. a closed national network—the nexus being cyber power and its use by states.

[56] By this I mean an emphasis on the study of actual or potential aggressive and offensive Russian behaviour against Western states in cyberspace in Western academic and policy circles, usually based on English-language secondary sources. For example cf. Jensen, Benjamin, Valeriano, Brandon and Maness, Ryan. Fancy bears and digital trolls: Cyber strategy with a Russian twist, Journal of Strategic Studies, Vol. 42, No. 2 (2019), 212-234; Blank, Stephen. Cyber War and Information War ál la Russe. In Perkovich, George and Levite, Ariel E. (eds.) Understanding Cyber Conflict: Fourteen Analogies. Georgetown: Georgetown University Press, 2017, 81-98; Geers, Kenneth (ed.) Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn: CCDCOE, 2015. Moreover, cyber security itself is recognized as dependent of the knowledge practices of different communities (Dunn Cavelty, Myriam and Andreas Wenger. Cyber security meets security politics: Complex technology, fragmented politics, and networked science, Contemporary Security Policy, Vol. 41, No. 1 (2020), 5-32).

[57] Cf. George, Alexander L. and Bennett, Andrew. Case Studies and Theory Development in the Social Sciences. Cambridge: MIT Press, 2004; Van Evera, Stephen. Guide to Methods for Students of Political Science. Ithaca, NY: Cornell University Press, 1997; Bennett, Andrew and Elman, Colin. Qualitative Research: Recent Developments in Case Study Methods. Annual Review of Political Science, Vol. 9 (2006), 457-458.

[58] Cf. Libicki 2009 & 2016; Kuehl, Daniel T. From Cyberspace to Cyberpower - Defining the Problem. In Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K. Cyberpower and National Security. Washington, D.C.: National Defence University Press, 2009, 24-42; Betz, David and Stevens, Tim. Cyberspace and the State: Toward a Strategy for Cyberpower. Adelphi Series, Vol. 51, No. 424 (2011); Nye 2012; DeNardis 2014; Demchak & Dombrowski 2011.

[59] On the philosophical foundations behind this claim Cf. Chapter 2.

[60] Kukkola, Ristolainen & Nikkarila 2017 & 2019.

The analytical part of this thesis is to a large degree founded on the work done by Raymond Garthoff, Harriet Fast Scott and William F. Scott, David Glantz, Willian Odom, Mary Fitzgerald, Timothy Thomas, Julian Cooper, Andrew Monaghan and Dmitri Adamsky, who have done a remarkable job in analysing the different elements of Russian strategic thought. I also refer to the research done by Petteri Lalu, Katri Pynnöniemi and Pentti Forsström on Russian operational and strategic thought and thus aim to add to the Finnish discussion on Russian military thinking. Moreover, Slava Gerovich, Benjamin Peters and Ilmari Susiluoto have provided an invaluable analysis of the Soviet 'kibernetik' thinking which I use to contextualize my own historical approach.[61]

The analytical part concentrates, firstly, on the writings of the Russian civilian and military scholars in the time period from the late 1950s up to 2019, and, secondly, on the official policies of the Russian defence and security elites in the time period of 2000–2019. The reasons for these limitations are as follows. Firstly, as will be argued in Chapter 2, strategic cultural ideas are carried by epistemic communities and are adopted from them by the decision-making elites. Thus, the ideas promoted by the communities must be analysed in the period before any visible change in the policies of the elites. To understand the historical roots of the strategic cultural ideas the time-period from the 1950s to the end of the 1990s is chosen as a background timeframe for analysis because it includes the adoption of cybernetic ideas as the basis of Soviet science, and the first and second Soviet Military-Technological Revolutions, and the beginning of the third.[62] During this timeframe, the terms still influencing the Russian language on computers and networks were adopted for official use.[63] Additionally, the Soviet Union was faced with a technology-based arms race in relation to the United States[64], and the Russian 'information society' began to develop which led to

[61] Adamsky, Dima. The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel. Stanford, Caroline: Stanford University Press, 2010; Fitzgerald, Mary C. Marshal Ogarkov and the New Revolution in Soviet Military Affairs. Alexandria, Virginia: CNA, 1987; Thomas, Timothy L. Russian Views on Information-Based Warfare. Airpower Journal – Special Edition 1996, 26-35; Lalu, Petteri. Syvää vai pelkästään tiheää: neuvostoliittolaisen ja venäläisen sotataidollisen ajattelun lähtökohdat, kehittyminen, soveltaminen käytäntöön ja nykytilanne. Näkökulmana 1920- ja 1930-luvun syvän taistelun ja operaation opit [Deep or just dense: Soviet and Russian military thinking, development, application in practice and current situation. From the viewpoint of the theory of the 1920s and 1930s deep battle and operations]. Doctoral thesis. NDU Publication series 1, Department of Tactics, 3/2014. Helsinki: National Defence University, 2014; Forsström, Pentti. Venäjän sotilasstrategia muutoksessa. Tulkintoja Venäjän sotilasstrategian perusteiden kehityksestä Neuvostoliiton hajoamisen jälkeen. opit [The Russian military strategy under change. Interpretations on the development of the fundaments of the Russian military strategy after the fall of the Soviet Union]. Doctoral thesis. NDU Publication series 1, Research Publication No. 32. Helsinki: National Defence University, 2019; Pynnöniemi 2019a; Gerovitch 2002; Peters 2016; Susiluoto 2006; Cooper 2016; Monaghan 2017.

[62] Sushentsov, Andrei. The Russian Response to the RMA: Military Strategy towards Modern Security Threats. In Collins, Jeffrey and Futter, Andrew (Eds.) Reassessing the Revolution in Military Affairs: Transformation, Evolution and Lessons Learned. New York: Palgrave Macmillian, 2015, 112-131; Gerovitch 2002; Adamsky 2010; Glantz, David M. The Military Strategy of the Soviet Union: A History. Abingdon, Oxon: Frank Cass, 1992; Frank, Willlard, C. and Gillette, Philip S. (Eds.) Soviet Military Doctrine from Lenin to Gorbachev, 1915-1991. Westport, Connecticut: Greenwood Press, 1992; Kokoshin, Andrei A. Soviet Strategic Thought, 1917-91. Cambridge, Massachusetts: The MIT Press, 1998; Odom, William E. The Collapse of the Soviet Military. New Haven & London: Yale University Press, 1998; Westad, Odd Arne. The Cold War: A World History. London: Penguin Random House, 2017.

[63] Susiluoto 2006; Peters 2016; Gerovitch, Slava. InterNyet: why the Soviet Union did not build a nationwide computer network. History and Technology Vol. 24, No. 4, (December 2008), 335–350; Gerovitch 2002.

[64] Sushentsov 2015; Adamsky, Dima. Through the Looking Glass: The Soviet Military-Technical Revolution and the American Revolution in Military Affairs. Journal of Strategic Studies, Vol. 31, No. 2 (2008), 257-294;

the formative years of the first Information Security Doctrine in 1997–1999.[65] The basic premise is that the strategic cultural ideas analysed in this study were formed during this period so that the elites could employ them in 2000–2019.

Secondly, the presidency and premiership of Vladimir Putin (2000–) was arguably a clear break from the somewhat chaotic period of Boris Yeltsin.[66] It has been the end of the 'Time of Troubles' (or smutnoe vremia) after the collapse of the Soviet Union.[67] Thirdly, between 2000 and 2019 several changes occurred in the strategic environment in Russia, which could have affected its policies towards cyberspace, and the Internet.[68] Fourthly, during the time-period of 2000–2019 the Russian Internet developed rapidly, was 'tamed', and, according to some, militarized.[69] Consequently, this period offers a good timeframe to analyse how the changing environment has forced the state security and defence elites to adopt and adapt old ideas to new unknown and possibly threatening situations.

1.3 Theory, structure and methodology

This thesis belongs to the field of international relations (IR)[70] and more precisely to the multidisciplinary field of Strategic Studies.[71] The focus of Strategic Studies is the study of the use of force as an instrument of policy from a theoretical and practical

Adamsky 2010; Wolfe, Audra J. Competing with the Soviets. Science, Technology, and the State in the Cold War America. Baltimore: Johns Hopkins University Press, 2013.

[65] Thomas 1996; Thomas, Timothy I. Russia's information warfare structure: Understanding the roles of the security council, Fapsi, the state technical commission and the military, European Security, Vol. 7, No. 1 (Spring1998), 156-172; Heickerö, Roland. Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. Stockholm: FOI, 2010; Soldatov & Borogan 2010; Soldatov & Borogan 2015.

[66] Sakwa, Richard. Russian Politics and Society (4th ed.) London and New York: Routledge, 2008; Lo, Bobo. Russia and the New World Disorder. Washington, DC: Brookings Institute Press, 2015; Myers, Steven Lee. The New Tsar: The Rise and Reign of Vladimir Putin. New York: Vintage Books, 2015; Cadier, David and Light, Margot. Russia's Foreign Policy: Ideas, Domestic Politics and External Relations. New York: Palgrave Macmillan, 2015.

[67] Blank, Stephen J. The Sacred Monster: Russia as a Foreign Policy Actor. In Stephen, Blank J. Perspectives on Russian Foreign Policy. Army War College Strategic Studies Institute (SSI), 2012, 25-194 [Online]. Available: http://ssi.armywarcollege.edu/pdffiles/pub1115.pdf [Accessed: 29th October 2018]. 'Time of Troubles' is not used in this thesis as an analytical concept. It refers more to a perception of time and history that actual chronological events. On the concept of 'smutnoe vremia' cf. Kåre, Johan Mjør. Smuta: cyclical visions of history in contemporary Russian thought and the question of hegemony. Studies in East European Thought, No 70 (2018), 19–40; Petersson, Bo. The eternal great power meets the recurring times of troubles: twin political myths in contemporary russian politics. European studies, No. 30 (2013), 301-326.

[68] Cf. Chapter 6.

[69] Soldatov 2017, 39-59; Агора. Россия. Свобода интернета 2016: на военном положении [Online]. Available: https://meduza.io/static/0001/Agora_Report_2017_Internet.pdf [Accessed: 8th August 2018].

[70] In this thesis I use the term International Relations to denote the discipline of study of international relations to separate it from the object of that discipline i.e. international relations. (Cf. Dunne, Tim, Kurki, Milja and Smith, Steven. International Relations Theories: Discipline and Diversity (4th ed.) Oxford: Oxford University Press, 2013, v).

[71] On Strategic Studies cf. Baylis, John, Wirtz, James J. and Gray, Colin S. Strategy in the Contemporary World (4th ed.) Oxford: Oxford University Press, 2013, 1-6; Mahnken, Thomas G. The Future of Strategic Studies. The Journal of Strategic Studies, Vol. 26, No. 1 (2003), x-xviii.

perspective.[72] It has a close and somewhat strained relationship with security studies[73], which takes a broader and more critical view on security issues, and to military studies[74], which deals with operational and tactical issues, or pedagogical and psychological issues. Strategic Studies was established during the Cold War and afterwards it has faced extensive criticism from multiple directions. It has been accused of being amoral in its search for the efficient use of force, nuclear force in particularly.[75] Additionally, it has been charged of misunderstanding the nature and character of war, of being state-centric and ethno-centric, of not taking social and cultural forces and historical change seriously, and of being generally theoretically barren.[76] This criticism has led to a certain amount of self-reflection and infighting between 'strategists' but not to the end of Strategic Studies.[77] To be clear, Strategic Studies is not a theoretical school and has not produced explanative or constitutive theories in the social scientific sense.[78] It primarily offers a conceptual framework which is based on the study of historical phenomena.[79]

I will address the shortcomings of the philosophical and theoretical side of Strategic Studies in Chapter 2 where I will construct a theoretical framework for this study. In that Chapter, I will adopt a form of 'realist analytic pragmatism' as my philosophical approach. Basically, this means that reality exists and can be studied on a case-by-case basis in its social and historical context and scientific truth, and generalizations are the

[72] Jordan, D., Kiras, James D. Lonsdale, David J., Speller, Ian, Tuck, Christopher, Dale, Walton. Understanding Modern War. Cambridge: Cambridge University Press, 2008, 17-22. According to Robert Ayson "*[S]trategic* studies has been focused primarily on the role of armed force in the context of *security* challenges that arise from the nature of the *international* system of *political* relations." (Ayson, Robert. Strategic Studies. In Reus-Smith, Christian & Snidal, Duncan (2010): The Oxford Handbook of International Relations. Oxford University Press: Oxford. 558-575, 571).

[73] Vennesson, P. Is strategic studies narrow? Critical security and the misunderstood scope of strategy. Journal of Strategic Studies, Vol. 40, No. 3 (2017), 358 - 391; Williams, Paul D. (ed.) Security Studies: An Introduction (2nd ed.) New York: Routledge, 2013; Miller, Benjamin. The Concept of Security: Should it be Redefined? The Journal of Strategic Studies, Vol. 24, No. 2 (2001), 13-42; Smith, Steve. The increasing insecurity of security studies: Conceptualizing security in the last twenty years, Contemporary Security Policy, Vol. 20, No. 3, 1999, 72-101.

[74] On Military Studies Cf. Williams, Alison J., Jenkings, Neil K., Rech, Matthew F. and Woodward, Rachel. The Routledge Companion to Military Research Methods. New York: Routledge, 2016.

[75] Strachan, Hew. The Direction of War: Contemporary Strategy in Historical Perspective. New York: Cambridge University Press, 2013, 41; Vennesson 2017, 359; Mahnken 2003, x.

[76] Creveld Van, M. The Transformation of War. New York: The Free Press, 1991; Keegan, J. A History of Warfare (2nd ed.). London: Pimlico, 2004; Kaldor, Mary. New and Old Wars: Organized Violence in a Global Era (3rd edition). Stanford: Stanford University Press, 2012; Hammes, T. X. The Sling and the Stone: On War in the 21st Century. St Paul: Zenith Press, 2006; Smith 1999.

[77] Gray, Colin S. Modern Strategy. Oxford: Oxford University Press, 1999; Strachan, Hew and Herberg-Rothe, Andreas. Clausewitz in the Twenty-First Century. Oxford: Oxford University Press, 2009; Mahnken, Thomas G. and Maiolo Joseph A. Strategic Studies: A Reader, Routledge, New York, 2014; Sloan, Elinor C. Modern Military Strategy: An introduction. New York: Routledge, 2012; Milevski, Lucas. The Evolution of Modern Grand Strategic Thought, Oxford University Press, Oxford, 2016; Strachan 2013; Freedman, Lawrence. The Revolution in Strategic Affairs. The Adelphi Papers, Vol. 45, No. 379, 2006.

[78] Cf. Gray 1999; Freedman, Lawrence. Strategy: A History. Oxford: Oxford University Press, 2013; Strachan 2013. Caveat to this claim are the game-theoretical and rationalistic models produced by, for example, the RAND corporation during the Cold war. Cf. Klinger, Janeen M. Social Science and National Security Policy. Deterrence, Coercion, and Modernization Theories. Cham, Switzerland, Palgrave Macmillan, 2019.

[79] "In this bewildering world, the search for predictive theories to guide strategy has been no more successful than the search for such theories in other areas of human existence." (Murray, Williamson, Knox, MacGregor and Bernstein, Alvin (eds.) The Making of Strategy: Rulers, State, and War. Cambridge: Cambridge University Press, 2009, 645).

product of the judgement of the scientific community. Then I will introduce the neoclassical realist (NCR) theory of IR which attempts to explain state behaviour through both internal and external variables. As the original version is mainly interested in material power and foreign policy, I amend it with the ontological and epistemological premises of the Constructivist theory of IR. I will also add to it my own interpretation of the concept of strategic culture to build a theory that supports the study of ideas and the shaping of cyberspace by state defence and security elites for military purposes. Consequently, the theory will legitimize the study of cyber issues in the context of Russian strategic thought through the writings of scholars, or epistemic communities, as well as official documents such as strategies, policies and laws and news about real events. This is important as the Russians do not use terms with a 'cyber' prefix in official legal or policy level documents and instead use the term 'information'. As will be demonstrated in Chapter 4 and 5 this terminological difference does not mean that the Russians would not be thinking and writing about the same objective reality. Political and intentional use of certain terms are, however, a different issue.

Proceeding from my IR theoretical approach, in Chapter 3, based on previous cyber security and warfare scholarship, I will construct definitions for the concepts of cyberspace, cyber power, cyber warfare, cyber strategy, and closed national network as descriptions of real objects or processes. Thus, the concepts might be understood, created and used differently by different actors, but still have an objective, independent substance and effects. A nuclear bomb is still a nuclear bomb, and a router is still a router whatever we might think of them. Most importantly Chapter 3 presents a theory on how cyberspace is shaped through cyber power, how this shaping is a distinct way to use power, and how this way relates to the concept of strategy in the context of threats and the use of military force. A closed national network is one of the results of this kind of use cyber power, and because strategy is informed by strategic cultural ideas, all closed national networks are, by definition, different. Ultimately, Chapters 2 and 3 provide answers to the subproblems from A to C.

Chapter 4 introduces the strategic cultural ideas chosen for analysis in this study. It uses the concepts defined in Chapter 3 to interpret certain Russian terms or words as denoting/signifying the same real phenomena.[80] The ideas have been chosen because they appear frequently in the current official and unofficial Russian texts which relate to issues which Western sources would call cyberspace, cyber power, and cyber warfare. They have also been noted by previous scholars and/or seem to have had temporal persistency in the Russian discourse.[81] Thus, through a preliminary reading of Russian texts and Western research on Russian information and cyber warfare and by observing ideas related to the Russian discourse on the developing digital society and economy, I have chosen a group of ideas that I argue offer a comprehensive understanding of the Russian thinking about cyberspace, power, warfare and strategy. This process has been admittedly hermeneutical and thus is not free of personal bias or potentially failed interpretations. The chosen ideas are interstate struggle (protivo-

[80] To put it simply, terms signify concepts which indirectly relate to real world objects (Chandler, Daniel. Semiotics. The Basics. New York and London: Routledge, 2007, 16-17).

[81] On the concept of discourse cf. Milliken, Jennifer. The Study of Discourse in International Relations: A Critique of Research and Methods. European Journal of International Relations, Vol. 5, No. 2 (June 1999), 225-254.

borstvo), digital sovereignty (tsifrovoi suverenitet), strategic deterrence (strategicheskoe sderzhivanie), asymmetric response (asimmetrichnyi otvet), information superiority (informatsionnoe prevoskhodstvo), information-technological warfare (informatsionno-tekhnicheskaia voina/bor'ba), automated command and control systems (avtomatizirovannaia sistema upravleniia), and unified information space (edinnoe informatsionnoe prostranstvo). I will present the arguments for choosing these ideas in Chapter 4.

My overall argument is that the above-presented terms have persistent historical meanings attached to them. Their contemporary terms and formulations are consistently and often used in the texts produced by modern Russian military and civilian scholars and in official policy documents. It is probable that there exist other causal and principled Russian beliefs[82] on cyber issues, but I argue that I have chosen the most influential strategic cultural ones, and I claim to be able to show that the chosen ideas are persistent and central to interpreting how the Russians understand cyberspace and warfare in its context. Nevertheless, if my analysis brings forth other important ideas, I will acknowledge them and incorporate them into my analysis. Moreover, I am aware that I might miss some ideas altogether because of the way I have chosen my sources or conducted my analysis. There is also the possibility that the sources I use do not reflect genuine Russian thinking. This is not a problem because I do not strive for a deductive nomological causal explanation.[83] Further research may well complement my study. I also recognize that there has been interaction between Soviet/Russian and foreign (such as Western or Chinese) ideas, but I shall partially set this issue aside as it would be a study subject of its own. However, I will note the cases where I think that the Russians have adopted ideas from the outside. This is critical for understanding how Russian ideas themselves have developed.

Chapter 4 is structured around the analysis of the chosen strategic cultural ideas in the period of late 1950s up to the year 2000. It is based on an inductive content analysis in which I interpret the substance of the ideas from previous studies and primary Russian sources.[84] The method used to collect the sources in Chapter 4 and 5 is based on the appearance of particular Cyrillic words, or English-translated versions of them,

[82] Causal beliefs are about means and ends—they provide an understanding of the world and guidelines for achieving goals in this context. Principled beliefs consist of values and attitudes describing right and wrong and proscribing appropriate behaviour. (Tannenwald, Nina. Ideas and Explanation: Advancing the Theoretical Agenda. Journal of Cold War Studies Vol. 7, No. 2 (Spring 2005), 165–173; Tannenwald, Nina and Wohlforth, William C. Introduction: The Role of Ideas and the End of the Cold War. Journal of Cold War Studies, Vol. 7, No. 2 (Spring 2005), 3–12).

[83] D-N law: An explanation is only valid if it invokes a law which covers all the cases of the phenomena to be explained (Wight, Colin. Philosophy of Social Science and International Relations. In Carlsnaes, Walter, Risse, Thomas and Simmons, Beth A. (eds.) Handbook of International Relations. London: SAGE Publications, 2005, 23-51, 41-42).

[84] Here a content analysis refers to reading sources using the terms related to the strategic cultural ideas as a means to discover the meanings attached to those terms. The reading involves such an amount of texts produced by certain sources designated as belonging to the subject of the study that no more new meanings are found, i.e. saturation is achieved. This is not a formal process involving coding or statistics—it is qualitative and interpretive process. In this thesis a content analysis is a method of interpretation and understanding through texts to gain as comprehensive understanding of an idea in its historical context as possible.

denoting the presence of strategic cultural ideas in primary sources or secondary studies.[85] Although this is a crude method for collecting material, the over 1,000 Russian language sources analysed in this thesis should provide a level of certainty that a necessary limit of saturation has been achieved. During the analysis I provide the historical context for the ideas and provide an overview of the Soviet 'kibernetik' thinking from which many of the ideas are derived. I do not strive to achieve a historical analysis—only a preliminary understanding of the ideas and a proof of their existence and nature before the 2000s. In both Chapters 4 and 5 I will present short descriptions and biographies of the institutions and writers producing the texts in footnotes, which enables me to make arguments about the sources of ideas and the relationship between epistemic communities and the elites.

Chapter 5 continues the analysis of strategic cultural ideas in the period of 2000–2019. This chapter aims to examine what kinds of ideas were present when the Russian policy towards cyberspace changed after 2011 and the state began to increase its control over the national segment of the Internet. The analysis is based on an inductive content analysis, but it analyses a wider group of sources than in Chapter 4. It introduces the Russian concept of strategic planning to help understand the process of making national strategy in Russia and to understand how ideas might end up as part of policies. Accordingly, the highest-level strategic planning documents are analysed in this chapter to examine the interaction of epistemic communities, ideas, and elites. After I have analysed the strategic cultural ideas, I present an interpretation of the Russian understanding of cyber power, cyberspace, cyber warfare, and strategy. This is an abductive[86] exercise in which my theory and concepts meet my interpretation of Russian ideas. I then summarise the development of strategic cultural ideas and examine the composition and role of epistemic communities related to cyber and information security issues. Chapters 4 and 5 provide answers to subproblem D and provide the basis for answering subproblem E because the interpreted substance of strategic cultural ideas is used in Chapter 6 to analyse how the ideas resonate with Russian policies and thus have perhaps provided reasons for adopting them.

Chapter 6 provides answers to the thesis' subproblems E and F. The Chapter is mostly based on an exercise of a loose process tracing[87] in which I firstly follow the developments in Russia's strategic environment between 2000 and 2019 to demonstrate that there was cause for a clear change in the perceptions of the defence and security elites

[85] The Cyrillic versions of the words used in the collection of material were: противоборство, цифровой суверенитет, стратегическое сдерживание, асимметричный ответ, информационное превосходство, информационная техническая война / борьба, автоматизированные системы управления, единое информационное пространство and their derivatives. There are several issues related to the translations of these Russian words into English and they will be discussed accordingly in the following chapters.

[86] In this thesis abduction is understood as interpreting social and material reality though interaction between existing theories and concepts and data to produce new understanding of a phenomenon. Cf. Chapter 2.

[87] "[Process tracing] involves the detailed study of a case to determine whether or not the hypothesized causal variables were present and/or reached the thresholds specified by the theory being tested; whether they were temporally linked (and appropriately sequenced) with any hypothesized intervening variables and the changes in the dependent variable that one is trying to explain; and whether there is evidence that the purported causal mechanism, and not other factors, actually brought about those changes." (Ripsman, Norrin M., Taliaferro, Jeffrey W. and Lobell, Steven E. Neoclassical Realist Theory of International Relations. New York: Oxford University Press, 2016, 132; Mahoney, James. Process Tracing and Historical Explanation. Security Studies, Vol. 24, No. 2 (2015), 200-218; Tannenwald, Nina. Process Tracing and Security Studies. Security Studies, Vol. 24, No. 2 (2015), 219-227; Waldner, David. Process Tracing and Qualitative Causal Inference. Security Studies, Vol. 24, No. 2 (2015), 239-250).

in 2011–2014.[88] A new and threatening change in Russia's international environment required the 'fitting' of new and old strategic cultural ideas to find ways to reasonably answer the new challenges. This part includes an analysis based on the news, reports, statistics and previous studies of the development of the Russian Internet, the international system, and cyberspace as real material or social phenomena. Secondly, I will analyse the international treatises, strategies, policies and laws that have been formed by the Russian government to tackle the new security issues brought forth by the changes in the strategic environment. I analyse the documents in a chronological order to demonstrate that they were adopted in synchronization with the changes in the strategic environment. Here official documents are considered to be representative of the will and beliefs of the elite, although their intentional political use is also noted. I will also take note of the different actors participating in this process of making and implementing strategy to better understand how Russian cyber strategy is made. I will limit myself to official declarations and news from established Russian sources and will not speculate on Russian offensive capabilities or actors. Thirdly, I will examine the civilian and military information systems and networks that the Russian regime is building or directing the private sector to build. These are approached as the practical results of making strategy and thus they reflect the ideas driving the strategy. I will use Russian news, reports, statistics, publications of various organizations and military journals as sources representing objective reality, although I retain a critical view of the declarations about the developments and the actual state of different systems. Fourthly, the question of how the national segment as a closed national network could function is answered through a synthesis of Russian and Western ideas. I will present a model of the Russian national segment of the Internet as a system of systems of information security and defence in a continuum of interstate relations in the context of military threats to understand how a closed national network could function. This cross-cultural, theoretical concept aims to make Russian strategic thinking understandable and offers a model or a framework to analyse other national segments. Moreover, this approach highlights the continuity of Russian thinking and the Soviet legacy it imposes upon the efforts to digitalize Russia. This is purely an abductive theoretical construct and it is not offered as a representation of a true object or an example of genuine Russian thinking. It is however an interpretive model that makes sense in the context of strategic, Russian, cultural ideas. It also provides a systemic synthesis of Russian strategic thinking instead of just listing separate laws and programs.

Finally, Chapter 7 provides a summary of the thesis main findings and a conclusion. The main emphasis is on demonstrating how the strategic cultural ideas and Russian

[88] The research on the influence of epistemic communities starts by discovering some interesting policy change in the past. It then backtracks to study what kinds of communities had corresponding or competitive ideas or subcultures before the policy change was initiated. External events and decision-makers, as well as interpretations of and initial reactions to them are examined to understand what the policy change was a reaction to. Then, the way in which epistemic communities package their ideas, i.e. develop statements, is studied and how different statements compete on public forums, including media. This debate might take place long before the elites discover they have a need for a new policy. After that, the process of how the elites choose from the statements or subcultures available is examined through policy documents and official statements by the elite. The actual interaction between communities and elites might be opaque, particularly in autocracies. Consequently, the implementation of a chosen policy is observed to see if it corresponds to the ideas one or another epistemic community had. (Libel, Tamil. Explaining the security paradigm shift: strategic culture, epistemic communities, and Israel's changing national security policy. Defence Studies, Vol. 16, No. 2 (2016), 137-156).

policies have interacted, facilitated by epistemic communities, over time and in a certain strategic environment to produce a national segment of the Internet as a reasonable strategic answer to perceived challenges. I will also provide critical reflections on this project and its possible future as well as on the nature of closed national networks. Furthermore, I will discuss the broader issue of the Russian understanding of cyberspace, power, and warfare. I will also reflect upon my own research and possible avenues of further research.

1.4 Sources

I use previous Western scientific-philosophical writings on IR, and neoclassical realist and constructivist IR theoretical texts, and research on strategic culture and cyber security and warfare in Chapters 2 and 3. The material consists mainly of monographs published by leading scholars and articles published in peer-reviewed IR, political science and Strategic Studies journals.[89] I have used article databases such as the EBSCO Military & Government Collection, JSTOR Arts & Sciences and Taylor & Francis Strategic, Defence & Security Studies to ensure that I have included a comprehensive and current scholarship on international relations, strategy, and cyber security issues as best as possible up to January 2019. I have added some more recent sources as they appeared during and after the review process of my manuscript from August to December 2019.

The collection and selection of sources in both Chapters 4 and 5 is based on my theoretical arguments in Chapter 3, according to which there are separate although tightly connected epistemic communities discussing Russian policies towards cyber or information space. 'Tightly' is a qualitative modifier indicating that many of the people who write publicly about cyber or information security issues have similar backgrounds in military or security services. I have chosen the sources listed below based on the premise that the members of these communities publish their ideas in a group of military and other journals, and that either the writers or their products reach the elites. I have complemented the journals with monographs published by individual writers who I have deemed to be influential, as they have either been referred to in other works or have held important advisory positions in the Russian government. Because of how I have chosen my source material I will not be able to analyse all communities and all ideas. For example, civilian technology experts and academicians publishing in regional journals are not included. Nevertheless, I claim that the material allows me to capture some of the most important communities and ideas possibly influencing the defence and security elites.[90] However, it must be kept in mind that

[89] The journals include among others Journal of Slavic Military Studies, Journal of Strategic Studies, Security Studies, International Affairs, Survival, European Security, World Politics, Political Science Quarterly, Contemporary Security Policy, Cambridge Review of International Affairs, International Organization, Connections, Strategic Analysis, Comparative Strategy, Bulletin of The Atomic Scientists, Problems of Post-Communism, Baltic Defence Review, Journal of Information Warfare, International Studies Quarterly, International Security, European Journal of International Relations, International Studies Review, among others.

[90] My argument is based on Fitzgerald 1987a; Fitzgerald, Mary C. Marshal Ogarkov on Modern War: 1977-1985. Alexandria, Virginia: CNA, 1987; Thomas, Timothy. Russia – Military strategy: Impacting 21st Century Reform and Geopolitics. Fort Leavenworth, KS: FMSO, 2015; Thomas, Timothy. Kremlin Kontrol: Russia's Political' Military Reality. Fort Leavenworth, KS: FMSO, 2017; Adamsky 2008 & 2010; Bukkvoll 2011; Nocetti 2015; Marten, Kimberly. The 'KGB State' and Russian Political and Foreign Policy Culture, Journal of Slavic Military Studies, Vol. 30, No. 2 (2017), 131-151; Bateman, Aaron. The Political Influence of the Russian Security

not much is known about the theoretical thinking of the Soviet or Russian secret services, and that knowledge about Soviet strategic thought is still based on testimonies, declassified military journals and interviews.[91] My analysis of strategic cultural ideas is based on strictly open and public sources.

The Russian language primary source materials for Chapter 4 and 5 were initially chosen by searching through the EastView Russian Military & Security Periodicals database, the Russian eLibrary database and the Electronic Dissertation Library of the Russian State Library using key words deducted from the strategic cultural ideas.[92] I also searched the databases of declassified Cold War era documents of the CIA and some others for translated secret Soviet material.[93] Thus, the source material includes both the available basic and top-secret versions of the Military Thought journal.[94] After analysing the initial findings in the context of previous studies, the databases were explored again to collect the final set of source material. Lastly, this set of sources was complemented with sources indicated by the previous research on Russian IW but not found in the above-mentioned databases. A second set of sources is a collection of monographs which were chosen because they were referred to multiple times in the journal articles or because their writers have participated as experts on the formulation of Russian cyber/information policy.[95] Some articles from these same writers have also been chosen to add more depth and actuality to the quite theoretical monographs. Consequently, much of the source material comes from the people associated with the Russian Academy of the Military Sciences and other various military academies, various military research centres, and State Universities who write in the leading military and information security journals and who have had some connection

Services, The Journal of Slavic Military Studies, Vol. 27, No. 3 (2014), 380-403; Skak, Mette. Russian strategic culture: the role of today's chekisty. Contemporary Politics, Vol. 22, No. 3 (2016), 324-341; Soldatov & Borogan, 2010 & 2015; Haslam, Jonathan. Near and Distant Neighbours. Oxford: Oxford University Press, 2015; Garthoff, Raymond L. Soviet Leaders and Intelligence: Assessing the American Adversary During the Cold War. Washington, DC: Georgetown University Press, 2015.

[91] The most current history of Russian secret services is a proof of this statement. Cf. Haslam 2015.

[92] Key words were: кибер*, информацион*, асимметр*, сетев*, сетецентрическ*, автоматиз*, управлени*, противоборств*, суверенитет* and сдерживани*. The main journals used as sources are the Bulletin of the Academy of Military Sciences (Вестник Академии военных наук), the Military Thought (Военная Мысль), the Red Star (Красная звезда), the Military Industrial Courier (Военно-промышленный курьер), the Nezavisimaia Gazeta - Military Review (Независимая газета - Военное обозрение), the Information wars (Информационные войны), the Bulletin of the Moscow State Institute of International Relations (Вестник МГИМО) and some others. EastView [Online]. Available: https://www.eastview.com/ [Accessed: 16th July 2019]; Electronic Dissertation Library (Russian State Library) [Online]. Available: http://sigla.rsl.ru/search.jsp?e=Cp1251&c=14i&i18n=ru&s= [Accessed: 5th December 2018]; Научная электронная библиотека [Online]. Available: https://elibrary.ru/defaultx.asp [Accessed: 16th July 2019].

[93] University of Texas Libraries [Online] Available: https://guides.lib.utexas.edu/c.php?g=524005&p=3584595 [Accessed: 5th December 2018]; Central Intelligence Agency Library [Online]. Available: https://www.cia.gov/library/readingroom/historical-collections [Accessed: 5th December 2018]; Wilson Center – Digital Archive [Online]. Available: https://digitalarchive.wilsoncenter.org/collection/37/end-of-the-cold-war/2 [Accessed: 5th December 2018].

[94] Cf. Lalu, Petteri and Kivimäki, Veli-Pekka. The leading Russian Military journal Voennaia mysl' available in the EastView digital database. The Finnish National Defence University Department of Warfare Series 3: Working Papers No. 15, 2019 [Online]. Available: https://www.doria.fi/bitstream/handle/10024/173304/Lalu%26Kivim%C3%A4ki_VoeannaiMysl_database_web.pdf?sequence=1&isAllowed=y [Accessed: 28th December 2019].

[95] The writers are, among others, I. Ashmanov (И. Ашманов), A. A. Efremov (А.А. Ефремов), A. Kondrat'ev (А. Кондратьев), S. I. Makarenko (С. И. Макаренко), A. V. Manoilo (А.В. Манойло), I. Panarin (И. Панарин), S. P. Rastorgyev (С.П. Расторгуев), L. V. Savin (Л.В. Савин), A.A. Streltsov (А. А. Стрельцов), and V. N. Tsygichko (В.Н. Цыгичко).

to the defence and security elites of the Russian Federation in the time frame of 2000–2019. The guiding principle in choosing the source material has been saturation—not a total and comprehensive representation—because no amount of time would be enough to analyse all that the Russians have written about information or cyber security.[96] The earliest of these sources are from the 1950s and the most recent from the late 2019.

A third set of sources are the official government documents, strategies, policies and federal laws, of the Soviet Union or the Russian Federation.[97] The documents have been chosen based on their place in the hierarchy of official security documents, the importance that previous research has given to the documents, and their relation to the subject of cyber or information security.[98] Every strategy, policy and law from the period of 2000–2019 concerning the cyber or information security is included in the analysis.[99] Some important documents from the early 2020 have also been included. Although speeches and statements by foreign and security policy elites could be considered a legitimate source of analysis I shall, nevertheless, omit them almost completely and concentrate on strategies, policies and laws because it is through these that cyberspace is shaped—through administration, planning, and resource allocation not so much by the statements Vladimir Putin or people around him.

In Chapter 6 I will almost exclusively use previous studies or news to track the development of the strategic environment of Russia. Previous studies quite often provide data on both real events and the interpretations of the Russian decision-making elite of the events. Furthermore, they use sources that complement the ones used in this study, i.e. statements of the elites, media and public opinion and economic data. Sources on the Russian segment of Internet and its systems consist of a multitude of news, reports, statistics, and statements. I will use news services such as TASS, RIA Novosti and Izvestiia, which could be considered non-independent, but also RBK, Kommersant and Vedomosti, which at least try to remain semi-independent, and Meduza, Novaia Gazeta and Roskomsvoboda, which are definitely critical of the Russian regime. I shall also use public statements, reports and other publications by the

[96] Journal articles or monographs based on mathematical modelling are not included in this study. I do not have the required competency to examine these models. In the context of the era of 2000-2018 one group that is left out are the private sector lobbyists with commercial interest and the second are the ‘technopeople’ i.e. engineers, programmers etc. The third group are the active representatives of security services and others who do not publicly publish their ideas but may still write memorandums etc. which affect the elites. The fourth and perhaps the most important group are some of the private think-tanks such as the Medvedev era liberal INSOR think tank and the Putin era anti-liberal Izborskii Club and forums such as the Valdai Club. I have included some NGOs that directly and actively engage in information security issues but have tried to otherwise avoid think thanks whose main audience are foreign experts and governments. (Cf. Vendil Pallin, Carolina and Oxenstierna, Susanne. Russian Think Tanks and Soft Power. FOI, August 2017 [Online]. Available: https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4451--SE [Accessed: 5th April 2019].)

[97] A list of webpages and databases is provided at the end of the Bibliography.

[98] The main documents are the National Security Concept of 1997 and 2000, the National Security Strategies of 2009 and 2015, the Basic Provisions of the Military Doctrine of the Russian Federation of 1993, the Military Doctrines of 2000, 2010 and 2014, the Foreign Policy Concepts of 2008, 2013 and 2016, and the Information Security Doctrine of 2000 and 2016.

[99] The Law on Strategic Planning lists the main national strategic planning documents and it has been used to collect the middle and lower level implementation documents analysed in Chapter 6. (Федеральный закон от 28.06.2014 N 172-ФЗ (ред. от 31.12.2017) “О стратегическом планировании в Российской Федерации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_164841/ [Accessed: 26th March 2019]).

Russian military, government, institutions and private companies to investigate the nature of Russian information networks and systems. Throughout the thesis I make a conscious choice to use as many Russian-language primary sources as possible to offer some new substance to the Western debate on Russian cyber strategy.

1.5 Research limitations and self-reflection

I have already discussed some of the limitations of this thesis above. Here I will reflect on some more normative issues. Firstly, I am a Finnish military officer writing about Russian cyber strategy in the context of the threat or use of force and thus I am aware of my own cultural and political biases. I try offer as an objective interpretation of the Russian strategic cultural ideas and Russian policies as I can. Secondly, I am highly aware of the possible Western cultural bias inherent in IR research and theories (and Strategic Studies) as IR is a predominantly Northern American -Western discipline and its theories are very much based on interpretation of American-European history.[100] The theories of IR and Strategic Studies are induced from temporal experiences and might not be transferable in time. What Thucydides said about Athens and Sparta, is not directly translatable to the United States and Russia or China—to say nothing about cyberspace.[101] Moreover, theories might travel poorly between cultures and to use Western concepts to study Russian thinking might be considered problematic. My argument is that we all inhabit the same reality and there is knowledge to be gained by comparing our understandings. Some concepts are needed to initiate this comparison. I choose to start this comparison from the West, and then advance to the Russian side. I accept that my theory and concepts might lose their connection to the material and social reality as time passes.[102] This is in fact the case, as during the writing of this thesis the Russians began to adopt the term cyber into their official vocabulary.

Thirdly, I have made a conscious decision not to discuss the literature on alleged Russian offensive cyber operations or information-psychological operations. This is because this study does not examine offensives or operations and concentrates on the defensive information-technological aspects of the Russian IW. Fourthly, I also recognize that many of the documents I analyse are part of the diplomatic and strategic signalling, agenda setting, and are meant for domestic audiences to legitimize the policies of the elites. Nevertheless, I approach these documents as genuine expressions of worldviews, beliefs, interests, and intentions. Moreover, in Chapter 6 I analyse documents which are meant for implementation, and their effects can be observed in the allocation of resources, making of laws, and construction of information systems and networks. Thus, ideas materialize. Many of the Russian scholars whose texts I analyse in Chapters 4 and 5 write for semi-propagandistic purposes or at least to promote their own interests. This does not present a problem as the thesis examines ideas

[100] Darby, Philip. A Disabling Discipline. In Reus-Smith, Christian and Snidal, Duncan. The Oxford Handbook of International Relations. Oxford University Press: Oxford, 2010, 94-105.

[101] On the uses of Thucydides Cf. Misenheimer, Alan Greeley. Thucydides' Other "Traps" The United States, China, and the Prospect of "Inevitable" War. Washington, D.C.: National Defence University Press, 2019.

[102] I argue that the analysis of strategy or international relations is based on pragmatic knowledge. As such, I acknowledge that this thesis is not only an academic effort but also an attempt to make sense of the strategic behaviour of the Russian Federation. I also acknowledge that my study is connected to a certain political and historical context, to the resurgence of great power competition in the 2010s, and as such is itself a historically bound endeavour.

about reality, not reality itself. Furthermore, I use such a large mass of sources that no single view becomes too prominent. However, I do acknowledge that some military and civilian academicians have taken part in preparing national security documents and the relationship between their texts and official policies might be complex and political.

Fifthly, many of the concepts used in the thesis are 'essentially contested concepts'.[103] They have no agreed meaning and their definitions might carry political and cultural connotations. Culture is one such a contested concept as are concepts related to cyberspace, power and warfare.[104] Thus, I try to be as precise as I can in defining and using these concepts. Sixthly, my qualitative and interpretive methodology based on the pragmatic philosophy of science makes issues about reliability moot. The validity of this thesis is based upon the judgement of the scientific community. Thus, as I proceed with my analysis, I strive to compensate for the lack of rigorous, positivistic method with sharp, logical and critical thinking. Finally, as the Russian project to shape and control its national segment of the Internet is still ongoing, this thesis will not provide the final word on the issue.

[103] Collier, David, Hidalgo, Fernando Daniel and Maciuceanu, Andra Olivia. Essentially contested concepts: Debates and applications. Journal of Political Ideologies, Vol. 11, No. 3 October 2006), 211–246.

[104] On contested nature cf. Lango, Hans-Inge. Competing academic approaches to cyber security. In Friis, Karsten Friis and Rinsmose, Jens (eds.) Conflict in Cyber Space. Theoretical, strategic and legal perspectives. New York: Routledge 2016, 7-26.

2

NEOCLASSICAL REALISM AND STRATEGIC CULTURE

For its loose theoretical framework, this thesis adopts a tailored version of neoclassical realism (NCR), which is a school of IR. In this chapter I position my study in the theoretical field of IR and at the same time construct my theoretical framework. I start by presenting my philosophical and metatheoretical premises and then move on to examine the IR schools of realism and constructivism whose interaction has produced NCR as a school of IR. I then move on to examine the basic premises of NCR, which will form the basis of the theoretical framework of this thesis. I continue with an overview of the role of ideas and power in IR theory so that I can modify NCR for the needs of this study. Furthermore, I examine the theory of strategic culture so that I can draw together ideas, power and the use of force. I conclude this chapter by presenting a synthesis that will provide an NCR-based theoretical framework for this thesis. In the next chapter I will further develop my theoretical framework by introducing the key concepts of cyberspace, cyber power and cyber warfare. Additionally, I will integrate these concepts in the theoretical framework through the concept of strategy.

2.1 Philosophies of sciences

According to Steve Smith "The study of international relations has classically focused on the analysis of the causes of war and the conditions of peace."[105] The definition of the IR is however contested for many reasons, politics of science being not the least among them.[106] One reason that the definition of IR is so contestable is its disciplinary history, which has been under a constant review for the last 30 years. Traditionally IR's disciplinary history is understood through 'debates' between various theoretical positions, sometimes called 'paradigms' or 'research programs.' In some accounts these 'debates' have been seen as discourses about the scientific nature of IR, and in others more emphasis has been given to the historical context and to the change of international system or practical knowledge required by the clientele of IR.[107] The view shared by many textbooks is that there have been at least three maybe four great

[105] Dunne, Kurki & Smith 2013, 1.

[106] Brown, Chris and Ainley, Kirsten (eds.) Understanding International Relations (3rd ed.) Palgrave Macmillan: New York, 2005,7; Waever, Ole. Still a discipline after all these debates? In Dunne, Tim Kurki, Milja and Smith, Steven. International Relations Theories: Discipline and Diversity (4th ed.) Oxford: Oxford University Press, 2013, 300-321. For other views cf. Schieder, Siegfried and Spindler, Manuela (eds.) Theories of International Relations. New York: Routledge, 2015; Reus-Smith, Christian and Snidal, Duncan. The Oxford Handbook of International Relations. Oxford University Press: Oxford, 2010; Carlsnaes, Walter, Risse, Thomas and Simmons, Beth A. (eds.) Handbook of International Relations. London: SAGE Publications, 2005; Burchill, Scott, Linklater Andrew, Devetak, Richard, Donnelly, Jack, Paterson, Matthew, Reus-Smith, Christian and True, Jacqui. Theories of International Relations (3rd), New York: Palgrave Macmillan, 2005.

[107] Schmidt, Brian C. On the History and Historiography of International Relations. In Carlsnaes, Risse, & Simmons 2005, 3-22; Schieder & Spindler 2015; Reus-Smith & 2010; Carlsnaes, Risse & Simmons 2005; Burchill, Linklater, Devetak, Donnelly, Paterson, Reus-Smith, C. & True 2005; Brown & Ainley 2005.

'debates'.[108] The first two were between idealists and realists (1930–1940) and between traditionalists and behaviourists (1950–1960). The nature of their issues are relatively widely accepted. The third 'debate' (1970–1980/1990) is much more controversial and has been variously described as neorealism versus neoliberalism or realists versus pluralists versus Marxists[109] or positivism[110] versus post-positivism[111] or rationalism[112] versus reflectivism[113]. Clearly, there have been many simultaneous debates.[114]

What is important about the third 'debate' in the context of this thesis is that IR started to incorporate more ideas from the social sciences.[115] This gave birth to, among other things, the field of Security Studies[116] and back in the 1970s this affected

[108] Dunne, Kurki & Smith 2013; Schieder & Spindler 2015; Reus-Smith & Snidal 2010; Carlsnaes, Risse & Simmons 2005; Burchill et al. 2005; Brown, & Ainley 2005. It is only natural that the whole idea of 'debates' has been challenged by critical disciplinary historiography in the spirit of post-positivist self-reflection (Schmidt, Brian. Lessons from the Past: Reassessing the Interwar Disciplinary History of International Relations. International Studies Quarterly, Vol. 42, No. 3 (September 1998), 433-459; Katzenstein, Peter J., Keohane, Robert O. and Krasner, Stephen D. International Organization and the Study of World Politics. Vol. 52, No. 4, pp. 645-685).

[109] Neorealism refers to Kenneth Waltz's structural realism and its later versions by other authors. Neoliberalism concentrates on the effects of international institutions on rational actors and builds on the seminal work of Robert Keohane and Joseph Nye. Realism is a name for a heterogenous collection of approaches emphasizing the role of states, power and the balance of power in international relations. Pluralism refers to an even wider collection of approaches with or without a normative agenda which emphasize the role of sub-state actors. Marxism in IR can be described as critical approach to the current (capitalist) world-order. (Cf. Dunne, Kurki & Smith, 2015).

[110] "(a) 'a commitment to unified view of science, and the adoption of methodologies of the natural sciences to explain the social world'; (b) 'the view that there is a distinction between facts and values, and, moreover, that "facts" are theory neutral'; (c) 'a powerful belief in the existence of regularities in the social as well as the natural world. This, of course, licenses both "deductive-nomological" and the "inductive statistical" forms of covering law explanation'; and (d) 'a tremendous reliance on the belief that it is empirical validation or falsification that is the hallmark or "real" enquiry'". (Adler, Emmanuel. Seizing the Middle Ground: Constructivism in World Politics. European Journal of International Relations, Vol. 3, No. 3 (1997), 319-363, 348-349) Also cf. Smith, Steve. Positivism and Beyond. In Smith, Steve, Booth, Ken, and Zalewski, Marysia: International theory: Positivism and Beyond. Cambridge: Cambridge University Press, 1996, 11-44). According to Wight, Positivism is based on the following premises 1) Phenomenalism (appearances, not realities, are the only objects of knowledge) 2) Nominalism (there is no objective meaning to the words we use) 3) Cognitivism (value judgements and normative statements have no cognitive value) 4) Naturalism (unity of scientific method i.e. social sciences do not differ from natural sciences). (Wight 2005, 41-42).

[111] An approach that "rejects the possibility of a science of international relations which uses standards of proof associated with the physical sciences to develop equivalent levels of explanatory precision and predictive certainty." (Burchill et al. 2005, 2).

[112] "…conscious goal-seeking agents pursuing their interests within an external environment characterized by anarchy and the power of other states." (Adler 1997, 348.)

[113] "[Reflectivists] … stress the role of impersonal social forces as well as the impact of cultural practices, norms, and values that are not derived from a calculation of interest." (Wight 2005, 23-51, 39).

[114] Ole Weaver has provided perhaps the most detailed and empiricist accounts of the debates. (Waever, Ole. The Sociology of a Not So International Discipline: American and European Developments in International Relations, International Organization, Vol. 52, No. 4, Autumn, 1998, 687-727; Waever 2013. Katzenstein and Sil have proposed a divide between positivism (inductive and deductive reasoning) and subjectivism (interpretation) and pragmatism (context bound consensus-based knowledge) (Katzenstein, Peter and Sil, Rudra. Eclectic Theorizing in the Study and Practice of International Relations. In Reus-Smith & Snidal 2010, 109-130.) On debates Cf. Katzenstein, Keohane & Krasner 1998.

[115] For the role of sociology in the development of IR cf. Lawson, George and Shilliam, Robbie. Sociology and international relations: legacies and prospects. Cambridge Review of International Affairs, Vol. 23, No. 1, 2010, 69-86.

[116] Buzan, Barry. People, States and Fear: An agenda for international security studies in the post-cold war era. Colchester: ECPR Press, 2007; Buzan, Barry, Wæver, Ole and de Wilde, Jaap: Security: A New Framework for Analysis. London: Lynne Rienne Publishers inc., 1998; Buzan, Barry. 'Change and insecurity' reconsidered. Contemporary Security Policy, Vol. 20, No.3, 1999, 1-17; Smith 1999; Williams 2013.

the then heavily rationalistic and materialistic Strategic Studies by introducing the concept of strategic culture.[117] It also gave birth to the school of constructivism which has challenged (neo)realism's authority on the questions of power and the use of force in international relations. This has forced realists to refine their theories and has led to the development of the neoclassical realist school. Additionally, the third 'debate' made understanding or interpretivism a legitimate epistemological approach in IR—although what was exactly meant by it has been debated ever since.[118] All in all, the third 'debate' produced many of the theoretical ideas applied in this thesis.

The debates have not ended. Some accounts link a part of the third 'debate' to the fourth one beginning in the 1990s, and some consider the fourth 'debate' to be based on the convergence of IR and social theory characterized by 'the cultural turn'[119], 'the practice turn'[120], and 'the pragmatic turn'.[121] The debate has been framed by a philosophical disciplinary reflections and has led to the fragmentation of the field.[122] In this context, Patrick Jackson and Daniel Nexus argue that because IR theories are not incommensurable they should be viewed as alternative 'cuts' or 'ideal types' of the object that is studied.[123]

Discussions about the philosophy of science were already strongly present in IR during the 1990s and have continued up until this day.[124] This is understandable because IR is interested in the social reality, which is arguably a complex entity because of the varied and changing nature of social objects and their relations. It is also full of unobservable aspects—including its main objects of study: states, norms, power and the international system itself. The main points of the debate can be summarized by asking: Is there a reality? What kind of reality is it? What can be known about this reality? How can we gain that knowledge? and what kind of methods should be used for

[117] Snyder, Jack L. The Soviet Strategic Culture: Implications for Limited Nuclear Operations. R-2154-AF. Santa Monica, RAND corporation, 1977 [Online]. Available: https://www.rand.org/content/dam/rand/pubs/reports/2005/R2154.pdf. Accessed: 28 May 2018; Strachan 2013, 136-137.

[118] The distinction between explaining and understanding was first introduced to IR by Martin Smith and Steve Hollis (Smith & Hollis 1991). Their views have been criticized, for example, by Colin Wight who argues that the separation of explaining and understanding has no basis in the philosophy of science (Wight 2005, 23-51).

[119] Michael Desch has argued that there have been at least three cultural turns or 'waves' in IR studies. In 1998 he predicted that the current third wave will fail to supplant Realism. Desch, Michael C. Culture Clash. Assessing the Importance of Ideas in Security Studies. International Security, Vol. 23, No. 1 (Summer 1998), 141-170.

[120] "In seeing 'practices' as the stuff that drives the world and makes it 'hang together', the everyday practices of diplomats, terrorists, environmentalists, or financial analysts become the object of investigation." Bueger, Christian and Gadinger, Frank. The Play of International Practice. International Studies Quarterly Vol. 59, No. 3 (2015), 449-460, 449.

[121] Schieder & Spindler 2015, 4-9.

[122] Reus-Smith & Snidal 2010, 32; Katzenstein & Sil 2010; Kurki, Milja and Wight, Colin. International Relations and Social Science. In Dunne, T., Kurki, M. and Smith, S. International Relations Theories: Discipline and Diversity (4th ed.) Oxford: Oxford University Press, 2013, 14-35.

[123] Jackson, Patrick Thaddeus and Nexon, Daniel H. Paradigmatic Faults in International-Relations Theory. International Studies Quarterly Vol. 53, No. 4, (December 2009), 907-930. This view is also reflected in the approach taken in Strategic Studies at the Finnish National Defence University (Sivonen, Pekka. Suomalaisia näkökulmia strategian tutkimukseen [Finnish approaches to Strategic Studies]. Maanpuolustuskorkeakoulu, Julkaisusarja 1: Strategian tutkimuksia No. 33. Tampere: Juvenes Print, 2013).

[124] For a discussion about this in the context of political science cf. Gunnell, John G. Realizing Theory: The Philosophy of Science Revisited. The Journal of Politics, Vol. 57, No. 4 (November 1995), 923-940; Jonathan, Joseph and Wight, Colin (eds.) Scientific Realism and International Relations. Basingstoke: Palgrave, 2010; Jackson, Patrick Thaddeus. The conduct of inquiry in International Relations: philosophy of science and its implications for the study of world politics. London and New York: Routledge, 2011.

gaining knowledge? In the context of these debates, my thesis positions itself in the middle-ground between realism, pragmatism and practise theory.

Realism as a philosophy of science is understood in IR either as Alexander Wendt's Scientific Realism or Critical Realism advocated, for example, by Heikki Patomäki, Milja Kurki, Jonathan Joseph and Colin Wight.[125] Highly simplified basic premises of realism are that there is a material and social reality independent of the mind, and that we can have theories about this reality, study it through observation, but positivistic causality[126] is refuted.[127] Some versions of realism propose elaborate theories about the structure and mechanisms of reality—the nature of which can be observed though events etc. The critical version highlights these structures as a form of power and has an openly emancipatory nature.[128] However, to avoid determinism, Emmanuel Adler has argued that realism accepts 'emergent' properties of structures and mechanisms.[129] This basically means that social reality changes over time and we have to adapt our theories to it and thus cannot have universal explanative theories about social reality.[130]

Pragmatism[131] is a counter reaction to Marxist and overtly theoretical critical realism. It has been offered as a *via media* between rationalism/positivism and relativism.[132] Pragmatism has converged with 'the practice turn' which seeks to overcome, among other things, the agency – structure dichotomy[133] by introducing practices as an object of analysis. These developments cross-cut almost all schools of IR and there have been hopes that a synthesis of pragmatism and practice theory could provide IR with

[125] Wendt, Alexander. Social Theory of International Politics. Cambridge: Cambridge University Press, 1999; Chernoff, Fred. Scientific Realism as a Meta-Theory of International Politics. International Studies Quarterly, Vol. 46, No. 2, (June 2002), 189-207; Patomaki, Heikki and Wight, Colin. After Post-positivism? The Promises of Critical Realism. International Studies Quarterly, Vol. 44, No. 2 (Jun. 2000), 213-237; Jackson 2011, xiv.

[126] According to Wight this is based on the D-N law, i.e. an explanation is only valid if it invokes a law which covers all the cases of the phenomena to be explained (Wight 2005, 41-42). Cf. also Wendt 1999, 79.

[127] Wight 2005; Jonathan & Wight 2010; Jackson 2011.

[128] Archer, Margaret, Roy Bhaskar, Andrew Collier, Tony, Lawson and Alan Norrie (eds.) Critical Realism: Essential Readings. London and New York: Routledge, 1998; Nash, Roy. Explanation and quantification in educational research: the arguments of critical and scientific realism. British Educational Research Journal, Vol. 31, No. 2, (April 2005), 185-204; Patomäki & Wight 2000, 223.

[129] Cooper, Luke. Can contingency be 'internalized' into the bounds of theory? Critical realism, the philosophy of internal relations and the solution of 'uneven and combined development', Cambridge Review of International Affairs, Vol. 26, No. 3 (2013), 573-597.

[130] Kurki & Wight 2013, 28-29.

[131] Pragmatism has been claimed as 'the American philosophy'. Although, it has gained renewed popularity at the beginning of 2000s, it was already applied in IR in the first half of the 1990s. Kaag, John and Kreps, Sarah. Pragmatism's contributions to international relations, Cambridge Review of International Affairs, Vol. 25, No.2, 2012, 191-208; Hamati-Ataya, Inanna. Beyond (Post)Positivism: The Missed Promises of Systemic Pragmatism. International Studies Quarterly, Vol. 56, No. 2 (June 2012), 291-305.

[132] Hellman, Gunther (ed.) Pragmatism and International Relations. International Studies Review, Vol. 11, No. 3 (September 2009), 638–662; Pratt, Simon. Pragmatism as Ontology, Not (Just) Epistemology: Exploring the Full Horizon of Pragmatism as an Approach to IR Theory. International Studies Review, Vol. 18, No. 3 (September 2016) 508–527.

[133] This dichotomy refers to the relationship between structure and agent, i.e. which causes or constitutes which? "The agent-structure problem then, is concerned with the relationship between active and self-reflecting agents and the structural context in which their activity takes place." (Wight 2005, 24). Also cf. Wight, Colin. Agents, Structures and International Relations: Politics as Ontology, Cambridge: Cambridge University Press, 2006; Banerjee, Sanjoy. Rules, Agency, and International Structuration. International Studies Review, Vol. 17, No. 2 (June 2015), 274–297; Knafo, Samuel. Critical approaches and the legacy of the agent/structure debate in international relations. Cambridge Review of International Affairs, Vol. 23, No. 3, (September 2010), 493-516).

a new, unified path in the future.[134] The basic, yet again highly simplified, premises of pragmatism are: There is truth but it is context-bound, i.e. knowledge is situated; theory must be adapted to the reality it is describing; knowledge is achieved through academic consensus otherwise called the consensus theory; and the relationship of agents and structures is not a priori postulated.[135] Friedrichs and Kratochwil have proposed the ideas of a theory synthesis[136], analytic eclecticism[137], and abduction[138] as pragmatic methods of research. They also make a point about the importance of 'triple hermeneutics' in pragmatic research, involving: understanding human practice, the reflexivity of intersubjective rationalizations of the practitioners, and taking a critical approach to the concepts researchers themselves use.[139] Pragmatism has enjoyed increasing popularity in IR theorizing, but IR has also been criticized for a free-handed application of pragmatism's philosophical foundations.[140] Although pragmatism seems to share many similarities with realism(s) there are some differences which seem to be about the status of 'unobservable' entities and causal mechanisms.[141] However, because both theories acknowledge the ideal and material nature of 'social reality' it could be argued that what the differences boil down to is what kind of claims we can make before doing research and how comprehensively we can make them, whether we should study actions and experiences or structures and power, and what kind of universalist claims we can make about our findings. As Patrick Jackson has argued, the differences between IR approaches are methodological.[142] Thus, from a pragmatist point of view it is quite possible to adopt a scientific or critical realist ontology if the case under study so requires. The philosophical premises of the theory of this thesis are thus realist but analytically eclectic.

In the context of the 'third/fourth debate' discussions about pragmatism and scientific realism have mainly stayed on the metatheoretical level. On a more concrete level 'Practice theory' has been proposed as one way to move forward. It tries to step

[134] Adler, Emanuel and Vincent Pouliot. International practices. International Theory, Vol. 3 No. 1 (February 2011), 1-36.

[135] Jackson & Nexon 2009; Jackson, Patrick Thaddeus. Situated Creativity, or, the Cash Value of a Pragmatist Wager for IR. In Hellman 2009, 656-659; Friedrichs, J. and Kratochwil, F. On Acting and Knowing: How Pragmatism Can Advance International Relations Research and Methodology. International Organization, Vol. 63, No. 4 (Fall, 2009), 701-731.

[136] Different theories on different levels of explanation which share the same ontology are compared to alternative theories with a different ontology. (Friedrichs & Kratochwil 2009, 723-724).

[137] The reinterpretation of analysis through different methods to find different explanations. (Friedrichs & Kratochwil 2009, 723-724). According to Katzenstein and Sil, analytic eclecticism means the problem-based application of different theories and methods, combining them creatively—not using the same theories and methods as the criteria for the accumulation of knowledge (Katzenstein & Sil 2010; Sil, Rudra. Simplifying Pragmatism: From Social Theory to Problem-driven Eclecticism. In Hellman 2009, 648-652).

[138] "We therefore start collecting pertinent observations and, at the same time, applying concepts from existing fields of our knowledge. Instead of trying to impose an abstract theoretical template (deduction) or "simply" inferring propositions from facts (induction), we start reasoning at an intermediate level (abduction)." (Friedrichs & Kratochwil 2009, 709).

[139] Friedrichs & Kratochwil 2009.

[140] On recent theoretical efforts cf. Bauer, Harry and Brighi, Elisabetta (eds.) Pragmatism in International Relations. Oxon: Routledge, 2009; Ralston, Shane J. (ed.) Philosophical Pragmatism and International Relations. Plymouth, UK: Lexington Books, 2013; Pratt 2016.

[141] Cf. Patomäki & Wight 2000; Kurki & Wight 2013; Wight 2005; Kratochwil, Friedrich. Of False Promises and Good Bets: A Plea for a Pragmatic Approach to Theory Building (The Tartu Lecture). Journal of International Relations and Development, Vol. 10, No. 1, (March 2017), 1-15; Wight, Colin. A Response to Friedrich Kratochwil: Why Shooting the Messenger Does Not Make the Bad News Go Away. Journal of International Relations and Development, Vol. 10, No. 3 (September 2007), 301-315.

[142] Jackson 2011.

around the agent vs. structure debate and proposes practices as an object of study.[143] According to Emmanuel Adler and Vincent Pouliot practices are characterized by "the patterned nature of deeds in socially organized contexts."[144] They depend on reflexive, normative, and instrumental judgments. Practices are political processes that occur between communities, and they can be studied as intervening variables in the constitution of strategic interaction. Although agents and structures are persistent, practices are introduced to explain why states act as they do—practice precedes socialization.[145] Christian Bueger and Frank Gadinger divide Practice theory into critical continental and American pragmatist versions. The critical version concentrates on power and domination, that is, stability, regularity and reproduction of power, and the pragmatist version on continuous stream of acts without end i.e. situations, contingency, creativity, and change.[146] The importance of Practice theory for this thesis is in that it highlights the process of strategy making which I will return to below.

Before summarizing my philosophical scientific position, it is important to note the discussion on the normative characteristics of IR theory. Firstly, there is the uneasy possibility that researchers choose their theories based on ideology—that the way we scientifically approach international relations is based on political beliefs.[147] Secondly, it has been argued that many academics have flown 'too close to the sun', i.e. that the practical policy needs they have tried to serve have affected their research, or that their theorizing has been somehow amoral.[148] And thirdly, it is now widely accepted that IR is characterized by American/Western intellectual hegemony and insularity.[149] However, the claim that a more pluralistic, inclusive and regionalist IR would be somehow superior is suspect.[150] If 'Western exceptionalism' is replaced by 'Russian exceptionalism' based on a politically motivated ontology and relativistic epistemology then locally produced knowledge does not advance IR as a global discipline.[151] This is the main reason I do not apply Russian theories in my thesis. Although I subscribe to interpretivist epistemology, I believe that by using the so-called Western theories and by writing in English I expose my research to a wider audience, and through that to a more comprehensive criticism of the scientific community.

Because this thesis approaches social phenomena, such as power, states and their environment and cyberspace as a priori real, I subscribe to the realist philosophy of

[143] Vincent Pouliot introduced the concept to IR (Pouliot, Vincent. The Logic of Practicality: A Theory of Practice of Security Communities. International Organization, Vol. 62, No. 2 (Spring, 2008), 257-288).

[144] Adler & Pouliot 2011.

[145] Ibid.

[146] Bueger & Gadinger 2015.

[147] Rathbun, Brian. Politics and Paradigm Preferences: The Implicit Ideology of International Relations Scholars. International Studies Quarterly, Vol. 56, No. 3 (September 2012), 607-622; Onuf, Nicholas. Of Paradigms and Preferences. International Studies Quarterly, Vol. 56, No. 3 (September 2012), 626-628.

[148] Shapcott, Richard. Critical Theory. In Reus-Smith & Snidal 2010, 331-334.

[149] Maliniak, Daniel, Peterson, Susan, Powers, Ryanand and Tierney, Michael J. Is International Relations a Global Discipline? Hegemony, Insularity, and Diversity in the Field, Security Studies. Security Studies, Vol. 27, No. 3 (2018), 448-484; Reus-Smith & Snidal 2010, 27.

[150] Cf. Acharya on 'Global IR' (Acharya, Amitav. Global International Relations (IR) and Regional Worlds - A New Agenda for International Studies. International Studies Quarterly (2014) 58, 647-659).

[151] Makarychev, Andrey and Morozov, Viatcheslav. Is "Non-Western Theory" Possible? The Idea of Multipolarity and the Trap of Epistemological Relativism in Russian IR. International Studies Review, Vol. 15, No. 3 (September 2013), 328-350; Omelicheva, Mariya Y. and Zubytska, Lidiya. An Unending Quest for Russia's Place in the World: The Discursive Co-evolution of the Study and Practice of International Relations. New Perspectives, Vol. 24, No. 1, (2016), 19-51.

science. Nevertheless, I do not claim that these phenomena are unchanging or that they can be a priori objectively known to be true. They must be understood in the context of time and place through the interpretation of meanings given to them by social actors. Although knowledge about the social is fleeting, it does not mean we should not make claims about it. We must accept that these conceptual and theoretical claims are contextual and related to specific cases and based on the knowledge that is currently available. Therefore, my approach is based on a synthesis of pragmatism, scientific and critical realism and practice theory. Realism provides the basis for making a priori, ontological, theoretical assumptions about social reality but does not provide any practical views on methodology. Pragmatism provides a beneficial approach to theory-building and methodology which is based on abduction, problem-based theory synthesis and analytic eclecticism but is silent about ontology. It also emphasises the study of specific cases and unique outcomes the generalization of which is a result of the judgement scientific community. Both accept similar kinds of scientific explanations—claims about social reality in a specific context.[152] Practice theory provides an approach for studying the role of ideas in a social process that affects both the structure and the actors. It helps me to bring different schools of IR and Strategic Studies together. What these philosophical choices mean in the framework of this thesis is that I can claim that both Western and Russian concepts are representations related to the same reality and can be compared and used to examine that reality in a specific context.[153] In conclusion, I resort to throwing one more 'philosophical hand grenade'[154] and claim to be a realist analytic pragmatist.[155] To add some more 'shrapnel' to this grenade I also incorporate elements of Practice theory in my own theory through the concept of 'making of strategy' as will be shown in this and subsequent chapters. I will now continue to examine the IR schools of realism and constructivism to legitimize the theoretical part of my research question: why power matters and why ideas are important.

2.2 Realism and constructivism

The roots of the realist school can be traced either to a line of premodern political thinkers or to the first debate in IR in the 1930-1940s between idealists and realists—the first party were named idealists by the self-declared realists. Realism has gone through multiple phases and has branched into various distinct theories and schools which share some common basic assumptions which can be distinguished from each other, for example, by their chosen level-of-analysis and ontological assumptions about the agent-structure relationship.[156] For example, classical realists are interested in state action and usually find causes from the subunit level, whereas neorealists or

[152] For a discussion about Critical Realism and Pragmatism see Jackson 2009; Hamati-Ataya 2012; Kratochwil 2017; Wight 2007.

[153] "Social facts emerge from the attachment of collective meaning to a previously existing material reality […] Material reality is made meaningful by rules, reasoning and collective understandings. That can be studied to explain social reality." Adler, Emmanuel. Constructivism and International Relations. In Carlsnaes, Risse & Simmons 2005, 95-118, 98.

[154] The phrase is from Colin Wight (Wight 2005, 26)

[155] Pratt 2016; Gunnell 1995.

[156] Cf. Wohlforth, William C. Realism. In Reus-Smith & Snidal 2010, 131-149; Elman, Colin and Jensen, Michael A. Realism. In Williams 2013, 15-31; Temby, Owen. What are levels of analysis and what do they contribute to international relations theory? Cambridge Review of International Affairs, Vol. 28, No. 4 (2015), 721-742.

structuralists examine the international system and explain state actions based on the structure of the international system.[157] Realism has been defined, mainly by its critics, to consists of the following theoretical assumptions: instrumentally rational[158] unitary states are the most important actors in international relations; the main interest of states is power because international relations are characterised by anarchy, self-help and thus a struggle for power and survival; and power is material and thus a relative resource.[159] One important concept of realism is balancing, which refers to the way great powers try to match their power with other great powers either by acquiring more power or through alliances.[160] Balancing is difficult because states are faced with 'the security dilemma'.[161]

Realism is, in principle, based on materialism[162] and positivism, which has been a source of substantial criticism since the 1980s. It has also, unsurprisingly, been unable to produce a theory that manages to generally and universally explain international relations even if some of its versions have adopted elements of other theories—a source of further criticism.[163] Constructivists, for example, have criticized realism for not taking the effects of ideas seriously or for smuggling ideas into their theories to explain inconvenient outcomes.[164] Some of this criticism is a bit unfair, because there is no 'monolithic' realist school.[165] It is easy to construct some simplified version of

[157] Narizny, Kevin. On Systemic Paradigms and Domestic Politics: A Critique of the Newest Realism. International Organization, Vol. 42, No. 2, (Fall 2017), 155-190; Wohlforth 2010. Neorealism is usually associated with Kenneth Waltz. The basic premises of Waltz's theory of the international political system consist of the ordering principle (hierarchy or anarchy); the differentiation of the functions of units (states are like units—there cannot be any differentiation of tasks under insecurity so self-help is the only possible way to succeed); and the distribution of capabilities (number of great powers is the only explaining variable). Cf. Waltz, Kenneth. Theory of International Politics. Boston: Addison-Wesley, 1979; Mearsheimer, John J. Structural Realism. In Dunne, Kurki & Smith 2013, 51-67; Vasquez, John A. The Realist Paradigm and Degenerative versus Progressive Research Programs: An Appraisal of Neotraditional Research on Waltz's Balancing Proposition. The American Political Science Review, Vol. 91, No. 4 (December 1997), 899-912.

[158] "The efficient pursuit of exogenously determined interests within the constraints of available information, the interests and strategies of other actors, and the distribution of power." (Reus-Smith, Christian. The Moral Purpose of the State: Culture, Social Identity, and Institutional Rationality in International Relations. Princeton: Princeton University Press, 1999, 159-160).

[159] Vasquez 1997, 899-912; Elman & Jensen 2013; Legro Jeffrey W. and Moravcsik, Andrew. "Is Anybody Still a Realist?" International Security, Vol. 24, No. 2 (Fall 1999), 5-55.

[160] On the balance of power theories cf. Levy, Jack S. and Thompson, William R. Hegemonic Threats and Great-Power Balancing in Europe, 1495-1999. Security Studies, Vol. 14, No. 1 (January–March 2005), 1-33; Donnelly, Jack. Realism. In Burchill, et al. 2005, 29-54.

[161] Basically, when one actor becomes more secure the security of others is reduced. On security dilemmas cf. Jervis, Robert. Cooperation Under the Security Dilemma. World Politics, Vol. 30, No. 2 (January 1978), 167-214; Glaser Charles L. The Security Dilemma Revisited. World Politics, Vol. 50, No. 1, Fiftieth Anniversary Special Issue (October 1997), 171-201.

[162] According to Ian Hurd Realism at its core is "… about materialism (that is, the theory that states respond to material need, incentives, and power) and rationalism to be about instrumentalism (that is, the theory that states pursue individual advantage by calculating costs and benefits)." (Hurd, Ian. Constructivism. In Reus-Smith, & Snidal 2010, 298-316, 299).

[163] Vasquez 1997; Legro & Moravcsik 1999; Feaver, Peter D., Hellman, Gunther, Schweller, Randall L., Taliaferro, Jeffrey W., Wohlforth, William C., Legro, Jeffrey W. and Andrew Moravcsik. Brother, Can You Spare a Paradigm? (Or Was Anybody Ever a Realist?). International Security, Vol. 25, No. 1 (Summer 2000), 165-93; Finel, Bernard I. Black Box or Pandora's Box: State Level Variables and Progressivity in Realist Research Programs. Security Studies, Vol. 11, No. 2 (Winter 2001/2) 187-227; Narizny 2017.

[164] Cf. Ruggie, John Gerard. What Makes the World Hang Together? Neo-Utilitarianism and the Social Constructivist Challenge. International Organization, Vol. 52, No. 4, (Autumn, 1998), 855-885; Katzenstein, Peter J. (ed.) The Culture of National Security: Norms and Identity in World Politics. New York: Columbia University Press, 1996; Lebow, Richard N. Why Nations Fight: Past and Future Motives for War. New York: Cambridge University Press, 2010.

[165] Wohlforth 2010, 131-149.

realism and argue against it. In fact, realists do not agree amongst themselves on the sources of conflict in international systems, on how states assess one another's intentions and promote security for themselves, or even on the likelihood and causes of major wars.[166] The constant criticism has led to some self-reflection and historicism by realists.[167] Additionally, by drawing on classical realism, realists have tried to fix the perceived problems of Structuralist theories and to build some kind of synthesis.[168] NCR can be considered such a synthesis, although it is primarily a theory of foreign policy.[169]

The main challenger of realism has been constructivism which has also affected the development of neoclassical realism.[170] Constructivism developed in IR as a criticism of positivist, structuralist, rationalist and materialist theories in the 1980s and drew its inspiration from sources such as sociology and the English school.[171] Constructivism used its novel approach to study such phenomena as intersubjective[172] meaning in world politics, social norms, rules, and discourse[173], and the co-constitution of agents and structures[174].[175] This process divided Constructivist into diverse groups sometimes called 'conventionalist', 'critical', and 'postmodern.' Many of the groups are definitely anti-realist, anti-foundational and critical.[176]

Because of this multiplicity, constructivism has been called "a theoretically informed approach" instead of a theory or school and its core features have been defined by John Ruggie as follows: "…the building blocks of international reality are ideational

[166] Cf. Lobell, Steven N., Ripsman, Norrin M. and Taliaferro, Jeffrey W. Neoclassical Realism, the State, and Foreign Policy. Cambridge: Cambridge University Press, 2009; Mearsheimer, John. The Tragedy of Great Power Politics. New York: Norton, 2001; Glaser, Charles L. Rational Theory of International Politics: The Logic of Competition and Cooperation. Princeton: Princeton University Press, 2010; Jervis, Robert. Dilemmas About Security Dilemmas. Security Studies, Vol. 20, No. 3 (2011), 416-423; Elman & Jensen 2013.

[167] Scheuerman, William E. Hans Morgenthau: Realism and Beyond. Cambridge, UK: Polity Press, 2009; Williams, Michael C. Why Ideas Matter in International Relations: Hans Morgenthau, Classical Realism, and the Moral Construction of Power Politics. International Organization, Vol. 58, No. 4 (Fall 2004), 633-665; Cozette, Murielle. What Lies Ahead: Classical Realism on the Future of International Relations. International Studies Review, Vol. 10, No. 4 (December 2008), 667-679; Parent, Joseph M. and Baron, Joshua M. Elder Abuse: How the Moderns Mistreat Classical Realism. International Studies Review, Vol. 13, No. 2 (June 2011), 193-213.

[168] Wohlforth 2010.

[169] Lobell, Ripsman & Taliaferro 2009.

[170] Although Liberalism, Neoliberal Institutionalism, Constructivism, Critical theory and Postmodern theories have all influenced the development of Realism I shall concentrate here only on Constructivism. This is because 'ideas matter' and strategic cultural ideas in the minds of security elites matter greatly. On the other theories Cf. Burchill et al 2005; Reus-Smith & Snidal 2010.

[171] Reus-Smith, Christian. Constructivism. In Burchill et al. 2005, 188-212; Ulbert, Cornelia. Social Constructivism. In Schieder & Spindler 2015, 248-268; Adler 2005; Ruggie 1998; Reus-Smith 2005.

[172] "…occupying a public space external to the individual minds of the participants but not therefore independent of all minds in general." (Jackson 2011, 129.

[173] This can mean either the analysis of communication through speech or writing as a system of signs etc. or the analysis of discursive practices as process producing social reality. (Chandler, 2007).

[174] This view is based on Anthony Giddens's concept of structuration. Social structures are temporally and spatially persistent social practices (re)created by those same practices. Transformation of structures is possible at the macrolevel when time and space start to move and emergent phenomena transpire. (Giddens, Anthony. The Constitution of Society: Outline of the Theory of Structuration. Cambridge: Polity Press, 1984).

[175] McCourt, David M. Practice Theory and Relationalism as the New Constructivism. International Studies Quarterly, Vol. 60, No. 3 (September 2016), 475-485.

[176] Katzenstein, Keohane, & Krasner 1998; Weber, Cynthia. International Relations Theory: A Critical Introduction. London: Routledge, 2013; Kratochwil, Friedrich. Sociological Approaches. In Reus-Smith & Snidal 2010, 444-461; Sterling-Folker, Jennifer. Competing Paradigms or Birds of a Feather? Constructivism and Neoliberal Institutionalism Compared. International Studies Quarterly, Vol. 44, No. 1 (March 2000), 97-119.

as well as material; the ideational factors have normative as well as instrumental dimensions; that they express not only individual but also collective intentionality; and that the meaning and significance of ideational factors are not independent of time and place."[177] Another proponent of constructivism, Emmanuel Adler, has defined it as "…the view that the manner in which the material world shapes and is shaped by human action and interaction depends on dynamic and epistemic interpretations of the material world."[178] Accordingly, both the social reality and knowledge about it are constructed. This view does not dispute the reality of the material world. It only claims that the material world holds meaning for human action through collective and intersubjective understandings—this understanding enables objects to become agents and act in a meaningful way.[179] Constructivism thus focuses on the social construction of international politics.[180]

Constructivism has its own theoretical and especially methodological problems. These include the inability to devise empirical solutions to the study of the mutual constitution of agents and structure; the underdevelopment of constitutive explanations—and therefore the tendency to turn to causal explanations; and the ambivalent nature of agency which is related to choices in the level and unit of analysis, and how to explain rationalism.[181] Despite these problems constructivism has been extended to the examination of national security issues and has contributed to the opening up of the 'black-box' of state. It has provided concepts and theories for studying state actions based on internal attributes and the processes of states such as culture[182], norms[183], identities[184], and interests.[185]

Norms have been one of the main interests of Constructivist research. The basic questions have been how states' identities and interests are constituted by international norms, how international norms come into being in the first place[186], and why some

[177] Ruggie 1998, 879. For another summary cf. Hurd 2010; Fierke, K. M. Constructivism. In Dunne, Kurki & Smith 2013, 161-178; Reus-Smith 2005.

[178] Adler 1997, 322.

[179] Adler 1997 & 2005.

[180] Barkin, Samuel J. Realist Constructivism. International Studies Review, Vol. 5, No. 3 (September 2003), 325–342, 326. The most famous example is Alexander Wendt's social theory of international relations (Wendt 1999).

[181] Adler 2005; McCourt 2016.

[182] For Katzenstein et al. culture is an environment which consists of constitutive and regulatory norms which prescribe and proscribe behaviour and describe how to behave (Katzenstein 1996, 54).

[183] Björkdahl has provided a good summary on Constructivist research on norms: "From a constructivist perspective, norms are generally considered as a set of intersubjective understandings and collective expectations regarding the proper behaviour of states and other actors in a given context or identity. Norms entail a collective evaluation and future expectations of behaviour in terms of what ought to be done." (Björkdahl, Annika. Norms in International Relations: Some Conceptual and Methodological Reflections. Cambridge Review of International Affairs, Vol. 15, No. 1, (June 2002), 9-23, 15).

[184] Wendt defines state identity as: "…a property of intentional actors that generates motivational and behavioral dispositions." (Wendt 1999, 224).

[185] Katzenstein 1996. According to Adler: "…national interests are intersubjective understandings about what it takes to advance power, influence and wealth, that survive the political process, given the distribution of power and knowledge in a society. In other words, national interests are facts whose 'objectivity' relies on human agreement and the collective assignment of meaning and function to physical objects." Adler 1997, 337.

[186] Anna Björkdahl has presented the following "mechanism" for the birth of norms: Social practices (international interaction based on cultural knowledge), demand and supply (perceived needs, exogenous shocks, policy failures – supply from interest groups), domestic norms (socialisation and internalisation). (Björkdahl 2002).

ideas become norms and others do not.[187] The effect of norms is important because they are constitutive parts of the social structure of the international system. i.e. structure and are thus part of the explanation of how agents and structures are mutually constitutive[188]—one explanation being that states become socialized to norms.[189] Through norms, Constructivism has challenged realism's assumption about the rationality of states because the ex-ante objective nature of rationality and interests has been challenged. The point is that state rationality is context bound and only through an interpretive approach can state preferences[190] be discovered and examined in relation to behaviour.[191] As Barkin and other Constructivists have claimed, interests are socially constructed so their content is a context-bound empirical question.[192] There might be other interests also such as economic well-being and self-esteem.

Epistemologically and methodologically constructivism concentrates on language as it is the bridge between the reality and the mind. This calls for interpretation or, what John Ruggie has described as understanding the meanings subjects give to phenomena. This occurs firstly by understanding actions from the vantage point of the actor, secondly, explaining the act in the context of social practice recognized by a relevant social collective, and thirdly, by producing explanations.[193] These explanations are usually constitutive, that is "X is a Y in context C" where C represents ideas, norms, identities etc. C also provides reasons as causes.[194] As Adler has argued, "doing something for reasons means applying an understanding of "what is called for" in a given set of circumstances' […] norms and rules socially constitute the cause.'"[195] This means that all behaviour must be understood from the actor's point of view and put into a historical and intersubjective context to generate any explanation for it.[196] On a methodological level this has led to calls for abduction (or some variant of it) instead

[187] Cf. Checkel, Jeffrey. The Constructivist Turn in International Relations Theory. World Politics, Vol. 50, No. 2 (January 1998), 324-348; March, James G. and Olsen, Johan P. The Institutional Dynamics of International Political Orders. International Organization, Vol. 52, No. 4 (Autumn 1998), 943–969.

[188] Checkel, Jeffrey. Norms, Institutions, and National Identity in Contemporary Europe. International Studies Quarterly, Vol. 43, No. 1 (March 1999), 83-114; Checkel, Jeffrey. Social Learning and European Identity Change. International Organization, Vol. 55, No. 3 (Summer 2001), 553-588; Zürn, Michael and Checkel, Jeffrey T. Getting Socialized to Build Bridges: Constructivism and Rationalism, Europe and the Nation State. International Organization, Vol. 59, No. 4 (October 2005), 1045-1079.

[189] Zürn & Checkel 2005.

[190] Preferences are ranked dispositions to outcomes. Usually referred from behaviour which is tautologically problematic. They reflect the self-interest of the actor— the best and probable ways to achieve 'satisfaction'. (Yee, Albert S. Thick Rationality and the Missing "Brute Fact". The Limits of Rationalist Incorporations of Norms and Ideas. The Journal of Politics, Vol. 59, No. 4 (November 1997), 1001-1039).

[191] "…an analysis of interpretation and intersubjectivity can mitigate some of the anomalies and problems of thin rationality by illuminating the sources of actors' preferences. Instead of problematically assuming that preferences are given, analysts can ascertain the actual preferences of actors, prior to undertaking rational choice modelling, by examining their cultural ideas and beliefs." (Yee 1997, 1029-1030).

[192] Barkin, Samuel J. Realist constructivism: Rethinking International Relations Theory. Cambridge: Cambridge University Press, 2010, 70-71.

[193] Ruggie 1998. Hollis and Smith introduced the concepts of explaining and understanding to IR. Understanding referred to Weberian hermeneutics, i.e. understanding from the inside. (Hollis, Martin and Smith, Steve. Explaining and Understanding International Relations. Oxford: Clarendon Press, 1990; Patomäki & Wight, 2000).

[194] Banerjee 2015, 278-279.

[195] Adler 2005, 329. On reasons as causes cf. Jackson, Patrick Thaddeus. Civilizing the Enemy: German Reconstruction and the Invention of the West. Ann Arbor: University of Michigan, 2006; Hall, Ian. What Causes What: The Ontologies of Critical Realism (Review). International Studies Review, Vol. 11, No. 3 (September 2009), 629–630; Kurki, Milja. Causation in International Relations: Reclaiming Causal Analysis, Cambridge: Cambridge University Press, 2008.

[196] Kratochwil 2010. Cf. Fierke on criticism on this (Fierke 2013).

of induction or deduction.[197] Abduction has been given many definitions in IR theory.[198] In this thesis it is understood to mean interpreting social and material reality though the interaction between existing theories and concepts and data to produce a new understanding of a phenomenon. There is no testing or positivistic explanation involved, although hypotheses are possible as a form of preliminary understanding. Abductive reasoning combined with realist ontology is not without its pitfalls as concepts used in abduction lead to reification of social reality and chronocentrism. This can only be overcome through categories induced from historical analysis.[199]

Despite their differences, some forms of realism and constructivism can be combined. Both accept that ideas matter on the level of state foreign policy—the difference is by how much.[200] Samuel Barkin has in fact proposed that constructivism and classical realism can be combined into a realist constructivism.[201] One of the main assumptions of Barkin's theory is that foreign policy is the use of power by agents to effectively and intentionally reconstitute social structure. The agency's relationship to the structure is always positional and situational, which means that rationality is contextual. For Barkin national interest is an issue-specific social purpose, held by the foreign policy elite, and it is a reason for action. There can be multiple national interests and they consist of collective ideas.[202] The elite is intentional and reflexive, so it is capable of strategic action. This view is supported by James Gow who draws on Barkin's ideas and argues that the necessity for security is based on both material and social needs.[203] I find Barkin's approach to power as an intentional reconstitution of social structure to be helpful.[204] It provides tools for bringing neoclassical realism closer to constructivism and legitimizes the emphasise of ideas as reasons for strategy, or in other words, for utilizing power. After I have reviewed the theory of neoclassical realism, I shall return to this synthesis.

2.3 Neoclassical realism

In contrast to Neorealism and much of Constructivist theory, NCR is a theory of foreign policy. It tries to explain foreign policy behaviour of states and system-level

[197] Here induction and deduction refer to modes of reasoning. (Blagden, David. Induction and Deduction in International Relations. Squaring the Circle Between Theory and Evidence. International Studies Review, Vol. 18, No. 1 (June 2016), 195-213)

[198] Ruggie 1998.

[199] Lapointe, Thierry and Dufour, Frédérick Guillaume. Assessing the historical turn in IR: an anatomy of second wave historical sociology. Cambridge Review of International Affairs, Vol. 25, No.1 (March 2012), 97-121.

[200] Cf. Twomey, Christopher P. Lacunae in the Study of Culture in International Security. Contemporary Security Policy, Vol. 29, No. 2, (August 2008), 338-357, 52; Gray, Colin S. Out of the Wilderness: Prime Time for Strategic Culture. Comparative Strategy, Vol. 26, No. 1 (2007), 1-20.

[201] Barkin 2010.

[202] Ibid., 66-71.

[203] Gow, James. The Essence of Strategy: Constructivist realism and necessity. In Wilkinson & Gow 2017, 259-278.

[204] Samuel Barkin's ideas have been criticized, for example, by Jackson, Patrick Thaddeus and Nexon, Daniel H. Constructivist Realism or Realist Constructivism. International Studies Review Vol. 6, No. 2, 2004, 337-352; Sterling-Folker, Jennifer. Realist-Constructivism and Morality. International Studies Review Vol. 6, No. 2 (2004), 337-352; Mattern, Janice Bially. Power in Realist Constructivist Research. International Studies Review Vol. 6, No. 2 (2004), 337-352.

outcomes based on both structure and unit-level variables. Thus, NCR relies on foreign policy analysis (FPA)[205] for some of its premises. Walter Carlsnaes has described FPA's unit of analysis as those goal-directed actions pursued by governmental representatives acting on the behalf of their sovereign communities which are directed toward external actors or objectives.[206] Concurrently, state action is the action taken by state foreign policy decision-makers, so, from the analytic point of view, they are the state.[207] However, FPA is quite ambivalent about the level of analysis at which these decisions are analysed. It could be in the minds of decision-makers, or it may concern domestic politics or state relations.[208] NCR tries to square this circle by incorporating them all and then distancing itself from FPA to become a full-blown theory of IR.

The term 'neoclassical realism' was coined by Gideon Rose in a review article.[209] According to him NCR: "…explicitly incorporates both external and internal variables, updating and systematizing certain insights drawn from classical realist thought. Its adherents argue that the scope and ambition of a country's foreign policy is driven first and fore most by its place in the international system and specifically by its relative material power capabilities. This is why they are realist. They argue further, however, that the impact of such power capabilities on foreign policy is indirect and complex, because systemic pressures must be translated through intervening variables at the unit level. This is why they are neoclassical."[210] According to Rose, NCR theory accepts an international system based on anarchy and the distribution of power but assumes that states do not have full knowledge of this system. States themselves are differentiated internally based on their political system, culture, power resources etc. The theory's causal logic follows from independent systemic variables which are influenced by the state's internal intervening variables to explain foreign policy as the dependent variable. Because the theory is realist, power is a central concept. This is understood in terms of material capacity or resources and it is used "to control and shape their the external environment."[211] How the structural incentives based on power distribution are interpreted and how the state's power resources are mobilized is based on the perceptions of the policy makers and the intervening domestic variables. To study these causal relationships Rose calls for "…theoretically informed narratives, ideally supplemented by explicit counterfactual analysis, that trace the ways different factors combine to yield particular foreign policies."[212]

[205] FPA is not a coherent theory, research program or paradigm, but parts of it have been interested in the influence of ideas. Cf. Hill, Christopher and Light, Margot. Foreign Policy Analysis. In Light, Margot and Groom, A. J. R. International Relations: A Handbook of Current Theory. London: Bloomsbury Academic, 1985, 156-173; Carlsnaes, Walter. Foreign Policy. In Carlsnaes, Risse & Simmons 2005, 331-349.

[206] Carlsnaes 2005, 335.

[207] Stuart, Douglas T. Foreign-Policy Decision-Making. In Reus-Smith, Christian and Snidal, Duncan. The Oxford Handbook of International Relations. Oxford: Oxford University Press, 2010, 576-593.

[208] Kaarbo, Juliet. A Foreign Policy Analysis Perspective on the Domestic Politics Turn in IR Theory. International Studies Review, Vol. 17 (2015), 189-216; Hudson, Valerie M. and Vore, Christopher S. Foreign Policy Analysis Yesterday, Today, and Tomorrow. Meshon International Studies Review, Vol. 39 (1995), 209-238.

[209] Rose, Gideon. Neoclassical Realism and Theories of Foreign Policy. World Politics, vol. 51, no. 1 (1998), 144-172.

[210] Ibid., 146.

[211] Ibid., 152.

[212] Ibid., 154.

After Rose's article, Steven Lobell, Norrin Ripsman and Jeffery Taliaferro summarized a neoclassical theory as a basis of a research program.[213] Their neoclassical realist theory states that the international system is a form of anarchy and states can rely only on self-help to achieve security. However, states are not like-units and state interests derive from the system through the interpretation of foreign policy elites (FPEs) and are pursued based on domestic incentives and constraints.[214] According to neoclassical realism, the basic interest is survival. The ways and means of using power are dependent on the state's ability to extract and mobilize the nation's material resources. These variables come together in a 'transmission belt', which is a concept describing how national power resources are converted to state power at the international level.[215] Lobell et al. describe the underlying causal logic as follows: Relative power distributions are independent variables, domestic constraints and elite perceptions[216] are intervening variables, and foreign policy is the dependent variable.[217] Lobell et al. come very close to Rose's definition, but they argue that NCR should be based on deductive theorizing and hypotheses testing. Moreover, NCR should be based on the understanding of explicitly material and relative of power resources and instrumentally rational FPEs, and on the premise that ideas are only tools for power or 'wrong' beliefs.[218]

Ripsman, Taliaferro and Lobell developed their theory further in their book *Neoclassical Realist Theory of International Politics*.[219] In it they presented a more coherent theory of NCR, according to which systemic stimuli or independent variables are based on the structure of the international system, which can be understood as a polarity based on material capabilities, but modified by 'systemic modifiers', i.e. geography, rates of technological diffusion, and the offense-defence balance in military technologies. Ripsman et al. add 'clarity' to systemic stimuli as a systemic variable to explain how system "uncertainty" conditions the responses of states—through the nature of threats, time frames and optimal policy responses—and provides room for intervening variables to affect policy choices. They also add the 'strategic environment' to explain how the imminence and magnitude of threats and opportunities affect the freedom of action of states. Consequently, there are then, in fact, three independent

[213] Lobell, Ripsman & Taliaferro 2009. Other prominent scholars labelled Neoclassical realist cf. Zakaria, Fareed From Wealth to Power. The Unusual Origins of Americas World Role. Princeton: Princeton University Press, 1998; Schweller, Randall L. Deadly Imbalances. Tripolarity and Hitler's Strategy of World Conquest. New York: Columbia University Press, 1998.

[214] States are defined as: "…variety of autonomous polities with different geographic scopes, internal attributes, and relative material capacities [interacting] in an anarchic environment" and "In the foreign policy realm, the state consists of the foreign policy executive, principally the head of government and key ministers and officials charged with the conduct of foreign policy." Lobell, Ripsman & Taliaferro 2009, 26 & 280-281.

[215] State power is defined as the relative ability of the state to extract and mobilize resources from domestic society (Ibid., 38).

[216] These perceptions mainly relate to the level of threat based on "…the function of the relative distribution of power (both in the international system and in the particular region), the offense-defense balance in military technology, and geographic proximity." (Ibid., 213).

[217] Lobell, Ripsman & Taliaferro 2009, 20. On the application of NCR in a case study cf. Saltzman, I. Z. Growing Pains: Neoclassical Realism and Japan's Security Policy Emancipation. Contemporary Security Policy, Vol. 36, No. 3 (2015), 498 – 527.

[218] Lobell, Ripsman & Taliaferro 2009.

[219] Ripsman, Taliaferro, & Lobell, 2016.

variables.[220] Ripsman et al. replace the "transmission belt"[221] with perceptions, decision-making and policy implementation. These processes are affected by the intervening variables of leader images (beliefs), strategic culture[222], state-society relations, and domestic institutions. Ripsman et al. go on to propose NCR as a theory of international politics by naming state foreign policies, grand strategies and systemic outcome dependent variables. They claim that state balancing activities can eventually lead to structural change and, thus, they propose they can explain systemic change, which is deemed a weakness of structural realism.[223]

In their book Ripsman et al. explain 'soft positivism'[224] as an epistemological approach but seem to be more ambivalent about the rationality of FPEs who are "[officials] charged with the conduct of foreign and defence policy"[225] but separated from society due to their position, authority, perspective, access to information and attitudes.[226] They argue for a positivist approach with a standard methodology, i.e. process tracing, which should be based on the a priori deductive or inductive inference of independent, intervening, and dependent variables.[227] However, this approach has been rightfully criticized for being able to find a needed variable for any explanation.[228] Therefore, Ripsman et al.'s Neoclassical Realist Theory of International Politics is, firstly, an attempt to answer the criticism levelled against NCR and, secondly, an attempt to distinguish it as a research programme or 'school' from other IR theories. As such, it 'reifies' a version of NCR which I consider unbeneficial but shall, nevertheless, adopt in a modified form.

The problem with the approach by Ripsman et al. in the context of this thesis is that they treat ideas and beliefs as exogenous variables and leave them under-defined. Ripsman et al. claim that: "When states confront more permissive strategic environment, our theory expects ideas and ideology to exert a greater influence on states' foreign policies."[229] The challenge is to empirically claim when a system is restrictive

[220] That is, the distribution of power, systemic modifiers, and imminence and magnitude of threats, i.e. perception and interpretation (Ibid., 182).

[221] These are now closer to Schweller's definition: "[D]omestic processes act as transmission belts that channel, mediate and (re)direct policy outputs in response to external forces (primarily changes in relative power). Hence, states often react differently to similar systemic pressures and opportunities, and their response may be less motivated by systemic-level factors than domestic ones." (Schweller, Randall L. Unanswered Threats. A Neoclassical Realist Theory of Underbalancing. International Security, Vol. 29, No. 2 (2004), 159-201, 164).

[222] Rispman et al. have defined strategic culture either as organizational culture or wider culture shared by a society as a whole. It is a set of inter-related beliefs, norms, and assumptions or collective expectations which shape understanding of strategic environment and acceptable and unacceptable strategic choices. Ripsman Taliaferro, & Lobell 2016.

[223] Ripsman, Taliaferro, & Lobell, 2016.

[224] Ripsman, Taliaferro and Lobell argue that they search for law-like generalizations across cases and test these generalizations with rigorous case-study analysis of well-selected cases. Research should produce generalizations which allow prediction but not experimentation as theories are still probabilistic and are not falsifiable. (Ripsman et al. 2016, 106-107.) Ripsman et al. are closer to Patrick Thaddeus Jackson's Neopositivism than Positivism, which can be summarized as the evaluation of hypothetical statements to approximate nomothetic explanations. (Jackson, Patrick Thaddeus. Fear of Relativism. International Studies Perspectives, Vol. 16 (2015), 13-22.)

[225] Ripsman et al. 2016, 61.

[226] Ibid., 123-126.

[227] Ibid., 132.

[228] Tang, Shipping. Taking Stock of Neoclassical Realism. International Studies Review, Vol. 11 (2009), 799-803.

[229] Ripsman et al. 2016, 159.

or permissive. Moreover, contrary to Ripsman et al.'s claims, studies of strategic culture have shown that ideas matter when unexpected shocks, i.e. unpredicted significant negative events, occur.[230] Thus Ripsman et al. seem to be ready only to give ideas power when nothing else matters.

The second problem is that Ripsman et al. define an international system as a system of states based on the distribution power. This does not include ideas, or, most importantly, cyberspace. States can shape their environment only by changing its polarity through 'grand strategies'.[231] In relation to these deficiencies Michael Foulon points out the subjectivity of the geopolitical environment. NCR cannot ignore the meanings the FPEs give to the environment and how they perceive it.[232] Moreover, the elites play two-level games, as state decision-makers must satisfy both domestic and international constituencies—their rationality is thus connected to two different levels.[233] Admittedly, NCR is an amalgamation of different theories and thus suffers from poor parsimony as an IR theory.[234] The problems of NCR lie in the way it tries to be a theory of everything. To make its framework suitable for this thesis it must be streamlined, and its positivism and materialism must be replaced by Barkin's synthesis of ideas and power described above. Moreover, the concept of ideas must be distinguished from norms and structures like culture so that I can examine the role of individual ideas in elite decision-making as reasons for action.

2.4 Ideas and power

Ideas have been understood in the IR theory variously as individual, shared, collective or intersubjective beliefs.[235] Individual beliefs reside in the minds of individual human beings, while shared beliefs are based on consensus in a social group, and collective or intersubjective beliefs reside in some respects outside individual minds and have independent staying power.[236] In addition to levels of possessions, ideas have been

[230] Cf. Chapter 2.5

[231] "[T]he organizing principle or conceptual blueprint that animates all of the state's relations with the outside world… It is a future-oriented enterprise involving considerations of external threats and opportunities, as well as the specific material, political, and ideological objectives of the state." (Ripsman et al., 84.)

[232] Foulon, Michael. Neoclassical Realism: Challengers and Bridging Identities. International Studies Review. Vol. 17 (2015), 635-661.

[233] Their idea of two-level games was developed during 1980-1990s. (Katzenstein, Keohane, & Krasner 1998).

[234] For further criticism cf. Narizny, Kevin. The New Debate: International Relations Theory and American Strategic Adjustment in the 1890s. Security Studies, Vol. 11, No. 1, (Autumn 2001), 151-170, 181; Legro & Moravcsik 1999; Feaver et al. 2000; Narizny 2017; Finel 2001; Rathbun, Brian. A Rose by Any Other Name: Neoclassical Realism as the Logical and Necessary Extension of Structural Realism. Security Studies, Vol. 17, 294-332; Tang 2009; Kaarbo 2015. Moravcsik, Andrew. Taking Preferences Seriously: A Liberal Theory of International Politics. International Organization, Vol. 51, No. 4, (Autumn 1997), 513–553; Schieder, Siegfried. New Liberalism. In Schieder, Siegfried and Spindler, Manuela (ed.) Theories of International Relations. New York: Routledge, 2015, 107-129; Rathbun, Brian C. Is Anybody Not an (International Relations) Liberal? Security Studies, Vol. 19 (2019), 2-25).

[235] The terms ideas and beliefs are used interchangeably. Yee defines them "as mental events that entail thought." (Yee, Albert S. 'The Causal Effect of Ideas on Politics'. International Organization, Vol. 50 (1996), 69-108, 69). Ruggie, among others, has claimed that ideas were 'introduced' to IR by Judith Goldstein and Robert Keohane. They proposed world views (identities), principled beliefs (right-wrong) and causal beliefs (cause-effect) as norms affecting policy outcomes. They influence decision-making through 'road maps', 'focal points' (deciding in equilibrium situations), and 'institutionalization' (guiding policy in the absence of innovation). (Ruggie 1998).

[236] Laffey, Mark and Weldes, Jutta. Beyond Belief: Ideas and Symbolic Technologies in the Study of International Relations. European Journal of International Relations, Vol. 3, No. 2 (June 1997), 193–237; Goldstein,

divided into types such as policy prescriptions, norms, principled beliefs, cause-effect beliefs, ideologies, shared belief systems, and broad worldviews according to their generalizability.[237] According to Nina Tannenwald, worldviews are all-encompassing orientations to reality with changing and contradictory elements. She sees ideologies and shared belief systems as "a systematic set of doctrines or beliefs that reflect the social needs and aspirations of a group" which usually include an orientation to the future. In her view cause-effect or causal beliefs are about means and ends and they provide an understanding of the world and guidelines for achieving goals in this context. She notes that norms and principled beliefs consist of values and attitudes describing right and wrong and proscribing appropriate behaviour and policy prescriptions are derived from causal and principled beliefs which provide specific and exact solutions to problems.[238] This thesis will use the concept of causal beliefs to argue for the existence of specific strategic cultural ideas explained below. They are something that can be observed from texts and provide direct connection to policies. Admittedly, the borders of different types of ideas on the empirical level are blurred, so causal beliefs usually include elements of principled beliefs.

Ideas should be differentiated from norms which are "…standards of appropriate behavior for actors with a given identity"[239] or more exactly in an IR context "a set of intersubjective understandings and collective expectations regarding the proper behaviour of states and other actors in a given context or identity."[240] According to Annika Björkdahl norms have been seen to have regulative, constitutive and enabling powers through a variety of mechanisms, whereas ideas and beliefs might not have direct behavioural effects.[241] Ideas reside in the realm of the mind, culture, language, frames, representations and discourse—more as a potential than as a manifested social fact.[242] Ideas should also be distinguished from institutions which are "a relatively stable collection of practices and rules defining appropriate behavior for specific groups of actors in specific situations."[243] Institutions have their own causal and constitutive powers and independent existence outside people's minds, although, they might also be the carriers of ideas through their organizational processes, structure, and culture.[244] Nevertheless, the distinction between norms and ideas is not clear-cut and depending on theoretical approach they have been used interchangeably.[245]

Judith and Keohane, Robert O. (eds.) Ideas and Foreign Policy: Beliefs, Institutions, and Political Change. Ithaca: Cornell University Press, 1993; Jacobsen, Kurt. Much Ado about Ideas: The Cognitive Factor in Economic Policy. World Politics, Vol. 47 (1995), 283-310; Risse-Kappen, Thomas. Ideas Do Not Float Freely: Transnational Coalitions, Domestic Structures, and the End of the Cold War. International Organization, Vol. 48 (1994), 185-214; Legro, Jeffrey W. The Transformation of Policy Ideas. American Journal of Political Science, Vol. 44, No. 3 (Jul. 2000), 419-432; Wendt 1999, 158; Checkel, Jeffrey. Ideas and International Political Change: Soviet/Russian Behavior at the End of the Cold War. New Haven: Yale University Press, 1997.

[237] Tannenwald 2005; Tannenwald & Wohlforth 2005.

[238] Tannenwald & Wohlforth 2005, 16-17. Cf. Laffey & Weldes 1997; Legro 2000.

[239] Finnemore, Martha and Sikkink, Kathryn. International Norm Dynamics and Political Change. International Organization, Vol. 52, No. 4, (Autumn, 1998), 887-917, 891.

[240] Björkdahl 2002, 15.

[241] Björkdahl 2002, 21.

[242] Laffey & Weldes 1997; Yee 1996; Barnett, Michael. Culture, Strategy and Foreign Policy Change: Israel's Road to Oslo. European Journal of International Relations, Vol. 5, No. 1 (1999) 5-36.

[243] March & Olsen 1998, 948.

[244] Legro, Jeffrey W. Culture and Preferences in the International Cooperation Two-Step. The American Political Science Review, Vol. 90, No. 1 (Mar. 1996), 118-137; Yee 1996; Finnemore & Sikkink 1998.

[245] Cf. Farrell, Theo. Constructivist Security Studies: Portrait of a Research Program. International Studies Review, Vol. 4, No. 1 (Spring 2002), 49-72.

The traditional IR theory has usually approached ideas as commodities that are carried, owned and intentionally manipulated by actors, whereas postmodernists and post-structuralists have argued that ideas are independent of actors and have their own constitutive power.[246] Sometimes ideas are used to define preferences of instrumental rationalistic decision-making.[247] From a Constructivist point of view, ideas give meaning and causal effects to matter, and formulate decision-making through causal beliefs.[248] This means that rationality itself is contextual and affected by cultural beliefs and ideas.[249] When this kind of understanding of ideas is connected to explaining things, problems of proving causality follow. Thus, the use of ideas to depict causes usually results in producing descriptive research.[250]

The relation of ideas to material aspects has remained problematic in IR theory.[251] If reality is seen as a material aspect, then ideas do not matter or matter only a little — which is a slippery slope. On the other hand, if reality is a social phenomenon, then IR research is in danger of turning into a pure analysis of language, speech, and discourse without any claims on knowledge of reality which would be policy relevant, prediction included.[252] Related to this is the problem of change: How do ideas (norms) change and why some ideas become accepted as collective beliefs and others do not? Arguably, material and ideational aspects of reality interact and the interaction of actors and structures has emergent properties.[253] One solution to these problems would be to engage in mid-level theorising, which would mean concentrating on case studies and process tracing to evaluate both ideational and material effects on contextual decision-making and strive for causal explanations with limited generalizability or an interpretive understanding.[254] This is the approach taken in this thesis and it is in line with the philosophical assumptions presented above.

Ideas have a life of their own through a cycle of adoption or reformulation or production and then transmission, reception, and implementation.[255] They emerge out of external events or shocks necessitating new thinking, from outside pressure or domestic politics.[256] The adoption of external ideas or the promotion of domestic ideas

[246] Laffey & Weldes 1997.

[247] Frieden, Jeffry. Actors and Preferences in International Relations. In Lake, David and Powell, Robert (eds.) Strategic Choice and International Relations. Princeton: Princeton University Press, 1999, 39-76.; Tannenwald & Wohlforth, 2005.

[248] Tannenwald 2005.

[249] Yee 1997.

[250] Laffey & Weldes 1997; Finnemore & Sikkink 1998; Tannenwald & Wohlforth, 2005.

[251] This problem can be summarized as: do states primarily react to material or ideational incentives? (Barkin 2010, 49).

[252] This is exactly the criticism that Ripsman et al. express in relation Barkin's Realist constructivism. (Ripsman et al. 2017; Barkin 2010).

[253] Yee 1997; Moravcsik 1997; Guzzini, Stefano and Leander, Anna. A Social Theory for International Relations: An Appraisal of Alexander Wendt's Theoretical and Disciplinary Synthesis. Journal of International Relations & Development, Vol. 4, No. 4, (December 2001), 316-338; Brooks, Stephen G. and Wohlforth, William C. Power, Globalization, and the End of the Cold War. Reevaluating a Landmark Case for Ideas. International Security, Vol. 25, No 3 (Winter 2000/2001), 5-53; Brooks, Stephen G. and Wohlforth, William C. From Old Thinking to New Thinking in Qualitative Research. International Security, Vol. 26, No. 4 (Spring 2002), 93-111.

[254] Tannenwald 2015; Mahoney 2015; Waldner 2015.

[255] Legro 2000; Nye 2011a; Finnemore & Sikkink 1998; Tannenwald 2005.

[256] De Souza, Denise E. Culture, context and society —The underexplored potential of critical realism as a philosophical framework for theory and practice. Asian Journal of Social Psychology, Vol. 17 (2014), 141-151.

to an external audience is contested.[257] The life of ideas is connected to 'epistemic communities.'[258] This concept was invented by John Ruggie and developed by Ernst Haas and was later elaborated by Peter Haas and Emmanuel Adler.[259] Adler and Haas have described an epistemic community as: "…a network of individuals or groups with an authoritative claim to policy-relevant knowledge within their domain of expertise. The community members share knowledge about the causation of social and physical phenomena in areas they have a reputation for competence in. They also have a common set of normative beliefs about what will benefit human welfare in such a domain. While members are often from a number of different professions and disciplines, they adhere to the following: (1) shared consummatory values and principled beliefs; (2) shared causal beliefs or professional judgment; (3) common notions of validity based on intersubjective, internally defined criteria for validating knowledge; and (4) a common policy project."[260] Epistemic communities are not purely domestic actors. They have contacts with other communities across borders and this facilitates the exchange of ideas internationally beyond state interaction.[261]

Epistemic communities are not lobbyists. Their influence is based on the need for technological or other expert knowledge (residing mostly in academic circles) by decision-making elites to understand their changed, novel environment.[262] Ideas are not necessarily new but might be combinations of old ideas.[263] Ideas proposed by epistemic communities are not necessarily revolutionary or liberal in a normative sense. To have purchase, they must be constructed to 'fit' into or 'resonate' with existing ideas of decision-making elites.[264] In this way, through communicative actions and their bureaucratic position, epistemic communities provide decision-makers with principled and causal beliefs and perhaps also policy prescriptions which guide but do not determine their decisions.[265] This process is contested and the elites do not get to just pick-and-choose, and neither do communities get their ideas through intact.[266]

[257] Lantis, Jeffrey S. Nuclear cooperation with non-NPT member states? An elite-driven model of norm contestation. Contemporary Security Policy, Vol. 39, No. 3 (2018), 399-418.

[258] An alternative concept of the epistemic community are 'norm entrepreneurs' proposed by Finnemore and Sikkink. (Finnemore & Sikkink 1998).

[259] Ruggie, John Gerard. International Responses to Technology: Concepts and Trends. International Organization, Vol. 29, No. 3, International Responses to Technology (Summer, 1975), 557-583; Adler, E., and Haas, P.M. Conclusion: epistemic communities, world order, and the creation of a reflective research program. International organization, Vol. 46, No. 1 (1992), 367–390; Haas, Peter M. Introduction: Epistemic Communities and International Policy Coordination. International Organization, Vol. 46 (1992), 1-35; Ruggie, John Gerard, Katzenstein, Peter J., Keohane, Robert O. and Schmitter, Philippe C. Transformations in World Politics.: The Intellectual Contributions of Ernst B. Haas. Annual Reviews of Political Science, Vol. 8 (2005), 271-96. For a summary cf. Davis Cross, M.K. Rethinking epistemic communities twenty years later. Review of international studies, Vol. 39, No. 1 (2013), 137-160.

[260] Adler & Haas 1992, 101.

[261] Ibid.

[262] Ruggie was discussing technological changes in the 1970s which resonates quite well with the subject of this thesis: The unknowability and novelty of cyberspace and information society. (Ruggie 1975). See also, Risse-Kappen 1994; Rathbun 2010, 15; Rathbun, Brian. Uncertainty about Uncertainty: Clarifying a Crucial Concept for International Relations Theory. International Studies Quarterly, Vol.51, No. 3 (2007), 25-47.

[263] Adler, Emanuel. The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control. International Organization, Vol. 46, No. 1, Knowledge, Power, and International Policy Coordination (Winter, 1992), 101-145, 105, 123.

[264] Adler & Haas 1992; Yee 1996; Laffey & Weldes 1997.

[265] Haas & Adler 1992; Faleg, Giovanni. Between knowledge and power: epistemic communities and the emergence of security sector reform in the EU security architecture. European Security, Vol. 21, No. 2 (2012), 161-184.

[266] Faleg 2012.

Epistemic communities thus provide reasons for the actions of state decision-makers through causal and principled beliefs.[267] Michael Barnett has called this 'framing'. It is the intentional deployment of contextual meaning-providing structure[268] to make sense of the underlying reality, to fix meanings, organize experience, and to suggest courses of action.[269] This does not exclude strategic or instrumental rationality understood as means to ends calculations. It only means that rationality must be set in a context and an interpretive analysis must be used to understand how decision-makers understand their environment and its restrictions and their means and goals. Causal and principled beliefs and epistemic communities explain how ideas end up affecting decision-makers or elites in the NCR and transform them from intervening variables into reasons to use power in accordance with Barkin's ideas. [270]

A few words on power are required at this point. Ideas are related to power. This is because the concept of power that I subscribe to views power as relational and contextual.[271] Power is power over something and it gains its effect and meaning from this relationship and context. This is why cyber power must be discussed in the context of cyberspace and I shall return to this concept in Chapter 3. On a more theoretical level, power is basically understood as a material capacity or a set of resources and is used "to control and shape […] the external environment."[272] Related to this, constructivism offers a 'deeper' understanding of changing the environment of the agents. Agent behaviour changes the environment because it is guided by meanings given to power, behaviour and the environment.[273] In other words, Russia's project to control and shape cyberspace can be considered as a part of a process that will change cyberspace for everyone. Power then is imbued with meaning and, therefore, ideas are important.

It is also important to point out that power as a potential is only a set of resources and means.[274] It must be extracted, mobilized and used for some purpose to become what NCR calls 'state power'. This is compatible with Lawrence Freedman's definition of strategy as an art of creating power through process or practice which is informed by cultural 'scripts'.[275] I shall examine the relationship between strategy and power more in Chapter 3, but here it is essential to insert strategy, "the use that is made of force and the threat of force for the ends of policy"[276], into Ripsman et al.'s model.[277] Perception, decision making, and policy implementation are incorporated into the concept of strategy when we are discussing military matters. The making of strategy is a continuous process of these elements to create, mobilize and utilize power for strategic effect, the ultimate manifestation of which is the use of force.

[267] Yee 1996, 94.
[268] Hamati-Ataya 2012.
[269] Barnett 1999, 15 & 25.
[270] Cf. Libel2016), 137–156.
[271] Baldwin, D. A. Power and International Relations. In Carlsnaes, Walter, Risse, Thomas and Simmons, Beth A. (eds.) Handbook of International Relations. London: SAGE Publications, 2013, 273-297, 275; Barnett, Michael and Duvall, Raymond. Power in International Politics, International Organization, Vol. 59, No. 1 (Winter, 2005), 39-75.
[272] Rose, 1998, 152.
[273] Kratochwil 2010, 451-452; Barkin 2010.
[274] Although some Structural realists like Mearsheimer would argue that it is also the end (Mearsheimer 2001).
[275] Freedman 2013, xi, 620-621.
[276] Gray, Colin. S. Modern Strategy. Oxford: Oxford University Press, 1999, 17.
[277] Ripsman et al. 2016, 59.

A few words on the state are also required at this point. Although NCR opens the 'black box' of the state, it still considers states as the primary actors in international politics through FPEs. This might seem an anachronistic approach because the concept of modern state and its current role in international relations has been challenged.[278] Research has shown that state sovereignty is a socially constructed concept which has changed over time.[279] Nevertheless, the state can be characterized as a set of institutions and relationships of governance which are partially independent of society. Max Weber's definition of an institution that possesses a monopoly over the legitimate means of coercion is still widely accepted.[280] States have a foreign policy[281], and a security[282] and defence policy[283] based on their internal, autonomous, and exclusive authority over their territory, and externally recognized position by other states, i.e. sovereignty.[284] These policies are managed by designated foreign, defence and security policy elites—elites meaning here a group of people with official authority to represent the state. These have the legitimacy to use state power. This does not mean that they are independent of international or domestic pressures.[285] In the context of this thesis, and in line with NCR, defence and security elites are the people who make decisions on the state use of power for military and security ends and in responses to national threats. Thus, states use power based on the decisions made by the elites who are provided with reasons from ideas offered by, among others, epistemic communities. Power can be used in different ways and in different domains. As I will argue in Chapter 3, cyberspace is such a domain, in fact an environment, and power can be used to control and shape it. The connection of military power or use of force to state power can be found in ideas belonging to the sphere of strategic culture.

2.5 Strategic culture

Culture is either a type of idea, shared belief system, worldview, discourse, or a social structure, depending on the theoretical approach. It could be an environment which consists of constitutive and regulatory norms, which prescribe and proscribe behaviour and how to behave, or it could be "bundles of ideas and matter linguistically,

[278] Biersteker, Thomas J. State, Sovereign and Territory. In Carlsnaes, Walter, Risse, Thomas and Simmons, Beth A. (eds.) Handbook of International Relations. London: SAGE Publications, 157-176; Kaldor 2012, 91.

[279] Glanville, Luke. The Myth of 'Traditional' Sovereignty. International Studies Quarterly, Vol. 57 (2013), 79-90; Caporaso, James A. Changes in the Westphalian Order: Territory, Public Authority, and Sovereignty. International Studies Review, Vol. 2, No. 2 (Summer 2000), 1-28; Schmidt, Sebastian. To Order the Minds of Scholars: The Discourse of the Peace of Westphalia in International Relations Literature. International Studies Quarterly, Vol. 55 (2011), 601–623; Osiander, Andreas. Sovereignty, International Relations, and the Westphalian Myth. International Organization, Vol. 55, No. 2 (Spring 2001), 251-287; Branch, Jordan. Mapping the Sovereign State: Technology, Authority, and Systemic Change. International Organization, Vol. 65 (Winter 2011), 1-36.

[280] Biersteker 2005, 159.

[281] On the concept security foreign policy cf. Carlsnaes 2005, 335.

[282] On the concept security cf. Miller 2001.

[283] Understood in this thesis as the part of state policy which handles the threat or use of force by the state, including the assessment of threats, planning and preparation for, and implementing the threat or use of force.

[284] Biersteker 2005, 168. European Union seems to be an exception to this rule cf. Biscop, Sven and Whitman, Richard G. The Routledge Handbook of European Security. London: Routledge, 2013; Larive□, Maxime H. A. Debating European Security and Defense Policy: Understanding the Complexity. Surrey: Ashgate, 2014.

[285] Adler & Haas 1992, 373-374.

materially and intersubjectively mediated."[286] For Alexander Wendt, international system is a social structure consisting of "distribution of ideas" where shared ideas form a "culture" which gives meaning to power and defines the substance of interests.[287]

Strategic culture is a concept which was first used in the context of Strategic Studies by Jack Snyder in a study of Soviet nuclear strategy for the RAND corporation in the 1977.[288] Snyder was openly critical of the rational game-theoretical approaches of his time and of 'mirror-imaging' US nuclear strategic thinking to the Soviets.[289] He described strategic culture as: "the sum total of ideas, conditioned emotional responses, and patterns of habitual [cognitive] behaviour that members of national strategic community have acquired through instruction and imitation and share with each other with regard to nuclear strategy […] the body of attitudes and beliefs that guides and circumscribes thought on strategic questions, influences the way strategic issues are formulated, and sets the vocabulary and conceptual parameters of strategic debate."[290] This culture had a certain amount of staying power because individuals were socialized into it and because institutional interests were involved. It could change through evolution of technology, but it also affected how new technologies were implemented. Snyder also recognized that there were strategic subcultures which were traditions related to specific institutional associations.[291] Snyder proposed some ideas on how to connect culture to state behaviour but was cautious of giving either one too much credence or making overly precise predictions from them.[292]

After Snyder, there have been at least three maybe four 'generations' of thoughts on strategic culture.[293] Alistair Johnston was the first to describe different strains of strategic culture research as generations and his later debate with Colin Gray ingrained this division.[294] In short, Johnston claimed that the first generation was based on Snyder's concept of strategic culture. It had its heyday from the 1970s to mid-1980s and was theoretically over- and under-determined. This meant that strategic culture

[286] Katzenstein 1996, 54; Adler & Pouliot 2011, 14-15.

[287] Wendt 1999.

[288] Snyder 1977.

[289] Cf. also Gray, Colin S. What Rand Hath Wrought. Foreign Policy, No. 4 (Autumn 1971), 111-129; Strachan 2013, 136-137. Snyder also argued that public sources could be used to study Soviet strategic thinking because, for example, the ideas presented in the Soviet military journals, restricted to officers, did not drastically diverge from the secret versions (Snyder 1977). Garthoff has later pointed out that secret versions had more substance but rarely differed from the restricted ones (Garthoff 1990).

[290] Snyder 1977, 8-9.

[291] Ibid., 10.

[292] Ibid., 15-16. Jaffrey S. Lantis has summarized Snyder's thinking as follows: "Snyder suggested that elites articulate a unique strategic culture related to security-military affairs that is a wider manifestation of public opinion, socialized into a distinctive, semi-permanent mode of strategic thinking." Lantis, Jeffrey S. Strategic Cultures and Security Policies in the Asia-Pacific, Contemporary Security Policy, Vol.35, No.2 (2014), 166-186, 171.

[293] Ibid.; Tamil Libel has argued that the fourth generation combines ideas of Snyder and Alastair Johnston by accepting multiple subcultures and competition between them (Libel 2016).

[294] Gray, Colin S. Strategic Culture as Context: the First Generation of Theory Strikes Back. Review of International Studies, Vol. 25, No. 1 (January 1999), 49-69; Johnston, Alastair Iain. Strategic Cultures Revisited: Reply to Colin Gray. Review of International Studies, Vol. 25, No. 3 (July 1999), 519-523; Uz Zaman, Rashid. Strategic Culture: A "Cultural" Understanding of War. Comparative Strategy, Vol. 28, No. 1 (2009), 68-88; Bloomfield, Alan. Time to Move On: Reconceptualizing the Strategic Culture Debate. Contemporary Security Policy, Vol. 33, No. 3 (2012), 437-461; Poore, Stuart. What is the context? A reply to the Gray-Johnston debate on strategic culture. Review of International Studies, Vol. 29, No. 2 (Apr. 2003), 279-284; Sondhaus, Lawrence. Strategic Culture and Ways of War. New York, Routledge, 2006, 123-126.

alone strongly determined behaviour and culture was considered as an amalgam of potentially competing variables and inputs.[295] The second generation from the mid-1980s to early 1990s approached strategic culture as a tool or instrument but was unable to differentiate between occasions when decision-makers used culture and when they were influenced by it.[296] The third generation from the mid-1990s, that Johnston himself represented and improved upon, saw culture as an independent variable. It separated behaviour from culture and thereby avoided tautology and enabled culture to vary through subcultures and temporal change, and, most importantly, allowed competitive testing of positivist theory.[297] Later in 1999, Colin Gray defended the first generation, of which he had been a proponent, and introduced the idea of culture as a 'context' and thereby connecting strategic culture to Constructivist traditions.[298] Johnston and Gray are, of course, not the only ones who have tried to define strategic culture, but they and Snyder are the 'founding fathers' to which almost every scholar has referred and built upon.[299]

Johnson defined strategic culture as "as an integrated system of symbols (i.e. argumentative structures [causal axioms][300], languages, analogies, metaphors, etc.) that acts to establish pervasive and long-lasting strategic preferences by formulating concepts of the role and efficacy of military force in interstate political affairs, and by clothing these conceptions with such an aura of factuality that the strategic preferences seem uniquely realistic and efficacious."[301] This system of symbols consists of basic assumptions about the strategic environment, i.e. a 'central paradigm' and a limited ranked set of preferences derived from basic assumptions, which, based on hypotheses, could be tested against behaviour. For Johnston, culture should be persistent and change slowly for it to have a causal effect on decision-making. Most importantly, he separated culture from behaviour, because otherwise he would have been guilty of the same tautology of which he accused the first generation.[302]

Gray's definition of strategic culture is more complex than Johnston's and he has developed his concept over time. In his book *Modern Strategy*, Gray gave the following definition: "Strategic culture consists of the socially constructed and transmitted assumptions, habits of mind, traditions, and preferred methods of operation—that is, behavior—that are more or less specific to a particular geographically based security community. A security community may not be monolithic and can have several strategic (and military) cultures […] and it or they will be challenged constantly to adapt to new conditions. Strategic culture is likely to manifest itself in strategic behavior, though certainly not in a mechanistic or deterministic way."[303] For Gray, culture is

[295] Johnston, Alastair Iain. Thinking about Strategic Culture. International Security, Vol. 19, No. 4 (Spring 1995), 32-64 33.
[296] Ibid., 40-41.
[297] Ibid., 41-43.
[298] Gray 1999b. Johnston's reply to Gray did not really build any bridges between their approaches. (Johnston 1999; Poore, 2003).
[299] Cf. Booth, Ken. The Concept of Strategic Culture Affirmed. In Jacobsen, C.G. (ed.) Strategic Power: USA/USSR. New York: St Martin's Press, 1990, 121-128, 121; Rosen, Stephen Peter. Military Effectiveness: Why Society Matters. International Security, Vol. 19, No.4 (Spring 1995), 5-31; Katzenstein et al. 1996, 6-7.
[300] Johnston, Alastair John. Cultural Realism and Strategy in Maoist China. In Katzenstein 1996, 216-268, 222.
[301] Johnston 1995, 46.
[302] Johnston 1995 & 1996.
[303] Gray 1999a, 28.

both the shaping context of strategic behaviour[304], which gives it meaning, and 'the total warp and woof of matters strategic' (i.e. constituent of that behaviour).[305] Not surprisingly, this definition has caused some confusion.[306] Especially confusing is Gray's claim that that polities cannot always follow their culturally preferred policy choices and that all dimensions of strategy affect behaviour.[307] The influence of constructivism on Gray is clear when he claims that strategic culture and strategic behaviour are mutually constitutive, and the state's culture evolves based on how it itself and others interpret its behaviour.[308] Gray insists that behaviour is part of culture and by doing so disputes Johnston's project for a positivist study of strategic culture.[309] This has led Gray to champion interpretivist epistemology, although, however, always keeping in mind the practical needs of strategy. Moreover, according to Gray, strategic culture's influence is issue-dependent and changes gradually, but it also adopts outside influences through shocks, and it is negotiated and so always constrained by domestic factors and the international environment.[310]

Although the debate between Johnston and Gray did not solve the differences between their approaches, it highlighted some of the basic problems of a strategic cultural approach.[311] Strategic culture is difficult to operationalize for empirical study, the reasons for its stability or change are difficulty to prove, its added value to material explanations is suspect, and its ability to produce forecasts is low, and thus its policy relevance has been challenged.[312] Additionally, it has been claimed that by concentrating on *sui generis* cases, strategic cultural studies do not produce comparable knowledge or generalizations for scientific advancement.[313] Moreover, IR and Strategic Studies rely heavily upon the works of historians which are already interpretations in themselves and include implicit and explicit underlying assumptions.[314] They usually refer to historical studies or English-language media sources for their material. For example, many strategic cultural studies of Russia or China use mostly English-language secondary sources.[315] If a researcher aims to understand foreign social meanings and culture, he/she must immerse himself/herself in the subject, i.e. get to know the history, language, and the culture of foreign nations.

[304] By strategic behaviour Gray meant behaviour relevant to the threat or use of force for political purposes. (Gray 1999b, 49-69, 50).

[305] Ibid. It might also be a plot or a way of thinking (Gray 2007).

[306] Poore 2003.

[307] Gray1999a, 53, 130 & 150.

[308] Bloomfield, Alan and Nossal, Kim Richard. Towards an Explicative Understanding of Strategic Culture: The Cases of Australia and Canada. Contemporary Security Policy, Vol. 28, No. 2 (2007), 286-307, 288.

[309] Here Gray follows Raymond Williams. Cf. Storey, John (ed.) Cultural Theory and Popular Culture: A Reader (5th ed.) London: Pearson Longman, 2015.

[310] Gray 2007.

[311] Christopher Twomey has summarized these as over-determination, empirical failings, and the unresolved role of causality in epistemology (Twomey 2008, 344).

[312] Lantis, Jeffrey S. and Darryl Howlett. Strategic Culture. In Baylis, Wirtz & Gray 2013, 84-101, 91-95; Strachan 2013, 136-140. Desch 1998; Twomey 2008.

[313] Desch 1998. For response to Desch's criticism cf. Duffield, John S., Farrell, Theo, Price, Richard and Desch, Michael C. Correspondence—Isms and Schisms: Culturalism versus Realism in Security Studies. International Security, Vol. 24, No. 1 (Summer 1999) 156-180.

[314] Quirk, Joel. Historical Methods. In Reus-Smith & Snidal 2010, 518-536.

[315] For example, Payne, Keith B. and Foster, John S. Russian strategy Expansion, crisis and conflict. Comparative Strategy, Vol. 36, No. 1 (2017), 1-89; Eitelhuber, Norbert. The Russian Bear: Russian Strategic Culture and What it Implies for the West. Connections, Vol. 9, No. 1 (Winter 2009), 1-28; Becker et al. 2016; Marten 2017.

During the 2000s-2010s, the study of strategic culture has moved away from a monolithic understanding of culture towards subcultures, and the object of study has changed from national culture to decision-making elites who are given a larger role in shaping the culture. Instead of exploring the effects of persistent ideas, the research has explored why some ideas persist and others change.[316] One aspect of strategic culture which has remained unresolved is its source, the other is what exactly belongs to strategic culture. Current trends in strategic cultural studies have been categorized in diverse ways. For example, Jeffrey Lantis and Darryl Howlett describe approaches to strategic culture as value adding, explanatory and immersive, the distinction being what kind of explanatory power is given to culture. Value-adding perspectives are used to explain variation in realist models, explanatory views use culture as an independent variable to explain behaviour and the immersive approach is based on understanding and does not produce falsifiable theories.[317] On the other hand, John Glenn identifies four 'conceptions' of strategic culture: the epiphenomenal concept which considers culture as intervening variable, the conventional constructivist view which considers culture as the source of reasons, the post-structuralist conception which considers culture as an instrument to recreate reality through language, and the interpretivist view which considers culture as a framework of understanding.[318]

Below some ideas of current scholars of strategic culture are presented which specifically inform this thesis's theoretical framework. The synthesis is offered in Chapter 2.6. The starting point is that I will subscribe to the immersive or constructive category of strategic cultural research, and will thus bracket the issues of causality and the separation of ideas and behaviour, and I will abandon the concept of culture for a more fine-grained concept of strategic cultural ideas. Moreover, I will use Russian language primary sources in tracing the development of those ideas.

Jeffrey Lantis has been one of the most prolific writers on strategic culture in the 2000s and he points out that strategic culture has cognitive, evaluative and expressive dimensions.[319] The cognitive dimension includes empirical and causal beliefs, while the evaluative dimension consists of values, norms and moral judgement, and the expressive or affective dimension encompasses emotional attachments, patterns of identity and loyalty, and feelings of affinity, aversion, or indifference.[320] This definition pays attention to the nature of beliefs or ideas that restrict or constitute behaviour. It also explains how beliefs can at the same time guide strategic decision-makers and offer them tools for justification and legitimization policies—beliefs are frames

[316] Farrell 2002; Uz Zaman 2009; Sondhaus 2006; Gray 2007; Bloomfield 2012; Lantis 2014; Lantis & Howlett 2013.

[317] Lantis & Howlett 2013.

[318] Glenn, John. Realism versus Strategic Culture: Competition and Collaboration? International Studies Review, Vol. 11, No. 3 (2009), 523-551. For other categories cf. Christian Bueger and Frank Gadinger (2015) The Play of International Practice. International Studies Quarterly (2015) 59, 449–460, 451; Adler, Emanuel and Pouliot, Vincent (2011). International practices. International Theory, Vol. 3 No. 1, pp 1-36, 14; Desch 1998; Twomey 2008, 340.

[319] This is similar to what Alan Bloomfield has called 'schemas' or cognitive shortcuts (Bloomfield 2012, 451-452).

[320] Lantis, Jeffery S. Strategic Culture and National Security Policy. International Studies Review, Vol. 4, No. 3 (Autumn 2002), 87-113., 90. Lantis takes this division from John Duffield (Duffield, John S. World Power Forsaken: Political Culture, International Institutions, and German Security Policy After Unification. Stanford, CA: Stanford University Press, 1998, 23).

for understanding but also tools for mobilization. Lantis has also argued that institutions socialize members and provide 'frames' which offer them a cognitive framework to interpret what counts as a problem, how problems are presented, what strategies should be used to solve problems, and what kinds of constraints and requirements are placed on the solutions.[321] As Lantis has perhaps been more interested in continuity, Kelly Longhurst has instead argued that a change of culture is based on continuous self-evaluation vis-á-via external reality (fine-tuning) or occurs through shocks. Stability is based on institutional practices which sustain knowledge and limit the range of conceivable actions and responses. However, generational change may lead to re-evaluation.[322] The ideas of Lantis and Longhurst need to be kept in mind when analysing the continuity of Soviet ideas from one regime to another.

De Souza has offered a definition of culture based on critical realism.[323] According to her, community and culture are not united. The cultural system consists of all knowable proposed ideas and socio-cultural interaction, i.e. the relationship between social order and ideas. Change comes from internal and external sources. Internal changes come from how ideas interplay with each other and how the social system affects the relationship between the political and social order and ideas. External changes arise from events and outside influences. Cultural and social systems are open, emergent systems consisting of structures, powers and mechanisms. They produce intentional agents which adopt, adapt and manipulate ideas. Souza claims that knowledge of objects is based on prior social products (knowledge). This means that all new ideas must be fitted to old ones and are, in fact, products of the old ones.[324] Another view on this changing and reproductive nature of culture is to approach it as a practice or a continuous performance.[325] Thus, Soviet and Russian ideas interact, merge, and produce new meanings and the political, social and cultural elements cannot be disconnected.

Tamil Libel has studied Israel's changing security policy. He combines the ideas of 'epistemic communities' and subcultures with strategic culture to examine how policy crisis challenges hegemonic culture, how communities organize themselves around innovative statements, how they compete in public and how their ideas are diffused, how policy-makers select one of the subcultures and incorporate it to their policies and how a subculture then gains persistence and hegemony. Epistemic communities are not only academic circles whose influence is based on expertise, they also have power and resources needed to compete in public.[326] Libel's model is made to correspond to democratic systems so the 'competition' phase could be opaquer in autocratic political systems. Moreover, the existence and strength of distinct subcultures is also suspect or at least empirically difficult to prove in opaque political systems with one-party-rule.

[321] Lantis, Jeffrey S. Strategic Culture and Tailored Deterrence: Bridging the Gap between Theory and Practice, Contemporary Security Policy, Vol. 30, No. 3 (2009), 467-485.
[322] Longhurst, Kelly. Germany and the use of force. Manchester: Manchester University Press, 2004.
[323] De Souza, 2014.
[324] Adler 1992, 101–145.
[325] Adler & Pouliott, 2011; Bueger & Gadinger 2015.
[326] Libel 2016.

Renny Babiarz's study is also interesting in which he explains the Chinese approach to nuclear deterrence during the Mao Zedong era with strategic culture based on the concept of the 'People's War'.[327] Babiarz argues that instead of process-tracing certain foreign policy decisions, competing and hegemonic ideas about a particular issue can be studied. Then the development of concrete projects related to that issue are analysed, and finally the correspondence of ideas and the project can be analysed. This type of analysis is based on finding reasons for action, not on the causality of ideas. However, Babiarz's study concentrates only on one idea, whereas it is quite possible that there are any number of ideas influencing certain policy issues at any point of time. Finally, Dima Adamsky has proved the important point that the Soviet Union's or Russia's and the United States' strategic cultures have at least been in indirect contact and ideas have flown between them.[328] Ideas thus flow even between ideologically competing superpowers, which proves the point that epistemic communities are not necessarily insular.

Before I summarize my approach on strategic culture, a few parallel concepts of strategic culture need to be defined. These are: political culture, national character, security culture, organizational culture, military culture, the national way of war, and the character of war. Political culture refers to a subset of beliefs and values of a society that relate to a political system.[329] The national character is associated with the primordial characteristics of some ethnically related group of people and it is connected to a collective identity which might have effects on state foreign policy.[330] Security culture is more of a synonym of strategic culture than a parallel concept, but its scope of 'owners' and 'objects' of security is more extensive.[331] Organizational culture is a culture of a particular organization providing a collective understanding and shapes the perceptions of its members and thus frames and constrains the decision-making.[332] Military culture concerns only the military and includes perceptions of strategy, operations, and tactics.[333] The national way of war has been used to describe, and in some cases to predict, how nations use military power. It is sometimes derived from

[327] Babiarz, Renny. The People's Nuclear Weapon: Strategic Culture and the Development of China's Nuclear Weapons Program, Comparative Strategy, Vol. 34, No. 5 (2015), 422-446.

[328] Adamsky 2010.

[329] Almond, Gabriel A. and Verba, Sidney. The Civic Culture: Political Attitudes and Democracy in Five Nations. Princeton, N.J.: Princeton University Press, 1963, 11-14; Elkins, David J. and Simeon, Richard E. B. A Cause in Search of Its Effect, or What Does Political Culture Explain? Comparative Politics, Vol. 11, No. 2 (1979), 127-128; Geertz, Clifford. The Interpretation of Cultures. New York: Basic Books, 1973; Lane, Ruth. Political Culture: Residual Category or General Theory? Comparative Political Studies, Vol. 25 (October 1992), 362-387.

[330] Kowert Paul A. National Identity: Inside and Out. Security Studies, Vol. 8 (Winter 1998/99–Spring 1999), 1-34.

[331] Krause, Keith. Conclusions: Security culture and the non-proliferation, arms control and disarmament agenda. Contemporary Security Policy, Vol. 19, No. 1 (1998), 219-239, 221-222. Monica Gariup has claimed that security and strategic culture are two sides of the same coin: the first defines threats and the latter the means to counter them. (Gariup, Monica. European Security Culture: Language, Theory, Policy. Surrey: Ashgate, 2009, 41).

[332] Kier, Elizabeth. Culture and French Military Doctrine Before World War II. In Katzenstein 1996, 186-215, 202.

[333] Ruffa, Chiara. Military Cultures and Force Employment in Peace Operations. Security Studies, Vol. 26, No. 3 (2017), 391-422, 393.

a larger strategic culture and includes both culture and observed behaviour.[334] The concept of the character of war is based on the beliefs about the current and future meaning of war, its legitimate means and goals, and the utility of force.[335] Both the concepts of way of war and the character of war can be understood as component parts of strategic culture, although the character of war transcends national and state borders because war can be understood as an international social fact or a subjective understanding.[336]

What separates strategic culture from the above discussed parallel concepts is its connection to the threat or use of force to achieve political ends by the state military and security elites. Force in the context of strategic must been understood as all means of national power, i.e. military, political, diplomatic, economic etc. National ways of war and the character of war are incorporated in strategic culture as ideas and beliefs about the threat and use of force. Nevertheless, this culture is not a monolithic structure but it is fragmented, contested, and changing.[337]

To summarize, my approach to strategic culture is sympathetic to Snyder who on a conceptual level included almost everything that has been rediscovered by the later strategic culture scholars. Where I diverge from Snyder, and from many others, is that I concentrate on specific ideas and beliefs instead of a culture as a system or structure. I consider 'culture' as a pool of ideas whose influence and persistence are very much based on epistemic communities and the institutions carrying them. This is more in line with De Souza, Adler, and generally critical realism which excludes the possibility that culture is a closed system. From this it is clear, that I consider ideas as 'objects', the interaction of which produces emergent results. Ideas have power because they affect how agents understand their environment and their possible ways of action. I use the concept of 'strategic cultural ideas' to denote causal beliefs and sometimes principled beliefs as being about the threat and use of force—about how means and ends fit together on issues concerning state security interests—held by people belonging to epistemic communities and, consequently, to defence and security elites. These ideas are communicated by and connected to certain concepts (symbolic representations, i.e. words with meaning) which carry meanings about the reality. I must be clear here: I am not interested in how these ideas construct identities and interests, i.e. discourse analysis. Nor am I interested explicitly in the lifecycle of ideas or epistemic communities. I am interested in how agents understand certain objects or processes of reality through these persistent but adaptable ideas and what kinds of reasons for action these ideas might offer. I do not strive to explain Russian strategic behaviour in cyberspace through cultural preferences. I only want to examine how certain strategic cultural ideas resonate with Russian actions, how they provide reasons to shape

[334] Freedman, Lawrence. A Western way of war? Adelphi Papers, Vol. 38, No. 318 (2008), 11-17; Hoffman, Frank. Strategic Culture and Ways of War: Elusive Fiction or Essential Concept? Naval War College Review, Vol. 70, No. 2 (Spring 2017), 137-142; Gray 2007, 5; Hoffman 2017; Echevarria II, Antulio J. Strategic Culture Is Not a Silver Bullet. Naval War College Review, Vol. 70, No. 4 (Autumn 2017), 121-124.

[335] Raitasalo, Jyri and Sipilä, Joonas. Sodan tutkimus strategian näkökulmasta [The study of war from the perspective of Strategic studies]. In Raitasalo, Jyri and Sipilä, Joonas. Muuttuva sota [Changing war]. Jyväskylä: Kustannusosakeyhtiö Suomen Mies, 2005, 15-23; Milevski, Lukas. The nature of strategy versus the character of war. Comparative Strategy, Vol. 35, No. 5 (2016), 438-446.

[336] Of the latter 'the generations of war' literature is an exemplary case. Cf. Junio, Timothy J. Military History and Fourth Generation Warfare. Journal of Strategic Studies, Vol. 32, No. 2 (2009), 243-269.

[337] Gray 2007.

cyberspace in specific ways.

By combining NCR, Barkin's constructivist realism and an interpretive version of strategic culture with practices it can be argued that the ideas carried by strategic culture are made real through practices—through the making of strategy. Security elites apply culturally persistent ideas to understand and shape reality either consciously or unconsciously. They choose these ideas based on their interpretation of international system and rationally bounded means-ends calculations. In this way, through the practices of states, cultural ideas shape ideational and material reality, produce power by shaping reality, and by changing social reality, change the actors themselves. However, because reality constrains actions and has emergent properties, and because there are other international intentional actors with cultural ideas of their own, and because the defence and security elite's control of ideas is restricted and because elites must consider both international and domestic 'games', strategic cultural ideas do not determine outcomes. This is even more true when we are talking about cyberspace, which is a manmade and malleable environment. The point in combining constructivism, NCR, and strategic cultural ideas is to demonstrate how ideas affect the state's policies by influencing elite reasoning and how this shapes reality by directing power in a certain way. There is an objective, material reality but how this is understood and how the use of force is comprehended and then utilized differs between states. This is especially true concerning new environments, resources, and means like cyberspace, cyber power, and cyber warfare.[338]

2.6 Synthesis

The theoretical framework I am proposing here is by its nature constitutive. It describes the process through which ideas influence the way power is understood and used in a certain environment but does not make any claims of causality. It is also a lens to the world. Its task is to legitimize the approach I take in understanding how certain strategic cultural ideas influence the way in which the Russian state shapes cyberspace. It is a middle-level foreign policy theory more than a theory of IR. Accordingly, the basic premises of my theory are: power matters, while the material and social environments constrain and enable actors, and can be changed, ideas are important, and dissimilar states guided by elites are the primary actors in international relations.

Because power matters in state to state relations, the international system, or environment of states, is based on a division of power. Power by its nature is both material and social. Its division does not directly cause states to behave in any fixed way because power is affected by geography, institutions, norms, technology, and the offence and defence balance. Most importantly, this environment is strategic, and it gains its meaning through the perception of defence and security elites. Power is relational and contextual—one such context being cyberspace understood as a subdomain of the international system. Strategic cultural ideas as causal or principled beliefs are about the threat and use of force for political ends and they affect the way in which state defence

[338] To prove a point cf. Jordan et al. 2008; Sloan 2012; Angström, J. and Widen, J. Contemporary Military Theory: The Dynamics of War. New York: Routledge, 2015; Gartzke, E. J. and Lindsay, J. R. Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. Security Studies, Vol. 24, No. 2 (2015), 316-348.

and security elites understand their environment, of which clear and complete information is not available per se. Incentives of the environment are real but subjective.[339] Ideas influence the continuous strategic decision-making process, consisting of assessment, formulation, and implementation of strategy, i.e. its practice. Ideas affect 'the making of strategy'[340] but they do not determine it. This is because reality constrains actions and has emergent properties, and there are other international, intentional actors with cultural ideas of their own who the defence and security elites do not control (i.e. epistemic communities have power), and because elites must consider both international and domestic 'games.'

The ways in which a state uses power to pursue its interests, including creating more power, are influenced by ideas and thus ideas shape reality through power.[341] In other words, ideas shape the understanding of the environment, give meaning to material power, indicate acceptable and unacceptable strategic choices, and affect the interpretation of the use of power. In this way they are reasons for contextual social action.[342] Ideas have constructive effects, that is, they change the social and material reality through intentional and positional agents and emergent processes. Together ideas might amount to constitutive effects, but their individual effects and interaction is better captured by the concept of construction.[343]

Ideas influencing the state elites might be quite persistent. However, in situations when the environment is understood to be confusing or threatening, old and new ideas are employed in creative and innovative ways to make sense of it and to guide action. Cyberspace is arguably a new environment with unknown or poorly understood potential threats.[344] This does not mean that the material reality is ontologically prioritized over social reality—what matters is how defence and security elites understand the environment. Elites get their ideas primarily from epistemic communities who are the carriers of 'all knowable and proposed ideas' in society. This system of ideas is open and changing. Ideas are born through interaction of old ones and through influences from the outside. New ideas must be 'fitted' to old ones—they must make sense in order to have legitimacy. When old policies fail, or new ones are needed because of changes in the environment, epistemic communities articulate ideas in statements which might compete with each other. Defence and security elites choose and adapt

[339] Foulon 2015.

[340] Freedman 2013, xi; Popescu, Ionut C. Grand Strategy vs. Emergent Strategy in the conduct of foreign policy. The Journal of Strategic Studies, Vol. 41, No. 3 (2018) 438-460.

[341] Foulon 2015; Freedman 2013, xi; Popescu2018.

[342] Although I do not deny that ideas produce meaning for identities and interests, I bracket this process, and concentrate on interpretive dispositions for intentional actions which I shall call reasons.

[343] To study constructive effects is to show that particular ideas are present and then to examine how an agent's behaviour reflects these ideas in the temporal dimension and how that behaviour constructs reality. It starts by examining the meanings given to a certain phenomenon (how something is understood through ideas), then proceeds to examine how these meanings are present in intentional behaviour (how ideas are reflected in actions connected to this something), and finally examines how reality is changed (how this something is changed). In sum, ideas have the constructive potential to change reality. This potential actualizes as they provide reasons for actions, but do not determine it. Ideas shape reality through actions of intentional agents and ideas need to be carried and used. It is an emergent process because it consists of human beings and as such, it is not determined by either ideas or the environment. My concept of 'constructive' effects could be criticized for being just a synthesis of constitutive and causal effects. It might just be a new name for the process between agents and structures. Nevertheless, I consider it a beneficial tool to conceptualize how ideas affect reality by intentional agents adopting them and using them.

[344] On these arguments cf. Chapter 3.

those ideas that ‘fit’, i.e. those which are understandable and provide guidelines for appropriate means to ends. These are formed into policies and then implemented. The above described process is theoretical. Every real society and state have their own constellation of epistemic communities and elites and rules for their interaction.

Based on the above, an empirical analysis to understand how ideas affect the strategic decision-making in any particular case of state use of power must consider the strategic environment, the internal characteristics, and the internal processes of a state. Thus, the particulars of a political system and the composition of elites with power related to the issue under study must be examined. However, to be clear, I am interested in understanding how ideas influence the ways and means of implementing strategy and the outcomes of the implementation, not the specific decision-making process or the success or failure of policies, or the effects of the objective environment on state behaviour. Therefore, I reject NCR’s search for causality, explanation, and prediction. Nevertheless, I accept NCR’s modified ontological framework as proposed by Ripsman et al. as a middle-range theory of social reality.[345]

My ontology relies more on constructivism than the admittedly overly complex one proposed by critical realism.[346] Observations and theories are therefore dependent on the scholar. There is a social ‘reality’ but it cannot be fully captured, and knowledge claims can only be justified through ‘rational adjucation.’[347] I claim no direct causality between ideas and action, only that ideas shape the understanding of agents of their environment and of their own actions.[348] My epistemological approach is ‘interpretative’ in the sense that I believe ideas carried by elites can be known and understood in a similar way in which the elites themselves understand the ideas and the reasons they provide—I make no claims beyond conscious understanding. Methodologically I am interested in the constructive effects of ideas and beliefs held by agents to practices and structures—or in the context of this thesis: how ideas held by Russian defence and security elites shape cyberspace through Russian strategy and policies. Thus I am interested in the representations of particular ideas in the texts produced by epistemic communities and in the policies (texts and behaviour) formulated by the decision-making elites. My choices can be criticized, but I argue that I have constructed a theory and approach tailored for this study and its subject and that this is in accordance with realist analytic pragmatist philosophy. in the next Chapter, I will introduce the main concepts, which will enable me to apply my theoretical framework to the study of Russian Federation’s strategy to control and shape a part of cyberspace into ‘a national segment of the Internet.’

[345] On middle-level theory cf. Merton, Robert K. Social Theory and Social Structure. New York: Free Press, 1968.

[346] Adler 2005, 100.

[347] Adjucation refers to “a relative, working truth, that is, claims to validity that I expect to be true only in relation to other interpretive claims, not to some objective reality. The claims to validity are ‘working’ because they operate.” Hopf, Ted. Social Construction of International Politics: Identities and Foreign Policies, Moscow, 1955 and 1999. Ithaca, NY: Cornell University Press, 2002, 24. Cf. also Wight 2005; Kurki & Wight 2013.).

[348] Patomäki & Wight 2000; Adler & Pouliot 2013; Lebow 2010.

3

CYBER CONCEPTS AND CLOSED NATIONAL NETWORK

In this chapter I examine and develop the main concepts of this thesis: Cyberspace, cyber power, cyber warfare, cyber strategy and a closed national network. These are based on previous research and are offered as theoretical concepts to understand how states shape cyberspace in the neoclassical realist theoretical framework that was adopted in the previous chapter. The concepts guide the empirical analysis conducted in the following chapters in three ways: 1) They inform me of the kind of ideas or causal beliefs I should be looking for when interpreting Russian thinking on cyberspace and power—they provide a preliminary description of the objects of reality to which ideas give meaning; 2) they provide tools for analysing how Russian policies shape cyberspace; and 3) they enable the analysis of the Russian segment of Internet as a closed national network.

3.1 A short history of cyber issues

Strategic thinking about cyberspace and cyber power started in the 1990s but really got off the ground at the beginning of the 2000s.[349] Accordingly, concepts and theories have not yet matured or stabilized enough to form a coherent theory of cyber issues, 'cyber warfare' least among them, and many of the concepts with the cyber -prefix are academically and politically contested.[350] Additionally, cyberspace and military issues related to it are not defined by international law and there is no international consensus about them—although a UN workgroup of experts has proposed that international law should be applicable to cyberspace and there have been non-governmental efforts to create a basis for cyber law.[351] IR theory has just started to incorporate cyber issues in International Relations.[352] Thus, cyberspace and the scholarly understanding of it have both been in a constant flux for the past thirty years.[353] In this context, it is clear that no common definition of cyberspace or power, to say nothing about warfare can be found. Here I shall bracket the social and economic aspects of

[349] On the development of 'cyber' cf. Rid, Thomas. Rise of the Machines: A Cybernetic History. New York: W. W. Norton & Company Inc., 2016; Kaplan, Fred. Dark Territory. The Secret History of Cyber War. New York: Simon & Schuster, 2016.

[350] Valeriano, Brandon and Maness, Ryan C. Cyber War versus Cyber Realities Cyber Conflict in the International System. New York: Oxford University Press, 2015, 21-22; Choucri, Nazli and Goldsmith, Daniel. Lost in cyberspace: Harnessing the Internet, international relations, and global security, Bulletin of the Atomic Scientists, Vol. 68, No. 2 (2012), 70-77; Lango 2016.

[351] Kavanagh, Camino. The United Nations, Cyberspace and International Peace and Security—Responding to Complexity in the 21st Century. UNIDIR, 2017; Schmitt, Michael N. (ed.) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017.

[352] Cf. Choucri 2012; Kremer & Müller, 2016.

[353] On the development of the scientific discourse on cyber security cf. Dunn Cavelty & Wenger 2020; Sharp, Travis. Theorizing cyber coercion: The 2014 North Korean operation against Sony. The Journal of Strategic Studies, Vol. 40, No. 7 (2017), 898-926. It should be noted that as late as in 2012 a scholar complained that "there has been little systematic theoretical or empirical analysis of the cyber issue from the perspective of international security." Kello, Lucas. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. International Security, Vol. 38, No. 2 (Fall 2013), 7-40, 8,

cyberspace and concentrate mostly on texts produced from a military-strategic perspective.

The term cyberspace was coined by a science-fiction writer William Gibson in 1982.[354] Gibson defined the term as "'consensual hallucination' that takes place when humans interact with networked computers".[355] The prefix to space used by Gibson has its roots in the concept of 'cybernetics' which was developed by the mathematician Norbert Wiener in the 1940s. He was writing about human-machine analogies, the nature of information, control and feedback mechanisms, and borrowed the term cyber from the Greek word for steersman.[356] Cybernetics had its theoretical high tide in the West in the 1950-1960s when a group of American and British academics elaborated it into theories of automatization, robotization, and cyborgization.[357] Some of the academics were later involved in the development of ARPANET (Advanced Research Projects Agency Network)—the network upon which the Internet was later built.[358] Cybernetics later branched into multiple different theories under diverse disciplines and the term itself was largely abandoned. It was replaced in the 1980s by the term 'information' in management, business, and social sciences and policy circles, either referring to systems and artefacts of a new transformative technology or to a new kind of social order brought about by technological revolution—information society.[359]

In the 1980-1990s Western militaries got interested in virtual reality, precision guided weapon systems, sensor fusion, information warfare (IW), and Network Centric Warfare (NCW), in short, during the Revolution in Military Affairs (RMA) which brought information technology to the forefront of military affairs.[360] At same time information society[361] started to develop along with the Internet[362]. The cyber-term made

[354] Rid 2016, 209-201.
[355] Sheldon 2013, 304.
[356] Peters 2016, 17; Kline, Ronald R. The Cybernetics Moment, Or Why We Call Our Age the Information Age. Baltimore: Johns Hopkins University Press, 2015, 11-12.
[357] Peters 2016, 20-21; Kline 2015.
[358] ARPANET was the predecessor of the Internet put online in 1969 partly to explore the feasibility of packet switching techniques. It was not primarily meant as a 'nuclear war resistant network' but nevertheless later developed as a testbed for robust and survivable communications (Internet Society. Brief History of Internet. 1997. [Online]. Available from https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf. [Accessed 5 August 2018]. Cf. also Peters 2016, 18-19; Rid 2016, 47-53.
[359] Kline 2015.
[360] Cf. Alberts, David S. and Papp, Daniel S. (eds.) Information Age Anthology – Volume III: The Information Age Military – Volume III. CCRP Publication Series, 2001; Cooper, Jeffrey. Another View of the Revolution in Military Affairs, July 15, 1994 [Online]. http://ssi.armywarcollege.edu/pdffiles/00232.pdf [Accessed: 28th September 2018].
[361] According to Manuel Castells: "…a specific form of social organization in which information generation, processing, and transmission become the fundamental sources of productivity and power because of new technological conditions emerging in this historical period." (Castells, Manuel. The Rise of the Network Society (2nd ed.) Chichester: Wiley-Blackwell, 2010, 21 ft. 31). Cf. also Webster, Frank. Theories of the Information Society. London and New York: Routledge, 2006.
[362] The Internet was born from the interconnecting and commercialization of research networks in the 1980s (Internet Society 1997). "Internet" refers to the global information system that (i) is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; (ii) is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and (iii) provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure described herein." (U.S. Federal Networking Council. Resolution of October 24, 1995. Cited in Internet Society 1997, 17). Or more briefly "A global system of interconnected computer networks that use the

a 'comeback' when the popular culture (ála Gibson and others) and the need for novel concepts to understand the changing reality merged in the 1990s. In the English-speaking world the term 'cyber' transformed gradually to mean almost anything related to networks and computers.[363] Currently, 'information' and 'cyber' live side-by-side in English-language military discourses but have a somewhat contested and strained relationship.[364]

Cybernetics had a significant impact on the development of robotics, computers and networks during the Cold War on both sides of the confrontation.[365] It was adopted from Western thought by Soviet scientists as *kibernetika* which expanded later to influence large parts of the Soviet scientific field and guided the faith in the promise of computer based technocratic governance.[366] As Benjamin Peters has argued, Soviet science "...rejected, rehabilitated, adopted and adapted cybernetics for historically expedient and changing purposes."[367] The force of 'kibernetik' ideas was such that Slava Gerovitch claims that cybernetics affected almost all of the Soviet sciences.[368] Despite of the enthusiasm for cybernetics the Soviet Union never managed to produce its own version of the Internet.[369] The Soviet military was aware of the changing nature of war caused by the development of information technology perhaps earlier than its Western counterparts, and in fact provided the West with the concept of the Military-Technological Revolution. Nevertheless, it had only limited success in putting its own ideas into practise before the fall of the Soviet Union.[370]

Cybernetics left a whole sublanguage of input-output-feedback systems based on computer technology in the Russian language.[371] However, modern Russian official texts do not use the term cyber but instead use the term information.[372] Unofficially the term cyber is quite commonly used.[373] Previous studies have argued that the Russians see 'cyber' only as a technological (information-technical) subcomponent of a much larger 'information space' which includes cognitive, informational and infrastructural components and that there might be political motivations behind the usage of the term information.[374]

Internet Protocol suite and a clearly defined routing policy." (Schmitt 2017, 565).

[363] Rid 2016, 303-307; Kaplan 2016, 46.

[364] Cf. Betz, David. J. The more you know, the less you understand: The problem with information warfare. Journal of Strategic Studies, Vol. 29, No. 3 (2006), 505-533; Porche, Isaac III, Paul, Christopher, York, Michael, Serena, Chad C., Sollinger, Jerry M., Axelband, Elliot, Min, Endy Y., Held, Bruce J. Redefining Information Warfare Boundaries for an Army in a Wireless World. Santa Monica: RAND, 2013.

[365] Rid 2016, 76-82, 110; Peters 2016; Gerovitch 2002; Gerovitch2008.

[366] Peters 2016, 32-48; Gerovitch 2008, 337. It should be pointed out that similar ideas were circulated in the Soviet scientific circles already in the 1930s but were repressed by Stalin's purges (Susiluoto 2006.)

[367] Peters 2016, 29.

[368] Gerovitch 2008, 337.

[369] Gerovitch 2008, 336; Peters 2016, 172-175; Susiluoto 2006.

[370] Adamsky 2008, 257-294; Adamsky 2010, 54-57.

[371] Gerovitch 2002 & 2008.

[372] Russians favour the term 'information' (informatsionnyi or informatsiia). Cf. Godwin III, J. B., Kulpim, A., Rauscher, K. F. and Yaschenko, V. (eds.) Critical Terminology Foundations 2. Russia-U.S. Bilateral on Cybersecurity. Policy Report 2/2014. East West Institute and the Information Security Institute of Moscow State University [Online]. Available: https://www.files.ethz.ch/isn/178418/terminology2.pdf [Accessed: 22nd June 2019].

[373] 5th of July 2018 Yandex.ru produced 186 million hits on the word 'кибер' (cyber). For comparison Google.com produced 345 million hits on the word 'cyber'.

[374] Thomas, Timothy L. Dialectical versus empirical thinking: Ten key elements of the Russian understanding of information operations, The Journal of Slavic Military Studies, Vol. 11, No. 1 (1998), 40-62; Thomas 2015a;

Based on this short history of terminology it can be argued that the meanings of cyberspace and power are cultural constructs, i.e. that they are based on strategic cultural ideas. Moreover, there has been a transfer of ideas between, arguably hostile, cultures. Thus, I argue, based on the theoretical framework adopted in Chapter 2, that behind differing meanings there are real and objective phenomena that different cultures have tried to comprehend in their own way. To denote these objects this thesis uses the term 'cyber' as a prefix that gets its meaning in combinations with other terms. Brandon Valeriano and Ryan C. Maness have described cyber as meaning "computer and digital interactions."[375] It seems to resonate adequately with both Western and Russian understandings.[376]

3.2 Cyberspace

This chapter examines what previous studies have claimed about cyberspace. It will then proceed to take a more throughout look at cyberspace and the Internet to see how well previous, perhaps somewhat abstract definitions correspond with the technical and functional reality of local and global networks. Lastly, I will adopt a definition of cyberspace that will correspond with the empirical reality and my theoretical framework.

3.2.1 Previous concepts of cyberspace

In the Western cyber literature, there are many different definitions for cyberspace and the formulation of the definitions depends on the context they are used in. The Tallinn Manual 2.0, for example, defines cyberspace as: "The environment formed by physical and non-physical components to store, modify, and exchange data using computer networks."[377] Many definitions claim that cyberspace is a manmade space, medium or environment, distinct from the land, sea, air, and outer space.[378] Some definitions emphasize the electromagnetic transfer of information, interconnection of systems and networks.[379] Others concentrate more on the functionality of cyberspace,

Giles, Keir and Hagestad II, William. Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. In K. Podins, J. Stinissen, M. Maybaum (Eds.) 5th International Conference on Cyber Conflict 2013 - Proceedings. NATO CCD COE Publications, Tallinn, 2013, 413-429; Fitzgerald, Mary. Russian Views on IW, EW, and Command and Control: Implications for the 21st Century. CCRTS 1999. U.S. Naval War College, Rhode Island. June 29 - July 1, 1999 [Online] Available: http://www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/089fitzg.pdf [Accessed 5th August 2018].

[375] Valeriano & Maness 2015, 22.

[376] Cyber is also adopted as a central term instead of information because the understanding of information is much wider in both English and Russian. By concentrating my analysis on 'cyber' I can more clearly analyse the technical aspects of the Russian information space and produce comparable information structured around concepts created in this chapter.

[377] Schmitt 2017, 564.

[378] For different concepts cf. Reardon, R. and Choucri, N. The Role of Cyberspace in International Relations: A View of the Literature. Prepared for the 2012 ISA Annual Convention, San Diego, CA, 2012 [Online] Available: https://nchoucri.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf [Accessed: 6 August 2018]; Maurer, Tim and Morgus, Robert. Compilation of Existing Cybersecurity and Information Security Related Definitions. New America, Report October 2014 [Online]. Available: https://www.newamerica.org/ cybersecurity-initiative/policy-papers/compilation-of-existing-cybersecurity-and-information-security-related-definitions/ [Accessed: 6th August 2018].

[379] Rattray, Gregory J. Strategic Warfare in Cyberspace. Cambridge: MIT Press, 2001, 95.

i.e. creating, transmitting, receiving, storing, processing and deleting data.[380] Furthermore, some combine these two approaches.[381] Yet some take a more holistic view and combine cyberspace with the information sphere or environment.[382] They designate cyberspace as a platform or facilitator for the flow and use of information. Others have tried to separate the physical infrastructure, software, rules and processes, and information and its users from each other.[383] For example, the current United States' Joint Doctrine defines the 'information environment' as an aggregate of individual, organisation and system levels and physical, informational and cognitive dimensions; and cyberspace as a part of the information environment consisting of layers of physical network, logical network, and cyberpersona.[384] On the civilian side, Martin C. Libicki's division into physical (boxes and wires), syntactic (instructions and rules) and semantic (information useful for humans or instructions for services) levels is one of the most influential definitions.[385] John B. Sheldon has further divided the physical dimension into infrastructure (cables etc.) and the electromagnetic spectrum.[386] In these definitions the control of one level does not necessarily mean control of other levels.[387]

The architecture of cyberspace has been described as a flat, worldwide, interconnected network, without a centre.[388] Some argue that cyberspace is in fact not a separate space or domain, but a 'substrate' underlying all other domains.[389] Although cyberspace as a concept conveys a feeling of borderless and limitless space, it might also be considered inherently fragmented. This is because while cyberspace consists of networks that are largely technologically compatible, a conscious decision is required to connect and disconnect them.[390] The more philosophical understandings of cyberspace have changed over time. They have gone through visions of self-organizing anarchy to 'the Wild West' to global commons and now more towards regime or territorial and sovereign state-centric visions.[391]

[380] Kuehl 2009.

[381] Nye, Joseph. Cyber Power. Cambridge: Harvard Kennedy School, 2010, 2.

[382] Betz & Stevens 2011, 122-123; Sheldon 2013, 309.

[383] Nye 2011a, 123; Choucri 2012, 5.

[384] Joint Chiefs of Staff, the U.S. Department of Defence. Information operations (Joint Publication 3-13), 2014 [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf [Accessed: 6th August 2018]; Joint Chiefs of Staff, the U.S. Department of Defence. Cyberspace operations (Joint Publication 3-12), June 8th 2018 [Online]. Available: https://fas.org/irp/doddir/dod/jp3_12.pdf [Accessed: 17th August 2018].

[385] Libicki 2009, 12-13; Libicki 2016, 21.

[386] Sheldon, John B. Towards a Theory of Cyber Power: Strategic Purpose in Peace and War. In Reveron 2012, 207-224.

[387] Ibid., 215.

[388] Mattioli, R. The ´States(s)´of Cybersecurity. In: Giampiero, G. (ed.) Security in Cyberspace. Targeting Nations, Infrastructures, Individuals. New York: Bloomsbury Academic, 2014, 23-28, 27.

[389] Dombrowski, Peter and Demchak, Chris. Cyber War, Cybered Conflict, and the Maritime Domain. Naval War College Review, Vol. 67, No. 2 (2014), 71-96, 75.

[390] Mueller 2017, 49.

[391] Rid 2016, 239-240; Nye 2010, 15; Raymond, M. Puncturing the Myth of the Internet as a Commons. Georgetown Journal of International Affairs, International Engagement to Cyber III, 2015, 57 – 68, 61-62; Choucri 2012, 235; Demchak & Dombrowski 2011, 32-61; Sterling, Bruce. Short History of the Internet. The Magazine of Fantasy and Science Fiction, February 1993 [Online] Available: https://www.internetsociety.org/internet/history-internet/short-history-of-the-internet/ [Accessed: 6th August 2018].

Cyberspace has its own characteristics. Nazli Choucri lists instantaneity, geographical transcendence, permeation, fluidity, participation, non-attribution and non-accountability.[392] John Sheldon describes cyberspace as having a low cost of entry, multiple actors, an existence based on reliance on the electromagnetic spectrum and man-made objects, constant replication, and instantaneity.[393] According to Gregory Rattray, the strategic features of cyberspace are: the laws of physics, software logic, mutability, interconnectivity, limited limitlessness (actors have power but it is limited), human resources, and know-how.[394] Joseph Nye points out that the virtual level provides a low cost entry to the physical level and that technology has a dominant role in changing the nature of cyberspace.[395] This means that the architecture leads to diffusion of power and empowers multitude of actors.[396] Thus, cyberspace has been described as a domain of human activity with its own characteristics which affect the use of power in and through it.[397] When discussing cyber deterrence Martin Libicki emphasizes the role of man-made rules.[398] He also highlights the problem of attribution, that is, how to link actors in cyberspace to actors in the physical world.[399] A preliminary summary of these definitions is that the cyberspace is a manmade and malleable technological environment.

The connection between information space and cyberspace is apparent in the definitions presented above. This relationship can be understood through Russell Ackoff's data-information-knowledge-wisdom (DIKW) hierarchy.[400] According to Jennifer Rowley, data consists of discrete, objective facts which are unorganized and without meaning. When data is structured and given context and meaning it becomes information. Knowledge is information as part of the human mind, embedded in experience and values and enables action. Wisdom might be an ability for abstraction or critical reflection.[401] If we compare the American military definitions of the information space or environment to the DIKW hierarchy it seems logical that electronic data and electronic information reside in cyberspace, which is a subcomponent of the

[392] Choucri 2012, 4.
[393] Sheldon 2013, 288.
[394] Rattray, Gregory J. An Environmental Approach to Understanding Cyberpower. In Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K. Cyberpower and National Security. Washington, D.C.: National Defence University Press, 2009, 253-274, 256-257.
[395] Nye 2010, 4.
[396] Ibid., 9.
[397] Choucri 2012.
[398] Libicki 2009, 18.
[399] Ibid., 41-52.
[400] Rowley, Jennifer. The wisdom hierarchy: representations of the DIKW hierarchy. Journal of Information Science, Vol. 33, No. 2 (2007), 163-180; Zins, Chaim. Conceptual Approaches for Defining Data, Information, and Knowledge. Journal of the American Society for Information Science and Technology, Vol. 58, No. 4 (2007), 479-493.
[401] Rowley 2007, 170-174.

information space.[402] The idea that the information environment is composed of information, systems, infrastructure and users of information seems to be widespread among the militaries of the great powers.[403]

Based on the above, cyberspace forms the basis for the information space and is thus part of the material and social structure of the international system. This relationship between cyberspace and the information space is contested because of the political implications inherent in the use of information. Moreover, it can be argued that when states try to shape cyberspace, they are influencing something that is shared in objective reality. However, our understanding of this space is constantly changing.[404] Therefore, I shall take more comprehensive and technical look at what cyberspace is composed of.

3.2.2 Wires, protocols and governance

To understand how the Internet and the wider cyberspace really works it is necessary to briefly examine the physical and logical infrastructure of the Internet and its governance. This review is also necessary for understanding Russia's policies towards cyberspace in the later chapters of this thesis because cyberspace is shaped by controlling its physical and logical levels through governance. Therefore, I will highlight the potential vulnerabilities and threats related to the Internet. The overview will also help in devising the concept of a closed national network.

The Internet refers to an interconnected group of global networks whereas cyberspace is a collection of all computer networks, open and closed, public and private.[405] Therefore, the political and social borders of cyberspace refer more precisely to the

[402] "The information environment is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information." (United State Department of Defence (U.S. DoD). Cyberspace Operations, JP 3-12, 8th June 2018, viii [Online]. Available: https://fas.org/irp/doddir/dod/jp3_12.pdf [Accessed: 15th August 2018].) "The information environment is where humans and systems observe, orient, decide, and act upon information, and exists throughout the JFC's OE. The information environment consists of three interrelated dimensions—physical, informational, and cognitive—within which individuals, organizations, and systems continuously interact." (The United State Department of Defence (U.S. DoD). Joint Publication 3-0: Joint Operations, 2017 [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/ jp3_0.pdf [Accessed 20 August 2017]. How cyberspace become part of information environment in the American military doctrine cf. Khuel, Daniel T. Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age. International Law Studies 76. Newport, Rhode Island: U.S. Naval War College, 2002.

[403] This view is also shared by the Russians (cf. Chapter 6) and the Chinese Cf. Wortzel, Larry M. The Chinese people's liberation army and information warfare. The Strategic Studies Institute of The United States Army War College, 2014 [Online]. Available: https://publications.armywarcollege.edu/pubs/2263.pdf [Accessed: 22nd June 2019]; North Atlantic Treaty Organization (NATO). Allied Joint Doctrine for Information Operations, AJP-3.10, November 2009 [Online]. Available: https://info.publicintelligence.net/NATO-IO.pdf [Accessed: 22nd September 2018].

[404] A case in point are the two books written, respectively in 2010 and 2019, by Richard A. Clarke and Robert K. Knake. In the first book the authors claimed that 'cyber war' was imminent and in the second book they claimed that cyber threats had become part of the normal order of things. (Clarke, R. A. and Knake, R. K. Cyber War: The Next Threat to National Security and What to Do About It. New York: Harper Collins, 2010; Clarke, Richard A. and Knake, Robert K. The Fifth Domain. Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. New York: Penguin Press, 2019).

[405] Internet Society 1997; Schmitt 2017.

borders of the Internet—not the entirety of cyberspace. The Internet is not a commons.[406] The physical infrastructure of the Internet is always operated by someone and networks cannot be separated from the geographical territory in or through which they operate.[407] In fact, fibre cables, servers, routers etc. are owned and operated primarily by private, commercial, profit-seeking actors.[408] Additionally, the Internet is not a finite resource—bandwidth can always be increased[409]—and openness is in reality limited because states have shown the ability to pressure Internet Service Providers (ISPs) to shut down connections.[410]

On a physical level or layer[411], cyberspace consists of computers, servers, wires and optic fibre cables, satellite-communications or radio relay links and routers, switches and other equipment, i.e. mechanical, electrical, functional and procedural means of transferring bits (0s and 1s) as electrical signals or light.[412] On a logical level, cyberspace consists of intranets, extranets, internets and the Internet and protocols and applications running them and in them. Intranets are private networks, while extranets are networks which can be connected to the Internet in a limited manner and internets are multiple networks connected using the same protocols.[413] In all of these 'nets' the de facto[414] standard protocol for internetworking is the Transmission Control Protocol/Internet Protocol (TCP/IP). It is used to transfer packets of data ('packet-switching') between different networks to their destination in the right order and without errors.[415] Every host, i.e. computer, requires an IP address to take part in this network and networks are connected by routers, which are responsible for transmitting packets between networks.[416] These connect to other routers and advertise the addresses of the networks (hosts) they are connected to and keep registers of known addresses received from other routers.[417] It is important to note that the ARPANET and later TCP/IP (and many other protocols) were not designed for security but with accessi-

[406] Raymond 2015, 61-62; Nye 2010, 15.

[407] Cf. Starosielski, Nicole. The Undersea Network. Durham and London: Duke University Press, 2015; Dodd, Annabel Z. The Essential Guide to Telecommunications (5th ed.) Upper Saddle River, NJ: Prentice Hall, 2012.

[408] Pijenberg Muller, Lilly. How to govern cyber security? The limits of the multi-stakeholder approach and the need to rethink public-private cooperation. In Friis, Karsten & Ringsmose 2016, 116-129.

[409] Raymond 2015.

[410] For the state's ability to shut down the Internet cf. Vargas-Leon 2016, 167-188.

[411] Layer as a concept points to Open System Interconnections Reference Model (International Organization for Standardization. Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model. ISO/IEC 7498-1:1994. 15 June 1996 [Online] Available: http://standards.iso.org/ittf/ PubliclyAvailableStandards/index.html [Accessed: 7th August 2018].) Level is a more abstract concept and is connected to e.g. Martin Libicki's model of Cyberspace (Libicki 2016).

[412] Perlman, Radia. Interconnections, Second Edition: Bridges, Routers, Switches, and Internetworking Protocols. Boston: Addison-Wesley, 2012.

[413] Fall, Kevin R. and Stevens, Richard W. TCP/IP Illustrated, Volume 1: The Protocols (2nd ed.) Upper Saddle River NJ: Addison-Wesley, 2012, 19-20.

[414] Although ARPANET used TCP/IP it was not at all determined that this protocol would win the competition for the leading network layer protocol (Perlman 2012).

[415] There are also several other important protocols related to internetworking which have their own functions and weaknesses (Fall & Stevens 2012).

[416] Fall & Stevens 2012, 234-235; Perlman 2012, 408-423; Oki, Eiji, Rojas-Cessa, Roberto, Tatipamula, Mallikarjun and Christian Vogt. Advanced Internet Protocols, Services, and Applications. Hoboken, New Jersey: John Wiley & Sons, 2012, 13.

[417] Fall & Stevens 2012, 34-40, 48-50.

bility, reliability and connectivity in mind. Therefore, malicious actors can easily obfuscate their identity, manipulate and block data packets, access systems without authorization, launch Denial-of-Service (DoS) attacks etc.[418]

The Internet as a one type of network has its own architecture. The physical level consists of hundreds of fibre optic cables running under seas and oceans which transport the main portion of global data traffic.[419] These are owned by private cable companies or groups of companies.[420] These magisterial lines connect to smaller regional networks managed by service providers which use mainly land-built fibre cables and radio link relays to create their own backbone networks.[421] These Internet service providers (ISPs) are private and state owned companies who own and control almost all of the physical infrastructure of the Internet. ISPs run their own networks which provide connectivity to end users, companies, state institutions and private citizens. These networks may consist of edge routers, core routers, connections between them, data centres and different types of operations centres and client networks. They route their traffic based on protocols such as Multiprotocol Label Switching (MPLS).[422] Smaller ISPs rent capacity from larger ones and run their services virtually over the underlying infrastructure.[423] Internet Exchange Points (IXPs) are physical points where networks run by the largest ISPs physically connect. These are run by non-profit organizations, for-profit companies and government agencies.[424] Routing between large networks on the Internet is based on the Border Gateway Protocol (BGP) which is based on Autonomous System (AS) addresses. The ISPs use BGP to create connections between and through their networks. This is a system based on agreements, usually commercial. The BGP protocol advertises IP subnets found under it or through it so that the rest of the Internet can know where to send traffic reliably and efficiently.[425] It is possible to hijack these advertisements and manipulate the traffic flow of the Internet for example to spy or temporarily deny services.[426]

In addition to IP addresses and AS numbers, the Internet relies on the Domain Name System (DNS). The DNS protocol was developed to convert domain names to IP addresses in a process known as name resolution because human users could not be expected to memorize IP addresses. Domain names are organized as a tree. Top-level domains (.com) include generic TLDs (gTLDs), country-code TLDs (ccTLDs) (.su,

[418] Fall & Stevens 2012, 34-40, 25-26. Efforts to fix these deficiencies have included different forms of encryption, certification and authentication such as DNSSEC, TLS, IPsec and WPA (Fall & Stevens 2012).

[419] Submarine Cable Map 2018 [Online]. Available: https://www.submarinecablemap.com/#/ [Accessed: 7th August 2018].

[420] Oki et al. 2012, 33-35.

[421] Lee, Timothy B. 40 maps that explain the Internet 2 June 2014 [Online] Available: https://www.vox.com/a/internet-maps [Accessed: 7th June 2018]; Tanenbaum, Andrew S. and Wetherall, David J. Computer Networks (5th ed.) Boston: Prentice Hall, 2011.

[422] Dodd 2012.

[423] Network operators can be categorized as Tier 1, Tier 2 and Tier 3 classifications. Tier 1 is based on mutual peering (mutual exchange of traffic), Tier 2 refers to limited mutual peering and purchases and Tier 3 to reselling transit capacity (DeNardis 2014, 109-111).

[424] Internet Society. IXPs [Online] Available: https://www.internetsociety.org/issues/ixps/ [Accessed: 7th August 2018]; Oki et al, 2012.

[425] [RFC 4271] Y. Rekhter, T. Li, S. Hares "A Border Gateway Protocol 4 (BGP-4)" RFC 4271, January 2006.

[426] Winter, Martin. Monitoring BGP Anomalies on the Internet. 27 July 2018. RIPE NCC. [Online]. Available: https://labs.ripe.net/Members/martin_winter/monitoring-bgp-anomalies-on-the-internet [Accessed: 7th August 2018]; Demchak, Chris C. and Shavitt, Yuval. China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking. Military Cyber Affairs: Vol. 3, No. 1 (2018), Article 7.

.ru) and internationalized country-code TLDs (IDN ccTLDs) (.рф) and these are further divided into two levels of subdomains (example.com and www.example.com). Registry operators maintain domain name databases (registry) and provide zone files, which map IP addresses to domain names for domain name servers. ccTLD servers are delegated to national registry operators. DNS registrars are service providers who have a mandate to sell domain names to customers. On the technical side, name servers can provide a domain name to IP address resolutions. Thirteen root servers and their multiple backups maintain the root zone files which include TLD name server addresses and thus enable the Internet's global connectivity. The TLD servers maintain their own zone files as do subdomain servers. These servers usually have multiple logically and physically dispersed backups. In principle, name servers answer to the host name it requests. However, in practise, names are usually resolved through caches maintained by recursive servers.[427] The DNS is important for the functioning of the modern information society and state. If the names and addresses of a state's country code domain name servers were removed from the global root and other zone files, or access to the TLD servers were blocked, that country's Internet traffic would be greatly affected, perhaps even halted.[428] It is also possible to hijack and eavesdrop on DNS traffic.[429]

The Internet would not work without IP addresses, DNS root files and servers and AS numbers.[430] They are distributed and managed by a non-profit multi-stakeholder organization called Internet Corporation for Assigned Names and Numbers (ICANN) which functions as the Internet Assigned Numbers Authority (IANA). ICANN uses Regional Internet registries (RIRs) to distribute IP and AS addresses to customers.[431] This is a critical function because assigning duplicate addresses to networks and hosts would break the Internet routing. RIRs also maintain the Internet Routing Registry (IRR) which provides information on BGP routing policies of ISPs for common use and routing planning.[432] ICANN/IANA approves changes to the root zone file and has a contract with VeriSign which is responsible for distributing the file to the operators of root name servers.[433] Despite their functions and mandates ICANN and its associates do not control the Internet. Contrary claims have been

[427] Fall & Stevens 2012; Cloudflare. What is DNS? How DNS works [Online] Available: https://www.cloudflare.com/learning/dns/what-is-dns/ [Accessed: 7th August 2018]; IANA [Online]. Available: https://www.iana.org/about [Accessed: 7th August 2018]; Merrill, Kenneth. Domains of Control: Governance of and by the Domain Name System. In Musiani, Cogburn, DeNardis & Levinson 2016, 89-106.

[428] For example, cf. Sozeri, Efe Kem. Turkish Internet hit with massive DDoS attack, The Daily Dot, 17th December 2015 [Online] Available: https://www.dailydot.com/layer8/turkey-ddos-attack-tk-universities/ [Accessed: 29th December 2019].

[429] Greenberg Andy. Cyberspies Hijacked the Internet Domains of Entire Countries. A mysterious new group called Sea Turtle targeted 40 organizations in a DNS hijacking spree, WIRED, 17th April 2019 [Online] Available: https://www.wired.com/story/sea-turtle-dns-hijacking/ [Accessed: 29th December 2019].

[430] There is a finite number of each. AS numbers are not a problem but original IP addresses have already run out. Currently, a global transition from the IPv4 to IPv6 protocol is ongoing which should provide enough addresses for the Internet's future needs.

[431] RIPE NCC. Regional Internet Registry [Online] Available: https://www.ripe.net/about-us/what-we-do/regional-internet-registry [Accessed: 7th August 2018].

[432] RIPE NCC. The RIPE Routing Registry [Online]. Available: https://www.ripe.net/manage-ips-and-asns/db/the-ripe-routing-registry [Accessed: 7th August 2018].

[433] Fall & Stevens 2012; IANA 2018; Merrill2016.

based on the fact that for historical reasons the United States' National Telecommunications and Information Administration (NTIA) has supervised ICANNs IANA functions up until 2016.[434]

ICANN is not the only non-governmental multi-stakeholder organization with an influence on Internet governance.[435] The Internet Engineering Task Force (IETF), Internet Engineering Steering Group (IESG) and Internet Architecture Board (IAB) are responsible for setting technical standards for the Internet through meetings, working groups and Request for Comments (RFCs). The Internet Society (ISOC) functions as an umbrella organization connecting academics, governmental representatives and the private sector to govern and develop the Internet.[436] In effect, the technical standards regulating the development of the Internet are not controlled by nation-states, although there have been efforts to increase states' control through the United Nation's International Telecommunications Union (ITU).[437] The tug-of-war between the principles of state sovereignty and the multi-stakeholder model in the context of information (cyber) security has been visible in the work of the United Nations Group of Governmental Experts on Information Security (UN GGE) from 2004–2019. The UN GGE has tried to find some common global understanding on the questions of information security, wars and weapons but has so far failed to produce binding agreements.[438] Basically, the United States and some European countries and Russia and China and their allies have promoted conflicting views, and this has paralyzed international cyber security norm building on the UN level.[439] This does not mean that cyberspace is unregulated on the international level. There are already a great number of bi- and multilateral accords which regulate cyberspace[440] and create some level of transparency, confidence, and trust—as do the multitudes of commercial agreements.[441] The point is that cyberspace is not an anarchic or uncontrollably malleable

[434] ICANN. Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends, 1 October 2016 [Online]. Available: https://www.icann.org/news/announcement-2016-10-01-en [Accessed: 8th August 2018]; The United States Department of Commerce, 6 January 2017 [Online]. Available: https://www.icann.org/en/system/files/correspondence/strickling-to-crocker-06jan17-en.pdf [Accessed: 8th August 2018].

[435] "The primary task of Internet governance involves the design and administration of the technologies necessary to keep the Internet operational and the enactment of substantive policy around these technologies." (DeNardis 2014, 6).

[436] Denardis 2014, 69-70.

[437] Kavanagh 2017, 54-56.

[438] Osula, Anna-Maria and Rõigas, Henry (eds.) International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn: CCDCOE, 2016; Tikk, Eneken and Kerttunen, Mika. The Alleged Demise of the UN GGE: An Autopsy and Eulogy. New York: Cyber Policy Institute, 2017 [Online] Available: http://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf [Accessed: 7th August 2018]; Tikk, Eneken. International Cyber Norms Dialogue as an Exercise of Normative Power. Georgetown Journal of International Affairs. 17 (2016), 47-59. 10.1353/gia.2016.0036. [upcoming] [Online] Available: (http://ict4peace.org/wp-content/uploads/2017/02/Tikk-Normative-Power.pdf) [Accessed: 17 December 2017].

[439] Tikk & Kerttunen 2017; Schmitt, Michael and Vihul, Liis. International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms, 30 June 2017 [Online]. Available:
https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ [Accessed: 8th August 2018].

[440] Carnegie Endowment for International Peace. Cyber Norms Index [Online]. Available: http://carnegieendowment.org/publications/interactive/cybernorms. [Accessed: 8th August 2018].

[441] For a deeper discussion cf. Osula & Rõigas 2016.

space and that there are political, economic and judicial constraints to the actions of states and non-state actors—and these constraints are sources and objects of power.[442]

There are still other elements and functions that are important for the operation of the Internet and cyberspace. Encryption and authentication have become critical resources for the Internet and indeed for the whole of cyberspace.[443] Ben Buchanan has even claimed that encryption has affected state sovereignty as the use of public key encryption restricts states' access to information on their own territory.[444] As was mentioned above, the Internet protocol suite was and is not inherently secure. From a nation state's point of view this means that strong encryption is a national security interest, as is the capability to break potential or real opponent's encryption.[445] New and more powerful supercomputers and quantum computing are challenging current encryption solutions, although this 'arms race' is nothing new in computer-based cryptography.[446] Additionally, the importance of authentication, which is the cornerstone of public-key encryption, means that Certificate Authorities[447] are a point of vulnerability. If someone could fake certificates distributed by these authorities, the confidentiality of information on the Internet would be in danger.[448]

Despite of what some of the above-mentioned definitions claim, cyberspace is not a collection of independent, equal and similar nodes changing information. Content delivery networks have appeared inside the Internet to balance the ever increasing traffic load.[449] Cloud computing has led to the establishment of big data centres that offer computing and storage capacity for the public and private sector.[450] Public services and even government institutions have located critical data in commercial datacentres outside states' territorial borders and jurisdictions.[451] Disconnection from foreign data centres could lead to major disruptions, even the loss of life. Additionally, data located in some countries is, in principle, subject to that country's laws and is

[442] Cf. Buchan, Russell, Tsagourias, Nikolaos K. (eds.) Research Handbook on International Law and Cyberspace. Cheltenham: Edward Elgar Publishing, 2015; Stevens, Tim. A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. Contemporary Security Policy, Vol. 33, No. 1 (2012), 148-170.

[443] This is a point made by Thomas Rid. According to him, public-key encryption changed the nature of cyberspace and started the still ongoing 'arms race' between encryption and decryption (Rid 2016).

[444] Buchanan, Ben. Cryptography and Sovereignty, Survival, Vol. 58, No. 5 (2016), 95-122.

[445] Sanger, David E. The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. Melbourne: Scribe, 2018; Rid, Thomas. Cyber War Will Not Take Place. Oxford: Oxford University Press, 2017.

[446] Castro, Daniel and McQuinn, Alan. Unlocking Encryption: Information Security and the Rule of Law. ITIF, March 2016 [Online]. Available: http://www2.itif.org/2016-unlocking-encryption.pdf [Accessed: 11th August 2018].

[447] GlobalSign. Certificate Authorities & Trust Hierarchies [Online]. Available: https://www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies/ [Accessed: 22nd June 2019].

[448] Kuhn, Richard D., Hu, Vincent C., Polk, Timothy W., Chang, Shu-Jen. Introduction to Public Key Technology and the Federal PKI Infrastructure. NIST, 26 February 2001 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-32.pdf [Accessed: 8th August 2018].

[449] A content delivery network (CDN) is a network of geographically dispersed servers that enables faster web performance by locating copies of web content closer to end users or facilitating the delivery of dynamic content (e.g., live video feeds). (IBM. Content Delivery Networks: A Complete Guide, 3 June 2019 [Online]. Available: https://www.ibm.com/cloud/learn/content-delivery-networks [Accessed: 17th July 2019]).

[450] Data Center Map [Online] Available: https://www.datacentermap.com/ [Accessed: 8th August 2018]; Dodd, 2012, 25-33.

[451] Scrutton, Alistair and Mardiste, David. With an eye on Russia, Estonia seeks security in computing cloud. Reuters, 4 December 2015 [Online]. Available: https://www.reuters.com/article/us-estonia-cybersecurity/with-an-eye-on-russia-estonia-seeks-security-in-computing-cloud-idUSKBN0TN1BT20151204 [Accessed: 8th August 2018].

vulnerable to espionage at its destination and during traffic.[452] The geography, location of physical infrastructure, state borders and jurisdictions all affect the 'borderless' cyberspace.

Satellites have become part of cyberspace and at the same time are vulnerable to its threats. Although global data communications are not dependent on satellites some remote areas are. Moreover, satellites provide TV transmissions, navigation and time-signal services, and most importantly communications needed by the command and control of modern armies, including nuclear early-warning systems.[453] Satellites are vulnerable to attacks using software and malicious code through their terrestrial control links, and to electromagnetic interference and kinetic attacks. The number of satellites is increasing as micro-satellites are being deployed in Low-Earth Orbit (LEO). There are plans to create global Internet services based on hundreds or thousands of small satellites which would provide Internet services unhindered by terrestrial or governmental borders.[454] These satellites would in principle create a world-wide network connecting millions of IoT devices.[455] This service will aggravate the difficulties some states are facing in controlling the Internet-access of their citizens. Moreover, after the development of mobile broadband, plain old telephone networks (POTS) have been transformed into data networks. Digitalized telecommunications services have become indistinguishable from cyberspace—and also its threat landscape.[456] Wi-Fi and other short-range connections such as Bluetooth and Low Power Wide Area Networks (LPWAN), as well as 5G mobile, fixed broadband connections and different types of satellites will create a truly global multi-layered and multi-access data network in the near future. These kinds of connections make cyberspace truly ubiquitous and challenge the territorial borders of nation states.

Cyberspace, and in fact, the Internet now reaches inside factories and power plants, to electric networks, transportation and sewage systems. There is no cyberspace without electricity and as automatization proceeds soon there might not be electricity without cyberspace. Malfunctions or intentional attacks against a program running some logistical system might lead to the disruption of air or sea traffic and shortages of critical imports. These interdependencies and collateral effects make cyberspace an inherent part of information society, its security and defence.[457]

[452] Wolff, Josephine. Borders in the Cloud. Countries are increasingly putting limits on how data travels. Slate, 20 November 2017 [Online]. Available: http://www.slate.com/articles/technology/future_tense/2017/11/countries_are_increasingly_imposing_borders_on_the_cloud.html?via=gdpr-consent [Accessed: 8th August 2018].

[453] Bardin, Jeffrey. Satellite Cyber Attack Search and Destroy. In Vacca 2014, 309-323.

[454] Scoles, Sarah. Maybe Nobody Wants Your Space Internet. Wired, 15 March 2018 [Online] Available: https://www.wired.com/story/maybe-nobody-wants-your-space-internet/ [Accessed: 8th August 2018].

[455] Qu, Zhicheng, Zhang, Genxin, Cao, Haotong and Xie, Jidong. LEO Satellite Constellation for Internet of Things. IEEE Access, Vol. 5 (2017), 18391-18401.

[456] Dodd 2014; ENISA. Signalling Security in Telecom SS7/Diameter/5G EU level assessment of the current situation, March 2018 [Online] Available: https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g [Accessed: 10th August 2018].

[457] Edwards, Matthew (ed.) Critical Infrastructure Protection. NATO Science for Peace and Security Series. Amsterdam: IOS Press, 2014; Zhang, Nan, Krishna, Kant and Sajal K. Handbook on Securing Cyber-Physical Critical Infrastructure. Amsterdam: Elsevier, 2012.

Lastly, as big data analytics, neural network modelling, and machine learning advance, cyberspace might be populated by some kinds of self-modifying Artificial Intelligences (AIs).[458] Currently, the usefulness and effectiveness of AIs is an open question but their development is nevertheless taken seriously by state and private research institutions.[459] On a more mundane level the technical governance of cyberspace is being automatized and virtualized through semi-intelligent and self-learning programs which enable the control and configuration of networks from remote locations independently of hardware or software solutions. Security is increasingly being handled by centralized systems that can inspect traffic and react to anomalies semi-autonomously.[460] Arguably, as states are increasingly interested in controlling cyberspace, that space is being increasingly controlled by machines.

What makes all the above-mentioned systems and protocols critical resources for cyberspace is that if someone would disturb their governance, or logically or physically damage them or hinder their action, the Internet could temporarily stop working in a certain, perhaps targeted area. Confidential and critical information could be lost. Decision-making of governments could be impaired. Military, including nuclear weapons command systems, could be affected. Great economic losses could be suffered. Societal disorder could ensue, and people could die.[461] Local and regional services might be available, but international banking services such as SWIFT[462] and any foreign cloud-based services might be affected. Information could be secretly compromised or corrupted. Conversely, the inability of states and their security institutions to control connections to the global Internet, encrypted traffic inside their borders, and services located outside their borders can create political, social and economic problems—and weaken military defence.[463] It is thus understandable that states might seek guarantees against these vulnerabilities especially if their political system is authoritarian or if they fear outside interference based on information flowing on the Internet.

Another common theme that emerges from the issues discussed above is the 'newness' and constant change of cyberspace. The technology underneath cyberspace is rapidly evolving, new protocols are emerging, new hardware and software solutions are being produced.[464] Sometimes novel threats appear that seem to challenge the

[458] AI refers, for example, to an artificial entity that acts in response to its environment and performs 'well' based on its purpose and rationality i.e. doing the right thing based on knowledge and logical reasoning. (Russell, Stuart and Norvig, Peter. Artificial intelligence—A Modern Approach. New Jersey: Prentice Hall, 2014).

[459] Scharre, Paul. Army of None. Autonomous Weapons and the Future War. New York & London: W. W. Norton & Company, 2018.

[460] Software Define Network (SDN) technology allows hardware and software independent controlling of networks ([RFC 7426] E. Haleplidis, Ed. Software-Defined Networking (SDN): Layers and Architecture Terminology RFC 7426, January 2015). Semi-automated Security Incident and Event Management systems like EISENSTEIN, GosSOPKA and HAVARO could be automated to a great degree. Cf. The United States Department of Homeland Security. EISENSTEIN. [Online] Available: https://www.dhs.gov/einstein [Accessed: 8th August 2018]; Viestintävirasto. HAVARO havainnoi ja varoittaa tietoturvaloukkauksista. 24th May 2016 [Online] Available: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/05/ ttn201605-241520.html [Accessed: 8th August 2018]. For GOSSOPKA see Chapter 6.

[461] On threat images cf. Rattray 2001; Kramer, Starr & Wentz 2009; Clarke & Knake 2010.

[462] SWIFT. Messaging and Standards [Online] Available: https://www.swift.com/about-us/discover-swift/messaging-standards [Accessed: 7th August 2018].

[463] DeNardis 2014; Musiani et al. 2016; Mattioli 2014.

[464] Cerf, Vinton G. On the Evolution of Internet Technologies. Proceedings of the IEEE, Vol. 92, No. 9, September 2004 [Online]. Available: http://www.ismlab.usf.edu/dcom/Ch5_Cerf_IEEE_2004_Evolution.pdf [Accessed: 9th August 2018]; Naughton, John. The evolution of the Internet: from military experiment to

whole infrastructure of Internet.[465] According to the World Economic Forum, cyber-attacks are one of the main risks facing the world today.[466] This means that state defence and security elites are continuously forced to find new solutions to the challenges emerging from cyberspace.[467] Related to the constant change is the problem of attribution, i.e. the possibility to identify the source of an attack.[468] The constant evolution of cyberspace makes it hard to devise attribution techniques. This has direct consequences on strategic issues such as deterrence, early warning and the possibility for retaliation.[469]

Behind the idea of freedom and openness of the Internet has been the governance model of multi-stakeholderism, i.e. 'an ecosystem' that includes state and non-state actors.[470] This model is being increasingly challenged by states which claim that territorial state sovereignty, with its jurisdiction and borders, should be reflected into cyberspace.[471] This process has been called 'fragmentation', 'balkanization' and 'Cyber-Westphalia'.[472] A World Economic Forum report divides this phenomena into technical, governmental and commercial fragmentation.[473] Technical fragmentation challenges the universal connectivity of the Internet by affecting its technical standards and processes. Governmental fragmentation arises from the intentional policy to build 'national Internets' by blocking and filtering traffic. Commercial fragmentation is based on the manipulation of digital markets by companies and is manifested in policies such as network neutrality and the geo-blocking of content.[474] Proponents of this 'fragmentation' see it as the 'normalization' of the state role and interstate relationships in cyberspace or as economically logical policy to protect nascent digital economies, for example.[475]

General Purpose Technology, Journal of Cyber Policy, Vol. 1, No. 1, 2016, 5-28.

[465] As the ENISA Threat Landscape Report 2017 claims: "Cyber-war is entering dynamically into cyberspace creating increased concerns to critical infrastructure operators, especially in areas that suffer some sort of cyber crises." (ENISA. ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends Version 1.0. January 2018 [Online] Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017 [Accessed: 9th August 2018].

[466] World Economic Forum. The Global Risks Report 2018 – 13th Edition. Geneva: WEF.

[467] Cf. Hayden, Michael V. The Future of Things "Cyber. Strategic Studies Quarterly, Vol. 5, No. 1 (Spring 2011), 3-7. For a summary of the development of cyber threats cf. Center for Strategic and International Studies. Significant Cyber Incidents Since 2006 [Online]. Available: https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity [Accessed: 9th August 2018]; Council on Foreign Relations. Cyber Operations Tracker, September 2018 [Online]. Available: https://www.cfr.org/ interactive/cyber-operations [Accessed: 19th September 2018].

[468] Libicki 2016, 238-250; Rid 2017.

[469] Liff, Adam. Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. Journal of Strategic Studies, Vol. 35, No. 3 (2012) 401-428; Nye, Joseph. Deterrence and Dissuasion in Cyberspace. International Security, Vol. 41, No. 3 (2016/2017), 44-71; Harknett, Richard J. and Nye, Joseph S. Jr. Correspondence – Is Deterrence Possible in Cyberspace. International Security, Vol. 42, No. 2 (2017), 196-199.

[470] Levinson, Nanette S. and Marzouki, Meryem. International Organizations and Global Internet Governance: Interorganizational Architecture. In Musiani, Cogburn, DeNardis 2016, 47-71.

[471] Tuukkanen, Topi. Sovereignty in the Cyber Domain. In Rantapelkonen & Salminen 2013, 37-45; Mueller 2017; Musiani et al. 2016.

[472] Demchak, Chris and Dombrowski, Peter. Cyber Westphalia. Asserting State Prerogatives in Cyberspace. Georgetown Journal of International Affairs, Volume International Engagement on Cyber III, 2013, 29-38; DeNardis 2014; Mueller 2017.

[473] Drake, Cerf & Kleinwächter 2016.

[474] Ibid., 6.

[475] Demchak & Dombrowski 2011 & 2013; Inkster, N. China's Cyber Power. New York: Routledge, 2016; Siboni, Gabi and Kronenfeld, Sami. Iran and Cyberspace Warfare. Military and Strategic Affairs, Vol. 4, No. 3, (December 2012), 77-99; Aropa 2016.

There are obstacles in this process of nationalization of the Internet. The private sector owns the infrastructure and services of the Internet and also the critical infrastructure connected to it. Protocols running the data traffic in networks do not inherently support concepts such as 'national borders' or 'citizenship'. Encryption and proxy-services are available to those wanting to circumvent state control. There could be major economic expenses in creating 'national Internets' and in engaging in 'digital protectionism', and, according to the current understanding concerning cyber-attacks, computer networks will always be vulnerable to attacks either from outside or inside.[476] Therefore, based on all the technological, governance and political issues examined above, I argue that cyberspace is an environment which can be shaped by state actions influenced by strategic cultural ideas, but that it is not absolutely malleable and efforts to build closed national 'Internets' will be severely challenged.

3.2.3 Definition of cyberspace

Based on the above analysis and because this thesis is focused on the shaping of cyberspace by state actors who carry particular cultural ideas about strategic issues, a modified version of the definition by Daniel T. Khuel is used to describe cyberspace: *"…cyberspace is a [man made and governed] global domain within the information environment whose distinct and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies.*"[477] 'Man made and governed' is an addition to Khuel's definition. This definition highlights cyberspace's nature as a collection of networks, its physical and logical levels and its malleable character. It includes a distinction between physical, syntactic and semantic layers that have different rules, and which are interdependent but not necessarily controlled by each other. Cyberspace can be shaped by intentional actors by controlling its infrastructure, technical design and standards, and by laws, regulations and institutions. Through electronics and the electromagnetic spectrum, the definition connects cyberspace to the physical world, territoriality and kinetic effects. Information gives substance, resources, and effects to cyberspace and makes it possible to describe it as a domain, and a sphere of human activity[478]. The processing of information gives cyberspace meaning beyond its borders. The manipulation of information affects human activity. Khuel's definition combines structure (medium), substance (information) and processes (creation etc.) and emphasizes technical aspects. The additions emphasise the aspect of human control.

[476] Choucri & Clark 2013; Cerf 2004; Naughton 2016; Buchanan 2016; Aaronson, Susan A. What Are We Talking About When We Discuss Digital Protectionism? Institute for International Economic Policy, 14 July 2017 [Online] Available: https://www2.gwu.edu/~iiep/assets/docs/papers/2017WP/AaronsonIIEPWP 2017-9.pdf [Accessed: 9th August 2018]; Sanger 2018.

[477] Kuehl 2009, 24-42, 28. A more 'objective' definition would be "an electronic medium through which information is created, transmitted, received, stored, processed and deleted" taken from East-West Institute's Critical terminology foundations report. From a theoretical and research problem point of view East-West institutions definition is too narrow to be used in this thesis. (Godwin et al. 2014, 17).

[478] The term 'sphere' as a concept describing human activity was popularized by Jürgen Habermas. It was originally meant to describe the space where the public opinion is formed. (Habermas, J., Lennox, S. and Lennox, F. The Public Sphere: An Encyclopedia Article (1964). New German Critique, No. 3 (Autumn, 1974), 49-55).

Based on Khuel's definition and previous discussion a short summary of the basic characteristics of cyberspace can be deduced. These are: its artificial nature, physical base, inherent rules, interconnectivity, mutability, replication, ease of access, multiplicity of actors, difficulty of attribution, diffusion of power, non-significance of distance, and machine speed.[479] This means that cyberspace is clearly different from other physical domains, i.e. land, sea, air and the outer space. Its nature and properties can be intentionally shaped by states which may be affected by strategic cultural ideas, and by private companies and institutions if they have sufficient resources. However, the shaping may be contested by others and even by the functional logic of the space itself. This means that components of cyberspace can be damaged, but it is difficult to permanently destroy any part of it—backups can be restored—and even kinetic effects can be negated by rerouting traffic and by replicating services to other locations. This does not mean that cyberspace is invulnerable—it is based on physical infrastructure, electricity and human-made software which may contain errors and bugs. Cyberspace also differs from other domains because it is not continuous—it is a collection of internetworked or independent, air gapped, networks—the Internet being the most important. There are physical and logical control or pressure points in the Internet and other networks that can be used to control traffic and connections. Borders in cyberspace are perhaps even more real than in the physical realm where no human action can change the laws of nature.

Based on the above discussion I argue that cyberspace is indeed a new environment and is in fact a constantly changing environment which gives rise to unknown and poorly understood threats. This environment requires elites to fit new ideas to old ones to understand their position and to produce strategies to create power. It also enables the creation of closed national networks, although this might be difficult to achieve.

3.3 Cyber power

Power is a contested concept.[480] In IR theory there are three or four (depending on the view) different concepts of power, the so called 'Faces of power'.[481] The first one is based on Robert Dahl's formulation of "A getting B to do something B would otherwise not do."[482] This is basically the direct power over resources or effects approach and sees power and its results as measurable. The second one is based on Bacrach's and Barantz's critique of Dahl and states that "…power works more indirectly through both actors being positioned in an institutional setting and the ability of A to influence this setting 'against' B."[483] This approach is interested in agenda-setting, and the ability of A to exclude some agendas from the political process altogether. A structuralist version of this 'face' is an approach where the positions of A and B order their power relationship without direct intentionality from the part of

[479] These are quite close to Fred Schreier's list Cf. Schreier, Fred. On Cyberwarfare. DCAF Horizon 2015 Working Paper No. 7 [Online] Available: https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf [Accessed: 10th August 2018].

[480] Nye 2011a, 5.

[481] Nye 2011a, 11-14; Barnett & Duvall 2005, 42. Barnett and Duvall have categorized these as compulsory, institutional, structural, and productive.

[482] Quoted in Berenskoetter, Felix. Thinking about power. In Berenskoetter, Felix and Williams, M. J. Power in World Politics. London: Routledge, 2007, 1-22, 4.

[483] Ibid., 8.

A.[484] The third face is based on Steven Lukes who was interested in how A can manipulate B's inherent interests, basically changing B's preferences.[485] Finally, the fourth 'face' is based on poststructuralism and especially on the writings of Michel Foucault. Here power is seen as productive power, shaping the identities and interests of A and B.[486] It should be noted that all the different 'Faces of power' are based on different theoretical premises and are not necessarily commensurable.[487]

There are unresolved theoretical problems behind these seemingly simple presentations of the 'faces' of power. First, the causality of power is still being debated —do we identify power with change or continuity? Second, how do we make claims about unintentional and indirect effects of power? Third, what is the relationship between causal and constitutive power?[488] There is also the question of power as an objective material capacity and measurable quantity—either segmented and issue-specific or an aggregated 'lumped' indicator—versus the understanding of power as a relational and contextual phenomenon.[489] How are we supposed to measure power and how do we measure potential power? Measurement is linked to the question of the fungibility of power, i.e. the convertibility of power resources, which has been advocated, among others, by Robert Art and criticized by Stephen Baldwin and Stefano Guzzini. In short, the theoretical dispute is about whether one kind of power can be changed to another kind through some spill-over effects or linkage.[490] Art sees state power as a composite of wealth, political skill and military power which can be given net worth. However, for Baldwin power is multidimensional.[491] The dimensions are its scope (aspect of behaviour), domain (size of the target of power), weight (probability of influence), costs (cost of influence) and means (military, economic etc.)[492] To these dimensions could be added societal norms because power must have meaning, at least to its target, and norms influence the way power is used.[493] Any meaningful analysis of power must empirically define these dimensions that is, put power in a relationship and a context.

Consequently, Joseph Nye has argued that "…there is no standard value that can summarize all relationships and contexts to produce an agreed overall power total."[494] Nye himself has formulated the concept of 'soft power' which is "the ability to affect others through the co-optive means of framing the agenda, persuading, and eliciting

[484] Guzzini, Stefano. The Limits of Neorealist Power Analysis. International Organization, Vol. 47, No. 3 (1993), 443-478, 450.

[485] Berenskoetter 2007, 10-11; Lukes, Steven. Power: A Radical View (2nd ed.) Basingstoke: Palgrave Macmillan, 2005.

[486] Digiser, Peter. Fourth Face of Power. The Journal of Politics, Vol. 54, No. 4 (1992), 977-1007, 982-984.

[487] Barnett & Duvall 2005.

[488] Berenskoetter 2007, 13–14.

[489] Guzzini, Stefano. Power, Realism and Constructivism. London and New York: Routledge, 2013, 48-51.

[490] Cf. Baldwin, David A. Paradoxes of Power. New York: Basil Blackwell, 1989; Krasner, Stephen. Structural Conflict. Berkeley: University of California Press, 1985; Art, Robert J. and Greenhill, Kelly M. The Use of Force: Military Power and International Politics (8th ed). Lanham: Rowman & Littlefield Publishers inc., 2015; Guzzini 2013.

[491] Art, Robert J. Force and fungibility reconsidered, Security Studies, Vol. 8, No. 4 (1999), 183-189.

[492] Baldwin 2013, 275.

[493] For the meaning of power cf. Barkin 2010; Guzzini 2013, 4-5. John A. Gentry has argued that, for example, casualty aversion, international norms and military culture affect the way military power is used. (Gentry, John A. Norms and Military Power: NATO's War Against Yugoslavia, Security Studies, Vol. 15, No. 2 (2006), 187-224, 189).

[494] Nye 2011a, 5.

positive attraction in order to obtain preferred outcomes."[495] Behind Nye's concept is the separation of power resources and power behaviour, which obtain their meaning and produce different outcomes depending on the context. According to Nye, different forms of power have different modalities, for example, military power can be used to physically destroy, back up threats in coercive diplomacy, promise protection and provide many forms of assistance.[496] This is an interesting notion because it gives different forms of power characteristics which are dependent on the environment it is used in. Like Baldwin's dimensions it is worthwhile to also consider cyber power instead of just power.

Theorists of cyber power have had to combine the characteristics of cyberspace with different theories of power.[497] One of the most holistic descriptions is Betz's and Stevens': "…the variety of powers that circulate in cyberspace and which shape the experiences of those who act in and through cyberspace."[498] This is a product of their attempt to combine all 'Faces of power' into one concept and what it gains in brevity it loses in parsimony. In practice, Betz and Stevens use Barnett and Duvall's categories of power to show that concepts of power formulated in the field of political science are compatible with cyber studies.[499] Joseph Nye describes cyber power as "…the ability to obtain preferred outcomes through use of the electronically interconnected information resources of the cyber domain. […] …[it] can be used to produce preferred outcomes within cyberspace or […] in other domains."[500] This is a subject-centric, intentional use of power, compatible with the first and second faces of power, and highlights the fungibility of cyber power, i.e. its convertibility and scope.[501] Somewhat similar is Khuel's version: "…the ability to use cyberspace to create advantages and influence events in all operational environments and across the instruments of power."[502] The value of Khuel's definition is that it highlights the possible synergistic effect of cyber power. These formulations seem to suggest that cyber power is compatible with universal definitions ('faces') of power but has its own resources and context which give it a distinct character. In his survey of cyber power concepts Schreier summarizes it as "the capability to control IT systems and networks in and through cyberspace", which is in a sense tautology but nevertheless points to the object of power through which outcomes and effects are produced.[503] Gregory Rattray has also emphasised that power comes from the control of specific parts of the cyber environment which some have called 'key terrain'.[504]

Besides the above presented more conceptual formulations, there have been attempts to define cyber power by its resources. Nye, for example, offers infrastructure, edu-

[495] Ibid., 20-21.

[496] Ibid., 9-10 & 41-42.

[497] See Sheldon (2013) and Schreier (2015) for comprehensive list of different definitions.

[498] Betz & Stevens 2011, 44.

[499] Barnett & Duvall 2005.

[500] Nye 2011a, 8.

[501] See Art, Robert J. American foreign policy and the fungibility of force. Security Studies, Vol. 5, No. 4 (1996), 7-42; Baldwin, D. A. Force, fungibility, and influence. Security Studies, Vol. 8, No. 4 (1999), 173-183.

[502] Kuehl 2009, 38.

[503] Schreier 2015, 14.

[504] Rattray 2009, 262-272; Kern, Sean and Gaines, Charles. Expanding Combat Power Through Military Cyber Power Theory. Joint Forces Quarterly, Vol. 79, No. 4 (Quartet 2015), 88-95.

cation, legal control, markets, budgets, institutions and reputation as the power resources of states.[505] Brandon Valeriano and Ryan C. Maness propose a resource-based concept of power by differentiating between capabilities of offence, that is weapons and training, and dependence, i.e. reliance on the Internet, and of defence, meaning resilience, adaptation and protection.[506] They later change their model to consist of just infrastructure, broadly understood as connectivity and knowledge capital.[507] Somewhat similar is the more policy oriented view presented by Chris Demchak who argues that institutions, national mentality, and offensive and defensive forces are resources of cyber power.[508]

Alexander Klimburg has offered coordinated government policy, international alliances and agreements, and cooperation with non-state actors as the three dimensions for national cyber power.[509] He advocates a 'whole of nation' policy-based view of cyber power. Somewhat similarly, Robert Bebber has argued that potential cyber power is "the available human and material resources within a strategic environment that can be utilized to generate effects in and through cyberspace." These resources are information culture, technology industry, information networks, political institutions, civil-government relations, global norms, foreign partnerships, mass and scale, and foreign relationships. The resources should produce skilled forces for effective cyber power if the state organizes, trains, and resources them properly.[510] Considering purely military cyber power Rebecca Slayton has proposed technology, skilled people and well-developed organizations as resources of power.[511]

It is not surprising that education and thus human knowledge, technology, regulation and organizations are defined as resources because of the dual physical – non-physical nature of cyberspace. The problem is, that these resources are more difficult to measure than purely physical capabilities, which have already in themselves been proven to be notoriously difficult to measure, at least in the military context.[512] Moreover, there is no shared understanding between the great powers on how to measure cyber power.[513] Because there has been no conflict categorized as cyber war, there is not even a shared understanding of the enabling or strategic role of cyber power, i.e. whether it has independent strategic effect or not.[514] This means that the effect of, or

[505] Nye 2011a, 133.

[506] Valeriano & Maness 2015, 25-28.

[507] Valeriano, Jensen & Maness 2018, 59-60.

[508] Demchak, Chris. Cybered Conflict, Cyber Power, and Security Resilience as Strategy. In Reveron 2012, 121-136. Demchak's definition is quite similar to classical definitions of naval power (Gray 1999a, 261-262).

[509] Klimburg defines these dimensions as: 'integrated government capability', 'integrated systems capability' and 'integrated national capability'. (Klimburg, Alexander. Mobilising Cyber Power, Survival, Vol. 53, No. 1 (2011), 41-60, 43, 56).

[510] Bebber, Robert. Cyber power and cyber effectiveness: An analytic framework, Comparative Strategy, Vol. 36, No. 5 (2017), 426-436.

[511] Slayton, R. What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. International Security, Vol. 41, No. 3 (2017), 72-109.

[512] Biddle, S. Military Power - Explaining Victory and Defeat in Modern Battle. Princeton: Princeton University Press, 2004; Biddle, Stephen. Military Power: A Reply, Journal of Strategic Studies, Vol. 28, No. 3 (2005), 453-469; Schmidt, B. C. Realist conceptions of power. In Berenskoetter & Williams 2007, 43-61, 47-48.

[513] Inkster, Nigel. Measuring Military Cyber Power, Survival, Vol. 59, No. 4 (2017), 27-34.

[514] Colin Gray: "Strategic effect is the impact of strategic performance upon the course of events." (Gray 1999a, 20). In other words, the effects of a military use of force have direct relationship to with policy goals or political consequences (Ibid., 296). According to Hew Strachan, an enabling effect means that power has only a tactical or operational effect. It does not directly achieve the objectives of war. (Strachan 2013, 191-192). The concept of enabling is sometimes used interchangeable with 'force multiplier' which means a particular use of force or

at least, military effectiveness of cyber power is disputed.[515] David Betz has, for example, criticised visions of cyber power that liken it to strategic air power, such as long-range bombers, because Douhetian visions of cyber power have no empirical basis.[516] Others have criticised discursive and technological comparisons between nuclear weapons and cyber weapons.[517] Yet some have even seen cyber weapons as a threat to nuclear weapons, so in a sense, even more strategic in their effects than the thermonuclear bombs themselves.[518] All this considered, the usefulness and effects of strategic offensive military use of cyber power is still suspect.[519] Moreover, it is debatable if cyber power should be considered as a military means or a more comprehensive instrument of national or global politics. Consequently, Baylis, Wirtz and Gray argue that cyber power is used in the whole continuum of state relationships from peace to war.[520] This point is important because it takes note of the long term effects of cyber power and argues that the use of cyber power is not restricted to wartime even if it can be considered to have a military aspect.

The definitions presented above indicate that cyber power is not confined to cyberspace, it is not separate from other types of power and it can have persistent effects even though its domain is changeable. In addition to these observations, scholars have listed characteristics of cyber power. Stuart H. Starr would not apply the principles of war from other domains to cyberspace because cyber power is more diffuse, its speed and scope are different and it is very dependent on technology.[521] John B. Sheldon describes cyber power as pervasive, complementary, and stealthy.[522] Elinor C. Sloan takes a more military oriented view and lists unconquerable space, continuous change and adaptability, borderlessness, rapid and potentially wide scale effects and indirectness as characteristics of cyber power and space.[523] Joseph Nye offers the extinct monopoly of violence by states, difficulty of attribution, cheap and plentiful resources, low relevance of distance, strength of offense compared to defence, the unfeasibility of conquering space or destroying opposing forces and the high fog of war.[524] Erik Gartzke and Jon Lindsay note that the effects of cyber power are only temporary and that it is difficult to hoard it, because it is insubstantial and relative, and loses its utility when used.[525] Martin Libicki has declared that there is no forced entry into cyberspace, which means that power is tied to the rules of cyberspace, e.g. if you try to blow your

means enhances other uses of force (Valeriano & Maness 2015, 60).

[515] Cf. Rid 2017; Stone, John. Cyber War Will Take Place! Journal of Strategic Studies, Vol. 36, No. 1 (2013), 101-108; Valeriano & Maness 2015; Libicki 2016; Dombrowski & Demchak 2014.

[516] Betz, David. Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed, Journal of Strategic Studies, Vol. 35, No. 5, 2012, 689-711.

[517] Cf. Nye, Joseph. Nuclear Lessons for Cyber Security? Strategic Studies Quarterly, Vol. 5, No. 4 (Winter 2011b), 18-38; Geist, Edward. Deterrence Stability in the Cyber Age. Strategic Studies Quarterly, Vol. 9, No. 4 (Winter 2015), 44-61; Libicki 2016.

[518] Cimbala, Stephen J. Nuclear deterrence and cyber warfare: coexistence or competition? Defense & Security Analysis, Vol. 33, No. 3 (2017), 193-208.

[519] This is the main point of Thomas Rid's criticism of 'cyber war' hype (Rid 2017). John Stone is correct in pointing out that Rid is writing about a very narrow definition of warfare (Stone 2013).

[520] Baylis, John, Wirtz, James J. and Gray, Colin S. Strategy in the Contemporary World (4th ed.) Oxford: Oxford University Press, 2013, 306.

[521] Starr, S. H. Towards a Preliminary Theory of Cyberpower. In Kramer, Starr & Wentz 2009, 43-81.

[522] Sheldon 2013, 289.

[523] Sloan 2012, 89-90.

[524] Nye 2010, 5.

[525] Gartzke & Lindsay 2015, 345-346.

way in, you do not have cyberspace anymore.[526] Maness and Valeriano point out that cyber power can have a spill-over effect into other domains or issue areas and there can be unintentional second or third order effects. [527] Other definitions tell us that cyber power has its own physical, logical, organizational and cognitive aspects depending on which level power is used. It may be kinetic or non-kinetic depending on its object. As a defensive power it is resilient as it is based on networks. Furthermore, it might or might not be cheap—depending on creativity and vulnerabilities.[528] Concepts of cyber power have often concentrated on the active and offensive military use of power. Peaceful or civilian definitions of cyber power are scarce. However, the interest in offensive aspects has recently begun to change as resilience, deterrence, and offensive operations have been integrated into cyber strategy proposals.[529]

Because I am interested in the military strategic aspects of cyber power and approach power through a neoclassical realist framework, it is natural that the definition of cyber power adopted for this thesis should be centred on the first and second faces of power. This does not imply a concentration on just the direct influence or agenda-setting but also includes the shaping of the space or environment where direct power is used. Therefore, cyber power can have persistent effects and its means and ways are not necessarily military. This is the reason why the term cyber power is used in this thesis and not that of military cyber power. Accordingly, cyberspace can be shaped and controlled, and it retains its attributes for a length of time, even outside conflicts, and without the use of exclusively military means and resources. Cyber power's resources can be anything if the effect is in cyberspace or transmitted through it. However, the main resources can be argued to be technological, scientific, economic, normative, doctrinal, organizational and professional. Cyber power can be utilized in peace or wartime. It can be used to achieve strategic or enabling effects as part of a state's grand or military strategy.[530] Through strategic cultural ideas cyber power has meaning to its users. Thus, the use of cyber power is planned, intentional, and strategic and it is dependent on the actors' understanding and perceptions of cyberspace and cyber power. In short, *cyber power is an ability that empowers an actor to influence others in or through cyberspace and to control and shape cyberspace to its advantage according to its preferences*.[531] This is not a universal definition of cyber power. It emphasises the creative aspect of power and lays the ground for understanding how closed national networks or 'national segments of the Internet' are shaped into being and controlled. It does not exclude the direct use of force but, on the contrary, highlights an actor's ability to create conditions for a more efficient use of both offensive and defensive direct force. This kind of power cannot be measured outside the relationship and context it is used, although resources or its potential can be. Cyber power is based on

[526] Libicki, Martin C. Conquest in Cyberspace. National Security and Information Warfare. Cambridge: Cambridge University Press, 2007, 35.

[527] Valeriano & Maness 2015, 46-47.

[528] Andress, J. and Winterfeld, S. Cyber Warfare - Techniques, Tactics and Tools for Security Practitioners, (2nd ed.). Waltham: Syngress, 2014, 35-36, 182-183; Schreier 2015, 14; Bryant 2016.

[529] For example, cf. Geist 2015; Chen, Jim. Cyberdeterrence by Engagement and Surprise. PRIMS, Vol. 7, No. 2 (2017), 100-107.

[530] On grand and military strategy cf. Milevski 2016a.

[531] This definition is modified from Endresen, R. S. Hard Power in Cyberspace: CNA as a Political Means. In Pissanidis, N., Rõigas, H., Veenendaal, M. (Eds.) 8th International Conference on Cyber Conflict: Cyber Power. Tallinn: NATO CCD COE, 2016, 23-36, 25.

constantly evolving technological, human, regulatory and organizational potential and it becomes military only through its use, effects or outcomes.

3.4 War and warfare

To understand how strategic cultural ideas, i.e. ideas about the use of force, relate to cyber power and how this power becomes military power, the concept of cyber warfare needs to be examined. Cyber power is exercised in a military strategic context through the threat or use of force. This definition includes both offensive and defensive uses. Force is here understood as power that has been given (even if only implicitly) direction and/or an objective in a military context, that is a purpose. Power can be used or utilized based on a belief of effectiveness when applied for specific effect.[532] In line with these definitions, cyber power might be utilized as a force with potential violent consequences in and from cyberspace. Although there is legitimate criticism against defining cyberspace and cyber power in military terms, it does not relinquish us from the fact that cyberspace has become a military domain and as such requires study from a military perspective.[533]

War is a central term for understanding the use of force. According to the perhaps most famous Western military scholar Carl von Clausewitz war is "…a continuation of political intercourse, with the addition of other means."[534] Clausewitz and his followers have enshrined the idea of war as a political instrument understood as a struggle between two opposing sides affected by friction, and defined by an unchangeable nature composed of passion, chance and reason. However, war is also a 'chameleon' by character. The last premise means that war is a changing and historical phenomenon.[535] Clausewitz's views have been criticized over time but much of the criticism has been disputed, or has been adjusted to fit Clausewitz's ideas (or other way around).[536] Others have added to Clausewitz's ideas, for example, by pointing out that war is a social phenomenon, it is defined by people in historical context, or that the use of military force is not restricted to states or the state of openly declared interstate war.[537]

[532] The use of force does not explicitly include clear, political objectives. It might be disorganized, mindless violence. The use of force can also be implied, e.g. used to threaten (cf. Bufacchi, V. Two Concepts of Violence. Political Studies Review, Vol. 3, No. 2 (2005) 193 - 204.) Utility implies that force has a purpose and it is believed to be useful and efficient (function of cost and effectiveness) in the context of a pursued objective. Utility is the function of both costs and benefits or cost and effectiveness. (Knorr, Klaus. On the uses of Military Power in the Nuclear Age. Princeton University Press, 1966; Duyvesteyn, I. Exploring the utility of force: some conclusions. Small Wars & Insurgencies, Vol. 19, No. 3 (2008), 423-443; Smith, Rupert. The Utility of Force: The Art of War in the Modern World. New York: Vintage Books, 2008, 6-8; Milevski 2016a, 146-150).

[533] NATO has defined cyberspace as a military domain (North Atlantic Treaty Organization (NATO) Cyber Defence Pledge, 8 July 2016 [Online].
Available: http://www.nato.int/cps/en/natohq/official_texts_133177.htm [Accessed: 19 August 2017]). On militarization of cyberspace see Dunn Cavealty (Dunn Cavelty, M. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. International Studies Review, Vol. 15, No. 1 (2013), 105 – 122).

[534] Quoted in Gray 1999a, 12.

[535] Gray 1999a, 91-100; Strachan 2013, 48-55; Angström & Widen 2015, 17-20.

[536] Levy, J. S. Review Roundtable. Clausewitz on Small War. The Journal of Strategic Studies, Vol. 40, No. 3 (2017), 450 – 456; Gray 2007, 28-29; Kaldor 2012, 220; Creveld 1991, 57-58; Keegan 2004, 12; Milevski, 2016a, 439-441; Angström & Widen 2015, 15-17.

[537] Creveld 1991; Keegan 2004; Levy 2017.

Warfare is about fighting, the making of war.[538] Like war, warfare is an ambivalent concept because its use has emigrated from physical violence to cultural, economic and purely political realms.[539] It has acquired qualifiers such as 'information', 'economic' or 'political' warfare. In a way, this problem is inherent in the Clausewitzian idea of the changing character of war and, of course, also in the politicized use of the term.[540] In addition to war and warfare, conflict is defined as the use of force below the level of open war. Conflict is limited in its means and ends and perhaps outcomes.[541] Moreover, terrorism, insurgency, civil war, and intrastate war are associated with organized violence for political purposes inside states, possibly with the covert or semi-open interference from other states. Between states competition and confrontation might take such forms as political, economic, and military pressure, including sanctions, blockades and the show of military power. Different kinds of power can be used overtly or covertly, directly or indirectly in state to state relations before the threshold of war is crossed.[542] This means that state relations related to the use of force and warfare are a continuum from peaceful relations to open war and this affects the ways power is utilized for force and other purposes. More importantly, the understanding of this continuum changes as the understanding of war changes when, for example, new technologies are introduced, societies change, or the views on morally acceptable means of influence evolve.

3.4.1 Cyberwarfare

Cyberwarfare and war are part of the changing character of war. John Arquilla and David Ronfeldt coined the term 'cyberwar' in 1993 which: "…refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even the military culture upon which an adversary relies in order to "know" itself."[543] Their concept was rooted in the growing role of knowledge in warfare ("…who knows what, when, where, and why, and about how secure a society or a military is regarding its knowledge of itself and its adversaries").[544] During the 1990s the original concepts of cyber war and warfare where partly subsumed by the concepts of RMA, NCW, and Information Warfare or Operations (IW/IO).[545] The RMA and NCW emphasised the fusion of sensors, intelligence, communications and precision weapons enabled by new technology which promised to

[538] Jordan et al. 2008, 3.

[539] The latest evolution is the return of the concept of 'political warfare' cf. Robinson, Linda, Helmus, Todd C., Cohen, Raphael S., Nader, Alizera, Radin, Andrew, Magnuson, Madeline and Migacheva, Katya. Modern Political Warfare: Current Practices and Possible Responses. Santa Monica, Calif.: RAND, 2018.

[540] War and warfare have established meanings in international law which leads to politicized uses of the terms, cf. Rousseau, D. L., Thrall, T. A., Schulzke, M. and Sin, S. S. Democratic leaders and war: simultaneously managing external conflicts and domestic politics. Australian Journal of International Affairs, Vol. 66, No. 3 (2012), 349-364, 361.

[541] Cf. Valeriano & Maness 2015, 31-33; Libicki 2016; Valerio, Jensen & Maness 2018.

[542] Cf. Gray 1999a; Gray 2007; Jordan et al. 2008; Kaldor 2012; Kane, Thomas M. and Lonsdale, David J. Understanding Contemporary Strategy. New York: Routledge, 2012; Sloan 2012; Strachan 2013.

[543] Arquilla, John and Ronfeldt, David. Cyberwar is Coming. Santa Barbara: RAND, 1993, 30. According to Thomas Rid, the term was used already in 1987 by the Omni magazine and even before that Jonathan Post used the term 'cybernetic war' in 1979 (Rid 2016, 294, 301). Cf. also Ventre, Daniel. Information Warfare (2nd revised ed.) Hoboken: John Wiley & Sons, 2016, 75.

[544] Ibid., 27.

[545] For conceptual and operational histories, cf. Mitchell, P. Network Centric Warfare: Coalition operations in

change the future way of war.[546] NCW could be characterized as a semi-doctrine under RMA which emphasised the use of networks, the self-synchronization of units, and superior situation awareness in dominating the battlespace through increased speed and effectiveness command, control and communications.[547] The central concept for NCW is information superiority which is "[the] ability to collect, process, and disseminate an uninterrupted flow of information, while exploiting and/or denying an adversary the ability to do the same."[548]

The concept of an 'information war' was first used by Thomas P. Rona in 1976.[549] According to Daniel Khuel, Rona described information warfare later in 1994 as "the sequence of actions undertaken by all sides in a conflict to destroy, degrade, and exploit the information systems of their adversaries. Conversely, information warfare also comprises all the actions aimed at protecting information systems against hostile attempts at destruction, degradation and exploitation. IW actions take place in all phases of conflict evolution: peace, crisis, escalation, war, de-escalation and post conflict periods."[550] At the beginning in the 1990s, IW in the United States was understood as counter command and control warfare. It was about the development and adoption of digital technology.[551] As the 1990s advanced, information warfare was increasingly seen as a new generation of warfare in which material resources were replaced by information. Edward Waltz, whose book Information Warfare: Principles and Operations contained many of the ideas NCW theorists would adapt, claimed that: "Information warfare operations concepts are new because of the increasing potential (or threat) to affect capacity and perception in the information and perception domains as well as the physical domain. These information operations are also new because these domains are vulnerable to attacks that do not require physical force alone […] The second new aspect to information warfare is the expansion of the battlespace beyond the traditional military realm. Information targets and weapons can include the entire civil and commercial infrastructure of a nation."[552]

Consequently, IW was later upgraded in the Western military doctrines to apply to the whole information environment, explicitly targeting an adversary's information through information operations (IO) or protecting own information.[553] In the US

the age of US military primacy. IISS, The Alelphi Papers, Vol. 46, No. 385, 2006; Rid 2016; Kaplan 2016. For the concept of 'information society' cf. Webster 2006; Castells 2010.

[546] Krepinevich, Andrew. The Military-Technical Revolution: A Preliminary Assessment. Washington: Center for Strategic and Budgetary Assessments, 2002; Jensen, Benjamin M. The role of ideas in defense planning: revisiting the revolution in military affairs. Defence Studies, Vol. 18, No. 3 (2018), 302-317.

[547] Network Centric Warfare refers to the doctrinal concept developed in the armed forces of the United States of America during the 1990s. Its main theorists were Arthur K. Cebrowski and John J. Gartska (Cebrowski, A. K. and Garstka, J. J. Network-Centric Warfare: Its Origin and Future. Proceedings Magazine, Vol. 124, No. 1 (1998), 28 - 35).

[548] An information position is defined by the dimensions of timeliness, accuracy and relevant information (Alberts, David S., Gartska, John J. and Stein, Frederick P. Network Centric Warfare: Developing and Leveraging Information Superiority (2nd ed.) CCRP Publications, 2000, 54, 56).

[549] Rona defined it as "degrading the opponent's information flow and, conversely, to protect or improve our own." (Rona, Thomas. Weapon Systems and Information War. Washington, D.C.: Office of the secretary of defence, 1976, pp. 5 [Online]. Available: http://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf [Accessed: 14th August 2018].

[550] Khuel, 2002, 36.

[551] Kaplan 2016, 33.

[552] Waltz, Edward. Information Warfare: Principles and Operations. Boston: Artech House, 1998.

[553] Khuel 2002, 50-53; Jones, A. and Kovacich, G. Global Information Warfare: The New Digital Battlefield.

doctrine, IO consists, among other things, of kinetic attacks, psychological operations, military deception, operational security, electronic warfare and computer network operations.[554] NATO defines the targets of IO as the will, understanding of situation, and command and control capabilities of an adversary.[555] The substance of information warfare and operations has been debated in the 2000s-2010s because the means (kinetic and non-kinetic), targets (systems), information, people, behaviour, methods (direct and non-direct), and the environment (physical, electronic and cognitive) are more or less mixed in definitions.[556] The addition of 'strategic information warfare' and 'strategic communications' further muddled the distinction between the tactical, operational, strategic and political use of information.[557] It speculated that information means could be used for strategic effect by affecting the military and infrastructure of the opponent.[558]

After 2001 officials and politicians in the United States' administration started to talk about cyber catastrophes or 'Cyber Pearl harbours'.[559] Attempts were made to understand this new threat based on the ideas about the strategic role of the air force from 1920s and ideas about nuclear forces from the1950—1960s.[560] The cyber threat was combined with terrorism, which gave birth to the concept of 'cyber terrorism' where non-state actors would be able to use cheap and formidable cyberattacks to cripple modern societies. [561] Cyber threats became a high priority for states globally, which led to the creation of cyber military units, as well as the development of cyber weapons, and the writing of state strategies to militarily defend national networks (instead of delegating this to the realm of broader security) and, if need be, to attack hostile nation's networks.[562] In this context Adam Liff defined cyber warfare as "the deliberate hostile and cost-inducing use of Computer Network Attacks (CNAs) against an adversary's critical civilian or military infrastructure with a coercive intent to extract

Boca Raton: CRC Press, 2016.

[554] For an example, cf. U.S. Army War College. Information Operations Primer: Fundamentals of Information Operations. November 2011 [Online] Available: http://www.au.af.mil/au/awc/awcgate/army-usawc/info_ops_primer.pdf [Accessed: 14th August 2018].

[555] NATO 2009.

[556] Libicki, Martin C. What Is Information Warfare? Washington DC: National Defense University, Institute for National Strategic Studies, 1995; Libicki 2007, 16-17; Hammes 2006.

[557] Brooks, Rosa. How everything became war and the military became everything. New York: Simon & Schuster, 2016, 86-90; Brooks, Rosa. Evolution of Strategic Communication and Information Operations Since 9/11: Hearing Before the Subcomm. on Emerging Threats & Capabilities of the H. Comm. on Armed Services, 112th Cong., July 12, 2011 (Statement of Rosa Ehrenreich Brooks) [Online] Available: https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1112&context=cong [Accessed: 14th August 2014]; Paul, C. Strategic Communications. Santa Barbara: Praeger, 2011.

[558] Molander, R. C., Riddile, A. S. and Wilson, P. A. Strategic Information Warfare: A New Face of War. Santa Monica: RAND, 1996, 31. Later on writers such as Gregory J. Rattray wrote about strategic information warfare which was "…means for a state and non-state actors to achieve objectives through digital attacks on an adversary's center of gravity." (Rattray 2001, 14.)

[559] Geers, Kenneth. Strategic Cyber Security. Tallinn: NATO CCD COE, 2011, 29-31; Rid 2012, 5-6; Gartzke, Erik. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. International Security, Vo. 38, No. 2 (Fall 2013), 41-73.

[560] Rattray 2001; Libicki 2009.

[561] Dorothy Denning. Is Cyber Terror Next? In Calhoun, Craig, Price, Paul and Timmer, Ashley (eds) Understanding September. New York: The New Press, 2002; Devost, M. G., Houghton, B. K. and Pollard, N. A. Information terrorism: Political violence in the information age. Terrorism and Political Violence, Vol. 9, No. 1, (1997), 72 - 83; Lachow, Irving. Cyber Terrorism: Menace or Myth? In Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K.: Cyberpower and National Security, National Defense University Press, Washington D.C., 2009, 437-464.

[562] Choucri 2012, 148-151; Dunn Cavealty 2013.

political concessions, as a brute force measure against military or civilian networks in order to reduce the adversary's ability to defend itself or retaliate in kind or with conventional force, or against civilian and/or military targets in order to frame another actor for strategic purposes."[563] Interestingly, Liff's definition is very similar to the strategies of air power defined by Robert Pape with the addition of obfuscation and exclusion of decapitation.[564]

Cyber war 'hype' led to a pushback from sceptics, who discredited the idea of cyberwar, cyber power's ability to achieve strategic effects by itself, and the ability of cyber weapons to create sustained and kinetic effects, i.e. casualties and destruction on the magnitude compared to conventional weapons.[565] Erik Gartzke claims that cyberwar is a myth because as an isolated instrument cyber-attacks have only a temporal effect and lack coercive power, and deterrence is difficult to maintain without revealing critical capabilities.[566] Valeriano and Maness prefer the term cyber conflict because of the perception that cyberwar has not happened and that cyber weapons might only have limited military effect anyways.[567] There is no agreed, universal definition on what is to be considered an armed attack in cyberspace, and so no internationally accepted concept of the violation of sovereignty in cyberspace, or a basis for individual or collective self-defence.[568] However, there is an emerging consensus since the 2010s among academics that 'cyber war' will not take place.[569] Some even propose that cyber operations have become part of all conflicts and that the cyberspace is in a constant state of 'skirmish'.[570] Recently, in the context of the so-called hybrid and political warfare Martin Libicki has questioned the, admittedly Western, separation of cyber and information warfare.[571] This proves the earlier point that defining cyber power as a strictly military power and concentrating purely on its destructiveness in the context of the warfare aspect is too narrow an approach. Moreover, the Western debate demonstrates how the offensive military use of force has been overemphasised and defence has been delegated to the realm of cyber security. Furthermore, it demonstrates that the understanding of cyber warfare has changed and there is no agreed Western definition of what cyber warfare or war means.

[563] Liff 2012, 408.

[564] Cf. Pape, Robert A. Bombing to Win. Air Power and Coercion in War. Ithica and London: Cornell University Press, 1996.

[565] Libicki 2007, 100-101; Gartzke & Lindsay 2015; Rid 2017.

[566] Gartzke 2013, 57-60.

[567] Valeriano & Maness 2015, 19.

[568] Schmitt & Vihul 2017. Although there have been attempts such as the Tallinn Manual and Tallinn Manual 2.0.

[569] Liff 2012; Demchak 2012; Valeriano & Maness 2015; Rid 2017; Libicki 2016; Junio, Timothy J. How Probable is Cyber War? Bringing IR Theory Back into the Cyber Conflict Debate, Journal of Strategic Studies, Vol. 36, No. 1 (2013), 125-133; Mahnken, Thomas G. Cyber war and Cyber warfare. In Lord, Kristin M. and Sharp, Travis (ed.) America's Cyber Future Security and Prosperity in the Information Age volume II, Center for New American Security, 2011, 57-64.

[570] Lemieux, F. (ed.) Current and Emerging Trends in Cyber Operations. Policy, Strategy and Practice. New York: Palgrave Macmillian, 2015, 1-3; Demchak 2012, 122-128; Valeriano & Maness 2015, 210; Betz & Stevens 2011, 97.

[571] Libicki, Martin C. The Conversion of Information Warfare. Strategic Studies Quarterly, Vol. 11, No. 1, (Spring 2017), 49-65, 50. Timothy Thomas made a similar argument already in 2003 (Thomas, Timothy. Is The IW Paradigm Outdated? A Discussion of U.S. IW Theory. Journal of Information Warfare, Vol. 2, No. 3 (2003), 109-116.

3.4.2 Dialectics of cyber offensive and defence

War and warfare require weapons. Thomas Rid and Peter McBurney have defined cyber weapon as a code that can do harm.[572] The concept of cyber weapons is problematic because code (software) can be used in different ways and attacks are usually based on vulnerabilities of the target systems, not on tailor-made weapons as such.[573] Additionally, the term weapon refers to a certain purpose and an effect which arguably limits the ways in which the use of malicious code can be understood.[574] Instead of weapons, the term cyber-attack or threat has been used to categorize different forms of tools or methods.[575] Targeted cyber-attacks are, in fact, operations consisting of variously described chains of actions.[576] The code used in the attacks is constantly modified and malware polymorphs into new versions with new signatures which degrade the ability to detect them.[577] This means that attacks are constantly evolving, using newly found and unknown vulnerabilities, and, therefore, attribution based on code is difficult and defence based on previous incidents always lags behind. The problem of designating malware as a weapon is that computer code does not directly kill people and attacks usually consist of dual-use code. This is something that has caused a lot of consternation for those who have tried to define cyber weapons in legalistic terms and the whole concept has been politized.[578] Conversely, Forrest Hare has argued that developing precision cyber weapon systems to be used during a lawful conflict ought to be legitimized as it would reduce the need for conventional weapons and thus could be more ethical, operationally effective, and cheaper.[579] The problem is that cyber-attacks can be used by states, state proxy-actors and non-state actors (criminals and terrorists) and distinguishing them from each other based on the methods used is practically impossible.[580]

IR and cyber scholars have differentiated cyberattacks or weapons to more abstract categories to manage a world of constantly changing malware names and technical slang. The most common categorization of cyberattacks is by effect: deny, disrupt,

[572] Rid, T. and McBurney, P. Cyber-Weapons. The RUSI Journal, Vol. 157, No. 1 (2012), 6-13, 7.

[573] Libicki 2009; Slayton 2016/2017; Rid 2017.

[574] Fischerkeller, Michael. Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies, Survival, Vol.59, No.1 (February-March 2017), 103-134, 114-115.

[575] Carr, Jeffrey. Inside Cyber Warfare (2nd ed.) Sebastopol: O'Reilly, 2012, 141-159; ENISA 2017; CrowdStrike. Global Threat Report 2018: Blurring the lines between statecraft and tradecraft. 26 February 2018 [Online], Available: https://www.crowdstrike.com/blog/crowdstrike-2018-global-threat-report-reveals-the-trends-insights-and-threat-actors-you-need-to-know/ [Accessed: 9th August 2018]; FireEye. M-Trends, Special Report 2018 [Online]. Available: https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf [Accessed: 15th August 2018].

[576] Hutchins, Eric M., Clopperty, Michael J. and Amin, Rohan M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin, 2011 [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [Accessed: 15th August 2018]; Kim, Hyeob, Kwon, HyukJun, Kwon and Kim, Kyung Kyu. Modified cyber kill chain model for multimedia service environments. Multimedia Tools and Applications Vol. 78 (2019), 3153–3170.

[577] Libicki 2016, 46-55.

[578] Cf. Osula 2016; Schmitt 2017.

[579] Hare, Forrest B. Precision cyber weapon systems: An important component of a responsible national security strategy? Contemporary Security Policy, Vol. 40, No. 2 (2019), 193-213.

[580] Claimed objectives and used resources have been used to make claims about state influence behind some cyber-attacks. For examples of these claims cf. Sanger 2018. On cyber-proxies cf. Maurer, Tim. Cyber Mercenaries. The State, Hackers, and Power. Cambridge: Cambridge University Press, 2018.

degrade, or destroy.[581] Martin Libicki argues that a cyberattack is about making a code or system do something it should not by manipulating it or giving it incorrect information. He also emphasises that a cyberattack is different from espionage or crime—mostly based on the agenda, not the means used.[582] Others have abandoned the concept of a weapon and have categorized actions or emphasised the nature, mechanism or technical aspects of the attack instead of the effects of attacks.[583] Western militaries have integrated weapons and attacks into cyber operations which include Computer Network Attack (CNA), Computer Network Exploitation (CNE) and Computer Network Defence (CND) or more recently Offensive cyber operations (OCO), Defensive cyber operations (DCO) and DODIN operations (securing and sustaining Department of Defence's information networks).[584]

Networks are inherently vulnerable to attacks and thus networks and the services running inside them have been protected with various systems and policies. Martin Libicki has categorised these as those minimizing exposure to attacks, increasing resilience, accelerating recovery, and defeating cyberattacks.[585] A more technical approach distinguishes perimeter protection, filtering, monitoring, response, information sharing, authentication, encryption, deception, and patching systems which range from manually human controlled to fully autonomous. [586] These systems can be combined in a complex of hardware and software or a system of systems[587] that provides all services with centralized interfaces and control.[588] Information has a definite role in security: threat intelligence must be shared inside and outside an organization if constantly evolving cyber-attacks are to be countered.[589] Cyber security should be separated from cyber defence. The former refers to measures to protect computer systems, networks and information from intentional or unintentional harm. The latter refers either to protective systems or functions explicitly designed against malicious

[581] These terms were already used, although not in this format, by Andrew Krepinevich in his report on the Military-Technical Revolution in 1992 (Krepinevich 2002). For a more coherent use cf. Joint Chiefs of Staff 2018. Martin Libicki has categorized effects to destruction, disruption and corruption based on how the attack affects confidentiality, integrity, and availability of information (Libicki 2016, 19).

[582] Libicki 2016, 19-20.

[583] Denning, Dorothy. Reflections on Cyberweapons Controls. Computer Security Journal, Vol. XVI, No. 4 (Fall 2000), 43-53; Fischerkeller 2017; Rid & McBurney 2012; Whyte, Christopher, Valeriano, Brandon, Jensen, Benjamin and Maness, Ryan. Rethinking the Data Wheel: Automating Open-Access, Public Data on Cyber Conflict. In Minárik, T., Jakschis, R. and Lindström, L. (eds.) 10th International Conference on Cyber Conflict CyCon X: Maximising Effects. Tallinn: NATO CCD COE, 2018, 9-30.

[584] Lemieux 2015, 1. In the new version exploitation is part of all kinds of cyber operations, and whereas security is more about eliminating vulnerabilities, defence is composed of actions taken against anticipated or manifested threats. (Joint Chiefs of Staff 2018.)

[585] Libicki 2016, 53.

[586] Wu, Chwan-Hwa and Irwin, David J. Introduction to Computer Networks and Cybersecurity. Boca Raton: CRC Press, 2013, 786-788.

[587] Cf. Chapter 3.6.

[588] Kakareka, Almantas. Detecting System Intrusion. In Vacca, John R. (ed.) Network and System Security (2nd ed.) Waltham: Syngress, 2014, 1-28, 20-21.

[589] Cichonski, Paul, Millar, Tom, Grance, Tim and Scarfone, Karen. Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. NIST (National Institute of Standards and Technology), 2012 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [Accessed: 27th September 2018].

attacks or to defensive military actions in cyberspace.[590] Moreover, the meaning and scope of cyber security has changed over time.[591]

The management of networks and their security is usually given to designated organizations on corporate, governmental and national levels.[592] These are organizations run by humans, but because security systems are becoming increasingly complex and they monitor massive amounts of data, AI solutions being sought.[593] Additionally, the networks themselves have become so complex and expensive to maintain that technology is increasingly being used to manage heterogeneous network devices from a centralized location. This increases the efficiency of network security management, but centralization may also cause new vulnerabilities.[594] The threat of supply chain attacks has made the domestic production of hardware and software part of the national cyber defence. Moreover, education, training and internal security are inherent parts of cyber security as the insider threat, unintentional or intentional, is always present.[595]

Cyberspace is full of potential malicious activity produced by various actors with various objectives.[596] This makes it difficult to distinguish warfare from the 'noise' of other activity. Cyber-attacks and security systems are both constantly evolving and new vulnerabilities are discovered daily, and old exploits lose their effectiveness.[597] Therefore, there cannot be persistent dominance in cyberspace. Every kind of power relationship requires constant and proactive upkeep, or it will change and shift. Offensive and defensive cyber forces are in a constant dialectical relationship, even during peacetime, and cyber power provides a means to manage that relationship. Thus, if there is such a thing as cyber warfare, it can be tentatively defined as *the use of force based on cyber power in or through cyberspace with a coercive intent to make political gains in the context of the continuum of interstate relations.*

3.4.3 Cyber use of force

The use of cyber power on a strategic level has borrowed its language from nuclear strategy scholars such as Bernard Brodie, Herman Kahn, Albert Wohlstetter, and

[590] Rantapelkonen, Jari and Salminen, Mirva (eds.) The Fog of Cyber Defence. National Defence University, Department of Leadership and Military Pedagogy, Series 2: Article Collection N:o 10. Tampere: Juvenes Print, 2013; ENISA. Definition of Cybersecurity: Gaps and overlaps in standardisation Version 1.0, December 2015 [Online] Available: https://www.enisa.europa.eu/publications/definition-of-cybersecurity [Accessed: 7th August 2018].

[591] Dunn & Wenger 2020, 7.

[592] ENISA. Baseline Capabilities of National/Governmental CERTs. Update Recommendations 2012 [Online]. Available: https://www.enisa.europa.eu/publications/national-governmental-certs-enisas-recommendations-on-baseline-capabilities [Accessed: 5th August 2018].

[593] Newman, Lily Hay. AI Can Help Cybersecurity – If It Can Fight Through the Hype. WIRED, 29th April 2018 [Online]. Available: https://www.wired.com/story/ai-machine-learning-cybersecurity/ [Accessed: 15th August 2018].

[594] Ahmad, Ijaz, Namal, Suneth, Ylianttila, Mika and Gurtov, Andrei. Security in Software Defined Networks: A Survey. IEEE Communication Surveys & Tutorials, Vol. 17, No. 4 (Fourth Quarter 2015), 2317-2346.

[595] Kello 2012; Libicki 2016, 35-36; Rid 2017.

[596] Lemieux 2015, 6-9.

[597] Smeets, Max. A matter of time: On the transitory nature of cyberweapons, Journal of Strategic Studies, Vol. 41, No. 1-2 (2018), 6-32.

Thomas C. Schelling.[598] This has led, with a slight variance in terminology, to the adoption of the concepts of persuasion, compellence, deterrence, coercion and brute force as the ways to use cyber force in the Western cyber literature.[599] It must be noted that although the concepts are widely used there is variance in how they are understood and used in non-Western countries.[600] Also, these political-strategic-level concepts lose their meaning on the tactical and technical levels.[601]

Persuasion is something like Joseph Nye's 'soft power': agenda framing, persuading, and positive attraction.[602] The object of the use of force does not even notice the use of force or accepts it as legitimate that he/she is being influenced. Deterrence is based on the ability to hurt an opponent. It is based on the threat to use force to make an opponent not to take an action. The threat is based on punishment or on denying the opponents' objectives by inflicting unbearable costs. This means that deterrence can be divided into deterrence by punishment (imposing costs) and deterrence by denial (preventing gains). The latter is in practise achieved by an outwardly effective defence. The opponent must know about the threat, it must to be credible and it must affect the opponent's cost-benefit calculations.[603] Deterrence is about the manipulation of the risk-calculations of an opponent.[604] Deterrence is a theory on its own and has gone through at least three, perhaps four, generations with substantial criticisms at every turn. It is embedded in historical context and in the technological evolution of nuclear weapons.[605] The difference between deterrence and compellence is that the latter is aimed at making or stopping an opponent acting in a certain way. It is based on active measures and the power to hurt the opponent more. Additionally, the opponent must have a choice to comply or not to comply. Deterrence and compellence are the defensive and offensive or passive and active sides of coercion which is equated as the power to hurt.[606] Brute force does not include any kind of bargaining or cost benefit calculations on the side of the opponent. Brute force is meant to destroy and kill, to take something or to hold something – to win without bargaining.[607]

Both Joseph Nye and Martin C. Libicki have written about persuasion and cyber power. Nye gives it a role in his 'soft power' concept and Libicki writes about the 'friendly conquest of cyberspace.' Based on their views it can be argued that cyber

[598] Cf. Libicki 2009; Geers 2011; Lango 2016; Nye 2016/2017; Valeriano, Jensen & Maness 2018. On the development of the U.S. nuclear strategy theory cf. Freedman, Lawrence. The Evolution of Nuclear Strategy (3rd ed.) New York: Palgrave Macmillian, 2003; Kaplan, Fred. The Wizards of Armageddon. Stanford, Calif.: Stanford University Press, 1983; Klinger 2019.

[599] This taxonomy is based on the activity of the user of force, the perception of the opponent, and on the effects of force.

[600] For the Chinese and Russians cf. Babiarz 2015; Thomas 2015a; Adamsky 2018.

[601] Schelling, T. C. Arms and Influence. New Haven: Yale University Press, 2008, 5.

[602] Nye 2011, 21.

[603] Schelling 2008, 5; Snyder, Glenn. Deterrence and Defence. Princeton: Princeton University Press, 1961; Angström & Widen 2015, 47-49; Freedman 2013, 159.

[604] Freedman 2003, 303.

[605] Jervis, Robert. Review: Deterrence Theory Revisited. World Politics, Vol. 31, No. 2 (January 1979), 289-324; Knopf, Jeffrey W. The Fourth Wave in Deterrence Research. Contemporary Security Policy, Vol. 31, No. 1 (2010), 1–33.

[606] Schelling 2008, x. This terminology has not been fixed and some have used coercion to mean compellence (Cf. Pape1996, 12).

[607] Schelling 2008, 2.

power plays an enabling role in persuasion as a part of the wider information warfare.[608] Cyber deterrence has been a hotly contested issue.[609] The basic problems are: against whom to direct deterring actions; how to evaluate the costs and effects; how to compensate the loss of deterrent means after their usage; how to estimate collateral damage; and how possible and desirable escalation[610] into other domains would be.[611] All things considered, deterrence exclusively by punishment in cyberspace seems quite problematic. It would require proof, proximate temporal range, proportionality, and a specific weapon at the ready.[612] Deterrence by denial, i.e. an effective defence which makes the expected costs too high for the potential attackers, might be a better solution. In fact, as time has gone by, and technology and the understanding of cyber power have improved, the argument about 'cyber weapons always getting through' has changed to a careful optimism about the denial aspect of deterrence.[613] This aspect has been subsumed under the concept of resilience. Cyber resilience has been defined as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources."[614] The point is that whatever destruction an attack causes, systems can be restored in a quick and ordered manner which deprives the attacker of the sought benefits. The downside of resilience are the investments that must be made based on risk calculations.[615]

[608] Nye uses also the term 'entanglement' which refers to the perception of interdependence and 'normative taboos' and their effect on cost-benefit calculations (Nye 2016/2017, 58). Libicki (2007, 125-126) refers to this as a 'soft conquest' or 'dependency'.

[609] Valeriano, Jensen & Maness 2018; Borghard, Erica D. and Lonergan, Shawn W. The Logic of Coercion in Cyberspace. Security Studies, Vol. 26, No. 3 (2017), 452-481.

[610] "[A]n increase in the intensity or scope of conflict that crosses threshold(s) considered significant by one or more of the participants." (Forrest E. Morgan, Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter and Roger Cliff. Dangerous Thresholds: Managing Escalation in the 21st Century. Santa Monica: RAND, 2008, xi.) In the cyber literature escalation has been either connected to cross-domain escalation which means an inadvertent or accidental spill-over of a conflict from cyberspace into the realms of conventional or nuclear warfare, or to escalation dominance, i.e. "a condition in which a combatant has the ability to escalate a conflict in ways that will be disadvantageous or costly to the adversary while the adversary cannot do the same in return." (Forrest et al. 2008, 15-16; Valeriano & Maness 2015, 102-105; Valeriano, Brandon and Ryan C. Maness. Cyber Spillover Conflicts: Transitions from Cyber Conflict to Conventional Foreign Policy Disputes?" In Ringsmore & Friis 2016, 45-64; Libicki 2016, 280-28; Borghard, Erica D. and Lonergan, Shawn W. Cyber Operations as Imperfect Tools of Escalation. Strategic Studies Quarterly, Vol. 13, No. 3 (FALL 2019), 122-145).

[611] Deterrence is difficult because the problems of attribution make it hard to tailor the deterrence to any distinct opponent, non-state actors react differently from state actors, secrecy limits the effectiveness of signalling, proportionality cannot be guaranteed in the absence of information, repetition of punishment is difficult, and the absence of rules reduces predictability and transparency and increases the probability of escalation. (Lantis2009, 470; Libicki 2009. xiv-xix; Liff 2012, 417-422; Andress & Winterfeld 2014, 92-96 Hare, F. The Significance of Attribution to Cyberspace Coercion: A Political Perspective. In Czosseck, C., Ottis, R. and Ziolkowski, K. (eds.) 4th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, 2012, 125 - 140; Valeriano, Jensen & Maness 2018).

[612] Brantly, Aaron F. The Cyber Deterrence Problem. In Minárik, Jakschis, & Lindström, 2018, 31-53, 44-45.

[613] Slayton 2017; Rivera, J. Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk. In Maybaum, Osula & Lindström 2015, 7 - 24; Rid & Buchanan2015.

[614] Ross, Ron, Graubart, Richard, Bodeau, Deborah and Mcquaid, Rosalie. Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. Draft NIST Special Publication 800-160 Volume 2, 2018 [Online]. Available from: https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf [Accessed 13 June 2018].

[615] Gartzke & Lindsay 2015; According to one source, the total value of information security products and services in 2018 was 114.15$ billion U.S. dollars up from 55$ billion in 2011. (Statista. Information security products and services market revenue worldwide from 2011 to 2019 (in billion U.S. dollars) [Online]. Available: https://www.statista.com/statistics/305027/revenue-global-security-technology-and-services-market/ [Accessed: 24th August 2018].

Deterrence has branched out to include a so-called active defence, which basically means penetrating potential aggressor's networks and conducting intelligence gathering operations with the option of pre-emptive or preventive attack.[616]Admittedly, active defence might be considered the opposite to a deterrence because it is 'active.'[617] Some scholars claim that the development of technology enables more accurate and faster attribution as well as better defence, which would allow cross-domain punishment to be used in cyber incidents.[618] Cross-domain here means retaliation for cyber-attacks with diplomatic, economic, conventional military and even nuclear weapons.[619] There have also been attempts to fit cyber deterrence to the Cold War concept of the escalation ladder.[620] Be that as it may, cyber deterrence still suffers from the 'security dilemma', that is, an arms race and unintentional escalation induced by the search for security.[621] This is compounded by the fear that cyber-attacks could be used to degrade the C3 systems of strategic nuclear weapons.[622]

The coercive or compelling use of cyber power is also a problematic concept because of the above mentioned strategic enabling effect.[623] Consequently, Thomas Mahnken has stated that for cyber weapons to have an effect they need to be combined with other uses of force which makes states the primary cyber actors.[624] Additionally, Thomas Rid has argued that the coercive or compelling use of cyber power would require that there is a clear understanding of who is using force against whom and for what purpose. The inherent secrecy of cyberspace makes this difficult.[625] Conversely, cyber-attacks can target vulnerable and critical assets of a state and, consequently, are tools of strategic warfare.[626] Instead of decapitation, a compelling use of cyber power could be used to enhance negotiations by only temporarily paralysing the opposing leadership, which would allow the resumption of the bargaining process after a demonstrative attack.[627] The problem with arguments in favour of strategic effects is the shortage of empirical data on them and their low perceived effectiveness so far.[628]

[616] Libicki 2016, 84.

[617] Harknett & Nye 2017.

[618] Tor, Uri. 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence, The Journal of Strategic Studies, Vol. 40, No. 1-2 (2017), 92-117; Gartzke, Erik and Lindsay, John. Cybersecurity and Cross-Domain Deterrence: The Consequences of Complexity [draft], 2016 [Online]. Available: http://deterrence.ucsd.edu/_files/ LindsayGartzke_ConsequencesofComplexity_Draft.pdf [Accessed: 16th August 2018].

[619] Gartzke & Lindsay 2017.

[620] Chen, Jim. Effectively Exercising Deterrence in the Cyber Domain. In Chen, & Hurley 2018, 120-125; Fischerkeller 2017. On contrary views cf. Borghard & Lonergan 2017 & 2019.

[621] Glaser, Charles L. The Security Dilemma Revisited. World Politics, Vol. 50, No. 1 (1997), 171 – 201.

[622] Gompert, David C. and Libicki, Martin. Cyber War and Nuclear Peace. Survival, Vol. 61, No.4 (2019), 45-62.

[623] Valeriano, Jensen & Maness 2018, 32; Libicki 2009, xiv-xv; Libicki 2016, 201. Those in favour of strategic effects include Kenneth Geers, Richard Clarke, Robert Knake, Gregory Rattray (Rattray 2001; Geers 2011; Clark & Knake 2010).

[624] Mahnken 2011, 61-62. Continuing advantages of states, cf. Betz & Stevens 2011, 131. On diffusion, cf. Nye 2011, 150-151.

[625] Rid has been criticized by, for example, John Stone who claims that Rid confuses force, violence and lethality, and states that lethality is not a requisite of an act of war. (Rid 2012 & 2017; Stone 2013). Cf. also Nye, J. 2016/17, 48; Gartzke & Lindsay 2015, 347.

[626] Rattray 2001.

[627] Smeets, Max and Lin, Herbert S. Offensive Cyber Capabilities: To What Ends? In Minárik, Jakschis & Lindström 2018, 55-72.

[628] On the shortage of data and the debate about the strategic effects of offensive cyber operations cf. Valeriano, Jensen & Maness 2018, 17; Sanger 2018; Lindsay, Jon R. Stuxnet and the Limits of Cyber Warfare, Security Studies, Vol. 22, No. 3 (2012), 365-404. For a brief history of cyber warfare cf. Green, James A (ed.) Cyber Warfare: A multidisciplinary analysis. New York: Routledge, 2015. More on the debated cf.

Brute cyber force is related to destructive attacks against the critical information infrastructure on a strategic scale.[629] Be that as it may, destroying and killing with cyber power without any element of bargaining has some of the same limitations as coercion. Additionally, as some have noted, there might be no supremacy in cyberspace.[630] No one actor can control cyberspace in any meaningful way and destruction removes the access to it from both the defender and attacker.[631] Taking and holding cyberspace are problematic concepts in a mutable, man-made environment. There is also the fear that the use of brute force on a strategic level could trigger conventional and nuclear counter retaliation.[632] So, on a strategic level, brute force might be conceivable as an enabling and supporting force, but as a means to achieve political objectives, it could be unreliable and possibly suicidal. On an operational or tactical level holding 'key terrain' or even temporarily destroying or disrupting an adversary's systems might make sense as part of conventional military operations.[633]

A couple of issues concern all the ways of using cyber force. Firstly, the security dilemma applies also to cyberspace as the feeling of constant vulnerability and the creation of cyber forces will make states feel vulnerable, which will result in an arms race and possible conflict, which would reduce the security for all.[634] Secondly, the security dilemma in cyberspace has changed as the offensive has lost its claimed 'asymmetrical' advantage and trust in defence through resilience has increased. This asymmetry was based on the logic that an offensive needed to get through only once, and that absolute defence was prohibitively expensive, and offensive weapons could not be preventively targeted.[635] Thinking has changed as it was understood that true cyber weapons require nation-state-level resources, must be tailored for a specific use and do not store well.[636] Moreover, their effects are hard to predict, the risks are thus higher, and their acclaimed surprise effect is limited to the first strike.[637] Thirdly, as the experience and understanding on the cyber use of force has accumulated, its connection to war

[629] Cyber-attacks on critical infrastructure might cause death and destruction and beat an opponent to surrender without any bargaining by destroying the foundations of society and government, cf. Rattray 2001; Geers, Kenneth. The Cyber Threat to National Critical Infrastructures: Beyond Theory. Information Security Journal: A Global Perspective, Vol. 18, No. 1 (2009), 1 - 7; Clark & Knake 2010; Wirtz, J. J. Life in the "Gray Zone": observations for contemporary strategists. Defense & Security Analysis, Vol. 33, No. 2 (2017), 106 - 114.

[630] Libicki 2009, 141-142.

[631] This view contradicts current Western, Chinese and Russian military doctrines which emphasize the importance of gaining 'information superiority.' (Joint Chiefs of Staff, 2017. Joint Operations (Joint Publication 3-0). [Online]
Available at: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf
[Accessed 13 October 2017]; Указ Президента РФ от 05.12.2016 N 646 (2016b) "Об утверждении Доктрины информационной безопасности Российской Федерации" [Online]. Available: http://www. consultant.ru/document/cons_doc_LAW_208191/ [Accessed: 30th March 2019]; Johnson, James. China's vision of future network-centric battlefield: Cyber, space and electromagnetic asymmetric challenges to the United States. Comparative Strategy, Vol. 37, No. 5 (2018), 373-390

[632] Cimbala gives a warning on accidental nuclear war as a product of information warfare (Cimbala, S. J. Accidental/Inadvertent Nuclear War and Information Warfare. Armed Forces & Society, Vol. 25, No.4 (1999), 653 - 675).)

[633] Cf. Bryant 2016. The concept of 'key terrain' is present in the United States cyber doctrine as a physical, logical or personal element that should be targeted for an effect or be protected (Kern & Gaines 2015).

[634] Van Evera, Stephen. Offense, Defense, and the Causes of War. International Security, Vol. 22, No. 4 (Spring 1998), 5-43; Jervis 2011.

[635] Cf. Alberts, David S. Defensive Information Warfare. Washington: NDU Press, 1996; Rattray 2001; Libicki 2007; Kramer 2009; Nye 2010; Nye 2016/2017; Schreider 2015; Sharp 2017, 899.

[636] Libicki 2015; Rid 2017, 167-179; Gartzke 2013; Liff 2012.

[637] Lindsay 2012.

and thus to visions of massive destruction have been replaced by 'normalcy.' Cyber-attacks are now seen as part of an already ongoing 'grey zone' conflict under a nuclear strategic deterrence.[638] And fourthly, as there are no commonly shared, tested or agreed rules or theories regarding the use of cyber force, different solutions based on the strategic cultural ideas will be tried and this will affect the whole of cyberspace because of its man-made and malleable nature. Most importantly, the above-examined strategic-level concepts do not include the shaping of battlespace. However, cyber power can be utilized to control and shape cyberspace as part of the strategy of a state actor.

3.4.4 Cyber strategy

The use of cyber power and force require intentionality. This issue is captured by the term strategy. Strategy as a term has lost its connection to military issues and has become a synonym for 'a plan'.[639] Nowadays the term 'military' needs to be added in the front of 'strategy' to make clear that what is meant by it is: "…the use that is made of force and the threat of force for the ends of policy."[640] This is, of course, only one way to define a military strategy.[641] There are at least two opposing wills using force to resolve their dispute.[642] It is never done in a vacuum or out of context or relationship. 'Linear logic' in strategy produces failure. This is because, among other things, a strategy is never enacted on a passive opponent, every measure produces a countermeasure and different levels of action interact in unforeseen ways.[643] Strategy is also "the art of creating power"[644] and "a plan of action designed in order to achieve some end."[645] It is also a process to identify the character of future war, prepare for it and manage it.[646] According to one influential definition, strategy is "concerned with ways to employ means to achieve ends."[647] Hedley Bull states that military strategy "is the art or science of exploiting military force so as to attain given objects of policy."[648] Military strategy can even be considered as a culture-bound vision of the use of force. Thus, different nations and militaries have different notions of strategy.[649] In the

[638] Whyte, Christopher and Mazanec, Brian. Understanding Cyber Warfare. Politics, Policy and Strategy. London & New York: Routledge, 2019, 163-164.

[639] Strachan 2013, 249-252.

[640] Gray 1999a, 17.

[641] The term strategy can refer to the nature of a weapons system (e.g. nuclear), the nature of the target and the magnitude of the effects of an attack (e.g. leadership of a country), organizational level of armed forces (e.g. combatant command or military theatre) or the level of decision-making in technical-tactical-operational-strategic-political continuum.

[642] "The Art of the dialectic of two opposing wills using force to resolve their dispute." (Quoted in (Gray 1999a, 18) Strategy according to André Beaufre. Cf. Kolodziej, E. A. French Strategy Emergent: General Andre Beaufre: A Critique. World Politics, Vol. 19, No. 3 (1967), 417 – 444.

[643] Luttwak 2001.

[644] Freedman 2013, xii.

[645] Wylie, J. C. Military Strategy: A General Theory of Power Control. Annapolis: Naval Institute Press, 2014, 14.

[646] Handel, M. Masters of War: Classical Strategic Thought. London: Frank Cass, 1996, 36; Gray 1999, 24; Strachan 2013, 118.

[647] Lykke, Arthur F. Toward an Understanding of Military Strategy. Military Review Vol. LXIX, No. 5, (May 1989), 2-8.

[648] Bull, Hedley. Strategic Studies and Its Critics. World Politics, Vol. 20, No. 4 (1968), 593 – 605, 593.

[649] Gray 1999a, 141-150. According to Timothy Thomas China and Russia have, for example, their own concepts of military strategy (Thomas, Timothy. Nation-state Cyber Strategies: Examples from China and Russia. In Kramer, Starr & Wentz, 2009, 465-488).

Western literature strategy is nowadays related hierarchically to the concepts of operational art and grand strategy and it interacts with doctrine.[650]

From an analytical perspective, military strategy has at least five aspects. Firstly, it can be a theory about the conduct of war. Secondly, it can be a concept concerning national security objectives and the nature of current war, i.e. a national security concept. Thirdly, it can be a concrete plan for how to fight a war and what forces to develop for it at the strategic level of planning. Fourthly, it can be a process of analysing the environment and formulating plans. Fifthly, it can be the conduct of war on the highest level—sometimes referred to as theatre-level warfare. These aspects are based on the notion that military strategy is subordinate to policy. Strategy gets its objectives from politics and transforms them into military ends which are achievable by military and non-military means.[651] This somewhat overly rationalistic and mechanistic top-down view of strategy is challenged by the idea of 'emergent strategy.' This emphasises the ad hoc nature of strategy or *doing* strategy. Strategy emerges from individual acts through learning and practise in a continuous process.[652]

In the context of cyberspace, cyber strategies have been used mainly in the sense of a plan or concept.[653] About 40% of the states of the world in 2017 had a national cyber security strategy that defined threats, opportunities, responses, responsibilities, resources and a vision in some combination.[654] These strategies are not military strategies, but whole-of-government policies.[655] As I want to emphasise the actions and their effects conducted through strategy I will not define cyber strategy as a plan or document. Therefore, I combine Lawrence Freedman's definition of strategy as "the art of creating power" with Colin Gray's "the use that is made of force and the threat of force for the ends of policy" as the basis of my definition.[656] Behind these short definitions is the view that there are political ends which are achieved in various ways using means to achieve them. According to Lawrence, strategy is more than just a rational, materialistic plan. The unpredictability of human affairs challenges desired

[650] Operational art is usually defined as the use of military forces, string of battles or a campaign to achieve the objectives of war and grand strategy as the coordination of all of a nation's assets to pursue a policy objective (Milevski 2016a). Bert Chapman defines doctrine as providing: "…a coherent and consistent framework of concepts, tenets, and principles that are applicable in planning and conducting operations, and that these doctrinal attributes are intended to assist in developing and executing operational plans." (Chapman, Bert. Military Doctrine: A Reference Handbook. California: ABC-CLIO LLC, 2009, 2). According to Barry Posen doctrines are used to provide principles of how to fight and to reduce uncertainty. They prioritise efforts, the mobilize the support of society, the provide guidance on how to fight and they provide reasons to fight (Posen, Barry. The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars. Ithica: Cornell University Press, 1984).

[651] Gray 1999a.

[652] Popescu 2018.

[653] Valerian, Jensen & Maness 2018, 9-10.

[654] Cf. International Telecommunications Union (ITU). Global Cybersecurity Index (CGI) 2017 [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf [Accessed: 23rd August 2018]; Greiman, Virginia, Cyber Security and Global Governance. In Abouzakher, Nasser (ed.) Proceedings of the 14th European Conference on Cyber Warfare & Security. Hattfield: University of Hertfordshire, 2015, 71-78.

[655] Luiijf, Eric, Besseling, Kim and de Graaf, Patrick. Nineteen national cyber security strategies. International Journal of Critical Infrastructure Protection, Vol. 9, No. 1-2 (2013), 3-31; Shafqat, Narmeen and Masood, Ashraf. Comparative Analysis of Various National Cyber Security Strategies. International Journal of Computer Science and Information Security, Vol. 14, No. 1 (January 2016), 129-136; Sabillon, Regner, Cavaller, Victor and Cano, Jeimy. National Cyber Security Strategies: Global Trends in Cyberspace. International Journal of Computer Science and Software Engineering, Vol. 5, No. 5 (May 2016), 67-81.

[656] Freedman 2013, xii; Gray 1999a, 17.

ends and may change calculations altogether. Furthermore, strategy is a form of active interaction involving bargaining, negotiation, threats, pressure and physical effects.[657] Gray on the other hand specifies seventeen dimensions of strategy grouped under the categories of people and politics, preparation for war and war proper. Strategy is done under each of them. Gray argues that the use of force in specific 'geography' (meaning land, sea, air, space and cyberspace) has its own grammar and it is always culturally based. Material circumstances and 'laws of warfare' will punish those that try to overcome these objective rules.[658] Somewhat similarly Freedman argues that, interests which define ends are socially construed needs—they are connected to strategic cultural ideas, or scripts.[659] Thus, based on Freedman and Gray, it can be argued that cyber strategy is very much a cultural phenomenon and connected to the defence and security elites' understanding of their environment.

Cyber strategy is also a practice based on 'art' or experience and a knowledge-based ability which allows for multiple resources, ways and means to create an effect. This idea follows Joseph Nye's understanding of power resources which are converted to power in some context and relationship, using different ways or modalities.[660] This formulation goes beyond the pure military use of force, and permits concentration on non-kinetic and non-military ways of using cyber power for military ends during the whole continuum of interstate relations. A cyber strategy can thus be understood as ways of using means (based on power) to produce effects in or through cyberspace for some end. These ends, ways, means and power derive their characteristics from cyberspace, but might have effects outside it. To sum it up, *cyber strategy is one component of the ability to control and shape cyberspace when considering the use of military and non-military force in the context of cyberspace and the continuum of interstate relations*. It refers to the 'ways' of using power resources— which are inherently connected to the actor itself and its understanding of the environment and thus to strategic cultural ideas. The concept of strategy explains why power rarely produces lasting effects because conflicting objectives of a multitude of actors require constant evolution of ways and means.[661] Cyber power must be exercised constantly, and cyberspace must be shaped if any advantages are to be had.

3.5 Closed national networks

Cyber power can be used to control and shape cyberspace in various ways. Arguably states with significant resources and the sovereign authority over their territory are the most capable actors to shape cyberspace. As was shown above, cyberspace is highly dependent on physical connections and hardware which are tied to the geographical locations and international and domestic governance, over which the state has either relative or theoretically absolute power. Thus, the Internet, as a part of cyberspace, is not outside the scope of the states' cyber power. It was also argued that states can use cyber power for military purposes even if this does not amount to a use

[657] Freedman 2013, xi-xii.
[658] Gray 1999a.
[659] Gow 2017, 275-276.
[660] Nye 2011, 40-41.
[661] On instability of power relationships cf. Freedman, Lawrence. Strategic studies and the problem of power. In Mahnken & Manoilo 2014, 9-21.

of force. This could be considered as shaping the battlefield on a strategic level.[662] Therefore, it is argued below that the shaping of cyberspace can have military strategic objectives in all phases of intrastate relations.

According to the scholars of Internet governance, by shaping and controlling the Internet, states are mainly trying to protect and promote their traditional interests: managing the new threats emanating from and through the Internet, maintaining political control of their population by controlling information, and supporting the digitalization and development of their economy.[663] The most visible manifestations of the use of this power have been Internet 'shutdowns': the disconnections of Internet and mobile connections on a national level in times of domestic disorder.[664] Chris Demchak and Peter Dombrovski have argued that states respond to the existential vulnerability brought on by the borderless Internet by building virtual borders, establishing national cyber commands and ensuring the control of national cyberspace, i.e. territorial sovereignty in cyberspace.[665] This is part of the fragmentation of the Internet mentioned above.[666] Moreover, this fragmentation could have direct military effects if it results in 'cyber blockades' or Anti-Access/Area-Denial (A2/AD) zones which deny the use of cyberspace from designated actors.[667] The states' threat and use of force therefore have a role in the way states shape cyberspace.

As was argued in the introduction of this thesis, the Russian regime's project to control that portion of the Internet which resides on its territory and under its jurisdiction, i.e. its national segment of the Internet has been approached mainly as an issue of censorship, political control, and information warfare. However, Kukkola, Ristolainen and Nikkarila have argued that behind this project is an effort to gain military strategic advantage by creating a closed national network.[668] In this context a closed national network is a state controlled segment of Internet that can be technically disconnected from the global Internet.[669] The idea has its roots in a paper written by Nikkarila and Ristolainen in which they applied traditional elements of combat power, i.e. manoeuvre, fire, and protection to analyse the military implications of Russia's

[662] A cyber battlefield is an area of confrontation within the cyber domain where adversaries battle for control in order to achieve tactical and operational objectives. (Kukkola, Ristolainen & Nikkarila 2017b).

[663] Choucri 2012; DeNardis 2014; Musiani et al. 2016; Mueller 2017; Aaronson 2017; Freedom House. Freedom on the Net 2017: Russia, 2017 [Online]. Available: https://freedomhouse.org/report/freedom-net/2017/ russia [Accessed 11 January 2018].

[664] Vargas-Leon 2016.

[665] Demchak & Dombrovski 2011.

[666] Giampiero 2014; Mueller 2017; Kremer & Müller 2016.

[667] Russell, A. L. Cyber Blockades. Washington DC: Georgetown University Press, 2014; Lawlor Russell, Alison. Strategic Anti-Access/Area Denial in Cyberspace. In Maybaum, Osula & Lindström 2015, 153-168. "An anti-access [A2] strategy is a plan for keeping a strategically-superior military away from one's region. It is intended to either deter interference by an outside power while achieving a regional military conquest, or if deterrence fails, achieve a quick victory while avoiding a force-on-force contest." Area denial (AD) is a combat tactic supporting A2. (Tangredi, Sam J. CNO vs A2AD: Why Admiral Richardson is Right about Deconstructing the A2/AD Term, The Navalist January 2017. [Online] Available at: https://thenavalist.com/home/2017/1/8/ dissecting-the-buzz-words-that-control-the-defense-debates [Accessed 19 August 2017]).

[668] Kukkola, Juha, Ristolainen, Mari and Nikkarila, Juha-Pekka. Confrontation with a closed network nation: Open network society's choices and consequences. Presented at Military Communications (MILCOM) conference, Baltimore, USA, October 23.-25, 2017; Kukkola, Juha, Nikkarila, Juha-Pekka and Ristolainen, Mari. Asymmetric frontlines of cyber battlefields. Presented at International Command and Control Research and Technology Symposium (ICCRTS), Los Angeles, USA, November 6.-8., 2017.

[669] Kukkola, Ristolainen & Nikkarila 2017b; Kukkola, Nikkarila & Ristolainen 2017.

project to secure and, if needed, close its national Internet from outside traffic. They argued that although increased protection is the main benefit of closing the national Internet, Russia could gain a relative advantage in fire and manoeuvre in cyber warfare against opponents who keep their networks open.[670] Theoretically then, the closed national network provides better protection and a military advantage against those states that are not able to disconnect their national networks.

Kukkola, Ristolainen and Nikkarila continued to analyse the possible results of closing national networks and developed concepts of 'cyber asymmetry', 'asymmetric cyber frontlines' and 'structural cyber asymmetry' to describe the military advantage that the closing of national network could provide.[671] Basically, 'cyber asymmetry' refers to an offensive and defensive advantage of a nation closing its networks over a nation that keeps its networks open in cyberspace. 'Asymmetric frontlines' refers to a layered and echeloned defences inside a closed national network—a concept which has, in principle, been proposed by two Russian scholars. These 'frontlines' are asymmetric because open networks lack them. 'Structural cyber asymmetry' describes the result of shaping and controlling closed national networks from cyberspace. It is an attribute of cyberspace created by manipulating the infrastructure and rules of cyberspace by means of technology, governance, norms and politics.[672] The infrastructure and rules can be understood as 'digital territory' which refers to material, functional, normative and political elements of cyberspace.[673] This is an analytical concept which enables the visualization and mapping of hardware, software, infrastructure, interconnection, information, human resources, protocols, services, policies and norms. Because cyberspace was defined above as a man-made and governed, the digital territory needs to be mapped on a case-by-case basis. It this thesis, the case is the Russian national segments of the Internet which will be 'mapped' as system of systems in the way described below.[674]

The basic argument of Kukkola, Nikkarila and Ristolainen is that in a situation where one nation manages to disconnect its national segment of the Internet from the global Internet it would gain an asymmetrical advantage in computer network attack (CNA) and computer network exploitation (CNE) operations.[675] Figure 1 shows how the asymmetry achieved by closing national networks is achieved. In the figure, the attack vectors (arrows) between a nation closing its networks (solid circle) and a nation with open networks (smaller dotted cloud) towards the global Internet (larger dotted cloud) are illustrated. It is important to note that the closing does not necessarily mean disconnecting all traffic. It can be done in steps based on increased control of traffic to, from and inside the national segment of the Internet.[676] The model is based on

[670] Nikkarila & Ristolainen 2017. The paper was inspired by Ristolainen 2017a.

[671] Kukkola, Ristolainen & Nikkarila 2017b.

[672] Kukkola 2017a & 2018a.

[673] The concept was first introduced in Kukkola 2018a.

[674] The concept of digital territory is inspired by Critical Geopolitics which argues that geopolitical representations are products of power. Here its premises are deployed to point out that 'objective' pictures of networks based on physical connections or protocols do not necessarily tell us how these networks are governed and controlled and what their political, economic or strategic function is. (Cf. Ó Tuathail, Gearoid and Simon Dalby (eds.) Rethinking Geopolitics London: Routledge, 1998).

[675] Kukkola, Nikkarila & Ristolainen 2017.

[676] The 'closing process' concept refers to the process of establishing standards and developing technology and solutions for the ability to nationally control the reliability, integrity and availability of data transfer, storage and processing. The closing process is related to Internet fragmentation as a phenomenon. (Kukkola, Ristolainen

Russian policies which will be more extensively discussed in Chapter 6. The nation closing its networks would control the Internet routing architecture inside its national segment and so maintain operational capabilities, i.e. services outside the global Internet. Additionally, it could operate in the global Internet through various interfaces.

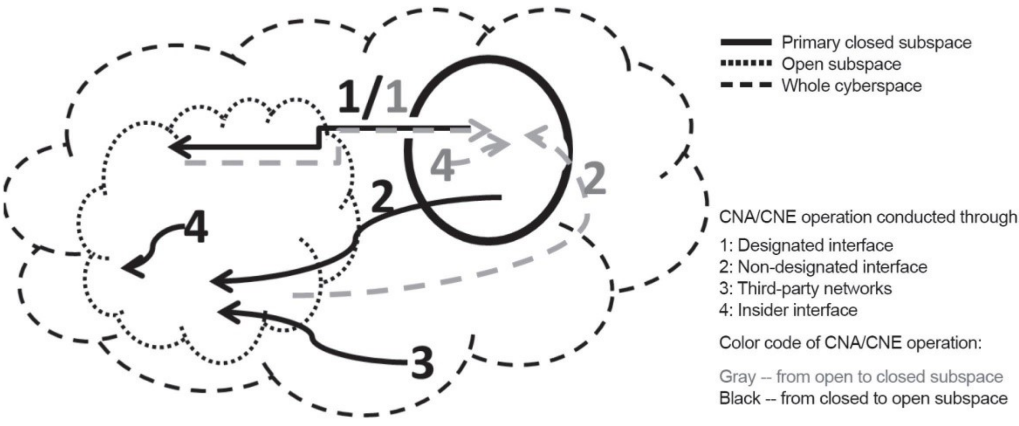
1/1
4
2
4
2
3
Primary closed subspace
Open subspace
Whole cyberspace
CNA/CNE operation conducted through:
1: Designated interface
2: Non-designated interface
3: Third-party networks
4: Insider interface
Color code of CNA/CNE operation:
Gray -- from open to closed subspace
Black -- from closed to open subspace

Figure 1. Schematic outline of the asymmetry between a closed and open national network. Source: Kukkola, Nikkarila & Ristolainen 2017.

In a confrontation between open and closed network nations, CNA/CNE operations from the closed network to the open network (solid arrows) can be conducted through interfaces officially designated for traffic, as well as through non-designated interfaces, through third-party networks and from inside the national network. Alternatively, CNA/CNE operations into the closed national network (dotted arrow) can be conducted through designated interfaces, non-designated interfaces that require additional measures to penetrate the defences of the closed national network, and from inside the closed network. Third-party networks operate towards closed networks like attacks through non-designated interfaces.

Designated interfaces are monitored and regulated points of traffic exchange points (IXPs) between national ISPs and their functions are based on agreements, AS advertisement, and physical lines of traffic. Traffic through these interfaces can be tracked, attributed (at least to the previous hop), and analysed efficiently in real-time, and the interfaces can be disconnected at will. The level of control of the designated interfaces by the state is an empirical question, but in the following analysis it is assumed that on the side that is closing its networks designated interfaces are highly controlled and regulated by the state. Non-designated interfaces are unregulated and possibly illegal interfaces, which nevertheless allow traffic from and into national networks.[677] Third-party networks are maintained by instances not connected to either nation. Insider interfaces require physical connections to the target network in the target country using USB, side-channel techniques or other media.

& Nikkarila 2017a, 52-53).

[677] These could be mobile data networks, satellite Internet services or unregulated optical fibre cable connections etc. which provide access into the wider national segment. They also include corporate networks which reside on the territory of a nation but are physically or logically disconnected from the national segment.

Kukkola, Nikkarila and Ristolainen analysed the interaction between open and closed networks by examining how the closing of a national segment of the Internet could affect the defence and offence of a nation closing its network contra a nation leaving its networks open.[678] In this context, Kukkola et al. used the freedom of movement, situation awareness and decision-making[679] capabilities to analyse a theoretical confrontation between an open and closed network nation on a conceptual level using the interfaces as points of analysis.

The advantages point to a disproportioned and exploitable advantage for the nation closing its networks. Furthermore, Kukkola et al. analysed the 'asymmetrical frontlines' inside closed national networks and claimed that this provided a further advantage for the closed network defender. This argument was based on a possible Russian project to use BGP routing, SDN technology and the nationalization of parts of the critical information infrastructure to create a centrally controlled national segment of the Internet. A hypothetical version of this project is shown in Figure 2.

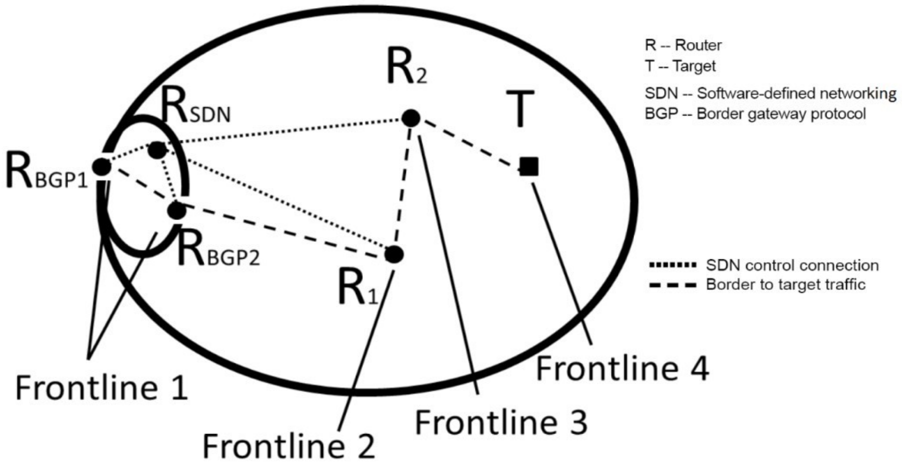

Figure 2. A simplified schematic outline of the asymmetrical frontlines inside a closed national network. Source Kukkola, Nikkarila & Ristolainen 2017.

In Figure 2 a network of routers form frontlines through which all traffic must pass. The first frontline is a border and customs zone through which all traffic must cross, and inside which its source and legitimacy are verified. It is a kind of nation-level demilitarized zone (DMZ)[680]. At the later frontlines the traffic is analysed and monitored, and the legitimacy of packets is checked based on routing tables. In effect, all

[678] Kukkola, Juha. The Russian Segment of Internet as a Resilient Battlefield. Presented at the International Society of Military Sciences Conference (ISMS) Warsaw, Poland, October, 18.-19., 2018.

[679] Kukkola et al. did not define these concepts. At this point, the following definition is sufficient for understanding the idea behind the analysis: Freedom of movement—the ability to conduct defensive and offensive cyber-operations in friendly and hostile networks. It is the function of fire, manoeuvre, and protection. Situation awareness—the ability to know all items of significance on the battlefield, predict the intentions of other players and evaluate the future. Decision-making capabilities—the ability to make better and faster decision and put them into effect faster and more efficiently than the opponent. (Kukkola, Nikkarila & Ristolainen & Nikkarila 2017). These concepts will be further developed in my upcoming General Staff Course thesis [2021].

[680] "A network segment outside an organization's inside firewall, usually used for hosts providing services to customers or the public." (Fall & Stevens 2012, 939).

traffic is registered, and unauthorized traffic is dropped. The last frontline consists of point defences, i.e. firewalls etc.[681]

To summarize, the claimed advantages in the defence and offence of the nation closing its networks are based on the argument that through technological solutions and by nationalizing the control of that portion of the Internet which resides on its territory and under its jurisdiction a nation can gain an asymmetrical advantage in freedom of movement, situation awareness, and decision-making capabilities because the properties of cyberspace would be decidedly different for each belligerent. Kukkola et al.'s main point is that if one nation or a group of nations decide to build national systems to control and disconnect their national segments of the Internet, those nations leaving their networks open would be in a position of a serious strategic disadvantage in a time of conflict. The project to prepare for the disconnection of national networks can be compared to the preparation of the battlefield on a strategic level. Or put in a different way in the words by Philippe Maigret: "the best kind of fortresses are those that forbid access to one's country while at the same time giving an opportunity to attack the enemy in his own territory."[682]

The Russian or any national segment of the Internet is a possible manifestation of the above described closed national network. Every national segment is however different because they are the result of the use of cyber power through strategy which is guided by strategic cultural ideas. Therefore, it is important to study how they have been shaped into being, how they are controlled and how they function. In this thesis I shall approach the Russian national segment of the Internet as a system of systems. This has been defined by Annette Krygiel as "a set of different systems so connected or related as to produce results unachievable by the individual systems alone. [...] They are capable of independent action. These constituents fulfil purposes of their own and can operate when disassembled from the whole. They are managed for their own purposes."[683] A system consist of objects in an interactive relationship which form a whole and thus have borders and relationships to other 'wholes'. They also have a function and a goal.[684]The argument is that the system of systems is designed for the state control of the national segment to provide different functions in different phases of interstate relations according to the reasons provided by the prevailing strategic cultural ideas. Thus, I am not assuming that the Russian national segment is meant for closing the national network, achieving cyber asymmetry, or any other predetermined function except as an exercise of cyber power. The reason why I choose to approach the Russian national segment as a system of systems is that, as Chapters 4

[681] Ibid. The asymmetry has been proven also mathematically cf. Nikkarila, J-P., Åkesson, B., Kuikka, V., and Hämäläinen, J. Modelling Closed National Networks – Effects in Cyber Operation Capabilities. Presented at the 17th European Conference on Cyber Warfare and Security (ECCWS), 28-29 June 2018, Oslo, Norway.

[682] Guerlac, H. Vauban: The Impact of Science of War. In Paret, Peter (ed.) Makers of Modern Strategy from Machiavelli to the Nuclear Age. New York: Oxford University Press, 1990, 64-90, 87.

[683] Krygiel, Annette J. Behind the Wizard's Curtain: An Integration Environment for a System of Systems. CCRP Publication Series, 1999, 33-34.

[684] Ackoff, Russell L. Ackoff's Best. His Classic Writings on Management. New York, John Wiley & Sons, Inc., 1999; Checkland, Peter. Soft Systems Methodology: A Thirty Year Retrospective. Systems Research and Behavioral Science Syst. Res. Vol. 17 (2000), 11-58; de Rosnay, Joël. The Macroscope A new world scientific system. New York: Harper & Row Publishers, 1975 [Online]. Available: http://pespmc1.vub.ac.be/ macroscope/ [Accessed: 23rd September 2019].

and 5 will demonstrate, cybernetic and systems theoretic thinking[685] influences Russian information security theorizing. Moreover, several types of national systems of information security and political control have been proposed by many Russian scholars. I do not argue that Russians are building such a system, just that it makes sense in the context of the prevailing strategic cultural ideas and provides one way to map a digital territory as a functional, normative, and political construct. This in my mind corresponds to the realist analytic form of pragmatism that was chosen as the thesis philosophical premise.

Now, that I have defined the main concepts of this thesis and provided a framework for analysing the Russian national segment of the Internet, and as such, answered the theoretical problems of this thesis, I shall continue to the analytical part. I have argued that the concepts developed here are preliminary descriptions of the objects of reality to which strategic cultural, in this case Russian ones, give meaning. The concepts are thus also tools to discuss, analyse and understand the objective and real phenomena of shaping and controlling cyberspace into a closed national network.

[685] Systems thinking is a scientific approach which came into being in the 1930s and 1940s. It spans diverse disciplines and includes multiple theories and methodologies which approach reality as holistic systems. One of the first developers of systems theory was the Russian Aleksandr Bogdanov (1873-1928). Austrian Karl Ludwig von Bertalanffy (1901-1972) is widely recognized as the actual creator of general systems theory. It aims to examine the whole of reality as systems which are entities composed of parts and the relationships between those parts. Systems theory is present in IR, for example, in the Neorealism of Kenneth Waltz (1924-2013). The modern version of systems theory argues that it is the responsibility of the researchers to search, describe and define systems. (Checkland 2000; Hammond, Debora. The Science of Synthesis. Exploring the Social Implications of General Systems Theory. Boulder: The University Press of Colorado, 2003; Lillienfeld, Robert. The Rise of Systems Theory: an Ideological Analysis. New York: John Wiley and Sons, 1978).

4

HISTORICAL IDEAS

This chapter begins to find answers to the thesis' research problem's analytical part by identifying the main strategic cultural ideas related to cyberspace and cyber power present in the discourses of Russian defence and security policy oriented epistemic communities and elites. I will begin this chapter by identifying a group of strategic cultural ideas that are connected to cyberspace, cyber power and cyber warfare and at same time I will present a critical literature review of previous studies on Russian information warfare. The ideas identified are: interstate struggle, digital sovereignty, strategic deterrence, asymmetric response, information superiority, information-technological warfare, automated command and control systems, and unified information space. I continue by examining the historical roots of the identified ideas through previous research and secondary literature and through some of the most important primary sources mainly to show the linguistic continuity of the terms and how the concepts were framed and perhaps understood in the time of writing. In the next chapter I follow the development of these strategic cultural ideas between 2000-2018.

4.1 Russian information warfare and strategic cultural ideas

Kier Giles, a senior consulting fellow at Chatham House, has been one of the most prominent proponents of the view that the Russians see cyber warfare as a Western concept and when they use it, they refer to Western concepts and actions. He argues "that any research on Russian capabilities and intentions which includes the word "cyber" risks providing fundamentally misleading results."[686] Instead of cyber, Russians use the term 'information'. Giles' argument can be empirically proven by examining the official information security documents of the Russian Federation.[687] To my knowledge no one has produced a proper explanation for why the Russians, who do borrow words from other languages quite readily, have not adopted the term cyber in the context of information and data networks of computers and software.[688] I claim that this phenomenon has at least three reasons. The first is the negative connotation with the term 'kibernetik' which refers to the Soviet (pseudo)meta-science of cybernetics that was discarded in the 1980s by Soviet scientists themselves. Conversely, the

[686] Giles 2016. Cf. also Giles, Kier. The Next Phase of Russian Information Warfare. Research paper. Riga: NATO STRATCOM COE, 2016; Giles, Keir. Russia's Public Stance on Cyberspace Issues. In Czosseck, Ottis, & Ziolkowski 2012, 63-76; Giles, Keir. Russia's 'New' Tools for Confronting the West – Continuity and Innovation in Moscow's Exercise of Power. Chatham House, Russia and Eurasia Programme, March 2016; Giles, Keir and Monaghan, Andrew. Legality in Cyberspace: An Adversary View. The Letort Papers, Strategic Studies Institute March 2014. Carlisle, PA: U.S. Army War College, 2014; Giles & Hagestad 2013.

[687] Cf. Указ Президента РФ от 9 сентября 2000 г. N Пр-1895. "Об утверждении Доктрины информационной безопасности Российской Федерации" [Online]. Available: http://base.garant.ru/182535/#ixzz4x5P8ZYEp [Accessed: 21st March 2019]; Указ Президента РФ 2016.

[688] Mustajoki, Arto. Kevyt kosketus venäjän kieleen [A Slight Touch on the Russian Language]. Helsinki: Gaudeamus, 2012, 147-151.

term 'kibernetik' already has a legitimate and established meaning in the Russian language.[689] The second is based on politics and relates to the official Russian policy of claiming that the content of information is a legitimate interest of sovereign states and that information is a form of weapon that should be regulated.[690] The third reason is connected to the taken-for-granted claim that the Russian approach to information is more holistic and consequently the cyber concept refers only to a means to an effect. According to Giles, for Russians "information itself [...] is important and is the object of operations, independent of the channel through which the information is transmitted. The aim is to control information in whatever form it takes. In this context, cyber in particular is just a technical representation of information, standing alongside other carriers such as print media, individual or mass consciousness, and much more besides."[691]

Giles' arguments are not novel. In her article from 1999 Mary Fitzgerald from the Hudson Institute, who was the leading scholar on the Soviet Military Technical Revolution (MTR)[692], claimed that by 1999 Russian military theorists were convinced of the strategic effects of information warfare and considered it to be a continuum of operations starting already in peacetime to intimidate the opponent and escalating to massive information-electronical warfare during conflict.[693] Moreover, modern means, forms, and methods made it possible to attain strategic objectives of war without the conquest of territory.[694] Fitzgerald claimed that the lessons drawn from the operation Desert Strom convinced the Russians that, a successful use of information warfare might resolve a conflict already at the initial period of war.[695] According to Fitzgerald, already in the late 1990s Russia was pursuing operational niche capabilities or asymmetries to exploit the United States' vulnerabilities and to counter its superiority until Russia managed to realize its own RMA. The defensive aspect of this strategy was the development of automated and autonomous ("intellectual") command-and-control systems and a state-level (intergovernmental), territorial unified telecommunications networks combined with early-warning radars, EW and air-defence assets. This "unified information-management system" would integrate separate armed forces networks and centralize the command. Fitzgerald presented the Deputy Defence Minister Andrei Kokoshin as one of the masterminds behind the idea of "scientific-technical reserve" which would allow Russia to leap-frog over a generation of technology to surpass the Western militaries.[696] In her article Fitzgerald touched upon

[689] Gerovitch 2002; Susiluoto 2006; Peters 2016.

[690] Tikk & Kerttunen 2017; Thomas, Timothy L. Russian Information Warfare Theory: The Consequences of August 2008. In Blank & Weitz 2010, 265-299; Patryk Pawlak. Reducing Uncertainties in Cyberspace through Confidence and Capacity-Building Measures. In Giacomello 2014, 39-58; Nocetti 2015.

[691] Giles 2016b, 6.

[692] According to Soviet sources, the Soviet Union went through at least two Military Technological Revolutions. The first was the mechanization of 1920s and the second was the development of the capability for intercontinental strategic nuclear weapons. The third would have been the 1970s and 1980s transition to technologically advanced conventional armed forces. (Adamsky 2010, 26-28.)

[693] Fitzgerald, 1999.

[694] Ibid. For the original cf. Самсонов, Виктор. Точка зрения. Нужна новая система коллективной безопасности, или Что сегодня может угрожать национальным интересам государств СНГ. Красная звезда 1995, № 279.

[695] This view was based on an analysis of the United States' use of EW capabilities. From a defender's viewpoint, effective defensive EW means were seen to reduce the surprise and the effectiveness of deep strikes, and to blind the enemy. The "electronic-fire" concept was considered as a new concept of war. (Fitzgerald, 1999).

[696]Ibid. For another view on the Russian 'RMA' cf. Kipp, Jacob W. The Russian Military and the Revolution in Military Affairs: A Case of the Oracle of Delphi or Cassandra? Fort Leavenworth, KS: FMSO, 1995.

many of the strategic cultural ideas I claim have had historical continuity, namely the interstate struggle, asymmetric response, information superiority, automated command and control systems, and a unified information space.

Timothy L. Thomas from the Foreign Military Studies Office at the U.S. Army War College has been steadfastly writing about the Russian approach to information warfare from the 1990s and because of this, his writings have had a defining effect on the Western understanding of Russian IW.[697] The writings of Thomas are important because he is one of the few Western scholars who has consistently and extensively used Russian language primary sources to study the Russian approach to IW. Below, I will briefly summarize his main points from different articles published first between 1996-2017.

Already in his 1996 article Thomas presented almost all the elements of Russian IW thinking that he elaborates in his later articles.[698] He introduced the concept of 'informatsionnoe protivoborstvo' which he translated as information war. He argued that the terms 'informatsionnaia voina,' 'informatsionnaia bor'ba,' and 'informatsionnoe protivoborstbo' all relate to the Western concept of IW. Thomas also claimed that the Russian approach to IW can be divided to information-psychological and information-technological/technical aspects[699]. The first refers to perception management, the moral-psychological preparation of own forces, and the concept of 'reflexive control'—which targets the brain.[700] The second refers to counter command and control warfare which includes attacks against the enemy's information systems—which targets machine processors.[701] According to Thomas, the Russians argued after the Gulf War that superior information processing had become at least as important in warfare as numerical superiority.[702] Additionally, Thomas argued that the Russians considered IW both in a broad national and societal context, where it might even have a strategic impact and at the same time in tactical-operational level, where it was more an enabling factor.[703] In a 2005 book 'Cyber Silhouettes' Thomas demonstrated that the information-psychological/technological divide, which he had proposed more as an analytical concept in 1996, was in reality concretely present in the Russian IW thinking and writings by 2003. Moreover, Thomas acknowledged that the Russian terms for

[697] In the Finnish context many of the studies written about the Russian IW are based on Timothy Thomas or scholars referring to his analysis. (Berger, Heidi. Venäjän informaatio-psykologinen sodankäyntitapa terrorismin torjunnassa ja viiden päivän sodassa [Russia's information-psychological warfare in the fight against terrorism and in the Five-day war], Maanpuolustuskorkeakoulu, Johtamisen ja sotilaspedagogiikan laitos, Julkaisusarja 1, 5/2010; Saarelainen, Jorma. Informaatiosodankäynti – venäläinen näkökulma [Information warfare - a Russian perspective]. In Saarelainen et al. 1999, 247-271; Pynnöniemi 2019a; Pynnöniemi, Katri. Information-Psychological Warfare in Russian Security Strategy. In Kanet 2019, 214-226).

[698] Thomas 1996.

[699] Thomas uses the terms technological and technical interchangeably (Cf. Thomas 1996; Thomas, Timothy. Cyber Silhouettes. Shadows Over Information Operations. Fort Leavenworth, KS: Foreign Military Studies Office, 2005.)

[700] "Reflexive control involves creating a pattern or providing partial information that causes an enemy to react in a predetermined fashion without the enemy realizing that he is being manipulated." (Thomas 1996, 31-32; Cf. Thomas, Timothy. Russia's Reflexive Control Theory and the Military, Journal of Slavic Military Studies, Vol. 17, No. 2 (2004), 237-256.)

[701] Thomas 2005, 166-167.

[702] Ibid., 31.

[703] Ibid., 27.

IW had important distinctions and he began to translate 'informatsionnoe protivobortsvo' first to mean confrontation and then later struggle.[704]

Through his articles Thomas has consistently referred to a group of Russian theorists who he sees to have influenced the Russian thinking on IW. These are primarily Admiral Vladimir Pirumov, the Scientific Advisor to the President of the Russian Federation until 1997 and the first head of the Scientific Council of the Security Council; a civilian analyst of the MoD V. I. Tsymbal; and a professor and member of the Russian Academy of Sciences (RAN) Colonel S. A. Komov. They have been later joined by professor S. V. Rastorguyev, a member of the Russian Academy of Natural Sciences (RAEN) and Academy of Military Sciences (AVN); professor Vitalii Tsygichko, a member of the RAS; and Major S. V. Markov.[705] These scholars have offered diverging views on IW and I will return to them more closely when analysing strategic cultural ideas. Nevertheless, Thomas' examination of their ideas shows that ideas about an information struggle, information superiority, and information-technological warfare were quite well-established by the early 2000s.[706] Although Thomas does not mention it, these scholars and probably many others with a security service background, especially from the FAPSI[707], probably took part in the interagency workgroup or committee on information security of the Security Council established in 1993-1996, and participated as experts in the subcommittee of information security of the Committee of Security of the State.[708]

[704] Ibid.

[705] Thomas 2015a & 2017.

[706] Thomas, Timothy L. The Russian Understandings of Information Operations and Information Warfare. In Alberts & Papp 2001, 777-814, 785-786; Thomas 2001; Thomas 2005.

[707] FAPSI was established in 1991 (its status was defined in law in 1993) to manage special communications, cryptographic and engineering-technical security of encrypted communications, intelligence gathering activities in the sphere of special communications, and the provision of special information to higher bodies of authority. (Thomas 1996, 28) Organization and tasks were based on the KGB's 8th Main directorate (communications intelligence and cryptography), 16th Directorate (radio-electronic surveillance and technical intrusion) and 12th Department (eavesdropping). FAPSI was a fully-fledged security service, in practice answering only to the president, and grew in personnel and power during the Yeltsin era. FAPSI was disbanded and its resources and responsibilities divided between the FSB and FSO in 2003. (Bennett, Gordon. The Federal Agency of Government Communications & Information. Royal Military Academy Sandhurst, The Conflict Studies Research Centre 2000 [Online]. Available: https://www.files.ethz.ch/isn/96806/00_Aug.pdf [Accessed: 3rd December 2018]; Soldatov & Borogan 2010; Agentura.ru. В спецслужбе создали новую структуру для противодействия компьютерным Преступлениям. 12.09.2018 [Online]. Available: http://www. agentura.ru/news/28975/ [Accessed: 18th April 2019].)

[708] According to Thomas, the 1995 draft law on information security clearly saw IW as a military threat mainly directed against command and control of military and critical information resources of military-industrial complex (Thomas 1998a, 159-160). What Thomas does not mention in his articles is that according to Professor Igor' Sheremet, Vice-President of the Academy of Military Sciences, in 1995 the Security Council of the Russian Federation formed an interagency workgroup consisting of the representatives from the SVR, FSB, FAPSI, MVD, MoD, Roskomnadzor, Academy of Sciences, military-industrial complex and Security Council. Its task was to investigate the issues concerning the developing global information infrastructure. (Шеремет, Игорь. Киберугрозы России растут — часть I. Ситуация в этой области изменяется в лучшую сторону гораздо медленнее, чем того требует развитие геополитической обстановки. ВПК, № 5 (523) за 12 февраля 2014 года.) It is possible that many of the articles published in military journals in the latter half of the 1990s, which Thomas analysed, were influenced by this working group and that the 2000 Information security doctrine was based on the work done by the group. Anatolii Strel'tsov argues that an interagency commission of information security under the Security Council was established already in 1993 (Стрельцов, А.А. Обеспечение информационной безопасности России. Теоретичнские и методологические основы. М.: МЦНМО, 2002, 10.). It is unclear if this is the same commission that Sheremet referred to. Strel'tsov also claims that in 1996 under the Committee of Security of the State Duma a subcommittee of information security was established (Ibid., 11.) In 1998 President Yeltsin gave a degree that designated V. P. Sherstiuk, the director of FAPSI, as the chairman of the Interagency Committee of Information Security (Указ Президента Российской

Based on the writings of Russian theorists and some practitioners, Thomas argues that the Russians purposefully did not copy American definitions because their needs and structural incentives were different.[709] Already in 1998, Thomas summarized ten key elements of Russian IW thinking, which (in a very condensed form) are described as follows: The incorporation of 'object laws and principles' of the military science into IW; The main objective and methods of implementation of IW change from peace to war time (peacetime includes reducing the information potential of the enemy and the protection own potential); The Russian focus is on society and consequently on information-psychological aspects; People are seen as information-psychological entities who can be influenced, for example, through energy; Superiority in information technologies challenges the geo-strategic balance by compromising nuclear command systems; The information potential of a country is a measurable quantity; Modern information operations affect military art by changing the nature of the initial period of war, tempo and importance of C4ISR; Computer research has produced and will produce unexpected results; IW is the interaction between opposing systems not unidirectional combat operations; Lastly, 'the infosphere' is understood to consist of computer programs and system are seen to become the most likely objects of military confrontation.[710] Later, Thomas distinguishes at least four different, non-exclusive, views of IW which are the geopolitical struggle of confrontation, information technology based military actions, systems-based warfare and an operational categorization of means including support, counter-measures, and defence.[711]

Timothy Thomas' writing reflects the wider lack of Western interest in Russian IW thinking from the mid-2000s to 2014 as he specialized in Chinese IW during those years.[712] During 2015-2017 Thomas wrote quite extensively about the Russian military and strategic thinking to an audience which was trying to understand the resurgent Russian military actions in Ukraine.[713] Thomas, for example, claimed that the Russian

Федерации от 24 декабря 1998 года N 1637 "Об утверждении составов межведомственных комиссий Совета Безопасности Российской Федерации" Российская газета" No. 248 30 декабря 1998). It was established as a part of the structural reconfiguration of the Security Council ordered by President Yeltsin in 1996 (Коротченко, Игорь. Реорганизация совета безопасности РФ завершена. Созданная структура, по мнению Ивана Рыбкина, позволяет решать задачи любой сложности. Независимая газета, № 9 21 января 1997.). According to Leonid Maiorov, vice-secretary of the Security Council in 1997, information security issues were handled by 'a directorate' before the establishment of the interagency committee (Майоров, Леонид Сергеевич. Информация и безопасность. Развитие современных технологий как реальная угроза будущему России. Независимая газета, № 180 25 сентября 1997.)

[709] Thomas 1998b, 44; Thomas 2005, 186-187; Thomas, Timothy L. The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia, Journal of Slavic Military Studies, Vol.22, No.1 (2009), 31-67. Heickerö argues that the Russian views have been affected by observing American doctrinal development and military successes from the viewpoint of a possible target, and also by the experiences of Afghanistan and Chechnya (Heickerö 2010; Heickero, Roland. Russia's Information Warfare Capabilities. In Lemieux, Frederick (ed.) Current and Emerging Trends in Cyber Operations. Policy, Strategy and Practice. New York: Palgrave Macmillian, 2015, 65-83).

[710] Thomas 1998b, 50-57.

[711] Thomas 2005, 186-187; Thomas 2009.

[712] Cf. Timothy, Thomas L. Decoding The Virtual Dragon - Critical Evolutions In The Science And Philosophy Of China's Information Operations And Military Strategy - The Art Of War And IW. Fort Leavenworth, KS: ISMS, 2007; Timothy, Thomas L. Three Faces Of The Cyber Dragon. Fort Leavenworth, KS: ISMS, 2012.

[713] Thomas, Timothy. Russia's 21st century information warfare: Working to undermine and destabilize populations, Defence Strategic Communications, Vol. 1, No. 1 (Winter 2015), 11-26; Thomas, Timothy. Russia's Military Strategy and Ukraine: Indirect, Asymmetric—and Putin-Led. The Journal of Slavic Military Studies, Vol. 28, No. 3 (2015), 445-461; Thomas 2015a; Thomas, Timothy. The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking. The Journal of Slavic Military Studies, Vol. 29,

leadership believes that the country is in a state of information war and that the regime survival is in question. He argued that Russia's means are deception, reflexive control, cognitive weapons, deflection and denial, fear mongering and building an alternative reality, and that it aims to deceive and destabilize opponents and unite citizens through fear of internal and external enemies.[714] Thomas tried to push back on some of the more erroneous interpretations of Russian military thinking such as the ideas of the 'Gerasimov Doctrine' and 'hybrid war/warfare'.[715] According to Thomas, the Russians considered hybrid warfare to be a Western concept, waged against Russia, and the Russians used it to deduce counter-forms and methods for their own use. Consequently, Thomas argued that the Russians used the concepts of 'New-generation warfare' (NGW) and later 'New-type war' (NTW) to characterise future war. The concepts were developed by civilians and adopted by the military.[716] One of the key arguments Thomas makes in his 2015-2017 texts is the Russian emphasis on information superiority.[717] In the NGW concept this superiority was based on principles similar to Network-Centric Warfare (NCW) with added EW and other capabilities to deny the aggressor information capabilities. In the NTW concept information superiority changed to emphasise the psychological aspect of IW.[718] Thomas argued that current Russian military approach seems to emphasise the attainment of information superiority before the initial period of war (IPW).[719]

The analysis of current Russian military thinking leads Thomas to the conclusion that the Russians show a definite interest in an asymmetric strategy, operations, tactics, actions and means at the theoretical and conceptual level. According to Thomas, asymmetry seems to be about off-setting an opponent's superiority, taking advantage of an opponent's unequal combat potential, avoiding direct confrontation, and deploying new and innovative forms and methods of conflict. Thomas argues that this emphasis on non-military and non-direct means and asymmetry led to the formulation of the concept of 'strategic deterrence' as an asymmetric measure publicised by M. A. Gareev in 2008.[720] He even argues that the Russian concept of asymmetry is more active than the American or British one, as it includes the creation of asymmetry.[721]

No. 4 (2016), 554-575; Thomas, Timothy. Thinking Like a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War. Fort Leavenworth, KS: FMSO, 2016; Thomas 2017.

[714] Thomas 2015b.

[715] For these concepts cf. Galeotti, Mark: Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right, Mayak Intelligence, 2016; Thornton 2016; Bartles, Charles K. Getting Gerasimov Right. Military Review, January-February 2016, 30-38; Renz, Bettina. Russia and 'hybrid warfare'. Contemporary Politics, Vol. 22, No. 3 (2016), 283-399; Galeotti, Mark. I'm Sorry for Creating the 'Gerasimov Doctrine'. Foreign Policy, 5 March 2018 [Online]. Available: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ [Accessed: 7th November 2018]; McDermott, Roger. Does Russia Have a Gerasimov Doctrine? Parameters, Vol. 46, No. 1 (Spring 2016), 97-105.

[716] Thomas 2016a.

[717] Ibid.

[718] Thomas 2016a & 2017.

[719] Thomas 2016b; Thomas 2015c.

[720] Thomas 2015, 97. Jonsson and Seely argue that the concepts of asymmetric and non-linear do not describe modern Russian doctrine because all strategy strives for asymmetry and non-linearity. They propose a concept of 'full-spectrum conflict' which includes all military, information, economic and political means. (Jonsson, Oscar and Seely, Robert. Russian Full-Spectrum Conflict: An Appraisal After Ukraine, Journal of Slavic Military Studies, Vol.28, No. 1 (2015), 1-22, 21).

[721] Thomas 2005, 294.

The view that successive Russian regimes, and most importantly Putin's current regime, have seen international relations as a geopolitical zero-sum competition between great powers, political and economic systems, or civilizations is a well-established view among Western Russia scholars.[722] As recently as 2018, Dmitr Adamsky claimed that the 'information struggle' (bor'ba/protivoborstvo)[723] plays a central role in modern Russian doctrine and that its nature is holistic (merges technological and psychological means), unified (synchronises kinetic and non-kinetic activities) and uninterrupted (conducted during peacetime and wartime in all domains). This struggle has both digital-technological and cognitive-psychological components. The information struggle includes electronic warfare, computer network operations, PSYOPS and deception.[724] This 'holistic' vision should not be pushed too far. No single state can integrate such complex issues as national interests into an indivisible, homogenous and fully coordinated policy. As Thomas' analysis of the 1990s has shown, there were multiple voices and interests at work in Russia, and as Chapter 6 will show there still are multiple voices. To perceive all Russian actions as a single approach only serves to placated current Western distress in the face of alleged Russian information or political warfare.[725]

Automated command and control systems and a unified information space have been mentioned only passingly by Giles, Fitzgerald, Thomas and Adamsky. Nevertheless, automated command and control systems (ASU) have been the subject of intense interest for Russians for as long as they have debated the post-Soviet period military reform.[726] Although the concept seems to include numerous different meanings it has particular cultural connotations which can help to understand how the Russians perceive the relations between networks, computers, computer programs, and information. In addition to previous studies, the concept of ASU has a central place in the Russian law on Critical Information Infrastructure.[727] Similarly, the concept of unified

[722] Trenin, Dmitri. The End of Eurasia: Russia on the Border Between Geopolitics and Globalization. Washington, DC: The Carnegie Moscow Center, 2001; Sondhaus 2006; Blank, Stephen. Threats to and from Russia: An Assessment. Journal of Slavic Military Studies, Vol. 21, No. 3 (2008), 491-526; Mankoff, Jeffrey. Russian Foreign Policy: The Return of Great Power Politics (2nd ed.) Lanham: Rowman & Littlefield Publishers, Inc, 2012; Donaldson, Robert H., Nogee, Joseph L. and Nadkari, Vidya. The Foreign Policy of Russia: Changing Systems, Enduring Interests. New York: M.E. Sharpe, 2014; Kipp 2014; Lo 2015; Porfiriev, Boris and Simons, Greg (eds.) Crisis in Russia: Contemporary Management Policy and Practice From a Historical Perspective. New York: Routledge, 2016 (original 2012); Cadier & Light 2015; Tsygankov, Andrei P. Russia's Foreign Policy: Change and Continuity in National Identity (4th ed.) London: Rowman & Littlefield, 2016; Jackson, William D. Encircled Again. Russia's Military Assesses Threats in a Post-Soviet World. Political Science Quarterly, Vol. 117, No. 3 (Autumn, 2002), 373-400.

[723] Adamsky seems to translate борьба and противоборство as 'struggle' (Adamsky 2018).

[724] Ibid.

[725] A case in point: "Russian military planners do not need to grapple with the problem of convergence in the same way as their Western counterparts, because—thanks to the holistic and integrated approach to information warfare—they never went through a process of divergence in the first place." (Giles 2016a, 69. Also, Blank, 2017). Michael Kofman manages to combine all Russian foreign and security policy into a 'grand strategy' (Kofman, Michael. Drivers Of Russian Grand Strategy. Frivärld, 23 April 2019 [Online]. Available: https://frivarld.se/wp-content/uploads/2019/04/Drivers-of-Russian-Grand-Strategy.pdf [Accessed: 31st December 2019]). Somewhat surprisingly a RAND report from 2018 is more objective in its approach (Robinson et al. 2018).

[726] Adamsky 2008; McDermott, Roger N. The Restructuring of the Modern Russian Army, The Journal of Slavic Military Studies, Vol.22, No.4 (2009), 485-501; McDermott, Roger N. Russian Perspective on Network-Centric Warfare: The Key Aim of Serdyukov's Reform. Fort Leavenworth, Kansas: FMSO, 2011; Kipp 2014; McDermott, Roger N. Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. Tallinn: International Centre for Defence and Security, 2017.

[727] Федеральный закон 2017a.

information space seems to refer to an optimal way of arranging communications and it has been mentioned in both civilian and military context already in 1950s-1960s.[728] Most recently it has been mentioned in the current Military Doctrine of 2014.[729] It has been replaced in the official documents by the concept of the national segment of the Internet since the publication of the 2016 Information Security Doctrine.[730] Previous Western research on Russian automated command and control systems and unified information space has mainly concentrated on analysing the Russian military reform and tactical and operational issues but they might also have national and strategic level applications.[731]

The most apparently novel aspect of the strategic cultural ideas chosen for the subject of this study is 'digital sovereignty'. This appeared in Russian official statements and documents around 2015 when the Minister of Telecommunications Nikolai Nikiforov made a proposal on 'sovereignty of the Russian Internet'.[732] Nevertheless, as Margarita Jaitner and Jari Rantapelkonen argue the idea had already been around in 2012.[733] The tendency of the Russians to project the idea of territorial sovereignty through virtual borders into cyberspace has been observed also by Julian Nocetti.[734] Others have noted the drive of the Russian government to 'tame' Internet through regulation and censorship.[735] The idea of sovereignty in cyber or information space is thus something that clearly defines Russia's approach to the shaping and controlling of cyberspace.

Based on above, the concepts of the interstate struggle, digital sovereignty, strategic deterrence, asymmetric response, information superiority, information-technological warfare, automated command and control systems, and unified information space seem to represent the most important ideas shaping Russia's strategy towards cyberspace. I shall now examine more closely each of the strategic cultural ideas with the intent to show that they have roots in the Soviet and Russian historical strategic thinking in the period between the 1950s and 2000.

[728] Gerovitch 2002; Peters 2016; Thomas 1998, 163; McDermott 2011, 21.

[729] Указ Президента РФ 25 декабря 2014 г., № Пр-2976. Военная доктрина Российской Федерации [Online]. Available: http://base.garant.ru/70830556/ [Accessed: 21st March 2019].

[730] Указ Президента 2016; Указ Президента РФ от 09.05.2017 N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" [Online]. Available: https://www.garant.ru/products/ipo/prime/doc/71570570/ [Accessed: 15th May 2019].

[731] Cf. Grau, Lester W. and Bartles, Charles K. The Russian Reconnaissance Fire Complex Comes of Age. Changing Character of War Centre, Pembroke College, Oxford [Online]. Available: http://www.ccw.ox.ac.uk/blog/2018/5/30/the-russian-reconnaissance-fire-complex-comes-of-age [Accessed: 30th October 2018]; Grau, Lester W. and Bartles, Charles K. Factors Influencing Russian Force Moderation. Changing Character of War Centre, Pembroke College, Oxford [Online]. Available: http://www.ccw.ox.ac.uk/blog/2018/9/19/factors-influencing-russian-force-modernization-by-dr-lester-grau-and-charles-k-bartles [Accessed: 30th October 2018]; McDermott 2011; Locksley, Christopher C. Concept, algorithm, indecision: Why military reform has failed in Russia since 1992. The Journal of Slavic Military Studies, Vol.14, No.1 (March 2001), 1-26; Bouldin, Matthew. The Ivanov Doctrine and Military Reform: Reasserting Stability in Russia, Journal of Slavic Military Studies, Vol. 17, No. 4 (2004), 619-641; McDermott 2017; Honkova, Jana. The Russian Federation's Approach to Military Space and Its Military Space Capabilities. Arlington, VA: George Marshall Institute, 2013.

[732] Голицына, Анастасия and Серьгина, Елизавета. Министр связи предложит правительству взять рунет под контроль. Ведомости. 26 Марта 2015. [Online]. Available: https://www.vedomosti.ru/technology/articles/2015/03/26/ministr-svyazi-predlozhit-gosudarstvu-vzyat-runet-pod-kontrol [Accessed: 4th December 2018].

[733] Jaitner & Rantapelkonen 2013, 83.

[734] Nocetti 2015, 114–115, 112.

[735] Soldatov & Borogan 2015; Soldatov 2017.

4.2 The strategic cultural ideas in the period of 1950–2000

This chapter examines how the chosen strategic cultural ideas manifested during the time of the Soviet Union and the first decade of the independence of Russia. The primary objective is to show that the strategic cultural ideas discussed above were active and present when Russia began to emerge from the 'Time of Troubles' of the 1990s and Vladimir Putin's regime started to search for ideas to fit the changing environment and Russia's interests.

4.2.1 Interstate struggle

The idea of a continuous interstate struggle is somewhat difficult to locate from secondary sources because the English translation of 'protivoborstvo' is variously either warfare, confrontation, countermeasure, or struggle.[736] The fact that Soviet civilian or military dictionaries do not directly recognize the term makes tracing the idea even more difficult.[737] Based on articles published in Voennaia Mysl' in the 1980s the term was used in connection to potential war between the United States and the Soviet Union, so the translation of warfare or confrontation might be suitable.[738] The term was also used in the Soviet times in connection to the continuous psychological warfare (psikhologicheskaia voina) between two competing systems even during peacetime.[739] On the political level the idea of a constant struggle against internal and external enemies was promoted by the Bolsheviks from the 1920s onward.[740] The idea of an international class struggle (klassovaia bor'ba)[741], which would eventually lead to the triumph of communism, informed Soviet military strategy and foreign policy—although it did leave room for 'realism', 'realpolitik' and détente.[742] Inherent in these ideas is a worldview of continuous competition, conflict, and possibly war with a peer or a counterpart, a system or a great power—a certain dialectic of power and eschatological view of war. In this context, politics is the continuation of war in another

[736] Cf. Ristolainen 2017a.

[737] Cf. Советская военная энциклопедия в восьми томах (СВЭ). / Гл. ред. комиссии А. А. Гречко (т. 1, 8), Н. В. Огарков (т. 2—7). М.: Военное издательство Министерства обороны СССР, 1976—1980; Большая советская энциклопедия: в 30 т. 3-е изд. (БСЭ) / Гл. ред. А. М. Прохоров. М.: Советская Энциклопедия., 1969 – 1978. The term is mentioned first time in connection to 'informatsionnoe protivobostvo,' in the Military Encyclopaedic Dictionary of 2001 (Военный энциклопедический словарь в 2 томах (ВЭС). / Редкол.: А. П. Горкин, В. А. Золотарев, В. М. Карев и др. М: Большая Российская энциклопедия; Рипол классик, 2001).

[738] Козлов, М. М. Вопросы стратегии в Советской Военной Энциклопедии. Военная мысль 1980 No. 10, 13-23; Кузнецов, Н. Н. О категориях и принципах советской военной стратегии. Военная мысль 1984 No. 1, 29-40.

[739] Волкогонов, Д. «Психологическая война» империализма. Военная мысль 1975 No. 1, 67-76, 67.

[740] Yablokov, Ilya. Fortress Russia: Conspiracy Theories in Post-Soviet Russia. Cambridge: Polity Press, 2018.

[741] КПСС. Программа коммунистической партии советского союза. Принята XXII съездом КПСС, 1961 [Online] Available: http://leftinmsu.narod.ru/polit_files/books/III_program_KPSS_files/056.htm [Accessed: 4th December 2018].

[742] McCauley, Martin. The Soviet Union Since 1917. London and New York: Longman, 1981, 62, 100; Gorodetsky, Gabriel. The Formulation of Soviet Foreign Policy – Ideology and Realpolitik. In Gorodetsky 1994, 30-44; Gaddis, John Lewis. The Cold War: A New History. New York: Penguin Books, 2005, 181-184.

guise.[743] This struggle went on by other means if military confrontation was not possible and did not exclude expedient alliances with third parties.[744] The degree of influence that this ideology had on Soviet military and foreign policy thinking is still unclear, but in theory the military strategy[745] should have reflected military policy that was based on the party's interpretation of Marxism-Leninism.[746] On the military technological side, Mary Fitzgerald has argued that Marxism-Leninism imposed the idea of "the dialectical law of unity and struggle of opposites" on Soviet thinking, which meant, "every means of attack generates a new means of defence, and every means of defence in turn generates a new means of attack."[747]

Petteri Lalu points out that military confrontation with capitalism was officially replaced with 'peaceful coexistence' in the 1957 XXI Party Congress of the Communist Party of the Soviet Union (CPSU), which allowed victory through other forms of competition.[748] Others have suggested that the international class struggle was abandoned by the disillusioned elites during Leonid Brezhnev's era (1964–1982) and was replaced by Russian nationalism and chauvinism but the official ideology still restrained great power realpolitik.[749] Raymond Garthoff has argued that from 1954–1956 the Soviets concentrated on the prevention of war.[750] Moreover, Oscar Jonsson has argued that by the 1980s the idea that war might be something other than strict violence had gained support amongst military scholars.[751] Be that as it may, David Glantz has argued that the basis of the Soviet military strategy during the Cold War developed from defending the achievements of the Second World War from the Western containment with massive conventional forces (1940–1950s), to a reliance

[743] Petteri Lalu has argued: "According to the Russian definition, war is a social and political phenomenon relating to radical changes in the relationships between states and peoples. War entails a transition towards armed and other violent methods in order to achieve desired objectives. The current Russian definition of war is Clausewitzian, however, it has a Marxist-Leninist amendment: war, by nature, is the continuation of the state's or its ruling elite's policy by violent means." Moreover, "The heritage of dialectic philosophy is still a part of the Russian view on wars and military security. The Clausewitzian definition of war has been refocused by Marx and especially Engels and Lenin and is still dominant. Dialectic philosophy argues that the struggle between two opposing forces goes on eternally as a zero-sum game, and each concession just increases your own risk." (Lalu, Petteri. On war and perception of war in Russian thinking. Finnish Defence Research Agency Research Bulletin 3 – 2016). Cf. also Scott, Harriet Fast and Scott, William F. Soviet Military Doctrine. Continuity, Formulation, and Dissemination. New York: Routledge, 2019 (org. 1988).

[744] Odom 1998., 1-15; Kokoshin 1998.

[745] "An integral part of and the highest realm of military art encompassing the theory and practice of preparing a country and its armed forces for war and of planning for and conducting war and strategic operations." ('Стратегия военная' СВЭ 1976-1980, 7:555-556).

[746] Glantz 1992, 1-4, 27-28; Lalu 2014. According to Kokoshin, armed forces were subject to party (i.e. military) politicians and war to politics. But the core of Bolshevik politics was the war and class struggle and possible total war with capitalist states (Kokoshin 1998, 49-55). "The views expressed in the Soviet military doctrine, from the very beginning of its origin were formed on the basis of laws, regulations and conclusions of historical and dialectical materialism and Soviet military science. Historical materialism, and in particular Marxist-Leninist doctrine." On the relationship of military doctrine, science and Marxism-Leninism cf. Завьялов, И. Диалектика войны и военная доктрина. Военная мысль 1975 №. 6, 23-34, 24.

[747] Fitzgerald 1987a, 3-4. The position of Marxism-Leninism was officially recognized by the Soviet military cf. Sushko, N. and Puzik, V. The Marxist-Leninist Theory of Knowledge and Its Significance in the Soviet Military Science and Practice. Military Thought – Secret version 1966, No. 1. Translated and published by the Central Intelligence Agency, Selected Translations, 23nd August 1966 [Online]. Available: https://www.cia.gov/library/readingroom/docs/1966-08-23e.pdf [Accessed: 5th December 2018].

[748] Lalu 2014, 280 ft. 1163.

[749] Zubok, Vladislav M. Soviet foreign policy from détente to Gorbachev, 1975-1985. In Leffler & Westad 2010b, 89-111, 93-94.

[750] Garthoff 1990, 33-34.

[751] Jonsson 2019, 33-34.

on strategic nuclear weapons and belief in the improbability of conventional war (1960s) and ultimately this led to the view that a major conventional war might still be possible without the use of nuclear weapons (1970s–1980s).[752]

By the 27th Party Congress in 1986 the rhetoric about class struggle had been toned down and, in fact, the struggle (bor'ba) was now conducted against poverty, corruption, alcoholism etc.[753] Interestingly, the General Secretary of the Central Committee of the CPSU Mikhail Gorbachev stated that "Thus, the objective […] conditions have taken shape in which confrontation [protivoborstvo] between capitalism and socialism can proceed only and exclusively in forms of peaceful competition and peaceful contest". [754] However, "The psychological warfare unleashed by imperialism cannot be understood as anything else than as a specific form of aggression, of information imperialism which infringes on the sovereignty, history, and culture of peoples. Moreover, it is a direct political and psychological preparation for war…"[755] At least on the political level, it seems that the struggle had become more of a metaphorical war against any ill or evil, and confrontation was upgraded to manage great power relations characterized by, among other things, psychological warfare or 'information imperialism' which was a threat to Soviet sovereignty.

This political shift was reflected in the Soviet military strategy and doctrine which changed from emphasising all-out war, an offensive military-technical doctrine, and the initial period of war[756] to one that was more or less defensive.[757] The reality was not quite so linear as the Soviet Union in the 1980s waged war in Afghanistan, was engaged in proxy wars in the 'Third World', pursued nuclear parity with the United States, deployed SS-20 missiles in Eastern Europe, developed new SSBNs and carriers, and continued, arguably offensive, chemical and biological weapons programs.[758]

[752] Glantz 1992, 169-171. For similar views cf. Garthoff 1990; Kokoshin 1998; Kipp 2014; Lalu 2014.

[753] Gorbachev, Mikhail. Political Report of the CPSU Central Committee to the 27th Party Congress, 1986 [Online]. Available: https://archive.org/details/PoliticalReportOfTheCPSUCentralCommitteeToThe27thPartyCongress/page/n41 [Accessed: 9th November 2018].

[754] Gorbachev, 1986, 83-84.

[755] Gorbachev, 1986, 110.

[756] "The initial period of war [nachal'nyi period voiny], the time during which the warring states fought with armed groups deployed before the start of the war to achieve the first strategic objectives at the beginning of the war or to create favourable conditions for the main forces to enter the war and conduct subsequent operations. At the same time, different measures of mobilization, strategic deployment of the armed forces, the mobilization of all the resources of the country for war, and foreign policy actions against enemies, and towards allies and neutral countries to strengthen international position of the state were conducted." ('Начальный период войны' СВЭ, 1976-1980, 5:554-555). The concept of initial period of war interested Soviet strategists already in the late 1920s and until the fall of the Soviet Union (Kokoshin 1998, 86-89, 122-123).

[757] Glantz 1992, 176-178, 189-190; Odom 1998, 120-123; Kokoshin 1998, 172-174; Garthoff 1990; Scott & Scott 1988.

[758] Glantz 1992, 190-191; Odom 1998, 82-83 & 80-81; Njølstad, Olav. The Collapse of superpower détente, 1975-1980. Leffler & Westad 2010b, 135-155; Fast Scott, Harriet. Soviet Military Doctrine in the Nuclear Age, 1945-1985. In Frank & Gillette 1992, 175-192; Hoffman, David E. The Dead Hand. The Untold Story of the Cold War Arms Race and Its Dangerous Legacy. New York: Anchor Books, 2009; Kagan, Frederick W. and Higham, Robin (eds.) The Military History of the Soviet Union. New York: Palgrave, 2002.

Additionally, the military doctrine[759] did not fully follow the fast political developments of the 1980s.[760] The Soviet military saw the correlation of forces (sootnoshenie sil i sredstv) based on military means in exclusion of non-military means.[761] Arguably, these means were based on material and spiritual strengths but the Soviet military leadership was quite clear that what mattered were strategic weapons.[762] Still, up until adopting a Warsaw Pact doctrine based on strategic defence in 1986/1988 the military strategy relied on pre-empting a NATO deployment through non-military means (deception and propaganda) and failing that on strategic and operational surprise.[763] It should be noted that whatever notions the Soviet military might have had about its mandate to contemplate the use of non-military means and despite the militarized nature of Soviet society, the Soviet armed forces were tightly subordinated to the Party during peacetime.[764] On its part, the Soviet military planned to fight a massive conventional war at least in the initial period of a war against NATO, but it never dropped the assessment that tactical and strategic nuclear weapons would eventually be used—presumably first by NATO as the Soviet Union officially denounced the first use of nuclear weapons in 1977.[765] These views are confirmed by post-Cold War era testimonies.[766] It is also important to note that unlike the United States, the Soviet Union's civil defence was an earnest attempt to maintain hope that the Soviet state could survive a nuclear attack in some form. It was not, however, a tool of coercion or deterrence.[767]

[759] The Soviet Union did not have an official publicized military doctrine but it was discussed from the 1920s onwards and was defined as: "A system of views adopted by the government at a certain moment of time on the objectives and nature of possible war, on the preparation of the country and armed forces to it, as well as on the methods of its conduct." ('Доктрина военная' СВЭ, 1976-1980, 3:225) Military doctrine had a political and technical dimension. The first was based on the political, social and economic character of society and war, the second on the changes in military technology, warfare, and ways to organize forces and fight Cf. Kokoshin 1998, 36; Odom 1998, 26; Glantz 1992, 34-36; Scott & Scott 1988, 29

[760] Rodionov, I. N. On Certain Provisions of Soviet Military Doctrine. Military Thought 1991, No. 3; Kokoshin 1998, 188-189.

[761] Correlation of forces: "An objective indicator of the combat power of the opposing forces, which makes it possible to determine the degree of superiority of one force over the other. The correlation of forces is determined by comparing quantitative and qualitative characteristics of […] friendly and enemy troops (forces). Correct calculations and estimates of relative strengths help make substantiated decisions during the preparation and conduct of combat operations…" ('Соотношение сил и средств' СВЭ, 1976-1980, 7:445).

[762] Куликов, В. Г. О военно-стратегическом паритете и достаточности для обороны. Военная мысль № 5 1988, 3-11.

[763] Glantz 1992, 206-210; Odom 1998, 75, 144; Kokoshin 1998, 126-128; Garthoff 1990, 103, Scott & Scott 1988, 112-113.

[764] Tsypkin, Mikhail Military Influence in Russian Politics. AD-A256 718. Montrey, CA: Naval Postgraduate School [Online] Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a256718.pdf [Accessed: 2nd October 2018]; Westad 2017, 190; Service, Robert. The End of the Cold War 1985-1991. New York: Public Affairs, 2015, 27-28, 59-61; Kokoshin 1998; Gaddis, 2005, 213-214; Odom 1998, 36-37.

[765] Odom, 70-71. It is possible that as the strategic nuclear weapons were divided between the Soviet services, they developed their own nuclear doctrines and strategies. (Cf. Huchthausen, Peter A. and Sheldon-Duplaix, Alexandre. Hide and Seek: The Untold Story of Cold War Naval Espionage. New Jersey, John Wiley & Sons, Inc., 2009, 235 & 260).

[766] Hoffenaar, Jan and Findlay, Christopher (eds.) Military Planning For European Theatre Conflict During The Cold War. An Oral History Roundtable Stockholm, 24–25 April 2006. ETH Zurich: Center for Security Studies, 2007; Hines, John G., Mishulovich, Ellis M. and Shull, John F. Soviet Intentions 1965-1985. Volume I: An Analytical Comparison of U.S.-Soviet Assessments During the Cold War. McLean, VA: The BDM Corporation, 1995, 12; Hines, John G., Mishulovich, Ellis M. and Shull, John F. Soviet Intentions 1965-1985. Volume II: Soviet Post-Cold War Testimonial Evidence. McLean, VA: The BDM Corporation, 1995.

[767] Geist, Edward M. Armageddon Insurance. Civil Defense in the United States and Soviet Union, 1945-1991. Chapel Hill: University of Northern Carolina Press, 2019.

The change to the defensive military posturing in addition to economic weakness necessitated prioritizing the prevention of war rather than preparing for it.[768] This led to a heated discussion about the feasibility of the defensive doctrine and posture which continued into the 1990s.[769] Additionally, the perceived impossibility of a nuclear war in the late 1980s increased the interest in strategic balance and other forms of struggle and confrontation.[770] This aversion to the use of nuclear weapons did not evidently stop the Soviet Union pursuing factual nuclear superiority over the United States up until the late 1980s.[771] However, thanks to the policy of glasnost and the importance of strategic arms control negotiations in restraining the United States, from the mid-1980s "civilian strategists" could take part in the discussions of military matters. Although they had limited influence, they introduced Western military strategic terms into the Soviet discourse.[772] Conversely, military strategists became interested in, among other things, information technologies and electromagnetic warfare.[773] These ideas were already discussed by the military at least since the late 1970s in the context of 'Military Technical Revolution' (nauchno-tekhnicheskaia revolutsiia) and 'informatization' (informatizatsiia).[774]

During the 1980s the Soviets translated the U.S. 'countervailing strategy' (Presidential Directive 59 July 1980), as 'a strategy of direct confrontation' (strategiia priamogo protivoborstvo).[775] Despite the use of the term confrontation or struggle to denote a strategic relationship, the Soviet military theorists seem to have used the word antagonistic/counterpart (protivoborstvuiuchshii) mainly in tactical and operational contexts to describe active or potential violent warfare or the use of force.[776] Thus, in an article discussing the military aspects of the 27th Party Congress of the CPSU General Lieutenant D. A. Volkogonov implies that the political and strategic level 'protivoborstvo' between systems is something which occurred mainly outside the open state

[768] This was the view of Colonel General I. N. Rodionov in 1991 (Rodionov 1991). Not all in the Soviet military saw this 'necessity' so clearly. Cf. Odom 1998; Hoffman 2009; Service 2015, 349.

[769] Воробьев, И. Н. Принципы формирования военной доктрины. Военная мысль № 11,12/1991. For a Western view cf. Hines, John G. and Mahoney, Donald. Defense and Counteroffensive Under the New Soviet Military Doctrine. Santa Monica: RAND Corporation, 1991.

[770] Fitzgerald 1987b, 23; Kokoshin 1998, 59-61, 133; Garthoff 1990, 151; Bellamy, Christopher. "Budushchaya Voyna; The Russian and Soviet View of the Military-Technical Character of Future War, Part Two" [Online]. Available: https://www.era.lib.ed.ac.uk/bitstream/1842/6892/2/504501_VOL2.pdf [Accessed: 11th November 2018].

[771] Hines, Mishulovich & Shull 1995a, 12; Hines, Mishulovich & Shull 1995b.

[772] Ibid. 134. Cf. Also Odom 1998,151-153.

[773] Kokoshin 1998, 138.

[774] Fitzgerald 1987a, 27; Kipp 2014; Kipp, Jacob W. Operational Art and the Curious Narrative on the Russian Contribution: Presence and Absence over the Last 2 Decades. In Blank & Weitz 2010, 193-263; Adamsky 2010, 26-31.

[775] Scott & Scott 1988, 108-109; Service 2015, 21-22; Westad 2017; Mitchell, Nancy. The Cold War and Jimmy Carter. In Leffler & Westad 2010b, 66-88; McGwire, Michael. Military Objectives in Soviet Foreign Policy. Washington, D.C.: The Brookings Institution, 1987, 287-294; Корочанский, И. Ф. Нарушение военно-стратегического равновесия — цель милитаристских приготовлений США. Военная мысль 1982 № 3, 15-22. The strategy of direct confrontation: "…was focused on active opposition to the USSR on the global and the regional scale, on achievement of the military superiority and on the restoration of the leadership role of U.S. in the world." It enabled the flexible use of nuclear strategic weapons and, conversely, the exclusive use of only conventional means to win a war. ('Прямого противоборства, стратегия' ВЭС 2001, 2: 412-413)

[776] Cf. Кузнецов 1984; Воробьев, И. Н. Новое оружие— новая тактика. Военная мысль 1984 № 2, 34-45.

of war and did not necessitate (nuclear) war.[777] Eventually, in 1988 General Lieutenant V. V. Serebriannikov argued that to prevent military aggression against socialism both military and non-military means were required. Military means preserved the parity while political means stopped the threats from materializing. For Serebriannikov, non-military means would replace military means in the future.[778]

The idea of an information confrontation began to gain traction in the early 1990s. After Operation Desert Storm Colonel A. I. Pozdniakov could claim that: "The content of military operations has increased the importance of information-technological confrontation [protivoborstvo]. Superiority [prevoskhodstvo] in information awareness is an indispensable condition of victory in air, sea and even land warfare."[779] In 1995 Colonel A. N. Lukashkin and Captain A. I. Efimov claimed that 'infosphera' (i.e. the aggregate of general and special software means for creating, processing and storing computerized data and the data itself) would become one the most probable objects of military confrontation (protivoborstvo).[780] Finally, in a conference paper in 1995 Professor V. I. Tsymbal presented the wider and narrower types of IW.[781] He argued that, "In the broad sense, information warfare is one of the varieties of the 'cold war' - countermeasures [sbosobov protivoborstva] between two states implemented mainly in peacetime with respect not only and not so much to the armed forces as much as to the civilian population and the people's public/social awareness, to state administrative systems, production control systems, scientific control, cultural control, etc."[782] Tsymbal's definition is clearly connected to the Cold War era system-versus-system confrontation/struggle idea. He also offers a narrower definition which refers to military actions aimed at achieving an overwhelming information advantage (podavliaiuchshee preimuchshestvo). The nature of IW changes from the wider to narrower type when peace changes to war.[783] According to Tsymbal and some others, IW means and their effects could be compared to nuclear weapons, i.e. they had strategic effects and they could require a response in kind.[784]

Around the mid-1990s both Russian officers and civilian scholars were claiming that the United States had used information war (informatsionnaia voina) to disintegrate the Soviet Union and continued to use activities in the information sphere to weaken Russia. The U.S. used its technological advantages and the control of the Internet against Russia's interests in a geopolitical struggle. New information weapons would be developed and if Russia did not catch up it would be destroyed.[785] The ideas of the

[777] Волкогонов, Д. А. Военные вопросы в Программе КПСС. Военная мысль 1986 № 5, 3-15, 4.

[778] Серебрянников, В. В. Диалектика политических и военных средств в защите социализма. Военная мысль 1988, № 10, 3-11.

[779] Поздняков, А. И. Информационная безопасность личности, общества, государства. Военная мысль 1993 No. 10, 13-18.

[780] Лукашкин, А.Н., Ефимов, А.И. Проблема безопасности компьютерной инфосферы стратегических оборонных систем. Военная мысль 1995 № 5, 48-52.

[781] Thomas 2001, 785-786.

[782] Quoted in Thomas 1998, 45. Original: Цымбал, В.И. О концепции информационной войны. Информационный сборник Безопасность, № 9 (1995), 35.

[783] Thomas 1998, 53-54.

[784] Thomas 1996, 26; Цымбал 1995; Смолян, Г., Цыгичко, В., Черешкин, Д. Оружие, которое может быть опаснее ядерного. Независимая газета от 18.11.95 г. no. 3 (18 November 1995), 1–2.

[785] Коротченко, Е.Г. Информационно-психологическое противоборство в современных условиях. Военная мысль № 1/1996, 22-28; Смолян, Георгий Львович, Цыгичко, Виталий Николаевич and Черешкин. Дмитрий Семенович. Куда ведет информационная супермагистраль. Независимая газета 1996, No. 33; Смолян et al. 1995; Цыгичко & Черешкин 1995; Черешкин, Д.С., Смолян, Г.Л., Цыгичко, В.Н. Реалии

scholars were echoed in 1996 by the First Deputy Minister of Defence A. A. Kokoshin, who argued that Russia needed "to develop theoretical and practical foundations of information confrontation [protivoborstvo], since it is becoming an integral part of the armed warfare [bor'ba]." He called for the creation of forces and means of information warfare which included EW, intelligence, communications, command and control, and means to protect C2 assets from the enemy. Kokoshin clearly had in mind information-technological warfare as part of armed warfare, not just the geopolitical struggle.[786] The views of officers and academicians were shared also by the vice-secretary of the Security Council Leonid Maiorov when he argued in 1997 that Russia's interests in the information sphere were the spiritual development of the nation and the rights and freedoms of its citizens, the development of Russian information industry and the functioning of information-telecommunications systems.[787]

The character of future war became a hot topic among Russian military scientists in the latter half of the 1990s.[788] General Major I. N. Vorob'ev for example argued that it was characterized by the use of military-technological means based on information sciences (informatika), informatization (informatizatsiia) and an information-psychological confrontation or struggle (informatsionno-psikhlogicheskoe protivoborstvo).[789] For General Vorob'ev this latter psychological aspect was understood as deception, demoralizing the army and population of the enemy, controlling its actions, and achieving surprise in the initial period of war. It was covert strategic level warfare conducted during peacetime and enhanced by modern technology. Rear Admiral V. S. Pirumov and Colonel M. A. Rodionov offered a more nuanced analysis of information warfare [informatsionnaia bor'ba] and divided it into two aspects: geopolitical rivalry (protivoborstvo v informatsionnoi sfere) which was a legitimate, objective process aimed at achieving state policy objectives in interstate relations, and information warfare which was aimed at gaining information superiority to win an armed conflict. They further divided information warfare into actions conducted during peacetime, the period of threat, and open hostilities.[790] In a later article Rodionov argues that information warfare (informatsionnaia bor'ba) should be understood as subordinate to strategic actions (strategicheskoe deistvie), as operations, actions and strikes of the Armed Forces, not as an independent strategic action.[791] Rodionov's article is an example of 'fitting' the novel phenomena of IW to the old ideas of military theory—it might also be an attempt to create a role for the military in the IW framework. The third example of this 'future through old glasses' approach is Colonel A. A. Komov who in 1998 proposed a Marxist-Leninist cybernetic philosophical basis for Russia's

информационной войны. Конфидент, 1996. № 4; Цыгичко В.И., Вотрин Д.С., Крутских А.В., Смолян Г.Л., Черешкин Д.С. Информационное оружие - новый вызов международной безопасности. Москва: Институт Системного Анализа Ран, 2000. It should be noted that the ideas and articles of Tsymbal, Korotchenko and Tsygischko et al. might have been connected to the creation of the workgroup on the development of the principles of Russia' s entry into the global Internet under the Security Council in 1995. (Шеремет 2014).

[786] Кокошин, А.А. Военно-политические и экономические аспекты реформы Вооруженных Сил России. Военная мысль № 6 (11-12) (1996), 2-11.

[787] Майоров 1997.

[788] Гулин, В.П. О новой концепции войны. Военная мысль № 2 (3-4) 1997, 13-17.

[789] Воробьев, И.Н. Какие войны грозят нам в будущем веке. Военная мысль № 2 (3-4) 1997, 18-24.

[790] Пирумов В. С., Родионов М. А. Некоторые аспекты информационной борьбы в военных конфликтах. Военная мысль, № 5 1997, 44-47.

[791] Родионов, М.А. К вопросу о формах ведения информационной борьбы. Военная мысль № 2 1998, 67-70.

upcoming information security doctrine.[792]

The most important of these 'modern cybernetists' was professor S. P. Rastorguev who in 1998 published a book (reprinted in 1999) named Information War (Informatsionnaia voina). In it he defined an information warfare as the open and hidden, purposeful and information-based influence of two systems (or more) on each other in order to obtain a certain advantage in the material sphere.[793] He categorized systems as A type systems, which were mechanical, and B type systems which consisted of two cybernetic and one social hierarchical subsystem—respectively, information communication systems, systems of automated management, and people and social structures. Rastorguev admitted that the means used against B type systems' cybernetic aspects (technical systems and data) should be called cyber weapons but took a wider approach in his book and adopted the term information warfare and weapons when discussing system B. The point of an information war was to manipulate the opposing system's algorithms by using information weapons.[794] Rastorguev's thinking summarized the idea of a confrontation or struggle between systems, cybernetic theory, and modern ideas about IW and cyber warfare.[795] Rastorguev continued his theoretical work in the 2000s—to which I shall return in Chapter 5.

General M. A. Gareev, the president of the Academy of Military Sciences from 1993, also took part in the discussion. In 1998 he disavowed arguments that claimed that war could be fought with non-military means because otherwise human history would have been a continuous war. War's essence was unrestricted military violence. Gareev distinguished war from political confrontation (protivoborstvo) which exploited political, diplomatic, and information actions. Information confrontation was part of all kinds of struggle (bor'ba) up to and including armed warfare and at the same time had a relatively independent character and aimed to demoralize and paralyze the will of the other side to dominate peoples and impose development models. To counter this new threat, Gareev argued, the efforts of all security ministries and agencies were needed under the coordination of the Security Council, combined with a strong economy, firm political system, and united society.[796]

The discussion on the interstate struggle and the character of future war was partially connected to the discussion about the character and content of the future Information Security Doctrine and Military Doctrine, the drafting of which started in 1995/1997.[797] Timothy Thomas has analysed this discussion and according to him there were at least four different views present: The Security Council was interested in the social stability

[792] Комов, С.А. О доктрине информационной безопасности Российской Федерации. Военная мысль, № 3 1998, 72-76.

[793] Расторгуев С.П. Информационная война. 2-е изд. Moscow: Радио и связь, 1999, 60.

[794] Ibid., 61. Also Расторгуев, С.П. Информационная война как целенаправленное информационное воздействие информационных систем. Информационное общество, № 1 (1997), 64-66.

[795] This analysis is partly based on Ristolainen, Mari and Kukkola, Juha. Western world order in the crosshairs? A theoretical review and application of the Russian 'information weapon'. Presented in 18th European Conference on Cyber Warfare and Security (ECCWS) University of Coimbra, Portugal, July 4.-5., 2019.

[796] Гареев, Махмут Ахметович. Война и современное международное противоборство. Независимое военное обозрение, № 1 1998.

[797] Kipp, Jacob W. Russian Military Doctrine: Past, Present, and Future. In Blank 2011, 63-151, 92-95 [Online]. Available: https://ssi.armywarcollege.edu/pdffiles/PUB1050.pdf [Accessed: 27th October 2018]; Thomas 1998a & 1998b. According to Komov, the drafting of the Information security concept started already in 1995 (Комов 1998).

of the Russian state and concentrated on information-psychological aspects; the FAPSI was interested in technological threats and security and defined IW as war (voina) using information technology;[798] the FSB was interested in regulating the Internet for internal security reasons; and the military was interestingly more interested in psychological (moral spiritual) issues than technological. However, the military saw the technological aspects of IW as belonging to wartime counter-C2 warfare and EW.[799]

The idea of struggle was present in the national security documents of the new Russian Federation. In the Foreign Policy Concept of 1993 Russia first dissociated itself from "obsolete ideas about the confrontation [protivoborstvo] of the "two systems" as a guideline of our foreign policy"[800] but recognized the continuing contradictions/conflicts (protivorechie) between governments and opposing (protivopolozhnoe) interests, and reserved for itself the ability to resist and counter (protivodeistvovat') other governments.[801] The Basic Provisions of the Military Doctrine of the Russian Federation from 1993 did not mention confrontation or struggle nor information except implicitly when discussing the military-technological needs of military.[802] A more assertive approach was affirmed in the National Security Concept (NSC) of 1997, which also claimed that 'other governments' tried to counter (protivodeitsvovat') Russia's strengthening through various non-military means. It also recognized Russian interests in the 'information sphere' (informatsionnaia sfera). Respectively, information threats were compared to military threats but were considered to mainly have a spiritual or psychological effect. Additionally, the NSC warned about a threatening technological backwardness which might lead to economic and military weakness.[803]

The national security documents published in 2000 echoed earlier views. The NSC of 2000 further elaborated the means used against Russia by introducing the concept of

[798] According to the First Deputy of the General Director of FAPSI Vladimir Markomenko, information war had become a priority issue for national security because 1) the destruction and disorganization of the information infrastructure of the country on the scale of weapons of mass destruction was possible, 2) the interstate struggle had shifted to the information sphere, and 3) information weapons had become available to criminals and terrorists in addition to nation states. Маркоменко, Владимир. Невидимая затяжная война. Независимое военное обозрение, № 30 1997.

[799] Thomas 1998a & 1998b.

[800] The national security documents of the Russian Federation from 1991 to 2000 have been published in a monograph by the Ministry of Foreign Affairs. This monograph is used as a primary source in this Chapter as the national security documents of the 1990s are poorly available from other sources and the monograph is published by an authoritative source. The monograph in question is Шаклеина, Т.А. (Сост.) Внешняя политика и безопасность современной России. 1991-2002: Хрестоматия в 4-х т. T.IV: Документы. М.: Моск.гос.ин-т междунар.отношений (ун-т) МИД России, Российская ассоциация международных исследований, АНО "ИНО-Центр" (Информация. Наука. Образование), 2002. Основные положения концепции внешней политики Российской Федерации утверждены Распоряжением Президента Российской Федерации Б.Н. Ельцина от 23 апреля 1993 г. (Шаклеина 2002, 20).

[801] Ibid.

[802] Известия. Основные поло жения военной доктрины Российской Федерации». ноября 1993 года Совет безопасности Российской Федерации одобрил доработанный документ. Указом Президента Российской Федерации от 2 ноября 1993 года № 1833 «Основные положения военной доктрины Российской Федерации» приняты. 18th November 1993. Izveztiia 1993 No. 221 [Online]. Available: https://yeltsin.ru/uploads/upload/newspaper/1993/izv11_18_93/FLASH/index.html [Accessed: 14th November 2018].

[803] Концепция национальной безопасности РФ 1997 г. (Шаклеина 2002, 59, 60).

a struggle or confrontation in the information sphere (protivoborstvo v informatsionnoi sfere).[804] The idea of an information struggle or confrontation was reiterated also in the Military Doctrine and in the Information Security Doctrine of 2000.[805] It should be noted that the idea was not defined in any of the documents and the Russian term 'protivoborstvo' was only used in the context of information. The term counter action or measure (protivodeistvie) was used to describe concrete actions related to the information space and other threats and environments. The Military Doctrine claimed that the military-political situation was characterized by aggravation of information confrontation and that hostile information-technological and information-psychological (informatsionno-tekhnicheskii, informatsionno-psikhologicheskii) actions were a threat to Russia.[806] Interestingly it defined information warfare (informatsionnaia bor'ba) as a wartime activity which was aimed at gaining information superiority in the initial period of war.[807] The foreign policy concept of 2000 was very different in its tone emphasizing shared global information space and promoting Russian views, although, it did connect information security to strategic stability.[808]

The most interesting case is of course the Information Security Doctrine of 2000. It follows the NSC and declares that a confrontation or struggle in the information sphere (protivoborstvo v informatsionnoi sfere) in currently ongoing.[809] It defines the information sphere as "an aggregate of information, information infrastructure, entities engaged in the collection, formation, dissemination and use of information, as well as a system for regulating the resulting social relations."[810] Information security is seen as elemental to the national security. It consists of the protection of the balanced interests of individuals, society, and the state. The state interests include territorial integrity, sovereignty, political, social, and economic stability, and cooperation based on equality.[811] Threats against information and telecommunications systems include the destruction, damage, or electronic suppression of information processing equipment and systems, telecommunications and communications, compromised encryption systems, etc.[812] Threats to Russian interests arise mainly from the actions of other states whose policies harm the development of the Russian ICT industry and who have developed the 'dangerous concept' of an information war (informatsionnaia voina). Threats originate also from the poor state of industry, criminality, insufficient domestic regulation and government institutions.[813] The Doctrine recognizes that the use of foreign information technology has led to a growing threat of 'information weapons' being used against 'information infrastructure' of Russia.[814] In fact, the Doctrine has both a civilian and military character as the security and protection of information systems is defined to include both civilian and military systems from peacetime to wartime.[815] Among the methods of securing information security, the Doctrine proposes the creation of a system of information security including monitoring,

[804] Концепция национальной безопасности РФ 2000 г. (Шаклеина 2002, 88).

[805] Военная доктрина Российской Федерации 2000 г. (Шаклеина 2002, 125).

[806] Военная доктрина Российской Федерации 2000. (Шаклеина 2002, 93, 101-102).

[807] Ibid., 96.

[808] Концепция внешней политики Российской Федерации 2000 г. (Шаклеина 2002).

[809] Доктрина информационной безопасности РФ 2000. (Шаклеина 2002, 125).

[810] Ibid., 122.

[811] Ibid., 124-125.

[812] Ibid., 127.

[813] Ibid., 129

[814] Ibid., 130.

[815] Ibid., 131.

protection, prevention, and certification functions.[816] The Doctrine names the prohibition of the development, dissemination and use of 'information weapons' as its main international agenda.[817] Arguably, the Information Security Doctrine of 2000 painted a picture of a Russian that was losing the control of its information sphere.[818] Previous studies on Russian strategic and political culture have observed that there is a persistent tendency to perceive international relations as a continuous great power struggle. The reasons given for this struggle differ and include, among others, messianism, imperialism, status competition, nationalism, geopolitics, balance-of-power realism, nature of domestic system (i.e. the sistema), bureaucratic interests, the mentality of 'the siloviki'[819] and the personality of leaders.[820] Consequently, it is argued, there is an inherent feeling of insecurity built into the Russian strategic thinking which has ebbed and flowed throughout its history. Therefore, the strategic cultural idea of an interstate struggle with its latest incarnation of 'information struggle' fits quite well into the wider Russian strategic cultural thinking.[821] It has functioned as a causal or perhaps even a principled belief by proving a framework for understanding international relations during and after the Soviet era. It connects and collects under it a group of more causal beliefs which provide ends, ways and means to manage those relations—these are basically the rest of the strategic cultural ideas analysed in this thesis. The language used in the national security documents of the 1990s differed from the more radical ideas presented by the military and civilian academics but there was clearly some resonance. The policy documents were, of course, the end-result of

[816] Ibid., 133.

[817] Ibid., 145.

[818] The authors of the 2000 Information Security Doctrine Vladislav Sherstiuk and Anatoly Streltsov argued that the doctrine was not aimed at restricting independent media but that the state must, nevertheless, be able to supervise all media. (Thomas 2010, 274). General Colonel Vladislav Sherstiuk is an ex-KGB officer, ex-FAPSI director and the current Adviser of the Security Council of Russian Federation, Director of Lomonosov Moscow State University Institute of Information Security Issues. Colonel Anatoly Streltsov is ex-officer, ex-head of Information Security Department of the Security Council of the Russian Federation and current Deputy Director of the Institute of Information Security Issues at Lomonosov Moscow State University.

[819] The term siloviki has no clear definition. Meakins has defined it as "referring to an active-duty officer or otherwise important individual in Russia's key security agencies: the FSB, FSO, MVD, SKR, SVR, GRU, Procuracy, and the new National Guard." (Meakins, Joss I. Squabbling Siloviki: Factionalism Within Russia's Security Services, International Journal of Intelligence and Counter Intelligence, Vol. 31, No. 2 (2018), 235-270, 238).

[820] Godzimirski, Jakub M. Russian national security concepts 1997 and 2000: A comparative analysis, European Security, Vol. 9, No. 4 (Winter 2000), 73-91; Donaldson, Nogee, & Nadkari 2014; Soldatov & Borogan 2010; Blank 2011; Monaghan, Andrew. Defibrillating the Vertikal? Putin and the Russian Grand Strategy, Chatham House Research Paper, October 2014; Galeotti, Mark. Heavy Metal Diplomacy: Russia's Political Use of Its Military in Europe Since 2014, ECFR, December 2016; Bateman 2014; Engström, Maria. Contemporary Russian Messianism and New Russian Foreign Policy, Contemporary Security Policy, Vol. 35, No. 3 (2014), 356-379; Gustafson, K. C. Echo of Empires: Russia's Inheritance of Byzantine Security Culture. The Journal of Slavic Military Studies, Vol. 23, No. 4 (2010), 574-596; Jackson 2002; Bratersky, Maxim. The Evolution of National Security Thinking in Post-Soviet Russia. Strategic Analysis, Vol. 40, No. 6 (2016), 513-523; Lukin, Vladimir. The Foreign Policy of Post-Soviet Russia: A Quest for Identity, Strategic Analysis, Vol. 40, No. 6 (2016), 486-497; Baev, Pavel K. Defying That Sinking Feeling: Russia Seeks to Uphold Its Role in the Multi-structural International System in Flux. In Blank 2012, 1-24; Vendil Pallin, Carolina. The Russian Power Ministries: Tool and Insurance of Power, Journal of Slavic Military Studies, Vol.20, No.1 (2007), 1-25; Eitelhuber 2009; Sondhaus 2006; Ledeneva, Alena V. Can Russia Modernise? Cambridge: Cambridge University Press, 2013.

[821] Kier Giles, for example, claims that Russian information policy flows from a feeling of vulnerability (Giles 2011). As do Martti Kari and Katri Pynnöniemi (Kari, Martti J. and Pynnöniemi, Katri. Theory of strategic culture: An analytical framework for Russian cyber threat perception, Journal of Strategic Studies, 2019 DOI: 10.1080/01402390.2019.1663411)

bureaucratic processes and compromises during a time when Russian domestic politics were highly volatile.[822]

Moreover, it can be argued that the translation of 'informatsionnoe protivoborstvo' as information warfare has distorted the Western understanding of Russian thinking on the use of information for political and military goals. The information confrontation or struggle is a political-strategic level concept with its roots in Marxist-Leninist thought.[823] It is not war or warfare but a constant struggle to influence the opponent with technological and psychological means. The technological and more destructive means gain primacy when interstate relations move into the initial period of war and war proper. This latter phase is clearly reminiscent of the Western views of counter C2, IW and cyber warfare concepts. During the 1990s Russian theorists, civilian and military, began to 'fit' modern ideas of IW to previous Soviet ideas about information, technology, politics, and warfare. Nevertheless, during the 1990s there was no single accepted definition of IW or information confrontation in the Russian discourse. Additionally, by the end of the 1990s civilian (or semi-civilian as many had a KGB-background) theorists had started to take part in the discussion and to formulate Russian theories of IW. The struggle for the meaning of IW was arguably a struggle for institutional interests and resources.[824] The ideas were eventually taken up by the security and defence elites and were reflected in the national security documents of 2000.

4.2.2 Strategic deterrence

Mary Fitzgerald wrote in 1986 that "[to] enter the world of Western Sovietology is to enter a debate as endless as Lenin's Collected Works."[825] She was stating this in a context of trying to understand the Soviet nuclear strategy but the same might be said about the current discussion on the Russian nuclear strategy.[826] Fitzgerald and later William E. Odom have claimed that during the Cold War the Western analysts were divided into those who thought that the Soviets shared the Western understanding of deterrence theory and mutually assured destruction (MAD) and to those who believed that the Soviets were preparing to fight a nuclear war.[827] Be that as it may, the problem for the Soviet political leadership was that nuclear weapons threatened to freeze the 'struggle' against capitalism which was the underpinning of their ideology.[828]

The political calculus changed after the 27th Party Congress of CPSU in 1986 after which the officials under Gorbatchev adopted the concept of 'defensive' or 'reasonable sufficiency'.[829] It was an implicit denouncement of the Western version of mutual

[822] On the politics of the Yeltsin era cf. Sakwa 2008.

[823] This claim is supported, among others, by Lalu (Lalu, 2014).

[824] On the Russian political system cf. Brannon, 2009, 165-166; Sakwa 1998; Soldatov & Borogan 2010; Ericson et al. 1998; Breslauer et al. 2000.

[825] Fitzgerald, Mary. Changing Soviet Doctrine on Nuclear War. Research memorandum AD-A187 722. Alexandria, Virginia: Center for Naval Analyses, 1986.

[826] Adamsky, Dmitry (Dima). Russian Nuclear Incoherence. Journal of Strategic Studies, Vol. 37, No. 1. (2014), 91–134; Oliker, Olga. Russian Nuclear Doctrine. Washington, DC: CSIS, 2016; Adamsky 2018; Tertrais, Bruno. Russia's Nuclear Policy: Worrying for the Wrong Reasons, Survival, Vol.60, No.2 (2018), 33-44.

[827] Fitzgerald 1986; Odom 1998, 66, 86. The dispute was also related to the argument between those who supported the idea that there was a Soviet strategic culture which influenced decision-making and those who approached the Soviets through rational actor-based game-theories (Gray 1992).

[828] Odom 1998, 67.

[829] Odom 1998, 106-107.

deterrence (i.e. MAD).[830] Testimonial evidence gathered after the end of the Cold War indicates that "Unlike their U.S. counterparts, the Soviets did not develop an elaborate doctrine of deterrence enhanced by various strategies of nuclear use, selective targeting, planned and deliberate escalation, etc."[831] The Soviets relied on massive retaliation, accepted the possibility of nuclear war and prepared for it, and aimed for superiority in nuclear arms up until the latter half of the 1980s. Nuclear deterrence was never seen as stable. Parity and balance were only theoretical concepts as power relations were constantly changing because of technological advances.[832]

The challenge of understanding the Soviet military thinking on deterrence was that the Soviets did not use the concept in the same way as Western theorists.[833] The term most similar was 'sderzhivanie putem ustrashenie' which refers to deterrence (restraining or holding back) through intimidation by nuclear weapons.[834] 'Sderzhivanie' was defined as a deterrence by containment, when referring to Americans, or dissuading an enemy from a decision to attack as a result of one's acquisition of a capability to retaliate with devastating effect, when referring to the Soviets.[835] 'Ustrashenie' is defined as deterrence through intimidation. It is used to frighten someone via fear. Moreover, 'prinuzhdenie' refers to forcing or coercing but does not have the same meaning as Western coercion.[836] Deterrence was to be achieved through "parity" which enabled nuclear retaliation.[837] However, the Soviet military was open to the pre-emptive, launch on warning, and retaliatory use of nuclear weapons as the situation demanded.[838] On the conventional side, the Soviet Union relied on quantitative superiority in military material and personnel and an offensive doctrine which would deter any aggression and enable counterattack in the event that the Soviet Union would be surprised by the West or the Chinese.[839] The organization and doctrine of conventional forces were modified to respond to the changes in technology and doctrine of the probable adversary.[840]

In the 1980s Soviet military theorists concentrated on analysing the initial period of war which gained new importance as the defensive doctrine was being adopted. The problem was, how to deter a surprise attack with forces in a defensive posture and then to mobilize for counterattack and assure mutual destruction if needed.[841] Surprise was connected to deception and disinformation, i.e. maskirovka.[842] Based on what

[830] Allison, Roy. Reasonable Sufficiency and Changes in Soviet Security Thinking. In Frank & Gillette 1992, 237-267; Odom 1998, 106.
[831] Hines, Mishulovich & Shull 1995a, 12.
[832] Ibid., 17.
[833] Hines et al. 1995b, 108.
[834] Hines 1995b, 6; Ven Bruusgaard 2016.
[835] Garthoff 1990, 22
[836] Thomas 2015a, 112; Ven Bruusgaard2016, 8; Adamsky 2018, 3.
[837] Podvig, Pavel. The Window of Vulnerability That Wasn't: Soviet Military Build-up in the 1970s—A Research Note. International Security, Vol. 33, No. 1 (Summer 2008), 118-138.
[838] Battilega, John A. Soviet Views Of Nuclear Warfare: The Post-Cold War Interviews. In Sokolski 2004, 151-174.
[839] Glantz 1992, 203-207; Odom 1998, 70-71; Kokoshin 1998, 177-180; Adamsky 2010.
[840] First to the nuclear weapons of the United States and then to the high-tech war envisioned in the Western Air Land Battle and Follow-on Forces Attack doctrines. Odom 1998, 72-80; Adamsky 2010, 33-34; Lalu 2014.
[841] Kokoshin 1998, 189-190.
[842] On the concept of maskirovka cf. Beaumont, Roger. Maskirovka: Soviet Camouflage, Concealment and Deception. Texas: Center for Strategic Technology, The Texas Engineering Experiment Station of the Texas ASM University System, 1982; Chotikul, Diane. The Soviet Theory of Reflexive Control in Historical and Psychological Perspective: A Preliminary Study. Monterey, CA: Naval Postgraduate School, 1986.

military officers wrote in the Voennaia mysl' journal in the 1970s and 1980s the fear of being surprised was indeed discussed among the high rank officers. Additionally, a future war was considered total and nuclear weapons were thought to be used eventually. This emphasised the need for either a strategic or operational surprise.[843] The role of strategic nuclear weapons was to 'prevent' inherently 'aggressive' capitalist countries from attacking. The economy had to be geared towards the future war and for the needs of the armed forces because otherwise 'a gap' in capabilities would open and enemies would use it to attack.[844] In this context, the Western deterrence (ustrashenie) was a form of 'nuclear blackmail' directed against socialist countries and was seen as a cover-up for building offensive forces.[845]

On the political level, the Soviet leadership tried from the 1970s onwards to avoid a nuclear war and to constrain their enemy and from 1980s onward to limit the economically disastrous arms race through international arms control treaties, conventional and nuclear force reductions and other military-political activities.[846] In addition to the military and political elements, there was a definite informational element in deterrence that, on the one hand, promoted a view of the Soviet Union as a non-aggressive super power and, on the other hand, produced enough ambivalence to keep the Western decision-makers guessing about the Soviet strategy.[847] This informational element had also an internal component based on protecting Soviet citizens from Western propaganda through censorship, counterpropaganda, restrictions on movement and communication, and the pursuit of dissidents by the KGB.[848] It included the jamming of Western radio and TV transmissions, and the physical control of a handful of fixed international phone lines and switches.[849] Moreover, the Soviet Union managed and maintained a global network of ideologically aligned allies, for political and military reasons, and a commitment to protect those allies—or more

[843] Gudz, P. The Modern Theory of Tactics and Some of its Problems. Military Thought – Secret version 1970, No. 2 (90). Translated and published by the Central Intelligence Agency, Intelligence Information Special Report, 14th January 1974 [Online]. Available https://www.cia.gov/library/readingroom/docs/CIA-RDP85T00875R000300010016-7.pdf [Accessed: 5th December 2018]; Gayvoronskii, F. New Questions of Operational Art at Its Present Stage of Development. Military Thought – Secret version 1970, No. 1 (89). Translated and published by the Central Intelligence Agency, Intelligence Information Special Report, 7th March 1974 [Online]. Available https://www.cia.gov/library/readingroom/docs/DOC_0001199073.pdf [Accessed: 5th December 2018].

[844] Povaliy, M. Military Strategy and Economics. Military Thought – Secret version 1971, No. 4. Translated and published by the Central Intelligence Agency, Foreign Press Digest, 25th March 1974 [Online]. Available: https://www.cia.gov/library/readingroom/docs/1974-01-14.pdf [Accessed: 5th December 2018].

[845] Средин, Г. В. Проблема войны и мира в современной идеологической борьбе. Военная мысль № 7 1986, 3-13.

[846] Menning 1992, 53; Garthoff 1992, 199-201; MccGwire 1987, 266-267; Garthoff 2002, 151.

[847] Gelman, Harry. Reconstructing the Soviet Perspective on U.S. Global Policy. In Nerlich, Uwe (ed.) Soviet Power and Western Negotiating Policies. Volume I: The Soviet Asset: Military Power in the Competition Over Europe. Cambridge, Massachusetts: Ballinger Publishing Company, 1983, 277-305; Service 2015, 93-101; Gaddis 2005, 184-188; The United States Department of State. Soviet "Active Measure". Forgery, Disinformation, Political Operations. October 1981 [Online]. Available: https://www.cia.gov/library/ readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf [Accessed: 15th November 2018]; Schoen, Fletcher and Lamb, Christopher, J. Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference. INSS Strategic Perspectives 11. Washington, DC: National Defense University.

[848] Service 2015, 77-83; Gaddis 2005, 184-188; Sakwa 1998; Haslam 2015, 15-26 & 268; Knight, Amy. The KGB, Perestroika, and the Collapse of the Soviet Union. Journal of Cold War Studies Vol. 5, No. 1, (Winter 2003), 67–93.

[849] Soldatov & Borogan 2015.

precisely their socialist/communist regimes.[850]

Some Western scholars have argued that the current Russian security and defence policy is based on the so-called Soviet era 'besieged fortress' syndrome.[851] According to Andrei Kokoshin, the concept was developed by Mikhail Frunze, a Bolshevik military leader and theorist, who wrote that "our country continues to be like a besieged fortress, and it will remain in this position as long as capital prevails in the world."[852] Conversely, Bobo Lo claims that the term 'besieged fortress' was first used by Lenin in a Pravda article from August 22, 1918.[853] In any case, the concept became to mean that the Soviet security and defence policy was highly sensitive to both external and internal threats, both real and imagined, and that it had a decidedly geopolitical view of security.[854] A part of this worldview emanated from the belief that in its history Russia/the Soviet Union had been a victim of repeated aggression, the other part was based on Marxism-Leninism and the inevitability of war.[855] As Eliot Borenstein argues, this kind of thinking fits quite naturally with the long tradition of Russian conspiracy theories which the regime has, at least tacitly, encouraged.[856] Such a conspiratorial worldview would have produced its own type of deterrence thinking—presumably something that would have tried to keep threats as far away from the Soviet borders as possible and tried very actively to prevent any internal or external threats from materializing. It is also quite easy to understand how through this kind of perspective the fall of the Soviet Union can be interpreted as a tragedy which external and internal enemies could be blamed for.[857]

After the fall of the Soviet Union, the Russians began to copy Western ideas about deterrence but did not produce any coherent domestic theory during the 1990s. Dmitry Adamsky claims that the Russian professional discourse began to use the terms coercion, deterrence and compellence interchangeably, and that there was no established term for coercion which would serve as an umbrella term for both deterrence and compellence.[858] By the end of the 1990s, deterrence referred to preserving the status quo mainly reactively, whereas compellence, or 'prinuzhdenie', referred to the efforts to change the status quo. Thomas and Kristen Ven Bruusgard argue that 'ustrashenie' is defined as deterrence through intimidation. It is used to frighten someone via fear and resonates with the Cold War era understanding.[859] According to Ven Bruusgard and Dmitry Adamsky the Russian deterrence 'theory' has gone through

[850] McCauley 1981; MccGwire 1987; Gaddis 2005; Westad 2017, 487, 489.

[851] Trenin 2001; Blank 2008; Jackson 2002; Kari & Pynnöniemi 2019; Jonsson 2019, 41.

[852] Kokoshin 1998, 66-67. Harriett Fast Scott and Williams F. Scott provide a direct quotation from Frunze: "our country is in the situation of a besieged stronghold and will remain there as long as capital reigns in the world…" Scott & Scott 2019, 8.

[853] Lo 2015, 245.

[854] Trenin 2001; Yablokov 2018; Blank 2008; Blank, Stephen. Can Russia Sustain Its Military Capability? Jamestown Foundation, 13th September 2016 [Online]. Available: https://jamestown.org/program/stephen-blank-can-russia-sustain-its-military-capability/ [Accessed: 15th November 2018]; Sondhaus 2006.

[855] Glantz 1992; Jonsson 2019.

[856] Borenstein, Eliot. Plots against Russia. Conspiracy and Fantasy after Socialism. Ithica and London: Cornell University Press, 2019, 239-240.

[857] Myers 2015, 278-290; Lo 2015, 20; Hill, Fiona. How Vladimir Putin's World View Shapes Russian Foreign Policy. In Cadier & Margot 2015, 42-61, 48-49.

[858] Adamsky 2014.

[859] Thomas 2015a; Ven Bruusgaard 2016; Adamsky, Dmitry (Dima). Cross-Domain Coercion: The Current Russian Art of Strategy. Proliferation Papers, No. 54, November 2015.

three stages.[860] The first from 1991 to 2000 was a response to the Western technological superiority and Russia's own conventional weakness which led to the emphasis of nuclear weapons as guarantees of security and great power status. By 1999, military scholars were figuring out how nuclear weapons could be used to deter a conventionally superior adversary. The second stage from 2000 to 2010 consisted of combining nuclear and conventional capabilities to deter nuclear and conventional threats including actual exercises. The third stage from ca. 2010 onward introduced 'strategic deterrence' which included non-nuclear and non-military components.[861]

The Russian unofficial military debate on deterrence at the beginning of the 1990s associated the term 'strategic' primarily with nuclear weapons but also used the term in the context of strategic stability (strategicheskaia stabil'nost') the meaning of which was debated. It had meant nuclear parity between the United States and the Soviet Union during the Cold War, but the security environment and Russia's posture and composition of forces did not anymore reflect or support that interpretation.[862] Especially the United States' performance in the Gulf War and the use of high technology weapons forced the Russian military to think again about the role of the non-nuclear high-tech forces in deterrence.[863] In 1998 Major General Lyzianin defined the previous understanding of the strategic stability as: "a state of military power of the parties in which none of them can achieve their military-political goals by aggression without unacceptable consequences for themselves as a result of the response of the other."[864] According to Lyzianin, this concept should have been modified to support Gorbachev's idea of 'sufficient defence'. It meant a minimum defence strength that would not provoke adversaries but ensured the deterrence of aggression, and in the case deterrence failed, the repulsion of aggression.[865]

In 1996 Andrei Kokoshin, then the vice defence minister, wrote that the 'nuclear shield' was more important than other means to prevent aggression. The main function of the armed forces was the deterrence (sderzhivanie) of aggression against Russia. This deterrence was based on the demonstration of Russia's material capacity and the readiness of the government to use it.[866] The problem was of course that nuclear weapons might not be usable in the current and future regional or local wars as Makhmut Gareev argued.[867] As the importance of information warfare grew towards the end of the 1990s, Rear-Admiral Pirumov and Colonel M. A. Rodionov implicitly supported the view that deterrence was connected to lethal weapons, although infor-

[860] Ven Bruusgaard 2016; Adamsky 2018.

[861] Ven Bruusgaard 2016; Adamsky 2018.

[862] Погожин, В. П. Система управления стратегическими силами и стабильность. Военная мысль № 8-9, 1992; Шаравин, А. А. Стратегическая стабильность в Европе системный аспект. Военная мысль № 2 1992; Кириленко, Г. В., Тренин, Д. В. Формула безопасности от паритета к стратегической стабильности. Военная мысль № 8-9 1992.

[863] Fitzgerald, Mary C. The Soviet Image of Future War: The Impact of Desert Storm. In Frank & Gillette 1992, 363-386, 382.

[864] Лузянин, В. П. Стратегическая стабильность и многополярная модель сдерживания. Военная мысль № 8-9 1998.

[865] Ibid. Cf. also Pirumov, V. S. Two Aspects of Parity and Defensive Sufficiency. Military Thought No. 2 1992; Fitzgerald, Mary C. The Dilemma in Moscow's Defensive Force Posture. In Frank & Gillette 1992, 347-362; Odom 1998, 171; For Soviet discussion on this subject in late-1980s Cf. Hines & Mahoney 1991.

[866] Кокошин 1996.

[867] Гареев 1998.

mation in its wider, confrontation/struggle aspect was seen as a way to influence opponents.[868] In 1998 General Major Iu. A. Nikolaev, Colonel V. P. Pchelianoi and Professor V. I. Tsymbal claimed that the weapon systems of the armed forces should consist of the means of nuclear deterrence to deter nuclear and non-nuclear opponents and means of non-nuclear deterrence to deter aggressors of local and small intensity conflicts—including information warfare.[869] Moreover, they argued that means of information warfare could perhaps be used to deter the enemy or demoralize it 'without a single shot'.[870] This utility of information in preventing (predotvrashenie) wars, among other non-direct means, was shared by M. A. Gareev.[871] The widening of the substance of deterrence was also reflected in the 'escalate to de-escalate discussion', i.e. the use of (mainly) tactical nuclear weapons to control regional or wider conflicts.[872]

In 1999 two academics of the Russian Academy of Sciences Evgenii Fedosov and Igor' Spaskii claimed that the meaning of 'strategic deterrence' (strategicheskoe sderzhivanie) now included deterring a nuclear attack and serious non-nuclear attack. For Fedosov and Spaskii, deterrence included the effectiveness of the threat of retaliation, the credibility of the threat, and the adversary's awareness of the consequences of a retaliatory strike. This definition shows how much Western concepts of deterrence had affected the Russians by the end of the 1990s.[873] The emphasis on nuclear deterrence in the Military Doctrine of 2000 also generated discussion on the survivability of nuclear weapons which led to the argument that deterrence was based on, among other things, resilient command and control systems.[874] By the end of the 1990s, military professionals and academicians doubted the sufficiency of pure nuclear deterrence as the guarantor of Russian military security and saw deterrence as consisting of something more than pure nuclear means.

The Basic Provisions of the Military Doctrine of the Russian Federation from 1993 uses the term 'deterrence' (sderzhivanie) in relation to preventing both nuclear and conventional aggression against Russia. This is achieved through civilian and military intelligence, the ability to retaliate with nuclear weapons, and the ability to repulse an aggressor with conventional forces.[875] The NSC of 1997 connects 'deterrence' more clearly to nuclear weapons which are the basis of Russia's security—their existence

[868] Pirumov, V. S. and Rodionov, M. A. Information Warfare in Armed Conflicts. Military Thought [English] No. 5 1997.

[869] Николаёв, Ю.А. Пчеляной, В.П., Цымбал, В.И. Реформирование Вооруженных Сил и система вооружения. Военная мысль 1998 № 2, 27-32, 29.

[870] Николаёв, Пчеляной & Цымбал 1998, 32.

[871] Гареев 1998.

[872] Левшин, В. И., Неделин, А. В., Сосновский, М. Е. О применении ядерного оружия для деэскалации военных действий. Военная мысль № 3(5-6) 1999, 34-37; Крейдин, С.В. Глобальное и региональное ядерное сдерживание: к системе принципов и критериев. Военная мысль 1999 No. 4; Сиволоб, Владимир Федорович, Сосновский, Михаил Евгеньевич. Реальность сдерживания. Независимое военное обозрение № 41 1999.

[873] Федосов, Евгений Александрович, Спасский, Игорь Дмитриевич. Высокоточное оружие заняло место бога войны. Независимое военное обозрение № 28 1999.

[874] Крейдин, С.В. Дискуссионная трибуна. Проблемы ядерного сдерживания: боевая устойчивость ядерного потенциала. Военная мысль No. 4 1999; Рукшин, А.С. Геополитика и безопасность. Ядерное сдерживание: совершенствование системы управления ядерными силами. Военная мысль № 6 2000; Сиволоб & Сосновский 1999; Воронин, Станислав Николаевич, Брезкун, Сергей Тарасович. Стратегически выгодная асимметрия. Независимое военное обозрение № 36 1999.

[875] Izveztiia 1993.

prevents war. The concept also states that Russia does not strive for parity with leading states and accepts the principle of 'realistic deterrence'.[876] The NSC of 2000 states that the most important mission of the armed forces is to implement deterrence to prevent aggression of any scale against Russia or its allies.[877] The Military Doctrine of 2000 further states that the Russian nuclear deterrence is a positive force for security and that Russia "will maintain its status as nuclear great power to deter (prevent [predotvrazhenie]) aggression against itself or its allies." The main priority of developing the military organization are "the forces providing strategic deterrence [strategicheskoe sderzhivanie] (including nuclear)." Russia maintains conventional and nuclear forces in constant readiness to deter and repulse (otrazhenie) aggression.[878] No official definition of strategic deterrence was offered, although, in 2000 Putin related it to the wider concept of preventing war. According to Putin, almost all state agencies took part in preventing war.[879] The term compellence (prinuzhdenie) appears in the Foreign Policy Concepts of 1992 and 2000 and the Military Doctrine of 2000 in a connection to internationally sanctioned peace enforcement (prinuzhdenie k miru) and seems to be a direct translation from the English term.[880] It is not so much about changing status quo than making the opponent to change his behaviour by incurring costs.[881] The primary security documents of the Russian Federation from 1993-2000 do not use the term intimidation (ustrashenie).

The concept of deterrence was adopted into the Russian unofficial and official discourse during the 1990s and experienced a definite expansion of substance at the informal level. The concept of 'strategic deterrence' was introduced but its official elaboration would be left to the 2000s. Deterrence has a clear connection to the concept of interstate struggle and its sub-concept of information struggle: from the 1980s onward to 2000 nuclear parity and later 'defensive sufficiency' were increasingly accompanied first by conventional and then by other means of deterrence, prevention, and repulsion of armed aggression (or other threats to state interests). Although Russian military thinkers strived to separate war and political competition and confrontation from each other they were more and more inclined to argue that Russia had to 'deter' a wide range of hostile measures with more active countermeasures even during peacetime. This 'deterrence' was influenced by the debate over the advantages between an offensive and defensive doctrine as the borders between offence and defence became increasingly hazy in the context of the future war.

4.2.3 Asymmetric response

The term asymmetry was first used in the context of conventional arms reductions in Europe in the 1980s before it became to define the Soviet 'asymmetric response' to Ronald Reagan's Strategic Defence Initiative (SDI) in 1986 and long before it became a kind of 'deux-ex machina' concept of solving the Russian military backwardness in

[876] Концепция национальной безопасности РФ 1997. (Шаклеина, 2002).

[877] Концепция национальной безопасности РФ 2000 г. (Шаклеина, 2002).

[878] Военная доктрина Российской Федерации 2000 г. (Шаклеина, 2002).

[879] Президент Российской Федерации. Выступление на совещании руководящего состава Вооруженных Сил Российской Федерации, 20 ноября 2000 года [Online]. Available: http://kremlin.ru/events/president/transcripts/21119 [Accessed: 19th November 2018].

[880] Концепция внешней политики РФ 1992 г. (Шаклеина 2002); Концепция внешней политики Российской Федерации 2000 г. (Шаклеина 2002).

[881] Военная доктрина Российской Федерации 2000 г. (Шаклеина 2002, 102).

relation to the United States during the 1990s and 2000s.[882] However, the somewhat anachronistic interpretations of the claimed Soviet 'asymmetric response' to the United States' SDI must be put into a historical context and understood as a concept that has been purposefully revived in the 2000s in the context of a dispute between the Russian Federation and the United States about the latter's ballistic missile defence programme.[883]

In the Russian language 'asymmetry' means the 'absence, disruption of symmetry' (otsutstvie, narushenie simmetrii)[884] which, as Timothy Thomas remarked, implies a more active aspect in the change of symmetry's parameters than the American or British definitions, even the creation of asymmetry.[885] Thomas claims that the Russian dialectic thought process of thesis and antithesis encourages an analysis of a situation from a different, more confrontational perspective.[886] According to Thomas, asymmetry seems to be about off-setting an opponent's superiority, taking advantage of the opponent's unequal combat potential, avoiding direct confrontation, and deploying new and innovative forms and methods of conflict.[887] Dmitry Adamsky has studied Soviet/Russian strategic culture and argues that asymmetry has long historical roots in Russian strategic thought in the guise of 'military cunningness' (khitrost') or stratagems. It is an ability or attribute which multiplies or substitutes the direct use of force with deceit, surprise and indirect approach.[888] Adamsky also claims that the Russian theory of victory is asymmetrical because it is based on a strategy which plays one's strengths against the opponent's weaknesses. Nevertheless, the Russian strategy is also symmetrical because the nature of a threat shapes the response.[889] Currently, asymmetry is seen by Western scholars as an inherent part of Russian strategic thought and the making of strategy.[890] For example, Pynnöniemi and Forsström both argue that asymmetric measures are part of Russian deterrence and strategy to prevent war.[891]

[882] Cf. also Snyder, Jack. Limiting Offensive Conventional Forces: Soviet Proposals and Western Options. International Security. Vol. 12, No. 4 (Spring, 1988), 48-77; Becker, Michael E., Matthew S. Cohen, Sidita Kushi and Ian P. McManus. Reviving the Russian empire: the Crimean intervention through a neoclassical realist lens, European Security, Vol. 25, No. 1 (2016), 112-133; Grigas, Agnia. Beyond Crimea. The New Russian Empire. New Haven: Yale University Press, 2016; Porfiriev & Simons 2016; Trenin, Dmitri. Russia's Breakout from the Post-Cold War System: The Drivers of Putin's Course. Carnegie Moscow Center, 22 December 2014; McDermott 2015.

[883] Cf. Chapter 5. On missile defence debate cf. Arbatov, Alexei and Dvorkin, Vladimir (Eds.) Missile Defense: Confrontation and Cooperation. Moscow: Carnegie Moscow Center, 2013.

[884] 'Асимметрия' Ожегов, С.И., Шведова, Н.Ю. Толковый словарь русского языка. 4-е изд., доп. М.: ООО «А ТЕМП», 2006 [Online]. Available: https://dic.academic.ru/dic.nsf/ogegova/7566 [Accessed: 22nd March 2019]. A Soviet era encyclopaedia defines asymmetry as "an absence of symmetry" ('Асимметрия' Большой советской энциклопедии. М.:"Советская энциклопедия", 1969 – 1978 г. [Online]. Available: https://dic. academic.ru/dic.nsf/bse/65510/Асимметрия [Accessed: 22nd March 2019].

[885] Thomas 2005, 294-295. However, Thomas mistakenly translates 'narushenie' as destroy.

[886] Ibid., 294.

[887] Thomas 2015c, 445-461.

[888] Adamsky 2018.

[889] Adamsky 2015, 26.

[890] Cf. Covington, Stephen R. The Culture of Strategic Thought Behind Russia's Modern Approaches to Warfare. Cambridge: Harvard Kennedy School, Belfer Center, 2016; Defence Intelligence Agency. Russia Military Power: Building a Military to Support Great Power Aspirations [Online]. Available: http://www.dia. mil/Military-Power-Publications/ [Accessed: 20th November 2018]; Jonsson & Seely 2015; Norberg, Johan and Westerlund, Fredrik. Military Means for non-Military Measures: The Russian Approach to the Use of Armed Forces as Seen in Ukraine, The Journal of Slavic Military Studies, 2016 Vol. 29, No. 4, 576-601; Bukkvoll 2011, 690; Cooper 2016, 52.

[891] Pynnöniemi 2019a & Forsström 2019.

The Soviet military was aware of the technological ever-widening gap between itself and NATO's conventional forces in the early 1980s. Marshal Ogarkov and others had seen the coming of MTR and understood that doctrinal and organizational changes were not enough to counterbalance the Western advantage.[892] However, Ogarkov's call for comprehensive reform was rejected because of political, economic, strategic cultural, and bureaucratic reasons.[893] When the United States' president Ronald Reagan declared his Strategic Defence Initiative (a space-based ballistic missile defence system) the Soviet Union had to accept the technological challenge or lose the strategic parity it had strived to achieve the last two decades.[894]

In this context the Soviet civilian scientists declared that the SDI was practically impossible. In fact, Soviet scientists had studied a similar defensive system already in the 1960s and 1970s but their proposals were discarded.[895] Moreover, military theorists and politicians saw SDI as threatening the offence-defence balance, which would lead to further arms race and insecurity.[896] The Soviet leadership could not be sure if the SDI was in fact a cover for the offensive militarization of space.[897] Scientific 'proof' for these views was provided by the so-called 'institutchiki' or people from science institutions foremost among them Evgenii Velikhov, Aleksei Arbatov, and Andrei Kokoshin.[898] As president Ronald Reagan refused to let go of his project, General Secretary Gorbachev stated that the Soviet Union would give an 'asymmetric response'.[899]

This response was based partly on ballistic missile defences and hardened silos for ICBMs, space deployed defences, and exotic weapons such as lasers directed against American satellites, and partly on updating the strategic nuclear missiles (mainly SS-18) to be able to penetrate any defences the United States might be able to deploy, and partly on diplomatic measures.[900] The idea was to make SDI obsolete and preserve the retaliatory capabilities of Soviet strategic nuclear weapons.[901] Therefore, the 'asymmetric response' was at least partly based on the Marxist-Leninist oriented strategic dialectical thinking on historical arms development through cycles of measures and

[892] Kipp 2010; Adamsky 2008 & 2010; Fitzgerald 1987a.

[893] Blank, Stephen J. Preparing for the Next War: Reflections on the Revolution in Military Affairs. In Arquilla & Ronfeldt, 1997, 61-77; Adamsky 2008 & 2010; Menning, 1992, 53.

[894] Podvig 2008; Hoffman 2009; Green, Brendan R. and Long, Austin. The MAD Who Wasn't There: Soviet Reactions to the Late Cold War Nuclear Balance, Security Studies, Vol.26, No.4 (October-December 2017), 606-641.

[895] Kokoshin 1998, 182; Service 2015, 194.

[896] Kokoshin 1998, 181-182; Service 2015, 194-195. For analysis of this discussion cf. Fitzgerald 1987a.

[897] Service 2015, 194-195.

[898] Fitzgerald, Mary C. Soviet views on SDI. The Carl Beck Papers in Russian and East European Studies No. 601. Pittsburgh: University of Pittsburgh Center for Russian and East European Studies, 1987, 6.

[899] Hoffman 2009, 262. Gorbachev stated in a press-conference in Reykjavik on October 1986, "There will be an answer to the SDI. It will be asymmetrical, but nevertheless it will be an answer. And we don't have to sacrifice much." (Выступление генерального секретаря ЦК КПСС М. С. Горбачёва на пресс-конференции в Рейкьявике [Online]. Available: http://perestrojka.su/documents/1986/Reykjavik.htm [Accessed: 22nd March 2019].)

[900] Hoffman 2009, 215-216, 220; Service 2015, 195-196.

[901] Kokoshin 1998, 183. On Kokoshin cf. Fitzgerald 1987c. Kokoshin claims that the 'asymmetric response' was a 'military-political plan' including diplomatic, political and propaganda activities and programs for the development of weapon systems and for the needed scientific base. He argues that, although the concept was officially adopted, a 'symmetric response' i.e. conventional and nuclear arms race still continued until the fall of the Soviet Union. (Кокошин 2007).

countermeasures.[902] It was also compatible with the calculations about the correlation of forces by introducing extra 'asymmetric' variables. The military part of the 'response' was driven by the military and military-industrial complex. The diplomatic and political part was driven by Gorbachev and his circle of reformers. It consisted of the elimination of the threat through arms control measures, defensive doctrine, diplomacy, and propaganda—measures which would change the thinking of the opponent. It resulted into the Intermediate-Range Nuclear Forces Treaty (INF), the Strategic Arms Reduction Treaty (START I) and the Treaty on Conventional Armed Forces in Europe (CFE). The two versions did not fully support each other, and both contributed to the fall of the Soviet Union and the end of the Cold War.[903] Consequently, the 'asymmetric response' was dropped from the political vocabulary and practical policy when the military standoff between the Soviet Union and NATO ended in 1988-1989 and the new U.S. president George W. Bush pushed SDI to the side lines of his political agenda. Nevertheless, the Soviet military and military-industrial complex sought asymmetric responses up until the end of Soviet Union.[904]

Against the above presented background, it can be argued that the roots of 'asymmetry' are historically contextual. Andrei Kokoshin has claimed that the 'ideology of asymmetry' was born in the 1980s when he and some others rehabilitated Soviet military theorist A. A. Svechin's ideas of strategic defence and combined them with the ideas of ancient Chinese strategist Tzun Tsu.[905] The asymmetric response was an idea created by Soviet civilian scientists in a reinterpretation of Soviet military history which incorporated technological evidence—perhaps to package it to a more attractive form for the military.[906] This technique was also used when Kokoshin and Colonel General V. Larionov published an article based on historical analogies to argue for a defensive strategy in the 1988.[907]

Asymmetry was discussed implicitly by the Soviet military in the 1980s mainly due to the perceived destabilization of the military balance. For example, General Colonel Cherpov used the term when referring to force reductions in Europe.[908] In an article by a nameless writer in 1985 Voennaia Mysl' journal the U.S. SDI project was attacked as an effort to gain military-strategic superiority over the Soviet Union by militarizing space. If the United States continued with its plans the Soviet Union must "respond to restore the strategic balance" which might require either defensive or offensive measures which "will not be those that the United States tries to make the Soviet Union to take".[909] In 1986 General Major M. M. Kozlov, declared that the military-strategic parity between the Soviet Union and the United States guaranteed world peace. He defined this parity as the approximate equality of the military potentials of

[902] Fitzgerald 1987c, 19-20.

[903] Hoffman 2009, 215-216, 220; Service 2015, 195-196.

[904] Hoffman 2009.

[905] Ознобищев, Потапов & Скоков 2008. On the rehabilitation of Svechin cf. Glantz 1998.

[906] Kokoshin promoted the idea of the unfeasibility of SDI and the 'unexpected' answer of the Soviet Union if the United States continued to pursue SDI in military forums cf. Кокошин, А. А., Герасёв, М. И. Американские планы милитаризации космоса. Военная мысль № 4 1987, 69-80.

[907] Кокошин А. А., Ларионов В. В. Противостояние сил общего назначения в контексте обеспечения стратегической стабильности. Мировая экономика и международные отношения № 6 1988. The ideas presented by Kokoshin and Larianov were widely discussed at the time. Cf. Frank & Gillent 1992; Glantz 1998.

[908] Червов, Н. Ф. Разоружение: кто против? Военная мысль № 12 1983, 3-15.

[909] The article basically summarizes a propaganda leaflet from 1985 "Star wars": Illusions and dangers. (Военная мысль. «Звездные войны»: иллюзии и опасности. Военная мысль № 9 1985, 15-18.)

the opposing sides based on socio-economic, political and scientific-technical factors and expressed in the quantity and quality of weapons and military material and the strategic posture and organization of forces. Kozlov claimed that the Soviet Union with other 'fraternal peace-loving countries of socialism' would always respond to actions taken by the United States and NATO aimed at acquiring military superiority.[910] Apparently, this was something that some Soviet writers recognized the West claimed the Soviet Union was aiming for; which was 'of course' not based on any facts.[911] Military scientific and technological development were offered as tools to respond to the West's destabilizing efforts—Mikhail Gorbachev's words about asymmetric response were repeated, including the response's cost-effectiveness.[912] In 1987 Andrei Kokoshin wrote that the purpose of the SDI was to make nuclear war winnable and so to provide military superiority through space and to economically wear out the Soviet Union in an arms race.[913]

In the late 1980s these ideas and calculations about parity were disturbed by the adoption of a defensive Warsaw Pact doctrine followed by force reductions.[914] The military leadership had to convert the political idea of a 'sufficient defence' to fit with the idea of parity and to produce a doctrine and force structure that would still prevent surprise attack by the capitalists.[915] In this process asymmetry was related to the dissimilarity of the structure of military potential of the different sides. Possible force reductions could be replaced by enhancing the 'human factor', i.e. through skills instead of spending money on new weapons—thus the idea of low-cost solutions persisted.[916] The declared principle was that the Soviet Union would not strive for more security but would not settle for less.[917] In the end of the 1980s the term 'asymmetry' was almost exclusively connected to the calculations concerning strategic force-rations between peer competitors and to finding low-cost ways to undo the great power adversary's moves.[918]

During the 1990s the Russian military theorists used the term 'asymmetry' or 'asymmetric response' infrequently. Asymmetry appeared, for example, in the calculations of the correlation of forces between NATO and Russia and mathematical models of symmetric and asymmetric strategies.[919] General Gareev wrote implicitly about asymmetry when he claimed in 1995 that indirect actions expressed as political efforts to

[910] Козлов 1986. Marshal of the Soviet Union V. G. Kulikov defined parity in a military context as: "an approximate equality in the military power of the parties, above all in nuclear and other strategic means of warfare that are critical to the conduct of war, the main indicator of the ratio of the military forces of the parties, which we are forced to take into account when making decisions on political and military issues." (Куликов 1988).

[911] Дмитриев, А. П. Политика КПСС в области обороны и безопасности страны на современном этапе. Военная мысль № 4 1987, 58-68.

[912] Ibid.; Андреев, В. Ф. Военно-стратегический паритет — объективный фактор сдерживания агрессивных сил. Военная мысль № 2 1989, 45-53.

[913] Кокошин & Герасёв 1987.

[914] Odom 1998.

[915] Куликов 1988.

[916] Куликов 1988; Тюшкевич, С. А. Разумная достаточность для обороны: параметры и критерии. Военная мысль № 5 1989, 53-61.

[917] Ibid.

[918] For more Western views cf. Коротченко, Е. Г. Об эволюции принципов военного искусства. Военная мысль № 9 1988, 22-30

[919] Klokotov, N. P., Kasenkov, M. M. For the Question on Military Danger. Military Thought No. 8 1991; Bachkalo, B.I. and Ivanov, P.I. On the Question of Validating the Optimum Structure of a Ground Force Grouping. Military Thought No. 12 1993.

prevent war, surprise and misdirection in the event of war, and massing fire and manoeuvring to bypass the enemy, and using psychological and special operations during battles would be very much part of the future wars.[920] General Major Vladimir Dvorkin used asymmetry in 1997 when referring to the new intercontinental ballistic missiles (ICBMs) that the Soviet Union began to develop in response to the SDI but noted that this project was very expensive and progressed slowly.[921] In 1999 two academics from the Russian Academy of Sciences (RAN) Evgenii Fedosov and Igor' Spasskii argued that the development of long-range precision strike weapons had created an asymmetry in conventional forces which could lead to the lowering of the threshold of nuclear weapons use.[922] This ignited a debate about whether strategic nuclear weapons could provide an asymmetric response to mitigate the degraded state of the Russian military and the U.S. BMD programme.[923]

The First Deputy Defence Minister Nikolai Mikhailov argued in 1998/1999 that although Russia was economically weaker than the United States it had time and knowhow and should pursue 'the principle of asymmetry' in developing its military technology, i.e. not to strive to develop all capabilities towards parity but to asymmetrically concentrate on those in which the opponent was weak. This strategy would eventually lead the opponent to produce expensive countermeasures and further weaken him.[924] Ironically, this was exactly what Mikhail Gorbachev claimed Reagan had tried to achieve through his SDI project.[925] Mikhailov's ideas were echoed by the Minister of Defence Marshal I. D. Sergeev in 1998 when he argued "that in the coming years Russia will not be able to maintain military-strategic and military-technical parity with the leading military powers of the West on a 'symmetric basis' and that this required effective 'asymmetric development paths' (asimmetrichnoe napravlenie) of new military technology. This should be achieved through the optimal use of limited resources to produce new information technology-based weapons and ASUs. Ultimately, Russia should avoid "direct military-technological rivalry with the most developed countries by creating 'asymmetric' means of warfare. These would allow it to strike the most vulnerable functional elements of the main systems and key infrastructure of the enemy and thereby significantly devalue their military-technical advantages."[926]

Based on database searches (EastView) and the analysis presented above it would seem that the term 'asymmetry' was not widely used in military journals until the end of the 1990s.[927] Although the term 'asymmetry' could be used in connection to correlation of conventional forces, the 'asymmetric response' was usually connected to the

[920] Gareev, Makhmut. If War Comes Tomorrow? The Contours of Future Armed Conflict. London & New York: Routledge 1998 (org. 1995), 100-101.

[921] Дворкин, Владимир Зиновьевич. Ядерное сдерживание и договор СНВ-2. Независимое военное обозрение № 3 1997.

[922] Федосов & Спасский 1999.

[923] Воронин & Брезкун 1999; Басистов, Владимир Анатольевич. Развитие должно быть гармоничным. Независимое военное обозрение № 40 1999.

[924] Михайлов, Николай. Россия может сохранить статус великой державы. Независимое военное обозрение № 36 1998; Михайлов, Николай. Весомые ответы на военные вызовы. Независимое военное обозрение № 16 1999.

[925] Hoffman 2009, 243.

[926] Сергеев, И. Д. Основы военно-технической политики России в начале XXI Века. На Боевом Посту № 99 1998.

[927] Kipp 2010; Adamsky 2015.

strategic level and often explicitly to the 1980s policy against the SDI. There was no single accepted use of the term in the professional discourse. Nevertheless, during 1998-1999 'asymmetric responses' were repeatedly connected to technology-based cost-effective solution to Western military superiority in the context of strained Russia-West relations.[928] The term was not used in any of the national security documents of the 1990s. It is safe to argue that for Soviet and Russian military scholars of the 1990s asymmetry was associated with the strategic balance of power, capabilities that could be measured, and cost-effective measure-countermeasure dialectics. It was not, however, an exclusively military response as by the end of the 1990s it also had acquired elements related to the economy and technological-scientific development of the county. The Russians did not widely adopt the Western version of the term which referred to non-state actors and terrorism.

4.2.4 Kibernetika

The discussion about the ideas of information superiority, information-technological warfare, automatic command and control systems, and the unified information space must start with cybernetics or kibernetika. The above-listed strategic cultural ideas are inherently connected to the late Soviet cybernetic thinking and cannot be understood without it.

According to Slava Gerovitch, kibernetika was a social movement in search of a universal method to solve all problems through modelling and new objective language.[929] The roots of Soviet cybernetic thinking and theory go back the 1930s to men like Nikolai Bukharin and Aleksandr Bogdanov who applied international trends in systems theory to social and political thinking. Their legacy was purged by Stalin in the 1930s, and systems theory and later Western cybernetic theory remained condemned as "idealist, anti-proletarian and imperialist" during Stalin's reign.[930] Nevertheless, formal sciences were freed from the ideological supervision which enabled the Soviets to develop computers or EVMs (electronic calculating machines or elektronnaia vychislite'naia mashina) for nuclear weapon, ballistic missile, and radar development programmes.[931] This independent and secretive development and the ideological requirement to eschew Western terms led to a particularly Soviet language in the computer sciences.[932] Cybernetics was rehabilitated from a "a reactionary pseudo-science" in the late 1950s and 1960s to a "science in the service of communism."[933] By the 1970s cybernetics had gone through a fashionable phase and subsequently lost its intellectual content and appeal and was displaced by informatics.[934] Later, in the 1990s cybernetics was blamed for many of the shortcomings of the Soviet sciences.[935] The popularity of cybernetics was partly based on its use in the de-Stalinization of Soviet

[928] Sakwa 2008, 371; Trenin, 2001.
[929] Gerovitch 2002, 1.
[930] Susiluoto 2006.
[931] Ibid., 390-391.
[932] Ibid., 114-118; Gerovich 2002, 8.
[933] Kolbanovski, E. Kol'man, Eds., The Socio-Economic Literature Publishing House (Sotsekgiz), Moscow, 1961. Quoted and translated in Willis, H. Ware and Holland, Wade B. Soviet Cybernetics Technology: I. Soviet Cybernetics 1959-1962. Santa Monica: RAND Corporation, 1963, 4.
[934] Gerovich 2002, 4; Peters 2016, 47-48.
[935] Gerovich 2002, 4. Susiluoto and Peters share this view of the development of Soviet cybernetics (Susiluoto 2006 & Peters 2016).

science and in the way it resonated with the ideal of scientifically controlled Soviet society and system.[936] Nevertheless, it was later embraced by political power and turned into a vehicle of the status quo.[937] Despite its failure, the United States saw the Soviet adoption of cybernetics as a possible threat worthy of surveillance.[938] This is understandable as the Americans were themselves trying to win the Vietnam war based on systems analysis and operational research.[939]

The Soviet cybernetics were already being deployed by the military in the 1950s and its ideas were eventually transferred to the civilian side through experimental economic policy proposals.[940] Cybernetics was attractive because on the economic side it promised to reform the Soviet economic system and on the military side it provided automated command and control systems for military purposes.[941] Pioneers of cybernetics argued in 1955-1963 for its ability to manage the Soviet economy through networked computers which would greatly increase the economy's efficiency and reduce red tape.[942] This project ultimately failed because of the unofficial features of the Soviet economic system and because of the political and armed forces' opposition. The idea surfaced again in the 1970s and 1980s, however, without any marked success except perhaps pushing the Soviets towards developing and producing personal computers.[943] Personal computers were copied from the Western models with poor success, and they were not allowed to connect through networks.[944] During the 1970s-1980s there was a real interest in the development of networks, as the Soviets were aware of the development of the ARPANET and the technological lead that the West had begun to gain in the 1970s, but no real progress was made.[945] Ilmari Susiluoto has summarized this evolving Soviet 'information society' as closed, centralized, vertical, and controlled by the security services.[946] According to Gerovitch, Soviet scientists and politicians never accepted the idea of a network gradually growing from below, because it would have been inefficient and politically dangerous. They tried to build networks from the top down but ended up duplicating exciting hierarchies of power

[936] For example, cf. Афанасьев, В.Г. Общество: системность, познание и управление. М: Издательство политической литературы, 1981.
[937] Gerovich 2002, 8-10; Peters 2016, 53.
[938] Cf. Levien, Roger and Maron, M. E. Cybernetics and Its Development in the Soviet Union. Santa Monica: RAND Corporation, 1964.
[939] Bousquet, Antoine. Cyberneticizing the American war machine: science and computers in the Cold War. Cold War History Vol. 8, No. 1 (February 2008), 77-102.
[940] Gerovitch 2008, 338-339.
[941] Peters 2016, 78; Gerovitch 2002, 265.
[942] These were men like Anatoli Ivanovich Kitov (1920-2005), Sergei Sobolev (1908-1989), Aleksei Lyapunov (1911-1973), Alexander Kharkevich (1904-1965), Aksel Berg (1893-1979) and Viktor Glushkov (1923-1982), among many others. (Берг, А. И., Китов, А. И., Ляпунов, А. А. "О возможностях автоматизации управления народным хозяйством" Москва. Ноябрь 1959 [Online]. Available: http://www.kitov-anatoly.ru/naucnye-trudy/izbrannye-naucnye-trudy-anatolia-ivanovica-v-pdf/o-vozmoznostah-avtomatizacii-upravlenia-narodnym-hozajstvom [Accessed: 23rd November 2018]).
[943] Gerovitch 2002 & 2008.
[944] Susiluoto claims that from the end of 1960s Western computers developed towards general and universal functionality, whereas Soviet computers were tailored towards specific functions which reduced their combability. Susiluoto argues that the inherent secrecy of the Soviet system and the relations between information and power led to the backwardness of the Soviet computer science. However, the Soviet Union produced its own family of Elbrus micro- and super-computers which were advertised as comparable or superior to Western ones. Most personal computers were poor copies of Western models. In 1989 50% of Soviet computers were 20-25 years behind Western ones and 49% were 10-15 behind. (Susiluoto 2006).
[945] Peters 2016, 166-169; Gerovitch 2008, 364-365.
[946] Susiluoto 2006, 174-175.

which nullified the expected benefits of networks.[947]

The cybernetics dreams culminated in the variously named state-wide Economic Automatic Management System (EASU), All-state Automated System (OGAS) or All-State Automated System of Management (OGAS(U)). They were based on the idea of a system that would have connected Soviet decision-makers and factories etc. for sharing information and to rationalize planning and production on a national scale. This would have been the nervous-system and the brain of Soviet command economy. Officially the system of networks and computers connected to it would have been hierarchical, pyramidical and centrally controlled, but the Soviet scientists had visions that corresponded to the Western ideas of freely networking systems and even surpassed them.[948] The main concepts related to OGAS(U) were automated management systems or ASUs (avtomatizirovannaia sistema upravleniia) which referred to "...a kind of local area network that allowed mainframe computers to control and communicate with factory machinery through a series of automated feedback loops and programmable control processes"[949] and "the unified information network" (edinaia sistema svyazi) or "unified territorial network" which would enable centralized command of computation centres.[950] The ASU was not only a computer but also a system that enabled planning and management of processes based on the collection and processing of information.[951] The unified information network would connect computer centres through phone lines and would provide computation power to industry and agencies that did not have their own computers.[952]

Although ideas about automated command and control systems (ASU)[953] and networks migrated from the military to the civilian side, the infrastructure of the military remained separated and closed. It resisted civilian ideas of dual use of its networks

[947] Gerovitch 2008, 347. Also cf. Кутейников, Алексей Викторович. Проект общегосударственной автоматизированной системы управления советской экономикой (ОГАС) и проблемы его реализации в 1960-1980-х гг. Диссертации на соискание ученой степени кандидата исторических наук. Кафедра Исторической информатики Московского государственного университета имени М.В. Ломоносова. Москва, 2011 [Online]. Available: http://www.hist.msu.ru/Science/Disser/Kuteinikov.pdf [Accessed: 23rd March 2019]; Виртуальный компьютерный музей [Online]. Available: http://www.computer-museum.ru/ [Accessed: 23rd March 2019].

[948] Peters 2016, 108, 120; Gerovitch 2008, 335.

[949] Peters 2016, 86.

[950] Peters 2016, 221; Gerovitch 2002, 265.

[951] Берг, Китов & Ляпунов 1959.

[952] Берг А. И., Китов А. И., Ляпунов А. А. Радиоэлектронику – на службу управления народным хозяйством. Коммунист № 9 1960, 21-28. [Online]. Available: http://odasib.ru/openarchive/Document Image.cshtml?id=Xu1_pavl_635766969644249164_16578&eid=L5_0003_0866 [Accessed: 23rd March 2019]. On Soviet cybernetic thought cf. Анатолий Иванович Китов [Online]. Available: http://www.kitov-anatoly.ru/home [Accessed: 23rd March 2019].

[953] As Eglé Rindzeviciuté argues the Soviets translated the word 'control' used by Norbert Wiener as upravlenie which means regulation aimed at correction or management by supervision. Christopher Donnelly claims that 'upravlenie' in the context of running the military should be translated as management or administration whereas 'upravlenie voiskami' translates to command and control. However, 'upravlenie voiskami' also includes maintaining readiness and training. 'Kontrol' means monitoring and checking, not commanding which is 'rukovodstvo voiskami'. I shall use 'command and control' when discussing military systems because that is an established term in military English, and I shall use management in the civilian context. (Rindzeviciuté, Eglé. Constructing Soviet Cultural Policy: Cybernetics and Governance in Lithuania after World War II. Linköping, Linköping University, 2008; Donnelly, Christopher. Red Banner. The Soviet Military System in Peace and War. Coulsdon: Jane's Information Group, 1988, 136). A Soviet engineer Colonel P. Tkachenko defined upravlenie in the context of military cybernetics as "the process of functioning of command and control organs aimed at obtaining specified results under known initial conditions." These included both technological and social systems. (Ткаченко, П. Кибернетика в управлении войсками. Военная мысль № 1, 1962, 35-48, 38.)

and produced its own computers which were advanced but tailor-made for military systems and did not support civilian industry.[954] The Soviet military built networks for an air defence system, a missile defence system, and a space surveillance system—each with its own centralized computer network during the 1950-1960s.[955] The military knew about the United States' SAGE (Semi-Automatic Ground Environment) air defence network and later ARPANET.[956] It approached networks through the lens of an arms race and possible nuclear war. The dual-use of military technology and networks would have been a risk, which the military did not want to take.[957]

Based on the articles in the Voennaia Mysl' journal the Soviet military was aware of cybernetic ideas from the late 1950s onward.[958] In 1961, A. Berg, A. Kitov and A. Liapunov published an article named "Cybernetics in military affairs" in which they defined the science of kibernetika and its role in military affairs as: "The use of cybernetics in the military is aimed at increasing the effectiveness [speed and accuracy] of the command and control [upravlenie] of weapons and troops through the use of scientific methods and modern technical means for collecting and processing information and developing control commands."[959] The tasks of kibernetika would be the development of the autonomous guidance systems, automated command and control systems, in addition to automated planning and management processes for headquarters. These systems and processes were supposed to handle processes that were becoming too complex and fast, and involved too much information for humans to handle. They would also offer optimal solutions for human decision-makers, even on military operational issues.[960]

The ideas of Berg, Kitov and Liapunov were repeated in later articles although not without criticism and discussion.[961] During the 1980s kibernetika as a term was replaced on the pages of Voennaia Mysl' by informatics[962], mathematics etc. but its influence was arguably felt through the 1990s.[963] Based on the USSR General Staff Lectures from 1969 which were translated by the U.S. Central Intelligence Agency in

[954] Susiluoto 2006, 174; Gerovitch 2008, 344.

[955] Gerovitch 2008, 338.

[956] Gerovitch 2008, 344. ARPANET's military connections might have been a surprise for the Soviets (Peters 2016, 91-92).

[957] Gerovich 2008; Hoffman 2009.

[958] Kipp, Jacob W. Confronting the RMA in Russia. Military Review Vol. LXXVII - May-June 1997, No. 3, 49-55; Kipp, Jacob W. The Methodology of Foresight and Forecasting in Soviet Military Affairs. Fort Leavenworth, KS: SASO, 1987; Womack, James K. Soviet Correlation of Forces and Means: Quantifying Modern Operations. Master's thesis. Fort Leavenworth, KS: U.S. Army Command and General Staff College, 1990.

[959] Берг, А., Китов, А. and Ляпунов, А. Кибернетика в военном деле. Военная мысль № 2, 1961, 19-31, 19.

[960] Ibid., 22.

[961] For example, Colonel P. Tkachenko pointed out that 'automated command and control' could never be truly automated because the commanding of troops included creative elements which cannot be automatized. He proposed as a replacement the term "automated data processing system for command and control" (Ткаченко 1962). Tkachenko was criticised in turn by others. (Bape, B. Кибернетика в управлении войсками. Военная мысль № 7 1962, 17-30; Дмитриев, А. Кибернетика и военное дело. Военная мысль № 1 1970, 89-96; Аниреев, П. И. Расширение сфер применения кибернетики в военном деле. Военная мысль № 4 1978, 71-77.

[962] The late Soviet era definition of informatics stated that cybernetics was its subcomponent which dealt with the applied methods of studying automation etc. ('Информатика' Большой советской энциклопедии. М.: "Советская энциклопедия", 1969 – 1978 г. [Online]. Available: https://dic.academic.ru/dic.nsf/bse/90897 [Accessed: 22nd March 2019].)

[963] Kipp 1997.

1976, automated command and control systems and cybernetics featured strongly in the Soviet command and communications theory and practice.[964] Cybernetics then was not only written about in journals, it was taught in the highest military academies of the Soviet Union. Furthermore, the so-called "third" Soviet military-technological revolution was related to cybernetics.[965]

In the 1970s Soviet military scholars started to perceive a forthcoming military-technological revolution (MTR) in the military applications of future technologies—partly based on the American conduct of the Vietnam war.[966] The Soviets developed the concepts of the reconnaissance strike (RUK) and fire (ROK) complexes, i.e. 'system of systems' that combined reconnaissance, fire, and command and control. According to Adamsky, the Soviet and Western discussion about RUK/ROK shows how the Soviets deliberately used 'Western concepts' to discuss their own ideas through Western concepts and thus masked their own theoretical development. Ironically, the Westerners referred to RUK/ROK as genuinely Soviet concepts.[967] Ultimately, at the end of the 1980s Andrew W. Marshall and others in the Office of Net Assessment (ONA) argued that the Soviets had identified a kind of revolution in military affairs brought about by technological development.[968] In practice the Soviet MTR was interrupted by the fall of the Soviet Union which seriously affected the Armed Forces budget, while the U.S. Armed Forces began their RMA.[969] During the 1990s there were no economic resources or enough political will to push through modernization of the military forces in the way envisioned by the MTR/RMA advocates.[970] This history explains why the Russians feel a certain affinity with the American NCW and its principles.

Cybernetics thus had its civilian and military aspects, and it manifested as theoretical dreams and practical solutions. Moreover, it is quite likely that it also affected the way in which the Soviets planned and prepared to mobilise for war. Furthermore, it is likely that cybernetics affected the way in which the Russians began to see information security as a system.[971]

4.2.5 Information superiority

During the 1960s and early 1970s the benefits gained from automated information management systems were discusses by the Soviet military in connection with the

[964] CIA. "General Staff Academy Lectures: Principles of the Automation and Mechanization of Troop Control." Document VII-211. Prepared 6 September 1968, published October 1969; CIA/DO Intelligence Information Special Report, 11 November 1976 [Online]. Available: https://www.cia.gov/library/ readingroom/docs/1976-11-11.pdf [Accessed: 6th November 2019].

[965] Cf. Adamsky 2008 & 2010.

[966] Adamsky 2008, 263.

[967] Adamsky 2008 & 2010.

[968] Ibid. "In 1993, the Office of Net Assessment (ONA) contracted an alumnus, Jeff McKitterick, and his team at the Strategic Analysis Center (SAC) within SAIC organized a series of workshops and war-games related to exploring the Soviet concepts of a military-technical revolution. McKitterick went on to change the name MTR to RMA and organized a series of war-games around key concepts: dominant manoeuvre and precision engagement." (Jensen 2018, 302-317). Cf. Also Palmer, Diego A. Ruiz. The NATO-Warsaw Pact competition in the 1970s and 1980s: a revolution in military affairs in the making or the end of a strategic age? Cold War History, Vol. 14, No.4 (2014), 533–573.

[969] Locksley 2001.

[970] Renz, Bettina. Russia's Military Revival. Cambridge: Polity Press, 2018, 54-55.

[971] Cf. Расторгуев 1999.

efficiency of command and control and helping the commander to handle large amounts of information.[972] The idea of information superiority appeared implicitly in the Soviet military thinking during the 1970s as the importance of automated information systems increased. They were seen to provide faster planning and decision-making relative to the enemy.[973] This development was related to the establishment of military command and control as an independent subject in the Soviet military sciences in 1979 and to the development of the first ASUs by the Soviet military.[974] Interestingly the idea of 'spiritual' and 'ideological' superiority, in addition to technological, was also already present in the 1970s.[975] The idea of faster command and control cycles (tsikla upravleniia) was expressed in 1978 by professor General-Major I. I. Anureev who stated that: "If the time of command and control cycle is long enough and the conditions of efficiency [operativnost'] are not met, then the losses will be significant and the effectiveness of the troops may be low, despite their potentially high combat capabilities."[976] As the tempo of current and future war was increasing, a faster process of command and control was required to avoid destruction.[977] During the first half of 1980s, the importance of ensuring the functioning of command and control led logically to the importance of denying the opponent his capabilities—or to counter C2 warfare (narushenie upravleniia voiskami).[978] This increased the role of EW in warfare and gave birth to the term radio electronic superiority (radioelektronnoe prevoskhodstvo).[979] General Major I. I. Vorob'ev summarized these developments in 1984 by stating that: "The confrontation [protivoborstvo] in the sphere of command and control, along with the struggle [bor'ba] for fire superiority, for air supremacy, and with the anti-tank combat [bor'ba] becomes the most important component of the content of modern battle [boi] (operation)."[980]

In 1990 this set of ideas was mature enough that Colonel A. Ia. Vainer could call it "a struggle in the sphere of control and command" (protivoborstvo v sfere upravleniia).

[972] Берг, Китов & Ляпунов 1961; Ткаченко 1961; Дружинин, В., Конторов, Д. Методика решения оперативных задач с применением средств автоматизации. Военная мысль № 1, 1970, 40-52; Дружинин, В., Конторов, Д. Руководство и автоматизация. Военная мысль № 6 1973, 24-34; Лифшиц, А., Розенберг, В. О комплексе математического обеспечения автоматизированных систем управления войсками. Военная мысль № 6 1974, 41-48; Дружинин, В. В. and Конторов, Д. С. О некоторых новых аспектах проблемы автоматизации управления войсками. Военная мысль № 12 1975, 28-40.

[973] Помбрик, И. Д. Обеспечение непрерывности управления войсками в современных операциях. Военная мысль № 3 1976, 50-57; Жованик, А. А. О роли связи в автоматизированных системах управления войсками. Военная мысль № 11 1976, 28-39; Стишковский, В. М. Задачи и возможности военной связи. Военная мысль № 3 1977, 40-50; Евстигнеев, Е. А., Вичугов, Е. С. О повышении эффективности использования ЭВМ в штабах и учреждениях. Военная мысль № 9 1977, 60-69.

[974] Савченко, В.Ф. Теория военного управления история и современность. Военная мысль № 11 2007, 50-58.

[975] Зайнуплин, Р. Х. Средства массовой информации и идеологическая борьба в современных войнах. Военная мысль, № 5 1978, 16-30.

[976] Анuреев 1978, 74.

[977] Лосик, О. А. Развитие оружия, боевой техники и способов боевых действий. Военная мысль № 2 1979, 12-21; Сенюков, А. В. О некоторых аспектах применения кибернетики в управлении войсками. Военная мысль № 4 1979, 76-80; Шурупов, Г. Управление войсками—на уровень современных требований. Военная мысль № 5 1979, 33-44.

[978] Назаренко, В. А. Нарушение управления войсками — важная боевая задача. Военная мысль № 7 1983, 46-51; Евстигнеев, Е. А., Сухоруков, Ю. С. Об основных направлениях обеспечения устойчивости автоматизированного управления войсками в операции (бою). Военная мысль № 9 1989, 42-50.

[979] Воробьев 1984a; Воробьев, И. Н. Новое оружие— новая тактика. Военная мысль 1984 № 6, 47-59; Салманов, Г, И. Советская военная доктрина и некоторые взгляды на характер войны в защиту социализма. Военная мысль № 12 1988, 3-13.

[980] Воробьев 1984b, 49-50.

Vainer distinguished three elements of this struggle. The first according to Vainer was the struggle for information superiority. Information is circulated in and between command and control systems and the side that can secure faster and better information while denying the opponent the same ability gains the superiority. The second was a creative- and knowledge-based intellectual struggle which is conducted through reason and ideas related to the optimization of one's own decisions and deceiving the enemy through stratagems. The third element was a technological struggle which was based on computer software, its algorithms and optimization, including artificial intelligence, and software/information security.[981] Vainer's article was followed by others emphasising the different aspects of 'command and control warfare' etc. They were probably inspired by the Gulf War.[982]

By 1993 the terms 'information weapon' (informatsionnoe oruzhie) and 'information support' or 'security' (informatsionnoe obespechenie or bezopasnost') were introduced into the Russian military thinking in the context of information superiority. Both concepts had technological and psychological aspects from the start.[983] Consequently, in 1996 Colonel S. A. Komov could argue that information warfare had been conducted in all wars, but during the previous ten years, IW had begun to predetermine the course and outcome of all hostilities.[984] Komov also considered information superiority as an important element of IW and offered an operational definition of IW divining it into information support, information counter-measures and information defence measures.[985] According to General Major I. N. Vorob'ev, the information-psychological struggle could already be conducted during peacetime and, therefore, could be understood as 'a strategy of indirect action' (strategiia nepriamykh deistvii) which promised the achievement of objectives without the use of direct, open military force.[986] For Vorob'ev this meant that the actual future wars would be short and fought with information-technological means and long-range precision weapons, which meant that information superiority (including its technological and psychological aspects) was the key to victory.[987] Similarly, Pirumov and Rodionov claimed in 1997 that information superiority was required to win wars and it necessitated more comprehensive, accurate, authentic, and timely situation information than that possessed by the enemy's command and control agencies.[988]

The idea of information superiority was quite-well established in the Russian military thinking by the end of 1990s, although some commentators argued that its theoretical

[981] Вайнер, А. Я. О противоборстве в сфере управления. Военная мысль № 9 1990, 12-16.

[982] Португальский, Р. М. О борьбе в сфере управления войсками. Военная мысль № 3 1991; Палий, А. И. Борьба с системами боевого управления в операциях вооруженных сил НАТО. Военная мысль № 4 1991; Захаров, А. Н. Тенденции развития вооруженной борьбы. Военная мысль № 11 1991, 9-15; Владимиров А.В. Информационное оружие: миф или реальность? Красная звезда № 5 (октября) 1991.

[983] Фефелов, Б.В. Информационное обеспечение системы управления войсками. Военная мысль № 1 1993, 36-39; Поздняков 1993; Комов, С.А О концепции информационной безопасности страны. Военная мысль № 4 1994, 12-17; Лукашкин & Ефимов 1995; Коротченко 1996.

[984] Комов, С. А. Информационная борьба в современной войне: вопросы теории. Военная мысль № 3 1996, 76-80; Комов, С. А. О способах и формах ведения информационной борьбы. Военная мысль № 4 1997, 18-22.

[985] Thomas 2001, 787.

[986] Воробьев 1997. Here Vorob'ev echoes the ideas presented earlier by Gareev (Gareev 1998).

[987] Ibid. Also Гулин 1997.

[988] Pirumov & Rodionov 1997.

aspects needed further development.[989] It is interesting to note, that although the Soviets saw the pursuit of conventional and nuclear military superiority as hopeless, they, and later the Russians, did not have the same view on information warfare.[990] It could be argued that information was seen as something novel, and as such, providing a decisive advantage. It is also more than possible that the Russians copied the concept of information superiority from Western sources, although who influenced who is more difficult to ascertain. Both shared the same core principle: information superiority was based on 'better' information than the opponent, protection of that information, and denying information from the opponent.[991] An important point must be made here that when some Soviet and Russian military writers argued that information superiority was becoming ever more important for future warfare many of them meant advanced digitalized command and control systems and counter-C2 warfare in the context of military operations. The psychological aspect was present in the texts, but information-technological warfare was clearly a distinct phenomenon.

4.2.6 Information-technological warfare

As was argued above, according to the Western research, the Russian view on information warfare has two aspects: information-technical/technological and information-psychological. Moreover, these aspects are connected by a view which emphasises the target or objective of an 'information struggle' instead of means of information warfare. In the context of modern Russian military thought (ca. 2015) Adamsky has argued that the Russian approach to information-technological warfare is based on historical continuity. The first source is the Soviet MTR/RMA thinking which emphasised disrupting the enemy's decision-making process by targeting its C4ISR capabilities. The second source is the tradition of maskirovka and active measures which aim to deny, deceit, disinform, and conceal, i.e. to manipulate enemy's consciousness and produce favourable behaviour. The third source is the Soviet science of cybernetics.[992]

What has been meant by information-technological war or warfare has changed over time.[993] However, during the 1970s and 1980s the technological aspect of warfare was emphasised by Marshal Ogarkov and others who were writing about the MTR.[994] Integration of reconnaissance and weapons through command and control channels gave birth to the ideas of ROK/RUK. Moreover, autonomous operational manoeuvring groups (OMGs) fighting deep inside NATO lines required advanced automated

[989] Костин 1997, 44; Родионо 1998; Круглов, В. В. О вооруженной борьбе будущего. Военная мысль № 5 1998, 54-58; Завадский, И.И. Информационная война — что это такое? Защита информации. Конфидент № 4 1996. Quoted in: Расторгуев 1999, 55.

[990] Fitzgerald 1987a, 4.

[991] Печуров, С.Л. Революция в военном деле взгляд с Запада. Военная мысль № 4 (7-8) 1997, 73-80; Суровцева, Елена. Запад переходит в информационное наступление. Красная звезда № 109 1997. Cf. Also Palmer 2014; Adamsky 2008 & 2010; Jensen 2018. On the American views in the 1990s: "[IW] consists of the actions taken to preserve the integrity of one's own information systems from exploitation, corruption, or destruction, while at the same time exploiting, corrupting, or destroying an adversary's information systems and, in the process, achieving an information advantage in the application of force." Fredrichs, Brian E. Information Warfare at the Crossroads. Joint Forces Quarterly, Summer 1997, 97-103 [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a529170.pdf [Accessed: 14th November 2018].

[992] Adamsky 2015 & 2018.

[993] Kline 2015, 191-192; Gerovich 2002 & 2008; Gerovich 2002, 140-141.

[994] Fitzgerald, 1992, 347-362; Fitzgerald 1987b, 31-32.

command and control systems (ASUV) (avtomatizirovannaia sistema upravleniia voiskami).[995] By the 1980s, Soviet military writers understood that the availability of automated command and control systems and communications had become a decisive factor on the modern battlefield—the ability to manoeuvre and fire upon the enemy was dependent on them.[996] This view elevated radio electronic warfare to a new status, and placed higher requirements of efficiency, high quality, stability, reliability, secrecy (operativnost', vysokoe kachestvo, ustoichvost', nadezhnost', skrytnost') on command and control.[997] The approach resonated with the Western ideas of Command, Control and Communications Countermeasures (C3CM), which later evolved into Command and Control Warfare (C2W) at the same time in the West.[998] Soviet military writers followed the developments in the West, and predicted the introduction of autonomous weapon systems, and digitalized C3I capabilities.[999]

By the late 1980s the term 'software' (programmnoe obespechenie) entered the Soviet lexicon from the West which indicated that the Soviet writers were aware of the qualitative changes in computer technology and the ways it could change warfare.[1000] Additionally, many Soviet theorists thought that the new conventional weapons based on novel physical principles would be as global in reach and as effective as weapons of mass destruction.[1001] Consequently, the Soviet military was highly aware of the vulnerability of its strategic communication and early warning systems and feared a surprise attack against them followed by a decapitation strike with nuclear weapons.[1002]

Counter command and control warfare and radio electronic warfare began to coalesce at the beginning of the 1990s into information warfare or struggle. The distinct technological aspect was the continuation of the MTR thinking, although the psychological aspect was also present from the early on, as was clear from A. Ia. Vainer's categorization of the information, intellectual, and technological struggle.[1003] Vainer highlighted the dual short-term and long-term nature of the technological struggle. The short term indicated that EW and software manipulation were connected to the bat-

[995] Ibid., 33-35.

[996] Стишковский 1977; Лосик 1979; Воробьев 1984a.

[997] Kokoshin 1998, 138; Шурупов 1979; Воробьев, И. Н. Новое оружие и развитие принципов общевойскового боя. Военная мысль No. 11 1983, 35-45.

[998] Kaplan 2016, 14-16; Layman, Gene A. C3CM – A Warfare Strategy. Naval War College Review, Vol. 38, No. 2 (March-April 1985), 31-42; Larson, Doyle E. Exploiting Electronic Warfare. Air Force Magazine, July 1981. The C2W concept was official defined as late as 1996 as "the integrated use of psychological operations (PSYOPS), military deception, operations security (OPSEC), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions." United States Department of Defence, Joint Chiefs of Staff. Joint Doctrine for Command and Control Warfare (C2W) Joint Pub 3-13.1, 7th February 1996, v. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a357635.pdf [Accessed: 27th November 2018].

[999] Поцщипов, И. Н. Американская концепция «управление, связь и разведка». Военная мысль № 7 1986, 63-72.

[1000] Ниесов, В. А. Состояние программного обеспечения автоматизированных систем управления вооруженными силами США. Военная мысль № 6 1988, 64-72.

[1001] Fitzgerald 1987b, 35.

[1002] Hoffman 2009, 147-150; Hines et al. 1995a, 16-19; Podvig, Pavel. The Operational Status of the Russian Space-Based Early Warning System. Science & Global Security, Vol.4 (1994), 363-384; Blair, Bruce. The Logic of Accidental Nuclear War. Washington, DC: Brookings Institution, 1993; Yarynich, Valery E. C3: Nuclear Command, Control Cooperation. Washington, DC: Center for Defense Information, 2003.

[1003] Вайнер 1990.

tlefield and the long term indicated the level and potential gap of technological development between adversaries.[1004] The information-technological component was so important that Rear-Admiral V. S. Pirumov argued that 'information support' (informatsionnoe obespechenie), i.e. electronic systems and computers, were an integral part of the combat potential and needed to be added to the correlation of forces calculations.[1005] At the same time Tsymbal and others were arguing that information weapons might be as destructive as the weapons of mass destruction.[1006] In 1996 S. V. Markov offered one of the first definitions of information weapons as pieces of information affecting the information processes of information systems.[1007] Later Vitalii Tsygichko and others classified information weapons into the means to locate and destroy equipment emitting signals in the electromagnetic spectrum, means to affect the components of electronic equipment and software and data traffic, as well as the means to spread propaganda and disinformation, and also psychotronic weapons.[1008]

These ideas were echoed by A. N. Lukashkin and A.I. Efimov who argued in 1995 that the computerization of critical systems would make the infosphere the future object of military confrontation.[1009] Although Lukashkin and Efimov did not refer to Western sources, it is quite clear that they were aware of the debate on the protection of critical infrastructure going on in the United States at the time.[1010] The way in which the duo attacked the so-called 'pessimists' (sceptics) informs us that by 1995 the possibilities of 'dangerous algorithms and software' was not taken seriously by all in Russia. Others, like General Major E. G. Korotchenko, saw information as a tool of information-psychological struggle and an ongoing geopolitical confrontation to control the Russian people, weaken the moral of its armed forces, and to gain scientific-technological superiority over Russia. For Korotchenko computer viruses, various means of EW, microwave generators and means of software-mathematical influence could be used to destabilize whole nations by striking at military and civilian targets during peacetime or war.[1011] This transitory and dual nature of IW was present in the 1995 edition of the Russian Military Encyclopaedia which equated information weapons with psychological warfare but 'military informatics' with theory about automated information processing.[1012] In the mid-1990s many Russian scholars followed the Western discourse on IW theory and not only the conduct of American military operations. However, they still employed Marxist-Leninist ideas and cybernetic models to conceptualize information-technical warfare.[1013]

[1004] Ibid.

[1005] Pirumov 1992.

[1006] Thomas 1998b, 45. Цымбал 1995; Владимиров 1991; Смолян, Цыгичко & Черешкин 1995.

[1007] Thomas 2005, 170.

[1008] Thomas 2005, 168.

[1009] Лукашкин & Ефимов 1995, 49.

[1010] Boys, James D. The Clinton administration's development and implementation of cybersecurity strategy (1993–2001), Intelligence and National Security, Vol.33, No.5 (2018), 755-770.

[1011] Коротченко 1996.

[1012] 'Военная информатика' Военная энциклопедиа, Том. III. М.: Военное издательство, 1995, 362-363.

[1013] Костин 1996 & 1997; Глазов & Ловцов 1997. A source of inspiration was John Wardens 'Five-ring model' (Warden, John. The enemy as a system. Airpower Journal, Vol. IX, No. 1, 1999 (Spring), 40-55.) On Warden's influence on the Western operational art cf. Vego, Milan. Joint Operational Warfare: Theory and Practise, Vol. 1. Newport: US Naval War College, 2007, XII-53-63.

For example, Rastorguev, who was commissioned to write a book called Information War for the Russian Security Council, defined IW as "a battle between states involving the use of exclusively information weapons in the sphere of information models." He was especially interested in modelling how information weapons could affect information systems and defined information weapons "as means directed at activating (or blocking) information system processes in which the subject using the weapons has an interest. An information weapon can be any technical, biological, or social means or system that is used for the purposeful production, processing, transmitting, presenting or blocking of data and or processes that work with the data."[1014] According to Rastorguev, information does not in itself destroy anything but it affects the enemy's system which might destroy itself.[1015]

In one way or another, many Russian scholars approached information-technological/technical warfare/struggle/confrontation in the context of a more expansive or comprehensive information-psychological confrontation/struggle. They also distinguished the information warfare means of wartime from those of peacetime. They highlighted the importance of technological means, although they perhaps saw the objective to reside at the strategic or political level.[1016] Information-technological warfare/confrontation was an integral part of the visions of the future character of war.[1017] Additionally, at the turn of the millennium, with nuclear deterrence as the backbone of Russia's defence, the vulnerabilities of the command and control systems of strategic nuclear forces were an important topic.[1018] Therefore, it can be argued that information-technological means were seen by the Russian military thinkers in the 1990s as an intrinsic part of the modern warfare and strategic stability, but there is no clear evidence that they had solved the question of how these concepts were supposed to be realized in organizations, or as concepts, and used by forces or implemented as means—let alone come up with a 'holistic' strategy. At the beginning of 2000s these ideas were still underdeveloped, but the basic elements had been formulated. When the Chief of the General Staff Valeri Gerasimov produced his presentation about future warfare in 2013 his views were based on ideas articulated already in the 1990s.[1019]

4.2.7 Automated command and control systems

Automated command and control systems were already explicitly and implicitly mentioned in the article by Berg, Kitov and Liapunov in 1961.[1020] Subsequently, they became the central concept around which the Soviet kibernetik ideas revolved. The terminology of ASUs is diverse and for clarity's sake I will use the term 'automated command and control systems' (abbreviated as ASU) to refer to a group of different terms

[1014] Quoted in Thomas 2005, 78. Original Расторгуев, Сергей Павлович. Введение в формальную теорию информационной войны. Москва: Вузовская книга, 2002.

[1015] Thomas 2005.

[1016] Комов 1996; Комов 1997; Pirumov 1992; Pirumov & Rodionov 1997; Расторгуев 1999; Смолян, Цыгичко & Черешкин 1995; Цыгичко, Вотрин, Крутских, Смолян & Черешкин 2000; Черешкин, Смолян & Цыгичко 1996.

[1017] Круглов 1998; Слипченко, Владимир. Война будущего (прогностический анализ). 1999 [Online]. Available: https://www.e-reading.club/bookreader.php/112810/Slipchenko_-_Voiina_budushchego_%28prognosticheskii_analiz%29.html [Accessed: 14th November 2018]; Воробьев 1997; Gareev 1998.

[1018] Рукшин 2000.

[1019] Герасимов, Валерий. Ценность науки в предвидении. ВПК № 8 (476) 2013, 1-3.

[1020] Берг, Китов & Ляпунов 1961, 19.

that were used during the Soviet and Russian times.[1021] I will concentrate here on the ideas about military ASUs as civilian ideas have been examined by Gerovich, Peters and Susiluoto and presented above in the context of 'kibernetik'.

The Soviet military was interested in ASUs from the 1960s.[1022] Colonel P. Tkachenko described them in 1961 as the "automation of information processing using electronic machines." He however argued that the creative processes inherent in command and control could not be automated.[1023] This statement expressed an argument which the Soviets had difficulties solving on the level of military theory: Could and should machines be more than support tools for commanders' subjective creativity and what were the 'scientific principles' of command and control?[1024] There was also the problem of how to fit ASUs into the Marxist-Leninist theory and 'partiinost'' or party-mindedness. A further problem was how the political principle of centralized control was to be combined with shared computation capabilities or decentralized command in general.[1025] Nevertheless, as one commentator stated: "typical representatives of cybernetic systems are automated command and control systems."[1026] And if cybernetics was politically acceptable after the 1950s, so were the ASUs.

According to the USSR General Staff Academy lecture materials from 1969, automated systems would increase the efficiency of control by reducing the time expended on the control cycle, i.e. obtaining information, processing it, making decisions and transmitting orders, and thus leaving more time for carrying out the orders by the forces.[1027] The main processes to be automated were the collection of primary information; processing, formulation, reproduction, and the visual display of information; performance of certain calculations; and transmission of information.[1028] ASUs would be used to connect the headquarters and forces of the Soviet Union and Warsaw Pact to an integrated automated system of control.[1029] Consequently, a Ministry of Defence directive from the 2nd of December 1967 commanded "the combining of computer centres of districts into a unified system connected to the ground forces computer

[1021] Military sources use the term 'avtomatizirovannaia sistema upravleniia voiskami' (ASUV) which translates to command and control systems of troops whereas civilian sources use 'avtomatizirovannaia sistema upravleniia' which translates to more general automated management systems. Berg, Kitov and Liapunov basically made this distinction in their article from 1961 (Берг, Китов & Ляпунов 1961).

[1022] Computers were, for example, used to calculate optimal use of tactical nuclear weapons and air defence systems. Chernov, L., Moiseyev, V. and Kiselev, A. Some Problems in the Use of Electronic Computers. Military thought – Secret version 1962, No. 6 (67). Translated and published by the Central Intelligence Agency, Intelligence Information Special Report, 2nd June 1978 [Online]. Available: https://www.cia.gov/library/ readingroom/docs/1978-06-02b.pdf [Accessed: 29th November 2018].

[1023] Ткаченко 1962.

[1024] Варе 1962; Дружинин & Конторов 1970 & 1973; Дружинин, В. В., Конторов, Д. С. Принципы создания и применения автоматизированных систем управления войсками. Военная мысль № 8 1976, 43-54; Андреев 1978; Горлов, А. И., Смирнов, С. С. О влиянии автоматизации на работу органов управления. Военная мысль № 12 1984, 49-55.

[1025] Алтухов, П. К. Предмет и содержание теории управления войсками. Военная мысль № 7 1975, 15-25; Евстигнеев & Вичугов 1977; Соловьев, С. Л., Терехов, И. П. К вопросу о совершенствовании управления войсками. Военная мысль № 11 1980, 48-51.

[1026] Жованик 1976, 28.

[1027] CIA 1976.

[1028] Ibid., 12. The distinctions between automated and automatic systems was already clear. Automatic systems were only monitored by humans whereas automated systems required human thinking, will and decisions to operate. (Ibid., 19)

[1029] Ibid., 13-14.

centre […]”[1030]

The 1970s and early 1980s were an intensive period of ASU development in the Soviet military. The command and control system of the strategic nuclear forces was upgraded multiple times from 1967 to 1985 and its automated functions increased in every iteration.[1031] The fear of a surprise nuclear attack and the establishment of the launch-on-warning doctrine made it necessary to build an early-warning (EW) system based on networks, radars and satellites.[1032] In the 1970s the military began to develop operational, tactical and technical level ASUs to enable the control of military actions from strategic operations on TVDs (theatre of military operations 'teatr voennykh deistvyi') down to individual weapon systems. It also built a naval reconnaissance system which included space, air, and naval assets to track U.S. carried battlegroups and an integrated territorial air defence network. These systems suffered from the deficiencies of Soviet computer technology and were introduced to troops only haltingly and partially.[1033]

The interest in automated systems was visible in the pages of the Soviet military encyclopaedia which in its 1976 edition gave a description only of automatic control systems but the 1986 edition of the military encyclopaedic dictionary dedicated almost a page to automated command and control systems (ASU/ASUV).[1034] They were defined as: “an interrelated set of information processing, data transmission and communication tools that automate the collection, analysis and assessment of the situation data, decision making, planning, giving orders, and delivering tasks to the troops (forces) and the controlling their implementation.” The main task of the automated command and control systems was to increase the efficiency, stability, flexibility, secrecy and quality of the processes of command and control of troops [operativnost', ustoichivost', gibkost', skrytnost', kachestva protsessov]. ASUVs were 'unified systems' that provided effective information-technological interaction between command posts.[1035] Based on this definition, ASUs were not just computers but cybernetic

[1030] Ibid., 27.

[1031] Hoffman 2009, 147-148.

[1032] Podvig, Pavel. History and the Current Status of the Russian Early-Warning System. Science and Global Security, Vol. 10 (2002), 21–60; Podvig 2008.

[1033] Nauta, Frank. Logistics Implications of Maneuver Warfare. Volume 3: Soviet Offensive Concepts and Capabilities. Bethesda, Maryland: Logistics Management Institute, 1988; Vego, Milan. Recce-Strike Complexes in Soviet Theory and Practice. Fort Leavenworth, KS: SASO, 1990; Тимошенко, Михаил. «Маневр» и маневры. Арсенал. Военно-промышленное обозрение» №6, 2010 г.; Мосиенко, Юрий Иванович. «Маневр» – Первая советская АСУВ поля боя. «Арсенал» № 3 2011 г.; Андреев 2011; Безель, Я. В. Этапы развития автоматизированных систем управления авиацией и ПВО. Вестник Концерна ПВО «Алмаз – Антей», №2, 2015 [Online]. Available: http://www.almaz-antey.ru/upload/iblock/e95/e95a21ddf357267fc0137dbd3cace605.pdf [Accessed: 11th December 2018]; Алехин, Ю., Прохоров, А., Проценко, А. «Пирамида» начиналась с «воздуха». Воздушно-космическая оборона №1, 2011 г; Huchthausen & Sheldon-Duplaix, 2009, 233-234.

[1034] 'Автоматическая система'. Советская военная энциклопедия в восьми томах (СВЭ), Том I. М.: Военное издательство Министерства обороны, 1976, 82.

[1035] 'Автоматизированная система управления войсками (силами)' Военный Энциклопедический Словарь, Том. I. М.: Военное издательство, 1986, 17. The term appeared with shorter definition already in 1983 Military encyclopaedic dictionary ('Автоматизированная система управления войсками (силами)'. Военный Энциклопедический Словарь, Том. I. М.: Военное издательство, 1983, 17). The 'quality' of communications was defined in a secret version of the Military Thought journal in 1970 as consisting of survivability, reliability, security and speed. (Stishkovskiy, V. The Principal Ways of improving the quality of Military Communications. Military thought – Secret version 1970, No. 1 (89). Translated and published by the Central Intelligence Agency, Intelligence Information Special Report, 1st February 1974 [Online]. Available: https://www.cia.gov/library/readingroom/docs/1974-02-01.pdf [Accessed: 29th November 2018].)

systems which were used to control and manage the process of command. Additionally, already in 1983, one of their benefits was seen to be decentralization and the mobility of command.[1036] Interestingly, the technical requirements for ASUs were being discussed under the term 'ustoichivost" which consisted of reliability, survivability, and noise immunity and which would later in the 2000s be understood as 'resilience'. This 'ustoichivost" could be affected by internal and external factors, the latter of which included kinetic force, EW, and software attacks.[1037]

In 1987 General Colonel V. N. Konchits argued that the contemporary aspects of command and control were related to the increased tempo and volume of information, the possibly to provide optimal solutions and forecasting, and the vulnerability of complex systems. These were the same kind of issues that the Western armed forces were starting to consider at the time.[1038] Nevertheless, at least Konchits did not argue for decentralization and networking or for adopting other future RMA concepts but, instead, for enhancing the role of staff and the commander who had to know everything with the help of information support, i.e. ASUs.[1039] The importance of ASUs was reflected in strategic assessments. According to testimonial evidence, the Soviet military in the 1970s and 1980s considered command and communications the second most important target of possible the Western attack after nuclear weapons.[1040] In more futuristic visions, command and control warfare was imagined as a kind of struggle between ASUs supported by EW conducted on an operational level under strict control of divisional staff etc.[1041] This view was different from the Western, perhaps more individualistic, 'cyber warrior' imaginary[1042] and it might have led to different operational and strategic conclusions.

In the 1990s ASUs remained an important topic and in the 1997 edition of the Military Encyclopaedia 'automatization of command and control' with subtopics covered multiple pages.[1043] The definition of ASU had practically remained the same but future perspectives now included further unification of systems, the use of personal computers and local networks, the use of common software and programming languages etc. Obviously tailor-made, customized, independent systems were out of vogue. Whatever the dictionaries claimed, the problems of inefficient and insufficient technology and theory seemed to be the reality.[1044] Kibernetika was replaced by informatika, informatization and information theory, and the rapid 'informatizatsiia' produced calls for standards and unification of ASU solutions. Military districts were offered as the basis of the information structure of the armed forces as they were peacetime and

[1036] 'Автоматизация управления войсками (силами)' Военный Энциклопедический Словарь, Том. I. М.: Военное издательство, 1983, 17-18; 'Автоматизация управления войсками (силами)'. Военный Энциклопедический Словарь, Том. I. М.: Военное издательство, 1986, 66-70.

[1037] Евстигнеев & Сухоруков 1989, 43.

[1038] Adamsky 2010; Krepinevich 2002.

[1039] Кончиц, R. Н. Совершенствование управления войсками в современном бою. Военная мысль No. 9 1987, 43-50.

[1040] Huchthausen & Sheldon-Duplaix, 2009, 260-261.

[1041] Евстигнеев & Сухоруков 1989.

[1042] At least according to Thomas Rid, the 1970s and 1980s in the West were the age of counter-cultures, cyberpunk and cyber cowboys (Rid 2016).

[1043] 'Автоматизация управления войсками (силами)' Военная Энциклопедия в восьми томах, Том. I. М.: Военное издательство, 1997, 67.

[1044] Фефелов 1993.

wartime formations and were responsible for operations in strategic directions.[1045] Arguments were made for dispensing with the term of ASU and replacing it with more modern 'information systems' and 'information networks' as automation had lost its distinctive meaning.[1046] By the end of the 1990s a few scholars offered artificial intelligence either as a replacement for ASUs or as a new core component of ASUs[1047]

On the eve of the new millennium General Lieutenant V. V. Barvinenko argued, after stating that previous efforts to create domestic ASUs had failed or were insufficient, that: "The unified (combined-arms) ASU for the Armed Forces should be centralized, hierarchical and territorial, have sophisticated horizontal links, and have vertical trunks." The modular, flexible and networked structure of automated systems of command and control, and the availability of functioning algorithms would make such a system adaptive, able to adequately respond to changes in "the means and methods of conducting military operations."[1048] Barvinenko's statement was born out of frustration with the fragmented field of multiple types of ASUs used by the services and branches of the Armed Forces. He also wished to create a global military information network similar to the United States' network which would facilitate the joint capabilities of the Armed Forces.[1049] Others saw informatization as a way to finally build an automated mobilization system.[1050] By the end of 1990s, the Russian military scholars were actively thinking about ways to adopt modern ASUs to the Russian approach to conducting war. However, at that time, a lack of resources hindered the 'fitting of ideas' to reality.

Although ASUs are not explicitly mentioned in other strategic documents, the Information Security Doctrine of 2000 recognizes the concept of ASU and connects it to almost all spheres of information security. In the context of the Doctrine ASUs might be understood as a shorthand for 'hardware and software', but they are more than that. They secure the functioning of the economy and society, public and secret telecommunications, the command and control of the military, the functioning of the judicial system etc. ASUs are systems, not pieces of hardware or pieces of code.[1051] Thus, the strategic cultural idea of ASUs was quite alive when Russia entered the 21st century. On the civilian side it offered ways to understand the information revolution gripping Russia. On the military side it provided visions of how to arrange command and control in future wars.

[1045] Безуглый, А. С., Гавриленко, С. П. Об информационном моделировании в АСУВ. Военная мысль № 5 1994, 29-33; Кежаев, В.А. Совершенствование управления войсками: аспект информатизации. Военная мысль № 4 1996, 42-45; Ловцов, Д. А. Информационная безопасность АСУ войсками и оружием: теоретические аспекты. Военная мысль № 6 1996, 32-38.

[1046] Калинин, Ю. П. Озеранскии, Л.И. Информационные сети — перспектива автоматизации процессов управления войсками. Военная мысль № 2 1997, 54-58.

[1047] Ibid; Sayfetdinov, Kh., Kulyanitsa, A. L. Information Technology and Artificial Intelligence. Military Thought No. 5 1997.

[1048] Барвиненко, В. В. Об автоматизации управления группировками Вооруженных Сил. Военная мысль № 2, 1999, 26-29.

[1049] Ibid.

[1050] Бобошко, А.А., Муравьев, Н. Л., Пономарев, С.Ю. Основные проблемы автоматизации организационно-мобилизационных органов ВС РФ. Военная мысль № 6, 1999, 50-53.

[1051] Доктрина информационной безопасности РФ. (Шаклеина 2002).

4.2.8 Unified information space

The idea of a unified information space (EIP) was already expressed by the pioneers of the Soviet kibernetika as "the unified territorial state network of information-computing centres with a centralized command." For Berg, Kitov and Liapunov this arrangement was necessary not only because of the their cybernetic ideas but because of the lack of computers and the size of the Soviet Union.[1052] However, this idea did not materialize in the way the pioneers had hoped and the civilian Soviet 'information space' remained fragmented.[1053] Nevertheless, the military needed redundant and resilient communications networks which would connect geographically distinct assets in conditions of conventional or thermonuclear war.[1054] It also had to create communications to the Soviet Union's allies in the Warsaw Pact, to its troops in Eastern and Central Europe and, from the 1960s onward and particularly in the 1970s, to its troops in Third World countries and to its blue water navy on the world's oceans—including ballistic missile nuclear submarines (SSBNs). The military had to prepare for a war in multiple theatres of military action or TVDs with the recognition that governmental central command might be wiped out by nuclear strikes.[1055]

One of the principles of command and control in the Soviet and later Russian military art has been continuity or uninterruptedness (nepreryvnost').[1056] This was a hierarchical relationship between the commander and the subordinates requiring a direct channel of communication.[1057] This, according to Colonel I. D. Pombrik, who was writing in 1976, meant that the commander and staff had to be able to influence the events of battle even under the effects of EW and nuclear weapons.[1058] By the late 1970s the Soviet signals officers agreed that communication systems had become the key to winning and, therefore, a target of enemy action. Because of this, continuity required that more depth, redundancy, and reserves were demanded of the systems.[1059] This required the unification and centralization of control of the communication systems.[1060] Moreover, another principle of 'edinonachalie' or unity of command emphasised the undivided responsibility of the commander to command and control.[1061]

[1052] Берг, Китов & Ляпунов 1960.

[1053] Gerovich 2008; Susiluoto 2006.

[1054] Elterman, Iu. Communications in an Automated Troop Control System at the Operational Level. Military thought – Secret version 1963, No. 1 (68). Translated and published by the Central Intelligence Agency, Intelligence Information Special Report, 2nd June 1978 [Online]. Available: https://www.cia.gov/ library/readingroom/docs/1978-04-20a.pdf [Accessed: 29th November 2018]; Abramov, Iu., Savelyev, V. and Cheremykh, V. A System for the Collection, Processing, and Transmission of Information in a Military District. Military thought – Secret version 1964, No. 2 (72). Translated and published by the Central Intelligence Agency, Intelligence Information Special Report, 20th June 1978 [Online]. Available: https://www.cia.gov/library/ readingroom/docs/1978-06-20a.pdf [Accessed: 29th November 2018]; Stishkovskiy, 1970.

[1055] MccGwire 1987; Glantz 1992; Westad 2017; Hoffman 2009; Petersen, Phillip A. The Northwestern TVD in Soviet Operational-Strategic Planning. OSD Office of Net Assessment, 2014 [Online]. Available: https://bit.ly/2ZRP24b [Accessed: 29th November 2018]; Sadykiewicz, Michael. The Warsaw Pact Command Structure in Peace and War. Santa Monica: RAND Corporation, 1988; Polmar, Norman, Brooks, Thomas A. and Fedoroff, George E. Admiral Gorshkov. The Man Who Challenged the U.S. Navy. Annapolis: Naval Institute Press, 2019, 170-171.

[1056] Lalu 2014, 378-379; Donnelly

[1057] Алтухов 1975.

[1058] Помбрик 1976.

[1059] Ibid.; Стишковский 1977; Stishkovskiy 1970.

[1060] Стишковский 1977, 42.

[1061] 'Единоначалие'. Советская военная энциклопедия в восьми томах (СВЭ), Том III. М.: Военное издательство Министерства обороны, 1979, 301.

Nevertheless, the principles were not fully consistent or historically constant and at times they emphasised the relative, initiative and independence of subordinates.[1062]

Since the late 1970s the Soviet military was aware of computer networks created in the United States on the basis of public telecommunications networks.[1063] It was understood that these kinds of digitalized networks which were connected to satellite communications required technological standardization and common interfaces—something that the Soviets lacked.[1064] However, in the context of continuity, uninterruptedness and unity of command, the control these new networks offered a solution to territorial defence. They provided centralized command during peacetime but were, nevertheless, able to function in a fragmented form after an initial period of war had destroyed their state-level unity.[1065] Many in the 1970s considered the main benefits of automation and networks to be the enhanced centralization of decision-making and commander-centric operations rather than the freedom and proactivity of subordinates.[1066]

During the 1980s the Soviet military continued to follow the Western efforts to unify tactical and operational networks and clearly admired what they were seeing.[1067] This did not stop Colonel E. G. Korotchenko claiming in 1988 that under massive aerospace attack using precision-guided weapons a strictly centralized command was required to prepare for and repulse aggression.[1068] Although Korotchenkos presented his views as universal principles of the military art, they were based on an analysis of NATO doctrine. Moreover, his views must be put in the context of the 1980s offence-defence debate in the Soviet military circles where the emphasis was put on surprise and the initial period of war. It is reasonable to argue that the Soviet military viewed the benefits of networks from the viewpoint of territorial defence and total war.

The civilian version of the idea of an EIP found new life after the fall of Soviet Union in the Russian Internet, commonly known as RuNet. It was born from the networks of universities and research academies in Moscow and St. Petersburg from 1989 onwards.[1069] RuNet started from 'zero' as there were no proper telecommunications infrastructure, cross-border connections or even demand for it—markets were splintered and the development of networks was highly regionalized.[1070] The scholars of Soviet era cybernetic institutions were instrumental in the development of the Internet, although many scientists left Russia during the economic hardships of the 1990's or had to change profession.[1071] State funding decreased and projects on super-computers etc. declined. Ilmari Susiluoto argues that the state IT sector basically ceased

[1062] Lalu 2014, 114.

[1063] Горлов & Смирнов 1984; Лощилов, И. П. О новом принципе построения автоматизированных систем управления войсками. Военная мысль № 7 1977, 46-57; Евстигнеев & Вичугов 1977.

[1064] Лощилов, 1977, 50.

[1065] Ткаченко, В. И., Фадеев, Ю. А. О соотношении централизованного и децентрализованного управления в Войсках ПВО страны. Военная мысль № 11 1978, 32-40.

[1066] Дружинин & Конторов 1976; Лощилов 1977; Лосик 1979.

[1067] Горлов & Смирнов 1984; Жованик, А. А. Космические системы связи и их использование для управления вооруженными силами. Военная мысль № 4 1983, 34-42; Ниесов 1988.

[1068] Коротчеiiко 1988.

[1069] Susiluoto 2006.

[1070] Перфильев, Ю. Ю. Российское интернет-пространство: развитие и структура. М.: Гардарики, 2003.

[1071] Susiluoto 2006. According to Roger Roffrey the state funding of R&D from 1990s to 2009 fell by 75% and 10,000-25,000 highly qualified professionals left the country since 1991. (Roffey, Roger. Russian Science and to exist.[1072] Consequently, the Russian information society was built from the bottom up by Soviet engineers who had been discarded by the system, destitute academics, and adventurous entrepreneurs. The groundwork for the Russian information society was laid in the 1990s, but the Russian information revolution did not begin until 2000-2002.[1073] Cities like Moscow and St. Petersburg were at the forefront of the development, but major energy- and mining companies provided funds for developing networks in parts of the periphery. Despite the relative success of the civilian IT sector, the lag in technology and resources afflicted the military, which in 1999 was mainly equipped with C3 systems from the 1970-1980s, and only about 10-15% of the equipment was modern. The armed forces lacked satellite and fibre optic communications, proper encryption and jamming resistance, digitalised networks, and end-user equipment. Because of the cost of developing purely military systems, civilian technology and cooperation was considered as a serious option. The military required the support of the civilian information infrastructure to cope with the changes.[1074]

In 2005 Russia was still 10 years behind the leading countries in information technology, and its telecommunications infrastructure was in the hands of state companies.[1075] For much of the 1990s the Russian telecommunications network was outdated if not obsolete from the point of view of modern data traffic. Regional telecommunications networks were owned by local companies, which reduced competition and therefore investment and the building of intraregional and state-wide connections. Civilian networks capable of supporting data traffic were splintered, fragmented, and partly non-existent. Satellite communications were used in many places instead of fixed connections.[1076] It is thus not surprising that kibernetik ideas returned in a new guise as the ‘unified information network’.

In 1995 President Yeltsin approved the Concept of the Formation and Development of a Unified Information Space of Russia and Relevant State Information Resources.[1077] The concept stated that the Russian information systems were fragmented, disconnected, and used mainly by government institutions which restricted access to their systems and did not cooperate with each other. It defined an EIP as “a set of databases and data banks, technologies of their management and use, and information-telecommunications systems and networks operating on the basis of common principles and according to general rules that ensure information interaction between organizations and citizens.” This space consisted of information resources, organizational structures, and means to use and exchange information, the latter two of which

Technology is Still Having Problems—Implications for Defense Research. The Journal of Slavic Military Studies, Vol.26, No.2 (2013), 162-188, 163-164).

[1072] Susiluoto 2006.

[1073] Susiluoto 2006. Perfil’ev argues that the intensive growth of the Internet in Russia or Runet began after the economic slump of 1998 (Перфильев 2003). Cf. also Росич, Ю. Ю География развития интернета в России. Dissertation. Московский государственный университет им. М. В. Ломоносова Географический факультет. Москва, 2005.

[1074] Saarelainen et al. 1999, 191-192. Wellman, David A. A Chip in the Curtain. Computer Technology in the Soviet Union. Washington, DC: NDU Press, 1989.

[1075] Susiluoto 2006, 154.

[1076] Перфильев 2003; Росич 2005.

[1077] Указ Президента РФ от 23.11.1995 N Пр-1694. “Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов” [Online]. Available: http://lawru.info/dok/1995/11/23/n453820.htm [Accessed: 23rd March 2019].

formed an information infrastructure. The Concept promoted the discarding of monopolization of information, bureaucratic stove-piping, and the tradition of secrecy. It encouraged the connection of the Russian information space to the European and global information spaces. The Concept contained many of the kibernetik ideas of the 1960s and 1970s, but instead of centralized control, it emphasised the benefits gained from the freedom of information. Nevertheless, the development of the EIP would be guided by vertical and horizontal cooperation in which the state customer would drive the development, and 'discipline' would be maintained through a state register, standardization, and licensing. The development of the policy of EIP was given to the FAPSI, i.e. the division of the KGB which had been responsible for eavesdropping and cryptography.[1078]

The planned unified information space would connect the state leadership and power ministries and could be used to coordinate 'operational' actions in peacetime and during special time[1079]. It would include information and communications necessary for the peacetime management of the military, strategic reconnaissance and warning, mobilization, command and control necessary for strategic deployment through a system named 'Shirota'. The concept does not indicated which parts of the Shirota system would be connected to the larger 'information space of public authorities' if any.[1080] When the discussion about the draft Information Security Doctrine began in 1995-1997, the ideas that the FAPSI and the military had were in fact based on an intranet, which would be protected against outside interference, and not on the Internet.[1081] The Concept of the Formation and Development of a Unified Information Space was eventually buried, although it gave rise to some plans to create unified communication networks between the Russian security institutions and between the countries belonging to the Commonwealth of Independent States.[1082] Moreover, the Concept had included a mention of the 'Automated information exchange system between member states of the CIS' (ASIO CIS).[1083]

Consequently, in 1996 the CIS adopted the Concept of the Formation of Information Space of the CIS.[1084] This Concept aimed at synchronizing the regulation and potentially integrating the national information spaces of the CIS countries. It defined the information space of the CIS as a collection of national information spaces that interacted based on intergovernmental agreements. Although the 'national information

[1078] Ibid. On the FAPSI cf. Soldatov & Borogan 2010, 13.

[1079] Special time is a Russian semi-legal concept and it refers to time of civilian crisis or a time before war (Федеральный конституционный закон от 30.01.2002 N 1-ФКЗ (ред. от 01.07.2017) "О военном положении", VII, 14-15 [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_35227/ [Accessed 10 June 2018]; Федеральный конституционный закон от 30.05.2001 N 3-ФКЗ (ред. от 03.07.2016) "О чрезвычайном положении", XII, v [Online]. Available: http://www.consultant.ru/document /cons_doc_LAW_31866/ [Accessed 10 June 2018]; Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 05.12.2017) "О связи", X [Online]. Available: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base =LAW&n=284294&fld=134&dst =417,0&rnd=0.1557327116187115#0 [Accessed 11 January 2018].)

[1080] Указ Президента РФ 1995.

[1081] Thomas 1998.

[1082] Красная звезда. Создается единое информационное пространство. Красная звезда. № 10 1995; Пельц, Александр. Единое информационное поле для силовых структур. Красная звезда № 282 1996; Krasnaia Zvezda. Будет ли в СНГ единое информпространство? Krasnaia Zvezda № 289 1996.

[1083] Указ Президента РФ 1995.

[1084] СНГ. Концепция формирования информационного пространства Содружества Независимых Государств от 18 октября 1996 года [Online]. Available: http://www.cis.minsk.by/page.php?id=7548 [Accessed: 7th March 2019].

space' was not defined, the information infrastructure was, and it basically referred to communications technology or 'information resources'. The information security aspect of the Concept was obvious as it emphasised the regulation of information, not so much infrastructure or economic aspects.[1085] Thus, despite the 'liberal' intentions of both Concepts, they were, at least partly, intended to impose state control over the emerging information space.

The military adopted the term 'information' in the 1990s and began to use it when writing about spaces, infrastructure, and systems of command and control, although without any clear agreement on what those concepts meant.[1086] For B. I. Glazov and D. A. Lovtsov the 'unified information environment' (edinaia informatsionnaia sreda) meant the Internet and other data networks that enabled command and control systems to interact.[1087] The principles of continuity, efficiency, resilience and stealth (nepreryvnost', operativnost', ustoichivost', skrytnost')[1088], and the unity of command were clearly present when Barvinenko in 1999 made his demand for the integration of all government bodies in a unified global information command and control network.[1089] This call was repeated by Contra-Admiral V. V. Biriukov who, moreover, defined the unified information space as the common and unified collection of information systems, resources, technologies, communications, languages, and infrastructure.[1090]

The concept of a unified information space eventually appeared in the 2000 Information Security Doctrine, but was not clearly defined.[1091] Consequently, the Military Doctrine of 2000 mentioned the creation of a unified command and control system of military organizations of the government, the centralization of command and control of all means and forces of air defence, and the creation of a unified defence space of the CIS countries.[1092] Considering the 1995 and 1996 Concepts it is safe to argue that the idea of the EIP had reached the elites already in 1990s. This was to be expected because Berg, Kitov and others had promoted the idea from the 1950s, and because the Internet and 'informatization' by the early 1990s was recognized globally as something important and promising in this regard.[1093]

The unified information space got its current name during the 1990s, but the idea was already present in the 1950s. Although it would exaggeration to claim that the 1990s concept of unified information space was like the kibernetik ideas of a computer controlled socialist command-economy, it had the same idea of controlling information flows to enable a more efficient management of the state. The military seems to have

[1085] Ibid.

[1086] Захаров 1991; Безуглый & Гавриленко 1994; Комов 1994; Фефелов 1993; Кежаев 1996; Калинин & Озеранскии 1997, 55.

[1087] Глазов & Ловцов 1997.

[1088] Игнатов, В.А., Сосюра, О.В., Гусев, В.Ф. О терминологии теории военного управления. Военная мысль № 6 (11-12) 1996, 38-41.

[1089] Барвиненко 1999.

[1090] Бирюков, В.В. Проблемы управления информатизацией ВС РФ. Военная мысль № 4. 1994

[1091] Доктрина информационной безопасности РФ. (Шаклеина 2002).

[1092] Военная доктрина Российской Федерации 2000 г. (Шаклеина 2002).

[1093] European Commission. Conclusion of the G7 Summit "Information Society Conference" DOC/95/2 of 1995-02-26 [Online]. Available: http://europa.eu/rapid/press-release_DOC-95-2_en.htm [Accessed: 24th March 2019].

enthusiastically adopted the information era language in the 1990s. This was unsurprising as it had pursued the unification of its own, but never all, networks already from the 1960s. The concept of EIP was very probably related to the Western terms and concepts associated with the Internet in the 1990s, such as: infospace, hyperspace, cyberspace, the global information society, the World Wide Web etc. Thus, the translation of the term 'edinnoe' in the 'edinnoe informatsionnoe prostranstvo' to 'single' might be more accurate in some cases. Instead of a vertically and horizontally integrated and regulated national network, the sources might have used the EIP to refer to open information sharing networks in the context of the developing (global) information society. However, in the sources used here, this was not usually the case.

4.2.9 Digital sovereignty

'Digital sovereignty', or its parallel concept 'information sovereignty', as a term, has not been used by military scholars writing for Voennaia Mysl' or, for that matter, by any Russian military or civilian theorists that I have been able to find until the 2000s. Nevertheless, 'information sovereignty' was used in the 1996 Concept of the Formation of the Information Space of the CIS, although its substance was not defined.[1094] It seems to have referred to the state's right to control the formation of its information space and especially security in that space. According to a Russian associated professor A. A. Efremov, sovereignty in the 'information sphere' was first discussed in Russia by V. B. Naymov in a conference article in 1999.[1095] Before that the issue was mainly discussed in Western sources.[1096] Be that as it may, territorial integrity and sovereignty have been guiding principles of Russian foreign and security policy from its rebirth after the collapse of the Soviet Union.[1097] Additionally, according to previous studies, a geopolitical approach which emphasises territoriality and sovereignty has been present in the Soviet/Russian security thinking at least from the 1930s.[1098]

The strategic cultural ideas of digital sovereignty and the EIP are related. It is quite clear that the Soviet cybernetists of the 1960s and 1970s were not thinking about a global information network but about a network which would control a territorially distinct economic system.[1099] Although, in the event that socialism had conquered the world, their system might have had acquired global dimensions. In the 1990s the concept of a unified information space of Russia was also clearly state oriented—it defined a distinct Russian information space which would be under state control.[1100] This connection to sovereignty and the EIP would produce the concept of the national segment of the Internet as the basis of digital and information sovereignty in the 2000s and 2010s.[1101] Furthermore, sovereignty in the information space was also strongly

[1094] Содружества Независимых Государств1996.

[1095] Ефремов, А.А. Формирование концепции информационного суверенитета государства. Право - Журнал Высшей школы экономики, № 1. 2017, 201–215; Наумов, В.Б. Интернет и государственный суверенитет. I Всероссийская конференция «Право и интернет: теория и практика». 1999 [Online]: URL: // http://www.ifap.ru/pi/01/r16.htm [Accessed: 10th December 2018].

[1096] Ефремов 2017.

[1097] Концепция внешней политики РФ 1992 г. (Шаклеина 2002, 23).

[1098] Cf. Chapter 4.1

[1099] Gerovitch 2002 & 2008.

[1100] Указ Президента РФ 1995.

[1101] Cf. Chapter 5 and 6.

related to the idea of interstate struggle which, during the 1990s, incorporated the new information-psychological and technological threats to state interests and concomitant modes of confrontation.

In the context of the drafting of the 2000 Information Security Doctrine, S. A. Komov, for example, stated that the Russian information security system is based on constitutional principles including the hierarchical division of power.[1102] Furthermore, the discussion concerning the draft was about protecting Russia from outside influences and was an indication of how important the idea of sovereignty was for the security services and the military.[1103] When the Information Security Doctrine of 2000 was released it connected information security to the sovereignty and territorial integrity of the Russian Federation.[1104] It is safe to argue that whatever ideas the pioneers of the Russian Internet might have had, the state approached the information space, sphere and environment from the viewpoint of state sovereignty.[1105] This was apparent already before 1999 when Russia's draft resolutions on information security was adopted by the United Nations General Assembly in 1998. It stated that "Expressing concern that these [information] technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the security of States."[1106] This expressed concern was about state interests, not about human rights or other global challenges.

Digital sovereignty was something that had been brewing for some time. Its proto version was already present in the thinking of the Soviet and Russian scholars and the security and defence elites in the 1990s in the form of information sovereignty. Moreover, many theorists saw the information struggle as a state- or system-based confrontation and thus related to sovereignty. It resonated quite well with other traditional ideas about the Russian state and its interests in the Russian strategic culture. Previous studies have shown that as the 1990s progressed, a nationalist, statist and civilizationist circle of academicians, politicians, and security and military officers gained influence in Russia.[1107] These people were more ready to see the cyber and information space as an extension of state sovereignty. Consequently, during the 2000s and 2010s information/digital sovereignty was to become a defining term and concept for how the Russian Federation strove to shape cyberspace.

4.3 Summary of historical ideas

From the analysis presented above a few conclusions can be drawn. Firstly, the Marxist-Leninist idea of a struggle between competing social and economic systems was transformed into an information struggle between great powers in which information-technological means are one of the primary tools—or conversely the idea of the struggle was updated to include modern notions of information. Nevertheless, the Russian military viewed these technological tools in a different framework than their civilian

[1102] Комов 1998.
[1103] Thomas 1998.
[1104] Доктрина информационной безопасности РФ. (Шаклеина 2002, 123).
[1105] On these pioneers cf. Soldatov & Borogan 2015.
[1106] United Nations General Assembly. Developments in the field of information and telecommunications in the context of international security A/RES/53/70 4 January 1999 [Online]. Available: https://digitallibrary.un.org/record/265311/files/A_RES_53_70-EN.pdf [Accessed: 24th March 2019].
[1107] Tsygankov 2016; Sakwa 2008, 381; Mankoff 2012; Donaldson, Nogee & Nadkari 2014.

counterparts. It was interested in the character of a future war.

The different views on a future war—oscillating between massive aerospace surprise attack, regional conflicts, and internal insurgency—seem to have produced a concept of deterrence that expanded from deterrence to prevention and consequently included all forms and means of state power. This was not a new idea. Information-technological means were effortlessly incorporated in the idea of constant struggle between great powers. It can be argued that a defensive strategy and an offensive doctrine were transformed through a dominantly defensive phase into an offensive grand strategy—in the Western parlance. In this context, the security of the state is guaranteed by constantly challenging the competing powers on multiple levels and fronts, to act otherwise is to risk being encircled and suffocated. Russia's foreign policy in the late-1990s reflected this concept, but there were no resources to truly act on it.[1108] Furthermore, during the 1990s Russian military thinkers searched for an alternative deterrence mechanism for the Soviet era's massive conventional and nuclear forces in a new environment which included new threats. In the turn of the millennium this process was still unfinished.

During the Cold war and in the 1990s the Russians considered asymmetry to relate to the correlation of forces between peer competitors—mainly between the United States and the Soviet Union—not, for example, terrorism. Asymmetry was something that affected parity and thus the balance of power, in a way it cost-efficiently exploited the weaknesses of the systems of the side that had temporarily gained advantage and restored the balance (and possibly gained an advantage) by employing science, technology and ingenuity. An asymmetric response (and strategy) was a strategic-level solution which negated the advantage of the opponent—it was part of the dialectics of war where measures and countermeasures were constantly developed. In this context, information superiority was a critical advantage. Informatization had made it so. The side that processed information faster and therefore made better and faster decisions would win a conflict. The Russians recognized the importance of information-technical means in a future war. These were weapons that could be used against the military's command and control systems and the critical information infrastructure of a nation and possibly had strategic effects. The Soviets and Russians recognized 'cyber warfare' even if they did not use similar terms and concepts. However, they approached information and computer technology from a wider perspective emphasizing the nation's scientific and technological potential as a source of power. Moreover, the psychological element was almost always understood as the primary aspect and technological tools subordinated to it.

The kibernetik ideas of ASUs, unified information space, and their ultimate end state of digital sovereignty went through a long and arduous incubation period. They brought with them into the next millennium the idea of a centralized, vertically commanded and controlled, horizontally integrated system of systems in the information sphere, where systems would fight systems. Ideally, the Russian information space would be free and controlled at the same time and it would provide unforeseen economic benefits through information sharing. Nevertheless, the Internet and the Rus-

[1108] Sakwa 2008; Mankoff 2012; Donaldson, Nogee & Nadkari 2014; Tsygankov 2016.

sian information society were left to develop on their own during the 1990s—admittedly there were more pressing issues that needed attention during that decade. When the Russian government called upon the power ministries, academia, and industry in 1995 to formulate a strategy for Russia to handle the challenges of the information era, sovereignty was the principle around which the approach was built. The implementation of this 'strategy' produced a persistent Russian policy of promoting information sovereignty in the UN, but domestically its effects would not materialize before the reign of Vladimir Putin.

The analysis of strategic cultural ideas conducted in this chapter points yet to one additional finding. The epistemic communities have had a definite role in providing new ideas to the Soviet and Russian elites in the course of history. There have been definite 'circles' of people who have offered their ideas to the elites. The military and civilian cybernetists of the 1950s and 1960s were such groups, kagebists and gereushniks (the KGB and GRU operatives who acquired party membership and influence)[1109] were another, the institutchiki of the 1980s were a third group, and the military and ex-KGB/FSB officers of the mid to late 1990s seem to form a fourth group. It is noteworthy that the formidable KGB was divided into the FSB, the SVR, the FSO and the FAPSI and that the military intelligence was much reduced in the 1990s.[1110] Like the future president Vladimir Putin who went to serve in the city administration of St. Petersburg, people retired from the security services because of economic problems and/or ideological disillusionment and formed new communities and (fragmented) interest groups with a certain worldview.[1111] These people had academic credentials and held high positions in scientific institutions sometimes emigrating to the decision-making elite itself.[1112] However, a shared worldview did not mean that these people held homogenous causal beliefs or that their institutional interests coalesced, quite the contrary.[1113]

Domestic politics, bureaucratic infighting, and the change of strategic environment probably affected the way strategic cultural ideas were adopted. According to William D. Jackson, the views of the Russian civilian leadership and the military were increasingly at odds in the 1990s.[1114] Nevertheless, as conservative forces made a comeback in the political arena around 1993, the ideas carried by the armed forces and security services started to influence political elites, which in many cases were themselves ex-military or ex-KGB/FSB.[1115] The national security documents of 2000 were practically

[1109] Haslam 2015; Garthoff, Raymond L. Soviet Leaders and Intelligence: Assessing the American Adversary During the Cold War. Washington, DC: Georgetown University Press, 2015.

[1110] Bennett, Gordon. The Federal Security Service of the Russian Federation. Conflict Studies Research Centre, March 2000 [Online]. Available: https://www.files.ethz.ch/isn/96631/00_Mar_3.pdf [Accessed: 5th December 2018]; Meakins 2018.

[1111] Jackson 2002; Myers 2015, 68; Sakwa 2008, 100-102; Herspring, Dale R. The Kremlin and the High Command: Presidential Impact on the Russian Military from Gorbachev to Putin. Lawrence, KS: University Press of Kansas, 2006; Marten 2017; Soldatov & Borogan 2010.

[1112] Cf. Chapter 5 for just such career-paths.

[1113] Coopersmith, Jonathan. The Dog That Did Not Bark during the Night: The "Normalcy" of Russian, Soviet, and Post-Soviet Science and Technology Studies. Technology and Culture, Vol. 47, No. 3 (July 2006), 623-637; Herspring 2006; Soldatov & Borogan 2010; Sakwa 2008.

[1114] The Russian military did not share the political leadership's optimism and claimed that the potential military threat of NATO and United States had not subsided. (Jackson 2002).

[1115] Bennett, Gordon. Vladimir Putin & Russia's Special Services. Defence Academy of the United Kingdom, Conflict Studies Research Centre, August 2002 [Online]. Available: https://www.files.ethz.ch/isn/96481/02_Aug_4.pdf [Accessed: 5th December 2018].

drafted by the siloviki and the future President, the ex-Director of the FSB, Vladimir Putin took part in writing them.[1116] The international environment of Russia had changed with the enlargement of NATO, the war in Yugoslavia with its consequences for Russia's status as a great power, with the two wars in Chechnya, and the economic crisis of 1998. Therefore, the epistemic communities involved in security and defence policy were able to offer their ideas to reorient Russia and practically moved from outside experts to inside policy makers as Putin started to build his regime.[1117] This was not a smooth and all-encompassing transition as the FSB, the Ministry of Defence, the General Staff and others fought with each other for power, money, and influence.[1118] It should be noted that the empirical use of the concept of epistemic communities has its challenges in such political systems as the Soviet Union of the Russian Federation. Available sources are not complete enough and political processes are quite opaque. However, it can be claimed that there was a community or communities of academics and specialists present and able to influence the elites as they faced a new and challenging millennium.

[1116] Blank 2011; Thomas 1998a; Godzimirski 2000; de Haas, Marcel. An analysis of Soviet, CIS and Russian military doctrines 1990–2000, The Journal of Slavic Military Studies, Vol.14, No.4 (2001), 1-34; Sakwa 2008.

[1117] Blank 2011; Thomas 1998a; Vendil, Carolina. The Russian Security Council, European Security, Vol.10, No.2 (Summer 2001), 67-94; Sakwa 2008, 101-102; Soldatov & Borogan 2010.

[1118] Blank 2011; Soldatov & Borogan 2010; Locksley 2001.

5

PUTIN ERA IDEAS

This chapter continues to find answers to the thesis' research problem's analytical part, that is, identifying and examining strategic cultural ideas related to cyberspace and cyber power present in the discourses of Russian defence and security policy oriented epistemic communities and elites. This chapter aims to examine what ideas were present when the Russian security policy towards cyberspace changed in 2011-2015 and the Russian state began to control and shape a part of cyberspace into a national segment of the Internet. The objective is to demonstrate that the strategic cultural ideas analysed in Chapter 4 were present and available to the elites and to observe how the ideas were reflected in the highest national security documents. Chapter 6 will concentrate on the policy and implementation level. The analysis in this chapter concentrates on studying ideas not the persons writing about them. However, in order to show how the ideas could have transferred from the epistemic communities to the security and defence policy elites I trace and present some academic and professional histories of the most important writers—I will do so mainly in the footnotes.

This chapter starts with an examination of how strategy is made in Russia to understand how strategic ideas might end-up in the highest national security documents and what these documents are. The structure of this chapter then follows the analysis of strategic cultural ideas in descending order from the more political and strategic to the more technical. In the sub-chapters, the ideas are analysed in chronological and thematical order. The contextualization of these ideas is included in the analysis where necessary, but the broader international environment is analysed in Chapter 6. I end the chapter with a comparison of the relationship between the Russian ideas and the theoretical concepts presented in Chapter 3. I also discuss the nature and role of the Russian military and epistemic defence communities which have been the carriers of the ideas analysed in this chapter.

5.1 Strategic planning and the national security documents

The Russian foreign and defence policies belong to the mandate of the president of the Russian Federation and many Western scholars argue that foreign policy and major national security policies are made, or at least ultimately decided by the president.[1119] Although the president's authority is paramount in foreign policy and security issues,[1120] the Russian political system has characteristics which influence national foreign and security policy decision-making. After Putin consolidated his power in the

[1119] Sakwa 2009; Mankoff 2012; Bobo 2015; Cadier & Light 2015; Tsygankov 2016 & 2018.

[1120] IIFFMCG. Independent international fact-finding mission on the conflict in Georgia, report, volume I-III, 2009 [Online]. Available: http://www.mpil.de/en/pub/publications/archive/independent_international_fact.cfm [Accessed: 25th March 2019]; Россия-24. Крым. Путь на Родину, ВГТРК, Россия-24, 15.3.2015 [Online]. Available: https://www.youtube.com/watch?v=t42-71RpRgI [Accessed: 15th March 2019]; Замахина, Татьяна. Совфед разрешил использование ВС в Сирии. Российкая Газета 30.09.2015 [Online]. Available: https://rg.ru/2015/09/30/armia-site.html [Accessed: 25th March 2019].

early 2000s, this system has been claimed to be either highly patrimonial, monolithic and vertical[1121], ruled by bureaucratic capitalists under Putin[1122], autocratic[1123], or, later on, to be based on clans, blocks and networks with tight connections between political and economic power and highly unofficial procedures in which the president is the final arbitrator.[1124] Thus, nothing definite about the way certain ideas end up in official documents, i.e. how and by whom they are chosen, will be offered in this analysis. The national security documents will be approached as the official and public presentation of the state elite's worldview, interests and strategies drafted through a bureaucratic process of negotiation under strong presidential guidance.[1125]

According to Julian Cooper and Andrew Monaghan, strategic planning (or strategy) and mobilization are particular features of Russian political culture and have be encoded in federal laws.[1126] Nation-level planning derives its attraction from the Soviet era economic planning.[1127] Cooper divides Russian strategic planning into socio-economic and national security activity, and places its modern roots in 1995–1997, although, the process was not institutionalized until 2006–2009.[1128] In 2006 the Security Council organized an inter-agency commissions for strategic planning and president Putin called for a more comprehensive approach to socio-economic development.[1129] No official reason for this interest in planning was offered—Cooper believes it was related to worsening Russia–U.S. relations and Monaghan points to internal problems

[1121] Blank, Stephen J. Perspectives on Russian Foreign Policy. Army War College Strategic Studies Institute (SSI), 2012 [Online]. Available: http://ssi.armywarcollege.edu/pdffiles/pub1115.pdf [Accessed: 29th October 2018]; Shevtsova, Lilia. Post-communist Russia: a historic opportunity missed. International Affairs Vol. 83(5) (2007), 891–912.

[1122] Trenin, Dmitri. Russia Redefines Itself and Its Relations with the West. The Washington Quarterly, Vol. 30 (2), 95–105.

[1123] Freedom House 2018.

[1124] Ledeneva 2013, 248-250; Gvosdev, Nikolas K. and Marsh, Christopher. Russian Foreign Policy: Interests, Vectors, and Sectors. Los Angeles: SAGE Publications, Inc., 2014, 49-54.

[1125] Russian military doctrines and other national security documents have been studied before by Western scholars, few of the most recent ones are. Cadier & Light 2015; Pynnöniemi, Katri and Mashiri, James. Venäjän sotilasdoktriinit vertailussa: Nykyinen versio viritettiin kriisiajan taajuudelle. [Russian military doctrines in comparison: Current version tuned to emergency frequency] FIIA-Raportti 42. Helsinki: Ulkopoliittinen instituutti, 2015; Forsström, Pentti. Venäjän sotilasdoktriinien kehittyminen Neuvostoliiton hajoamisen jälkeen. [The development of Russia's military doctrines after the fall of the Soviet Union] National Defence University, Department of Warfare, Series 3: Working Paper No. 3 [Online] Available: https://www.doria.fi/ bitstream/handle/10024/123521/Ven%C3%A4j%C3%A4n%20sotilasdoktriini%20ja%20sen%20kehittyminen%20Forsstr%C3%B6m%20%28netb5%29.pdf?sequence=2 [Accessed: 25th October 2018]; Tsygankov, Andrei (ed.) Routledge Handbook of Russian Foreign Policy. London: Taylor & Francis Ltd., 2018.

[1126] Monaghan 2014; Monaghan, Andrew. Russian State Mobilization: Moving the Country on to a War Footing, Chatham House Research Paper, May 2016; Monaghan 2017; Cooper, Julian. Reviewing Russian Strategic Planning: The Emergence of Strategy 2020. NDC Research Review [Online]. Available: http://www.ndc.nato .int/download/downloads.php?icode=338 [Accessed: 26th March 2019]; Cooper 2016; Cooper, Julian. Strategic Planning, Situation Centres and the Management of Defence in Russia: An Update. Changing Character of War Centre, Pembroke College, Oxford [Online]. Available: http://www.ccw.ox.ac.uk/ blog/2018/11/14/strategic-planning-situation-centres-and-the-management-of-defence-in-russia-an-update-by-julian-cooper [Accessed: 25th March 2019].

[1127] Cooper 2012, 1. According to the general secretary of the Security Council and ex-FSB director Nikolai Patrushev, this planning is based on the experience acquired during the Soviet times. (Патрушев, Николай. На сильных не нападают Крайне желательно понимать, как, а главное – зачем эволюционирует парк отечественных средств вооруженной борьбы во всей обозримой перспективе. ВПК, № 12 (480) за 27 марта 2013 года.)

[1128] Cooper, 2-3.

[1129] Ibid., 3.

and failed reforms.[1130] In 2009 the president gave a classified order 'On the foundations of strategic planning' which defined strategic planning as "determining the main directions, methods and means of achieving strategic goals of stable development of the Russian Federation and ensuring its national security"[1131] and gave guidelines for drafting the main documents.[1132] Additionally, around 2008-2009 an order for drafting a law for strategic planning was given. The law was finally adopted in 2014.[1133]

The law on strategic planning defines strategic planning as the activity of setting goals, forecasting, planning, and programming the socio-economic development of the state. Its objective is to ensure the national security of the Russian Federation and its sustainable socio-economic development.[1134] Strategic planning includes the monitoring and controlling of the implementation of the goals set in the strategic documents. It encompasses federal, subject and municipal authorities. The socio-economic part of the planning belongs to the government's responsibility and the national security part to the Security Council. The main goal-setting documents on the federal level of strategic planning include the President's Annual Address to the Federal Assembly, the Strategy of Social-Economic Development, the Strategy of National Security and the Strategy of Scientific-Technological Development of the Russian Federation. From these are derived the sectoral and regional documents of goal-setting, forecasting, planning and programming.[1135] Strategic planning also includes the secret Defence Plans (issued in 2013 and 2015).[1136] These Plans are presented to the President by the Minister of Defence but drafted in cooperation with 49 ministries and agencies.[1137] The Defence Plan "identifies potential risks and threats to the security of the state, determines the direction of development of the Armed Forces, the implementation of weapons programmes, as well as questions of mobilization preparation and territorial defence."[1138] Part of the strategic planning process include the state armament programmes (GPV-2021 and GPV-2027) which have been drafted for 10-year periods to produce future weapons, military and special equipment. Andrew Monaghan has argued that behind the idea of strategic planning is Putin's need for manual control of the power vertical of the Russian state.[1139] Monaghan also argues that the so-called May Edicts of 2012 have become part of strategic planning.[1140] A new set of Edicts was adopted in 2018.[1141]

[1130] Ibid., 4; Monaghan 2017, 22.

[1131] Указ Президента РФ от 12 мая 2009 года № 536. Об основах стратегического планирования в РФ [Online]. Available: http://lj.rossia.org/users/anticompromat/587675.html [Accessed: 26th March 2019].

[1132] Ibid; Monaghan 2017, 22.

[1133] Cooper 2012 & 2014.

[1134] Федеральный закон 2014a.

[1135] Monaghan 2017.

[1136] Ibid., 24-25.

[1137] Kremlin.ru. Президенту представлен План обороны Российской Федерации 29 января 2013 года [Online]. Available: http://www.kremlin.ru/events/president/news/17385 [Accessed: 12th February 2019]; Гаврилов, Юрий. Защитят по плану Оборону расписали на пять лет вперед. Российская газета - Федеральный выпуск № 260(6831), 17.11.2015 [Online]. Available: https://rg.ru/2015/11/17/oborona-site.html [Accessed: 12th February 2019].

[1138] РИА Новости. План обороны России на 2016–2020 годы введен в действие 1 января 2016 [Online]. Available: https://ria.ru/20160101/1352552856.html [Accessed: 12th February 2019].

[1139] Monaghan 2014, 16-17.

[1140] Ibid., 23.

[1141] Указ Президента Российской Федерации от 7 мая 2018 г. N 204 "О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года" [Online]. Available: https://rg.ru/2018/05/08/president-ukaz204-site-dok.html [Accessed: 26th March 2019].

Strategic planning is related to the Russian concept of mobilization. Mobilization has two aspects, military and economic, and it refers to the measures to activate state human and material resources for military-political and national grand strategic goals. It is a peacetime activity, conducted in advance of conflict through preparation (podgatovka) and readiness (gotovnost').[1142] The idea of mobilization has Soviet roots as it became one of the basic pillars around which Soviet economy and society were built.[1143] The system of mobilization degraded from the 1980s but it was reinvigorated around 2008-2011 and in 2013 Putin approved a new mobilization plan for the economy.[1144] According to the Law On Preparation of Mobilization and Mobilization of the RF, mobilization means a set of measures to transfer the Armed Forces and other military forces and the economy and administration of the state to war time conditions and organization. Its main principles are centralized leadership; timeliness, planning and control; complexity and consistency. Mobilization includes the state management of national telecommunications.[1145]

In this Chapter I will analyse the National Security Strategies of 2009 and 2015, Military Doctrines of 2010 and 2014, Foreign Policy Concepts 2008, 2013 and 2016 and the 2016 Information Security Doctrine as the main products of strategic planning. Other documents will be analysed in Chapter 6. The Security Council of the Russian Federation, led by the president, has an important role in drafting these documents. The Strategy and Doctrine of 2009 and 2010 were a result of a power struggle between the MoD and the General Staff and reflected a resurgent Russia and a poorly conducted war with Georgia in 2008, so the documents are more or less as a compromise of interests.[1146] It is safe to argue that the Foreign Policy Concept of 2013 was prematurely published. The Military Doctrine of 2014, and the rest were drafted in the context of the war in Ukraine, and in accordance with the new legislation concerning strategic planning.[1147] The public infighting between defence and security elites had at this point disappeared behind the need to show national unity and tightened security.[1148]

5.2 Interstate struggle

This chapter provides an in-depth analysis of the strategic cultural idea of interstate struggle or confrontation—the translation depending on the context the concept is used in. As was noted in Chapter 4, the idea of an interstate struggle or confrontation

[1142] Monaghan 2017, 10.

[1143] Cooper 2016.

[1144] Cooper 2016, 19-20.

[1145] Федеральный закон от 26.02.1997 N 31-ФЗ (ред. от 18.12.2018) "О мобилизационной подготовке и мобилизации в Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_13454/ [Accessed: 26th March 2019].

[1146] Bouldin 2004; Bartles, Charles K. Defense Reforms of Russian Defense Minister Anatolii Serdyukov, The Journal of Slavic Military Studies, Vol.24, No.1 (2011), 55-80; Herspring 2006; McDermott 2009, 485-501; McDermott 2015; Blank, Stephen J. "No Need to Threaten Us, We Are Frightened of Ourselves, " Russia's Blueprint for a Police State, The New Security Strategy. In Blank & Weitz, 2010, 19-149, 94. [Online] Available: https://ssi.armywarcollege.edu/pdffiles/PUB997.pdf [Accessed: 22nd October 2018]; Kipp 2011.

[1147] Monaghan 2017.

[1148] Forsström argues that that while the discussion about the 2010 Doctrine was open, in the case of the 2014 Doctrine it was not. The Doctrines of 1993 and 2000 were declared as documents of a transitional period while 2010 was not. (Forsström 2016).

frames all the other strategic cultural ideas. My focus will be on the information aspect of this struggle.

In 2001 the PIR Center[1149] published a book edited by A. V. Fedorova and V. I. Tsygichko called 'Information challenges of national and international security'.[1150] Among the contributors for the book were people from the SVR, the FSB, the Ministry of Interior, the Foreign Ministry, the Security Council, the General Staff of the Armed Forces like A. V. Krutskikh, G. L. Smolian, A. A. Strel'tsov, D. S. Chereshkin and V. N. Tsygichko who all would feature prominently in the Russian information/cyber policy circles in the years to come.[1151] The book is also proof of the concentrated effort of the 'siloviki' to form a united view on the rising challenge that was the Internet and, consequently, information warfare. The book was written to support the Russian effort in the UN to push through an international agreement to ban 'information weapons' and to create transnational regulation of the Internet.

The book defined information security as the countering of adversary influence towards the most important information systems of the state, and also towards democracy, development of society etc.[1152] Information space (also infosphere) was defined as "a sphere of human activity related to the creation, transformation, and usage of information, including individual and societal consciousness, information-telecommunications infrastructure and intrinsic information."[1153] The writers also claimed that globalization has led to the creation of a worldwide unified information space (edinnoe informatsionnoe prostranstvo). They also used the term cyberspace 'kiberprostranstvo.'[1154] The authors claimed that the information industry would form the basis for future economic systems and mass media had gained new powers to influence government policies and societies. The dependence of society, material production, and the armed forces on information technologies and infrastructures has emphasized the importance of resilience (ustoichivost') of communications systems and networks. The authors echoed Marxist-Leninist historical materialism when they argued that the 'information society' is a concept based on the forces and means of production, not the freedom and prevalence of information in societies.[1155]

The authors of the book claimed that the threats against the information infrastructure and resources, including critical infrastructure, are for a large part related to intergovernmental confrontation (protivoborstvo), the proliferation of information

[1149] The PIR Center is an independent organization and was established in 1994. Its main research subject is international security and it has a workgroup on international information security and global management of the Internet. It is connected to the Ministry of Foreign Affairs and the Ministry of Defence and to such academics as V. N. Tsygichko. (Иванов, И. С. (ред.) Военно-политические исследования в России. М.: НП РСМД, Весь мир, 2014). Tsygicko himself is a professor and member of RAN. He is a retired Colonel and worked at the Research Institute of the General Staff Headquarters in 1962—1971, took part in Soviet strategic planning in 1979—1985, and worked at the Institute of System Analysis of RAN from 1985 and as an expert of information security for the Ministry of Foreign Affairs from 1995 (Hoffenaar & Findlay 2007, 41-42).

[1150] Федорова, А.В., Цигичко, В.Н. (общ. ред.) Информационные вызовы национальной и международной безопасности. М.: ПИР-Центр, 2001.

[1151] ТАСС. В России создана Национальная ассоциация международной информационной безопасности 10 апреля 2018 [Online]. Available: http://tass.ru/obschestvo/5111643 [Accessed: 28th March 2019].

[1152] Федорова & Цигичко 2001, 11.

[1153] Ibid., 234.

[1154] Ibid., 91. This is defined as a synonym to information space or datasphere. Other words with a 'kiber' prefix have synonyms with the 'information' prefix (Ibid., 222).

[1155] Федорова & Цигичко 2001.

weapons (informatsionnoe oruzhie), and efforts to create a concept of an information war (informatsionnaia voina). Information weapons could be used through the global information network as tools of political pressure, deterrence, and warfare to produce strategic effects. Nevertheless, the kinetic information-technological aspect of these weapons was not their main function. The authors argued that the 'developed democratic countries' would resort to 'information weapons' in pursuit of their interests as the interdependence created by globalization and their technological advantages enabled it, and their political systems discouraged the use of direct force. Accordingly, they claim that borders are becoming increasingly eroded which leads to the loss of state sovereignty. Although the writers emphasised state-related threats they also discussed crime and terrorism-related threats.[1156]

For Fedorova and Tsygichko et al., in contrast to an information war, an information struggle or confrontation (protivoborstvo) is either a distinct phase of non-military relations which might lead to the achievement of political objectives without the use of force, or a type of warfare using special means to affect an opponent's information systems. In the military sense, information warfare is divided into counter C2 warfare, information security, EW, psychological influence, hacker wars, economic wars, and cyberwarfare.[1157] The authors claimed that information superiority (informatsionnoe prevoskhodstvo) will decide future wars and that it is based on the capability to acquire more information, to process it faster and to make decisions more efficiently. They defined an information war (informatsionnaia voina) as military actions in information space and divided this into offensive and defensive versions, both of which used information. Weapons were divided into information-psychological and technological weapons. Information weapons could be used independently or parallel to traditional weapons. They were used mainly to gain information superiority, which was not, however, an objective in itself. The weapons should be based on precise, covert, and non-lethal means in distinction from weapons of mass destruction. Militarily, information weapons could be used to gain a strategic surprise. Additionally, the secret or unseen nature of these weapons could lower the threshold for the use of nuclear weapons.[1158]

After analysing information weapons and warfare, Fedorova and Tsygichko et al. discussed the Unites States' and its allies' military operations from the 1980s and pointed out information warfare elements in them. This 'method' is repeated in most of the monographs and articles analysed in this thesis and it arguably shows who the Russians see as leading the military technological and doctrinal development, and who they consider as their probable or main enemy.[1159] Interestingly, the writers bring up the concept of netwars[1160] (setevaia voina) in the context of terrorism and argue that states can use networked terrorist organizations as part of information operations.[1161] As will become clear in this chapter, this view evolved during the next two decades

[1156] Ibid.

[1157] Martin Libick's categorization is used to discuss about 'informatsionnoe protivoborstvo'. Libicki 1995.

[1158] Федорова & Цигичко 2001.

[1159] For the terms 'main enemy' and 'probable enemy' cf. Haslam 2015, 265. China is also mentioned as a possible competitor but only passingly (Федорова & Цигичко 2001, 139).

[1160] The concept was introduced by John Arquilla and David Ronfeldt and it refers to low-intensity conflict on a societal level waged by networks using information, among other means. (Arquilla, John and Ronfeldt, David. The Advent Of Netwar. Santa Monica: RAND, 1996).

[1161] Федорова & Цигичко 2001, 137.

from terrorists and separatist, to colour revolutions, to controlled chaos, and to hybrid wars, and forms one of the main threat images of the Russian armed forces. Moreover, technological backwardness, and thus dependency on foreign technology, the possibility of Russia being disconnected from international information networks, and negative foreign cultural effects are mentioned as the main threats of an information confrontation. Therefore, the writers argued, Russia needs to adopt an active role in information confrontation instead of passive isolation. It must use information-psychological and information-technological offensive measures in the opponents' information space and defensive measures in its own space.[1162] In summary, the book by Fedorova and Tsygichko et al. includes many of the themes and concepts present in the later Russian IW debate and demonstrates that the Russians were keenly following Western debates.

Igor Panarin is a professor and political scientist who worked for the KGB from 1976 to 1991 and after that for the FAPSI. He is a member of the Academy of Military Sciences (AVN) and has academic positions in the Diplomatic Academy of the Ministry of Foreign Affairs of Russia and the Moscow State Institute of International Relations (MGIMO).[1163] He has specialized in psychological information warfare and has written over twenty books mainly on information warfare. Panarin bases his arguments on geopolitics and on ideas about Russia (or 'Rus') as a culturally distinct and special entity. He views these issues in the light of an information revolution which has turned information into power and information security into a critical security issue. During the latter part of the 20th century the great powers waged information war (informatsionnaia voina) against each other for spiritual, political and economic power, and consequently, the Soviet Union was destroyed by the West.[1164] Because Panarin approaches mental activity as an adaptive system, he can be grouped together with other Russian 'system theorists', although he does not favour formal logic or mathematical models.[1165]

According to Panarin, a unified global information space (edinnoe mirovoe informatsionnoe prostranstvo) has been created in which leading countries face each other in a geostrategic struggle (protivoborstvo) to attain information superiority in the global information space.[1166] Panarin argues that the Russian elites must develop a doctrine which would lead to the unity of humanity and to the prosperity of Russia

[1162] Ibid., 141.

[1163] According to Jolanta Derczewska Panarin's writings have influenced the formulation of the 2000 Information Security Doctrine and generally Russian views on information warfare. (Darczewska, Jolanta. The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study. Warsaw: Centre for Eastern Studies, 2014, 13-14.) AVN is a non-governmental interregional scientific-research institution which employs over 1,400 active and retired military personnel as researchers, press-correspondents and lecturers. It is tightly connected to the Armed Forces of the RF. Its main research subjects are military-political and strategic issues, the character of war and forecasting future war (Иванов 2014, 19). MGIMO is an academic institution run by the Ministry of Foreign Affairs of Russia. It is a teaching university with scientific centres like military-political studies and international information security and scientific-technological politics centres. (МГИМО. [Online]. Available: https://mgimo.ru/about/ [Accessed: 28th March 2019]).

[1164] Панарин, И.Н., Панарина, Л.Г. Информационная война и мир. Москва: ОЛМА-ПРЕСС, 2003; Панарин, И.Н. Информационная война и геополитика. М.: Поколение, 2006; Панарин, И.Н. Информационная война и Третий Рим. М.: 2003; Панарин, И.Н. Первая мировая информационная война: развал СССР. СПБ: Питер, 2010; Панарин, И.Н. СМИ, пропаганда и информационные войны. М.: Поколение, 2012.

[1165] Панарин & Панарина 2003, 18, 222-225.

[1166] Панарин & Панарина, 2003.

and the whole world.[1167] Panarin argues that the U.S., Great Britain and some other countries are waging an information war against Russia to weaken it because of its newfound strength, and, therefore, the elite and the people must be protected from negative information flows.[1168] Panarin distinguishes between information warfare (informatsionnaia bor'ba) and a geopolitical information struggle (geopoliticheskoe informatsionnoe protivoborstvo). The former is a form of warfare, possibly initiated already in peacetime, in which special (political, economic, diplomatic, military and other) methods, ways and means are used to influence the information environment, or systems of management and control of the opposing side and to protect one's own side to achieve desired goals.[1169] The struggle is defined as a modern form of interstate struggle, as well as a system of measures, to violate the information security (integrity and resilience of control systems, public opinion, state leadership and decision-making) of another country and to defend against similar actions and to gain information superiority in the global information space.[1170] Panarin, like other Russian writers divides information warfare into information-technological and information-psychological types according to their target, i.e. technological systems or the individual psyche, societal consciousness or decision-making systems.[1171] Panarin argues for the establishment of a centralized 'information-analytical bureau' and later develops this to 'a system of information struggle' (sistema informatsinnogo protivoborstva).[1172] Panarin's ideas are representative of the 'holistic' views that some Russians have had on information warfare. Moreover, the cybernetic idea of, usually centralized, intragovernmental, or a hierarchical 'government information management' system has been repeated by many Russian civilian and military scholars.[1173]

Andrei Viktorovich Manoilo is a professor and political scientist who served in the FSB from 1998 to, at least, 2002 after which he has worked at the Russian Academy of Public Administration (later incorporated to RANEPA)[1174], and the MGIMO. He is currently a member of the Scientific Council at the Security Council of the Russian Federation. He has specialized in and written extensively about psychological information warfare especially in the timeframe of 2003-2008. Manoilo has co-authored some of his most known works with Dimitrii Borisovich Frolov, a doctor of political science, and the Director of finCERT at the Bank of Russia, and Anatolii Ivanovich

[1167] Ibid., 301; Панарин 2006, 170-171; Панарин 2003.

[1168] Панарин & Панарина 2003, 248-249; Панарин, И.Н. Инструмент внешней политики. ВПК, № 32 (248) за 13 августа 2008 года; Панарин, И.Н. Система информационного противоборства. ВПК, № 41 (257) за 15 октября 2008 года.

[1169] Панарин & Панарина 2003, 20-21; Панарин 2006, 172-173; Панарин И.Н. Информационная война и дипломатия. М.: ОАО «Издательский дом «Городец», 2004.

[1170] Панарин 2006, 172-173.

[1171] Панарин & Панарина 2003, 38-39; Панарин 2006, 173; Панарин 2008b.

[1172] Панарин & Панарина 2003, 136-137; Панарин 2008b.

[1173] Цыганов, В.В., Бухарин, С.Н., Завьялов, О.Ю., Лукьянова, К.А. Национальная система информационного управления и противоборства. Информационные войны, № 2(10) 2009, 2-8; Сергеев, Н.А. Архитектура перспективной сетецентрической информационно-управляющей системы обеспечения национальной безопасности России в новых геополитических условиях. Информационные войны, № 2(14) 2010, 69-84.

[1174] The Russian Presidential Academy of National Economy and Public Administration (RANEPA) is a federal state-funded institution of higher professional education created by combining multiple state education institutions in to one in 2010. It is mainly a teaching institution but conducts also research in areas related to public administration (РАНХиГС [Online]. Available: https://www.ranepa.ru/ [Accessed: 28th March 2019].)

Petrenko, who has a Ph.D. in psychology and is an ex-KGB official.[1175] Below I shall summarize some of the ideas presented by Manoilo, Petrenko and Frolov.[1176]

Manoilo et al. approach their subject from a geopolitical, zero-sum worldview in which the competition (sopernichestvo) between states has moved over to the 'information-psychological space' (informatsionno-psikhologicheskoe prostranstvo). In this space the competition is conducted in the form of an information struggle (informatsionnoe protivoborstvo) which for the weaker side might provide the opportunity for 'an asymmetric response' (asimmetrichnyi otvet).[1177] In this context, globalization is seen as something that strengthens information-psychological aggression as it unifies the global information space, and this can lead to 'information neo-colonialism' (informatsionnyi neokolonializm) where weaker states become sources of strategic resources—information and knowledge.[1178] Accordingly, the control of information networks and flows on and through the state territory is a source of power.[1179]

Manoilo et al. define the information struggle as the rivalry of social systems in the information-psychological sphere over the control of limited strategic resources.[1180] Its principles are, among others, secrecy, surprise, asymmetry, and the massive use of force as means. The aim of an information war (informatsionnaia voina) is to acquire a certain gain in the material realm to secure information superiority (prevoskhodstvo) over the enemy and to inflict material, ideological, or other damage on it.[1181] This superiority is defined as the ability to collect, process and distribute uninterrupted information flows while at the same time denying the same from the enemy. It could also mean faster tempo of information operations than the enemy is capable of, which leads to domination.[1182] Mainoilo et al. argue that information is an inherently asymmetric object because it is constantly changing and takes on new, novel forms and is unpredictable. Additionally, it changes the environment it is part of.[1183] Therefore, information weapons are algorithms used to control other information systems for the someone's benefit and they transform the environment they are part of.[1184] Consequently, for Manoilo et al. the information space (informatsionnoe prostranstvo) is a sphere of action.[1185] It is a dynamic and constructed space and thus only temporary domination is possible. Its information processing functions are nation-dependent, and its nature defines the weapons and warfare used in relation to it.[1186] Information

[1175] Петренко, Анатолий Иванович. Межрегиональное бюро судебных экспертиз Им. Сикорского [Online]. Available: https://www.expertsud.ru/content/view/166/39/ [Accessed: 28th March 2019]; Фролов, Дмитрий Борисович. Высшая школа государственного аудита [Online]. Available: http://itlaw.audit.msu.ru/ [Accessed: 28th March 2019].

[1176] Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны. 3-е изд., стереотип. М.: Горячая линия – Телеком, 2012; Вепринцев, В.Б., Манойло, А.В., Петренко, А.И., Фролов, Д.Б. Операции информационно-психологической войны: краткий энциклопедический словарь-справочник. М.: Горячая линия – Телеком, 2011.

[1177] Манойло et al. 2012, 11-12.

[1178] Ibid., 15-16.

[1179] Ibid., 16.

[1180] Манойло et al. 2013, 318-319.

[1181] Ibid., 68-69, 74.

[1182] Ibid., 280.

[1183] Ibid., 21-23.

[1184] Ibid., 234-236.

[1185] Ibid., 310. Cf. also Information-psychological space (Манойло et al. 2012, 32-37).

[1186] Манойло et al. 2013, 313.

security (informatsionnaia bezopasnost') is the security of the information environment (sreda), and the security of the national interests in the information sphere includes sovereignty.[1187] The sovereignty of a state will be in danger if it does not control the information infrastructure.[1188]

Based on their theory, Mainoilo et al. propose, for example, the creation of a Eurasian information space to counter American unipolar politics.[1189] Although the threat of an information war is ever present, Manoilo et al. do not promote isolation but recommend developing national strength (psychological and technological) and an active policy towards the global information space.[1190] A system of state information confrontation or struggle should be created.[1191] All in all, Manoilo et al. create a synthesis of Western information warfare theories and geopolitical thought and develop the idea of a continuous interstate information struggle for (always temporary) information superiority.

Sergei Nikolaevich Griniaev is a doctor of technical sciences and has worked in various institutions of the Ministry of Defence from the 1990s—for example as a leading researcher at the Centre for Military Strategic Studies of the General Staff[1192]. He is currently the General Director of the Centre of Strategic Estimations and Forecasts (CSEF)[1193] and is a specialist on information warfare.[1194] Griniaev has made Western IW theory known in Russian perhaps more than created his own. In his writings from 2000–2004 Griniaev's basic claim was that information is the most important product and resource of the information economy, and that the 21st century battles will be fought in cyberspace (kiberprostranstvo) where information resides.[1195] Griniaev has argued that information is an instrument of power and that power is connected to geopolitics. Here he referred to Panarin. It should be noted that Panarin and Manoilo respectively refer to Rastorguev and that the Russian IW theorists know each other's work.[1196] Griniaev translated the Western IW as an information struggle or confrontation (informatsionnoe protivoborstvo) and defined it as a multifaceted impact on

[1187] Ibid., 28-29.

[1188] Ibid., 261. They refer to Батурин, Ю. М. Телекоммуникации и право (Вопросы стратегии). Москва: Центр "Право и СМИ", 2000. Baturin uses the term 'information sovereignty' multiple times in the context of law on information.

[1189] Манойло et al. 2012, 72-74.

[1190] Ibid., 85.

[1191] Ibid., 515-517.

[1192] The Centre for Military Strategic Studies of the General Staff (Tsentr voenno-strategicheskikh issledovanii General'nogo shtaba) was established 1985 to study the challenges posed by the U.S. SDI and other strategic weapons related issues. Currently, the Center prepares scientifically based proposals on the construction, development, and use of the Armed Forces and takes part in the drafting of the strategic planning documents and coordinates the drafting of basic main field regulations. (Чекинов, С. Г. Центр военно-стратегических исследований Генерального штаба Вооруженных Сил Российской Федерации история и современность. Военная мысль № 1, 2010, 3-5).

[1193] The Center of Strategic Estimations and Forecasts (Tsentr strategicheskikh otsenok i prognozov) (CSEF) is an independent non-commercial organization established in 2012. Its mission is to propagate Russian geopolitical views of the international order and to network domestic and foreign experts. (Иванов 2014, 110).

[1194] Гриняев, Сергей Николаевич. Центр стратегических оценок и прогнозов [Online]. Available: http://csef.ru/ru/team/5 [Accessed: 18th March 2019].

[1195] Гриняев, С.Н. Глобализация и информационная безопасность. Красная звезда № 4 2.11.10.2000.

[1196] Гриняев, С.Н. Поле битвы - киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. М.: Харвест, 2004, 13. For example, Griniaev's ideas almost completely resemble the ideas of the lesser known V. F. Prokof'ev (Прокофьев В.Ф. Тайное оружие информационной войны: атака на подсознание. М: СИНТЕГ, 2003.)

the system of state and military management of the opposing side, on its military-political leadership. This impact should already in peacetime lead to the adoption of decisions favourable to the initiator of the information measures, and during conflict to completely paralyze the functioning of the target's management processes and infrastructure.[1197] Griniaev claimed that the Western IW is a struggle for knowledge, i.e. "who will know the answers to the questions: what, when, where, why faster and more precisely" and that it aims for information superiority even in peacetime.[1198] Griniaev further argues that 'noonpolitiks' is the basis of the American 21st century information strategy and that the Americans aim to use 'soft power' to achieve national objectives.[1199] The means include 'controlled chaos' (upravliaemoi khaos) which is used to manipulate the networks of a target society.[1200] In an interesting twist of military academic sabre-rattling Griniaev was criticized by Iuri Gorbachev, an influential EW theorist, for misinterpreting Western terms.[1201]

Griniaev defined a proper information war or warfare as a new form of armed warfare, meaning large-scale warfare using methods of information influence to achieve the goals of the influencing party.[1202] Furthermore, he claimed that information war/warfare can be divided into information-psychological and information-technological. The main distinction of information warfare from physical warfare is that it is not aimed at destroying but manipulating the opponent.[1203] The aim of information war/warfare is to gain information superiority, secure the objectives of national military strategy, and foresee and eliminate threats before they emerge, or eliminate them in the initial stage of war—or even before that.[1204] Like Manoilo and Panarin, Griniaev emphasised the economic and financial aspects of information warfare and the grave consequences if a country were to be excluded from the Internet. Thus, he argued that the special services of different countries were strengthening the control of national segments of the global network which might eventually lead to 'virtual state borders in cyberspace' (virtual'naia gosudarstvennaia granitsa).[1205]

The more abstract theories of information confrontation have a definite kibernetik foundation. This is apparent in the works, for example, of Rastorguev, Tsyganov,

[1197] Later, Griniaev translates information warfare and information war both as 'informatsionnaia voina'. (Гриняев 2004, 93-94).

[1198] Ibid.

[1199] Гриняев 2004, 15. 'Noonpolitik' is a term used by John Arquilla and David Ronfeldt (Arquilla, John and Ronfeldt, David. The Emergence of Noonpolitik: Toward An American Information Strategy. Santa Monica: RAND, 1999). It should be noted that Griniaev is not the only Russian theorist who interprets Arquilla's and Ronfeldt's ideas and the concepts of netwars and network-centric warfare quite freely. For example, Vitalii Grigor'ev builds his theory of IW on the claim that NCW is an American geopolitical strategy to manipulate global networks through the Internet-based mass media (Григорьев В.Р. Информационные вирусы – Новое оружие массового поражения. Информационные войны, №3 (7) 2008, 2-29).

[1200] Гриняев 2004, 53, 70-71, 196-198.

[1201] Горбачев, Юрий. К вопросу о "войне в четвертой сфере". В США у нее иная терминология, чем в России, а задачи – всеобъемлющие. Независимое Военное Обозрение, № 14 20.4.2001.

[1202] Гриняев 2004, 96. An exact translation of war/warfare is difficult because Griniaev has to use the Russian words available to explain foreign Western theory while at the same time claiming that these terms had universal value. This problem is, of course, in the heart of this thesis also.

[1203] Ibid., 96.

[1204] Ibid., 101.

[1205] Ibid., 165-167.

Bukharin and Kruglov.[1206] In his book "Mathematical models of information confrontation" (2014) Sergei Pavlovich Rastorguev argues that human societies are self-learning and organizing systems which can be manipulated from the outside through information.[1207] Information weapons are like viruses which reprogram self-learning systems (society or the human mind) and change their structures until the system self-destructs. They are used to activate, destroy, block or create processes in the information system. Rastorguev claims that there is no difference between the concepts of information confrontation/struggle (protivoborstvo), war (voina) and warfare (bor'ba) because an information war is not defined by particular weapons or a state of relationship.[1208] In an earlier book from 1999 Rastorguev argued that systems could defend themselves by creating a barrier between themselves and the source of danger; avoiding danger by moving beyond its reach; through the destruction of the source of danger; and through self-modification beyond recognition. Rastorguev claimed that the last method would be self-destructive if it was done according to the wishes of the aggressor.[1209] Later, Rastorguev introduced the concept of the resilience (ustoichivost') of a system against information weapons, which was based on its ability to resist the change of its elements as societal structures are based on stable (non-fluctuating) knowledge.[1210] According to Rastorguev, the resilience and aggressiveness of systems can be mathematically modelled. This makes it possible to predict how different 'world models' affect each other, and so, in practice, to plan information warfare.[1211] Rastorguev was by far one of the most original Russian thinkers on information warfare. He was not unique in using cybernetic and systems theory but went further than anybody else in trying to give his theories a mathematical and logical basis.

Vladimir Viktorovich Tsyganov and Sergei Nikolaevich Bukharin are also quite influential cybernetists who have written about information security especially in the late 2000s.[1212] They have both worked at the Institute of the Control Sciences in the RAS, which has a strong history of systems theory and cybernetics.[1213] Their main interest has been the management (upravlenie) of information confrontation or warfare (protivoborstvo) as a complex system, and they have tried to formulate a single basic

[1206] Расторгуев 1999; Расторгуев С. П. Математические модели в информационном противоборстве. — М.: ЦСОиП, 2014; Бухарин С. Н., Цыганов В.В. Ситуационный анализ в информационных войнах. информационные войны, №2 (6) 2008, 47-58; Цыганов, В.В., Бочкарева, Ю.Г. Эволюция социальных систем при информационной конфронтации и партийные механизмы обеспечения общественной безопасности. Информационные войны № 3(31) 2014, 12-22; Круглов, В. В. Новый подход к анализу современного противоборства. Военная Мысль, № 12 2006, 50-61.

[1207] The analysis presented here draws on and complements Ristolainen & Kukkola 2019a. Расторгуев 2014, 14.

[1208] Ibid.

[1209] Расторгуев 1999, 116-117.

[1210] Расторгуев 2014, 73-77.

[1211] Ibid., 223-224.

[1212] Цыганов, В.В., Бухарин, С.Н. Информационные войны в бизнесе и политике. М.: Академический Проект, 2007; Бухарин, С.Н., Цыганов, В.В. Методы и технологии информационных войн. М.: Академический проект, 2007.

[1213] The institution was first established in 1939 as the Institute of Automation and Remote Control of the USSR Academy of Sciences. Throughout its history it has produced important theoretical and applied works on automation. Its current customers include almost all of the power ministries. (Васильева, С.Н. (общ. ред.) Институт проблем управления им. В.А. Трапезникова Российской академии наук. Москва: ИПУ РАН, 2014 [Online]. Available: https://www.ipu.ru/sites/default/files/page_file/ 75%20лет%20ИПУ%20РАН.pdf [Accessed: 28th March 2019].)

model and templates for waging information war (informatsionnaia voina).[1214] Tsyganov and Bukharin have used system-theoretical logic to analyse information confrontations and like Rastorguev have claimed that 'civilizations', understood as adaptive complex systems, are the main sources of values which guide the motivations of possible targets of information warfare or operations.[1215] This means that the modern world can be understood as a conflict between competing civilizations through information because kinetic warfare has lost much of its usability. Tsyganov and Bukharin claimed that the objective of an information war is to achieve capital and power, a claim which gives their theory a definite Marxist twist.[1216] Tsyganov and Bukharin have used the term 'voina' and 'protivoborstvo' interchangeably to define a phenomenon that exists in human relations from the corporate level up to the global level. In their view "information war [voina] is a dynamic process occurring in a complex self-organizing system."[1217] Depending on the context, 'protivoborstvo' then means either confrontation. i.e. state of affairs (condition), or warfare, i.e. active engagement through information means.[1218] In an article published in 2013 Tsyganov claimed that the constantly on-going information confrontation is aimed at achieving information superiority over the enemy in military, political, economic and other fields. Russia was losing and, thus, needed 'information troops'.[1219] Moreover, Tsyganov and Bukharin have argued that an information war should be conduct by a centralized and hierarchical 'intellectual mechanism of information war' (IMIV).[1220]

Major General, Professor, Viacheslav Kruglov, who is a member of the Military Academy of Sciences, has used mathematical models based on a theory of the symmetry of chaos and order to theorize about the modern confrontation—and to offer Russia a role as a 'Eurasian harmonizer'.[1221] He, like many others has argued that globalization is directed against Russia. Kruglov has claimed that living systems strive for harmony or equilibrium between their parts and resist forces opposing this process. The parts are ever moving because of a 'triad of forces' and this produces evolution.[1222] This means that war is an eternal condition even if its form changes. Information management and intellectual resources are power for Kruglov in this constant, ongoing battle. Kruglov concluded that Russia should use offensive and defensive actions during peacetime, and that it should use all available methods in wartime, including non-direct or asymmetric means. Moreover, Russia's state and military command and control systems should be unified with the military system having primacy over other control systems.[1223] The system-theoretical-thinking Rastorguev, Bukharin, Tsyganov

[1214] Цыганов & Бухарин 2007, 50-53. The principles of information war are: a systemic approach, self-organization, adaptability, progressiveness, and intellectuality (Цыганов & Бухарин 2007, 179).

[1215] Cf. Rastorguev on civilizations (1999, 99) He defines civilizations as a thing "…conceivable as a reality by a set of living beings with their own material and spiritual culture." Bukharin and Tsyganov define culture as corresponding to a certain level of the stage of social evolution, and material and spiritual culture. (Бухарин & Цыганов 2007, 27)

[1216] Cf. Цыганов & Бухарин 2007, 42-44, 188.

[1217] Цыганов & Бухарин 2007, 40. For an example of the ambiguous use of the terms Бухарин & Цыганов 2007, 166-168, 299.

[1218] Cf. Ibid., 304

[1219] Цыганок А.Д. Информационные войны в начале XXI века. Информационные войны, №4 (28) 2013, 17-29.

[1220] Цыганов & Бухарин 2007, 125-26; Бухарин & Цыганов 2007, 296; Цыганов et al. 2009.

[1221] Круглов 2006; Круглов, В. В. Фундаментальные законы мироздания - Основа новой теории войны. Обозреватель, №8 (187) 2005.

[1222] Круглов 2006, 56.

[1223] Ibid., 58-59.

and Kruglov carry with them the explicit policy recommendation to protect the Russian national information space (or system) from outside influences. This resonated with the widely shared claim that the Soviet Union had been destroyed by Western information operations and Russia was again under similar attack.[1224]

Professor Anatoly Strel'tsov is an ex-military, possibly ex-KGB or GRU, information warfare and policy specialist who has worked in the Security Council of the Russian Federation as an advisor from 1995 and in the Information Security Institute at the Moscow Lomonosov State University from 2012.[1225] Strel'tsov has written extensively about the information security (informatsionnaia bezopasnost') of the Russian Federation beginning from the late-1990s when the basic provisions of state information policy were being formulated.[1226] According to Strel'tsov, information security as a concept entered Russian law in 1992 and politically it was given form in the 2000 Information Security Doctrine, the drafting of which Strel'tsov took part in.[1227] He argued in 2002 that information security (obespechenie informatsionnoi bezopasnosti) is based on the protection of an object from a threat or harm through the action of securing it.[1228] Accordingly, there is such an object as state information security, meaning the functions of controlling society, the protection of which is paramount. Strel'tsov pointed out that information itself and information systems can also be an object of security, which means they must be protected from unauthorised use and manipulation, but also that access to them must be secured. The information sphere is recognized as a distinct sphere of human action and, accordingly, there are national interests in the information sphere which are connected to the legal rights and responsibilities of citizens, the development of society, and the control functions of the state involving information and the information infrastructure—the crosscutting interest being the preservation of national identity. Therefore the information security of the Russian federation is the responsibility of the state, and information security is characterised by a technological-spiritual dualism: social norms, morals and laws are

[1224] Федорова & Цигичко 2001, 144; Панарин 2003, 34; Расторгуев 1999, 174 & 2014, 240-241; Цыганов & 2007, 15; Ковалев В.И., Малков С.Ю. Что делать, чтобы не распасться как ссср? Информационные войны, № 3(35) 2015, 52-57; Калиновский, О.Н. Дискуссионная трибуна. "Информационная война" - это война? Военная мысль, № 1 1.1.2001.

[1225] Strel'tsov has been one of the Russian representatives in the international negotiations concerning cyber security norms and has written several articles and books on Russian information policy and international information security. He is a vice-chair of the National Association of International Information Security (NAMIB) which was established in 2017 and in which belong all the 'household names' of the Russian cyber diplomacy corps, i.e. people participating in the Russian international cyber norm-building project. NAMIB is supported by the Security Council. (Комов, С.А. (под общ. редакцией). Международная информационная безопасность: дипломатия мира. Сборник статей. М: Военинформ, 2009; Стрельцов, Анатолий Александрович. ПИР-Центр [Online]. Available: http://pircenter.org/experts/918-streltsov-anatoly-a [Accessed: 28th March 2019]; Газета.ru «Мы стоим перед новой угрозой» 12 апреля 2018 [Online]. Available: https://www.gazeta.ru/tech/2018/04/11/11714395/namib.shtml [Accessed: 28th March 2019]; НАМИБ. Устав Национальной Ассоциации международной информационной безопасности Протокол № 1 от «10» апреля 2018 г [Online]. Available: http://namib.online/wp-content/uploads/2018/11/Ustav_ NAMIB.pdf [Accessed: 2nd January 2020].

[1226] Емельянов Г.В., Стрельцов А.А. Проблемы обеспечения информационной безопасности субъектов Российской Федерации. Информационное общество, № 6 (1998), 38 - 41.

[1227] Садовничий В. А., Стрельцов А. А. Обеспечение информационной безопасности России: Теоретические и методологические основы. — Моск. центра непрерывного математического образования. М.: 2002.

[1228] Later defined as "activities to prevent harm to the properties of the security object, conditioned by the information and information infrastructure, as well as the means and subjects of this activity." Стрельцов А.А. (и др.) Организационно-правовое обеспечение информационной безопасности. М.: Академия, 2008, 22.

equally important tools as technological and organizational measures.[1229] Strel'tsov's definition of information security is state-centric an obviously formulated in such a way that the state control of information is legitimized.

Later, in 2009 Strel'tsov argued that Russia needed a state information policy to secure the stability and spiritual development of society, and the socio-economic development of the state to strengthen the Russian state as a great power (derzhava).[1230] According to Strel'tsov, the state information policy is about promoting values, strategic communications, and conducting an information-political (non-forceful) and military-technological (forceful) struggle (protivoborstvo).[1231] By 2011 Strel'tsov had updated his views on the information confrontation or struggle (protivoborstvo) to encompass a global information struggle (global'noe informatsionnoe protivoborstvo). Furthermore, he updated the concept of military-technological struggle to mean the creation of coercive (silovoi) means of information-technological influence against enemy governmental and military infrastructure, protection of own information and telecommunications systems related to critical infrastructure, and electronic radio and computer intelligence. The new technological means of confrontation enabled the achievement of political goals when other coercive means were unavailable or ineffective.[1232] Strel'tsov's views moved in a more state-interventionist, almost authoritarian direction between 2003–2011. As he worked during that time in the Security Council of RF, his views can be considered to reflect influential ideas circulating inside the decision-making apparatus.

Army General Makhmut Akhmetovich Gareev is perhaps the most influential Russian military scholar alive. He is Doctor of Science in History and Military Science and has been highly decorated.[1233] Gareev's views are quite traditional, and in 2003 he argued that Operation Iraqi Freedom was not an example of a kind of new type of war or warfare. He did however concede, that in that war, a wide variety of political, economic, and informational actions were used to prepare the battlefield.[1234] In 2005 Gareev pointed out that although states pursued their interest in various harmful ways, the competition between states was not a war if it did not involve the violent use of armed forces. He argued that the initial period of war had gained in importance because of the dominance of aerospace, and information domains had become decisive. Indirect actions with political, economic, and moral effects had become more important and armed combat was penetrated by information warfare (protivoborstvo). Gareev envisioned a war starting with a massive aerospace, information and EW operation followed by a conventional ground assault. To him, a 'non-contact' (beskontaktnyi) war would always be followed by a 'contact' war if the government, people, and most importantly the army (land forces) held together. Gareev openly criticized those Russian scholars promoting three-dimensional, network, asymmetric,

[1229] Стрельцов 2008, 41, 43-49.

[1230] Стрельцов А.А. Государственная информационная политика: основы теории. М.: МЦНМО, 2009.

[1231] Ibid., 48 & 51.

[1232] Стрельцов, А. А. Основные задачи государственной политики в области информационного противоборства. Военная мысль, № 5 2011, 18-25.

[1233] Gareev has been the President of the Academy of Military Sciences since its establishment in 1995. His articles published in various military journals during the 2000-2018 provide an insight into how the Russian military officers, or at least, those working at the Academy have seen the development of interstate struggle and warfare.

[1234] Гареев, М.А. Уроки и выводы из войны в Ираке. Военная мысль, № 8 2003, 68-76.

non-contact, information warfare etc.[1235] This included Vladimir Slipchenko, a fellow military scholar of Gareev, who promoted the idea of a future non-nuclear, non-contact precision war which would be aimed at destroying the economic potential of the opponent. This kind of war would start and end with massive surprise precision strike attacks—possibly by both sides.[1236] A similar view was promoted by the retired General-Lieutenant S. A. Bogdanov, a chief researcher of the Centre for Military Strategic Studies of the General Staff (TsVSI GSh VS RF), in 2003, although he emphasised the role of massive information-psychological pressure before the attack and information superiority (prevoskhodstvo) through disinformation, deception and EW during the attack.[1237]

Despite the official Russian foreign policy, Gareev considered the United States and NATO as potential adversaries.[1238] Consequently, in 2012 Gareev claimed that countries of the world were suffering from infringements on their sovereignty. Russia should work with countries who were prepared for equal partnerships, while at the same time strive to become an independent great power. As Russian national interests, Gareev listed, among others, the creation of a high-tech industry, the preparedness to wage information, psychological and cybernetic war, strategic deterrence, moral-psychological factors and patriotism, which he considered a part of military power. Gareev subscribed to the view that Russia was threatened by a controlled chaos aimed at disturbing the internal stability of the state and overthrowing it.[1239]

For Gareev an international confrontation or struggle are not the same as war.[1240] Before and after the annexation of Crimea, Gareev pushed back on the new concepts of war although he conceded that new forms of international confrontation (protivoborstvo) carried out on the brink of war by veiled or overt violence, required special attention.[1241] Consequently, the U.S. and its allies would use information means to create 'colour revolutions' and used military force in local conflicts to weaken Russia.[1242] Gareev also argued for more intragovernmental cooperation between power ministries and even a new state organ to counter new military and non-military threats.[1243] In the middle of the far-ranging military reform Gareev defended an undivided, unified and hierarchical command.[1244] Although Gareev clearly dismissed fash-

[1235] Гареев, М.А. О характере вооруженной борьбы будущего. Вестник Академии военных наук, №2, 2005, 11-14; Гареев, М.А. Отстаивая национальные интересы. ВПК, № 48 (115) за 21 декабря 2005 года.

[1236] Слипченко, В. И. Войны шестого поколения: оружие и военное искусство будущего. М.: ИД Вече, 2002.

[1237] Богданов, С. А. Вероятный облик вооруженной борьбы будущего. Военная мысль, № 12 2003, 2-7.

[1238] Гареев, М.А. Итоги деятельности Академии военных наук за 2009 год и задачи академии на следующий год. Вестник Академии военных наук, № 1 (30) 2010, 8-18.

[1239] Гареев, М.А. Итоги деятельности Академии военных наук за 2011 год и задачи академии на 2012 год» Вестник Академии военных наук, 2(39) 2012, 6-17,12.

[1240] Гареев, М.А. Система знаний о войне и обороне страны на современном этапе. Вестник Академии военных наук, 2(43) 2013, 7-14.

[1241] Гареев, М.А. Итоги деятельности Академии военных наук за 2012 год и задачи академии на 2013 год. Вестник Академии военных наук, 1(42) 2013, 8-21, 13.

[1242] Гареев, М.А. Опыт Великой Отечественной войны и работа Академии военных наук по дальнейшему развитию военной науки. Вестник Академии военных наук, 2(51) 2015, 16-25, 21-22.

[1243] Гареев 2013a; Гареев, М.А. Характер современных военных и невоенных угроз безопасности России и организация обороны страны. Вестник Академии военных наук, 4(45) 2013, 4-9.

[1244] Гареев, М.А. Итоги деятельности Академии военных наук за 2013 год и задачи академии на 2014 год. Вестник Академии военных наук, 1(46) 2014, 7-13.

ionable terms like 'soft power' (miagaia sila) and 'hybrid war' (gibrinaia voina) he argued that economic, politico-diplomatic, information warfare (bor'ba) and military means of confrontation (protivoborstvo) should be used in tight cooperation to achieve military objectives.[1245] In a co-authored article in 2017 with Major General N.I. Turko, Gareev seems to have finally given up on the distinction between politics and war as the article claims that modern war can be divided to a lower layer consisting of hard non-military means and soft non-traditional means, and a higher layer consisting of armed warfare.[1246] Accordingly, Gareev continued to emphasised the importance of whole-of-government cooperation, territorial defence and mobilization.[1247] In 2019 he argued that the new types of warfare, which were constantly changing, required international regulation. The importance of local wars and conflicts was rising as nuclear weapons prevented wars only between the great powers.[1248] All in all, Gareev's writings in the 2000s and 2010s promoted the Academy's official version of the character of war which tried to resist 'fads' like cyber or hybrid wars but seems to have failed in the end.

The discussion on information war and warfare in the military journals carried over from the 1990s into the 2000s. Military scholars studied the United States' armed forces' doctrine on information war and/or warfare (translated variously as either voina or protivoborstvo), compared Russian and American concepts and in some cases tried to merge them.[1249] For example, in 2005 a renowned military historian Vladimir Zolotarev described information confrontation (protivoborstvo) as a complex of measures and operations conducted in peace and wartime and as such distinct from war (voina). It included the destruction of the infrastructure of the government and military command, electromagnetic attacks on telecommunications (EW), communication and signal intelligence, data breaches and the destruction of data resources through 'hacker wars', and the spreading of mass disinformation. Zolotarev claimed that information had become important because the disorganization of national infrastructure had strategic effects, information enabled the struggle (protivoborstvo) between states in the post-Cold War era in the information sphere, and the means of information influence had become available to criminals and terrorists.[1250]

In 2009 Colonel General Vice-Chief of General Staff Anatolii Nogovitsyn defined an information war (voina) as: "a confrontation [protivoborstvo] between states in the information space in order to damage information systems, processes and resources, critical structures, to undermine the political and social systems, as well as to massively psychologically influence the military personnel and the population in order to destabilize society and the enemy's state as a whole." He claimed that its primary mission

[1245] Гареев 2015.

[1246] Турко, Н. И., Гареев, М.А. Война: современное толкование теории и реалии практики. Вестник Академии военных наук, 1(58) 2017, 4-10. Gareev seems to walk back on this in his next article (Гареев, М.А. Итоги деятельности Академии военных наук за 2016 год и задачи Академии на 2017 год. Вестник Академии военных наук, 2(59) 2017, 14-22).

[1247] Гареев 2018.

[1248] Гареев, М.А. Итоги деятельности Академии военных наук за 2018 год и задачи академии на 2019 год. Вестник Академии военных наук, 2(67) 2019, 12-18.

[1249] Лимно, А. Н., Крысанов, М. Ф. Информационное противоборство и маскировка войск. Военная мысль, № 5 31.5.2003; Комов, С. А., Коротков, С. В., Дылевский, И. Н. Об эволюции современной американской доктрины "информационных операций". Военная мысль, № 6 2008.

[1250] Крамар, Владислав. Любая война обходится дороже содержания мощной армии. ВПК, № 39 (106) за 19 октября 2005 года.

was "the destruction of the foundations of the national identity and the way of life of the opposing state." Nogovitsyn argued that victory in a modern war was possible only through information superiority and victory over an enemy was in its essence a psychological act. According to him, the main characteristics of information war were its cheapness, perception management, difficulty in prediction and estimating damages, and the transformation of the information infrastructure of a state into a strategic target.[1251] Nogovitsyn's ideas were not far from Western ideas of strategic information warfare.

In 2014 Retired Major General Kh. I. Saifetdinov, an ex-chief of the 27th TsNII of the MoD[1252] defined information warfare (protivoborstvo) as "the purposeful use of information to achieve political, economic, military and other goals." According to him, the objective of IW was to gain and maintain information superiority over the armed forces of the enemy and to create favourable conditions for the preparation and use of the Armed Forces. IW should be conducted continuously during peacetime as part of strategic deterrence, during threatening periods as supporting initiation of the defence plan, and during wartime to acquire superiority. The main tasks of IW should be monitoring and forecasting, deception, disorganization of enemy forces, degrading the psychological resilience of the enemy forces and population, supporting the moral-psychological state of one's own forces, and protecting one's own ASUs and weapons. Saifetdinov proposed that the Armed Forces should have a system of information warfare including multiple subsystems of offensive, defensive and supporting measures.[1253]

After the annexation of the Crimea and Russia's intervention in Syria, military scholars became more interested in the psychological than the technological aspect of information confrontation—mainly because of the perceived hostile and critical Western reaction.[1254] The antagonistic approach shared by the Russian civilian and military scholars towards the United States and its allies was based on the perceived geopolitical confrontation and the 'premeditated' fall of the Soviet Union. Moreover, the arguably selective and highly interpretive study of Western doctrines and theoretical writings led to the interpretation of the concepts of 'network or netwars' (setevaia voina) and 'noonpolitics' as a new type of Western warfare or even as a seventh generation 'information-network warfare' fought in the information environment and

[1251] Ноговицын, Анатолий. Некоторые аспекты обеспечения информационной безопасности Российской Федерации. Военная мусль, № 3 2009, 24-26; Ноговицын, Анатолий. Некоторые аспекты обеспечения информационной безопасности российской федерации. Российское военное обозрение № 3 (62) март 2009.

[1252] The 27th TsNII or Central Scientific-Research Institute of the Ministry of Defence was established in 1954. It has been responsible for the development of Soviet and Russian military ASUs and ASUVs under the guidance of the General Staff and it develops systems for all services. (Протасов, А. А. Институт автоматизации и совершенствования управления войсками (силами): история и современность. Военная мысль, № 7 2014, 3-8; 'Сайфетдинов' Академик 2019 [Online]. Available: https://dic.academic.ru/ dic.nsf/enc_biography/ 109590 /Сайфетдинов. [Accessed: 30th January 2019].

[1253] Сайфетдинов, Х. И. Информационное противоборство в военной сфере. Военная мысль, № 7, 2014, 38-41.

[1254] Микрюков, Василий. Победа в войне должна быть достигнута еще до первого выстрела. Независимое Военное Обозрение, № 1 15.1.2016; Балуевский, Юрий. Агрессия «общечеловеческого» Военными технологиями нематериального действия у нас никто не занимается. ВПК, № 18 (584) за 20 мая 2015 года; Сивков, Константин. Захват будущего в теории и на практике. на форуме "АРМИЯ-2018" обсуждены проблемы психологической обороны. ВПК, № 35 за 11 сентябрь 2018.

naturally directed against Russia.[1255] After Western scholars and media began to use the terms 'hybrid war' and 'hybrid warfare' to describe Russian actions in Ukraine, Russian writers quite effortlessly began to use these same terms to describe the Western use of 'controlled chaos' and 'colour revolutions', that is anti-government, possibly violent activities supported by foreign powers, which partially merged with hybrid warfare.[1256]

There were some critical views. I. M. Popov and M. M. Khamzatov pointed out in 2016 that many Russians had misunderstood the American concept of network-centric warfare to mean a new kind of war, whereas it was just a doctrine or concept of command and control.[1257] This observation did not prevent Popov and Khamzatov to claim that a new kind of 'system-network war' had been born. It was described as 'a technology to wage war' and it had different forms depending on the level at which it was engaged (political, strategic, operational and tactical). At the highest level, it was a struggle between systems (governments) to weaken their opponents' 'critical nodes' to win with as least bloodshed as possible by using state and non-state resources /actors. Conversely, the tactical level was reminiscent of the NCW.[1258] Arguably, Popov and Khamzatov thus tried to combine all the Russian theories on warfare examined above under one concept.

The character of future war has greatly interested Russian military scholars from the early 2000s. Retired Lieutenant General and Chief researcher of the Institute of Social and Political Studies of RAN, V. V. Serebriannikov continued (cf. Chapter 4) his theorizing about the changing character of war. He claimed that violent military means should be divided into direct (warfare) and indirect (intimidation and pressure) means. This produced a matrix of violent/non-violent, military/non-military, and direct/indirect means. Serebriannikov also noted that non-military means were being militarized, e.g. the use of economic means against the military-industrial complex or information-propaganda against the will of the people and armed forces.[1259] The theme of indirect actions or strategy heavily influenced the way Russian scholars have handled information warfare. I will return to this issue when discussing asymmetric responses

[1255] Дугин А.Г. Теоретические основы сетевых войн. Информационные войны, № 1(5) 2008, 2-9; Бовдунов А. Л. Неправительственные организации: сетевая война. Информационные войны, № 3(7) 2008, 30-39; Савин Л. В. Украина в сетевой войне. Информационные войны, № 3(7) 2008, 42-51; Никитенко Е.Г., Сергеев Н.А. «Мягкая сила» в контексте национальной безопасности России. Информационные войны, № 3(27) 2013, 36-52; Карякин В.В. Мир вступил в эпоху войн седьмого поколения – информационно–сетевых войн. Информационные войны, № 3(19) 2011, 2-7; Золотарев, Владимир. Когда нация становится жертвой: Концептуальные основы информационно-сетевых войн. ВПК, № 17 (485) за 1 мая 2013 года.

[1256] Basically, 'controlled chaos' is the clandestine inciting of terrorism, separatism and insurgency by an adversary power to enable regime change in its opponent. Лепский В.Е. Технологии управляемого хаоса – оружие разрушения субъектности развития. Информационные войны, № 4(16) 2010, 69-78; Воробьев, И. Н., Киселев, В. А. Стратегии сокрушения и измора в новом облике. Военная мысль, № 3 2014, 45-57; Киселев, В. А., Воробьев, И. Н. Гибридные операции как новый вид военного противоборства. Военная мысль, № 5 2015, 41-48; Чекинов, С. Г., Богданов, С. А. Эволюция сущности и содержания понятия "война" в XXI столетии. Военная мысль, № 1 2017, 30-43; Бартош, А. А. Стратегия и контрстратегия гибридной войны. Военная мысль, № 10 2018, 5-20.

[1257] Попов И.М., Хамзатов М.М. Война будущего: концептуальные основы и практические выводы. Очерки стратегической мысли. – М.: Кучково поле, 2016, 428.

[1258] Ibid., 498-450.

[1259] Серебрянников, В. В. О понятии "война". Военная мысль, 2004 № 10, 61-65.

because many military scholars have considered information warfare to be essentially indirect and asymmetric.

By 2008 the General Staff had embraced the idea of information war and its technological and psychological component, the latter of which was perhaps seen as more important.[1260] Following this view, Major General E. A. Derbin, the Head of the Department of Information Security of the Military Academy of the General Staff[1261], argued that information was the means of strategic confrontation (protivoborstvo) and strategic deterrence (sderzhivanie).[1262] Derbin's solution to information threats was a system of information security which consisted of multiple subsystems.[1263] To this system could be incorporated systems protecting state secrets, securing communications, and protecting ASUs, which would increase the resilience (ustoichivost') of the information infrastructure against threats. This system would protect Russia (and its allies) from direct and indirect actions of the enemy.[1264] Derbin's views must be taken as authoritative as he was the General responsible for training information security for high ranking officers. As the threats multiplied and became non-militarized, Derbin updated his views in 2019 and argued for the creation of the State Defence Committee, including STAVKA of the Supreme Command. This should have integrated the security efforts of all ministries.[1265]

A series of articles written in 2011-2012 by a senior researcher of the Military Academy of the General Staff, E. G. Shalamberidze, provided a complex model of international and largely indirect confrontation (mezhdunarodnaia protivoborstvo)[1266] which closely resembles the model of intergovernmental conflicts provided by the Chief of the General Staff Gerasimov in 2013.[1267] They also echoed the ideas presented by Serebriannikov in the early 2000s. According to Shalamberidze, indirect

[1260] Бурутин, А. Войны будущего станут информационными. Новые вызовы и угрозы безопасности России. Независимое военное обозрение, № 5 2008, 2-3.

[1261] The Department of Information Security of the Military Academy of the General Staff offers education and training for mid- to high-ranking military officers for information security issues of the state and the Armed Forces on the strategic and operational level. It also conducts research on these subjects. (Военная академия Генерального штаба Вооруженных Сил Российской Федерации. Кафедра информационной безопасности [Online]. Available: http://vagsh.mil.ru/Struktura-akademii/Kafedra-informacionnoj-bezopasnosti [Accessed: 29th March 2019].)

[1262] Дербин, Е.А. Информационная безопасность союзного государства как основа его обороноспособности в условиях непрямых действий противника. Вестник Академии военных наук, № 2 (27) 2009, 31-38.

[1263] The subsystems were: organization structural-functional, evaluation and forecasting of the situation, legal, educational and cadres, ideological work, linguistical, scientific, coordination and control, measures of information security, and technical security.

[1264] Дербин 2009. Cf. also Дербин, Е.А. О роли смысла в обеспечении информационной безопасности. Военная Мысль, № 11 2007, 68-77.

[1265] Дербин, Е.А. О Совершенствовании Стратегического Руководства Обороной России. Вестник Академии военных наук, № 2 (67) 2019, 46-52.

[1266] Although the Bulletin of the Academy of Military Sciences offers warfare as the English translation, it is clear that Shalamberidze does not write about warfare understood as fighting or use of force, and so 'confrontation' is used here.

[1267] Шаламберидзе Е.Г. Непрямое противоборство в сфере военной безопасности в условиях мирного времени. Вестник Академии военных наук, № 1 (34) 2011, 20-30; Шаламберидзе Е.Г. Теоретические вопросы развития политики национальной обороны России в условиях мирного времени с использованием системы мер невоенного и военного характера. Вестник Академии военных наук, № 4 (37) 2011, 35-43; Шаламберидзе Е.Г. Национальная оборона Российской Федерации: стратегические задачи и возможные перспективы. Вестник Академии военных наук, № 4 (41) 2012, 30-37; Шаламберидзе Е.Г.

means would be used to destabilize the opponent's state system, to weaken its elements, to take out its critical control systems, to introduce failures in subsystems, and finally to transform it to a system suited to the attacker's interests. The use of these means would be implemented according to a strategic plan during all phases of state relations.[1268] Thus, Shalamberidze claimed that strategic goals could be achieved in peacetime without the direct armed use of force.[1269] Shalamberidze's model was based on a continuum of relations between the belligerents and various combinations of non-violent/violent (or persuasion/coercion), non-military/military, indirect/direct and low, middle and high intensity means.[1270] Later, Shalamberidze argued that the strategic role of national defence was the prevention, reduction, and pre-emption of military threats and the achievement of the correlation of forces (sootnoshenie sil). To this effect, he introduced a functional structure for the optimization of national defence which resembles the system of information security proposed by Panarin et al.[1271]

The ideas of Serebriannikov and Shalamberidze were clearly present in the speech given by the Chief of General Staff Colonel General Valerii Gerasimov in 2013.[1272] Gerasimov presented a model to visualize the relationship between the different stages of interstate conflict and military and non-military means.[1273] Consequently, Gerasimov's Chief of the Main Operational Directorate Andrei Kartapolov provided in 2015 three models of current and future war. The first was 'a war of a new type' (voina novogo tipa) which included 'hybrid actions' and 'indirect actions' and was based on the use of information, covert action, and non-military force to destabilize and delegitimize the target state, which was followed by 'peace-keeping operations'. The second was a traditional war complemented by new environments and technology. The third was asymmetric warfare, which was from the GS point of view the weaker side's strategy (tactics) to level differences in power with minimal costs by acting against the vulnerabilities and weaknesses of the opponent in a coordinated way using all means available.[1274] In 2016 Gerasimov stated that wars fell under the overall concept of interstate confrontation or struggle (mezhgosudarstvennoe protivoborstvo) and could be divided to wars using 'global integrated operations' (from

Национальная оборона и информационная борьба государства в современных условиях мирного времени. Информационные войны, № 3(23) 2012, 11-19; Герасимов 2013a & 2013b.

[1268] Шаламберидзе 2011a. He later updates threats to measures (mera) and armed aggression to 'direct violent reorientation of the policy of the opposing side'. Шаламберидзе 2011a.

[1269] Шаламберидзе 2011b.

[1270] Ibid.

[1271] Шаламберидзе 2012a & 2012b.

[1272] Gerasimov gave the original speech in the annual meeting of the Military Academy and the subsequent article based on it and published in Voenno-Promyshlenyi Kurier gained much attention in the West after the conflict in Ukraine began. This was mainly because the first interpretations mistook Gerasimov's analysis of the character of war as a 'Russian doctrine of hybrid warfare.' (Герасимов 2013a & 2013b; Galeotti 2018; Bartles, Charles K. Getting Gerasimov Right. Military review, January-February 2016, 30-38).

[1273] In 2010 the previous Chief of General Staff N.E. Makarov gave a somewhat similar presentation on the character of future war. Makarov perhaps emphasized more than Gerasimov the changed geopolitical situation and the role of technology and was heavily influenced by American NCW concept. (Макаров, Н.Е. «Характер вооруженной борьбы будущего, актуальные проблемы строительства и боевого применения Вооруженных Сил РФ в современных условиях». Вестник Академии военных наук, № 2 (31) 2010, 18-26.) Iurii Baluevskii, the Chief of General Staff in 2004-2008 did not provide such public presentations of the character of future war.

[1274] Картаполов, А.В. Уроки военных конфликтов, перспективы развития средств и способов их ведения. Прямые и непрямые действия в современных международных конфликтах. Вестник Академии военных наук, 2(51) 2015, 26-36.

the U.S. doctrine) and wars using 'hybrid methods' (gibridnye metody). The latter was based on achieving political goals with the minimal use of armed force, which was substituted by economic and information-psychological means, and by support given to paramilitaries etc. to erode the stability of the opponent. Gerasimov stated that the Defence Plan of 2016-2020 had been drafted by keeping these threats in mind and was founded on an intragovernmental (mezhvedomstvennyi) approach, territorial defence (territorial'naia oborona) and international cooperation (with allies, i.e. the Collective Security Treaty Organization, the BRICS, and the Shanghai Cooperation Organization).[1275]

The official Russian approach to hybrid wars etc. voiced by the General Staff has oscillated between 2016-2019 between acceptance to rejection. The main problem for the Russian military seems to have been the relationship between non-military threats and war. It was related to the larger issue of what was considered as war in the modern era and, thus, linked to the tasks of the Armed Forces.[1276] In 2018 Gerasimov argued that the current era was characterized by 'wars of a new generation' (voina novogo pokaleniia) where the real opponent hides behind third parties (terrorists, insurgents etc.)[1277] Terminological ambivalence has not stopped civilian or non-military scholars and commentators from using the term 'hybrid' to describe the character of future war.[1278] Moreover, in his 2018 presentation at the conference of the AVN, Gerasimov argued that the character of war kept on changing to include more non-state actors and non-military means. Gerasimov listed the evolution of military strategy from the "strategy of annihilation" and the "strategy of attrition" to the strategies of "global war", "nuclear deterrence" and "indirect actions". The last one Gerasimov associated with regime change operations which used 'fifth columns' and precision weapon strikes in combination. Russia would, consequently, adopt a strategy of active defence based on a defensive doctrine. Despite this broadening definition of war, Gerasimov made the argument that it was the task of the Armed Forces to prepare for a confrontation (protivoborstvo) in the military sphere and non-military spheres were the responsibility of others—although coordination with different actors was important. Gerasimov further argued that the main principles of strategic action were surprise, decisiveness, and continuity (nepreryvnost')—he was in effect declaring a pre-emptive

[1275] Герасимов, В.В. Организация обороны Российской Федерации в условиях применения противником «традиционных» и «гибридных» методов ведения войны. Вестник Академии военных наук, № 2 (55) 2016, 19-23, 20.

[1276] Матвиенко, Ю.А. Невоенные угрозы как составная часть современного межгосударственного противоборства. Вестник Академии военных наук, 1(58) 2017, 35-41; Буренок, Василий. За рамками здравого смысла: Облик грядущих войн и новых систем вооружения определит только наука. ВПК, № 10 (478) за 12 марта 2013 года; Буренок, Василий. О некоторых видах межгосударственного противоборства. Вестник Академии военных наук, 2(43) 2013, 15-19; Сержантова, А.В. Современное понимание сущности и содержания войны. Вестник Академии военных наук, 2(43) 2013, 20-23; Новиков, Владимир, Голубчиков, Сергей. Олимпиада по безопасности. ВПК, № 14 (678) 12–18 апреля 2017 года.

[1277] Герасимов, В.В. Современные войны и актуальные вопросы обороны страны. Вестник Академии военных наук, 2(59) 2017, 9-13; Герасимов, В.В. Мир на гранях войны: Мало учитывать сегодняшние вызовы, надо прогнозировать будущие. ВПК, № 10 (674) за 15 марта 2017 года.

[1278] Бартош, А. А. Гибридная война: интерпретации и реальность. Независимое военное обозрение, № 35 (918) 16 сентября 2016; Чекинов, С. Г., Богданов, С. А. Прогнозирование характера и содержания войн будущего: проблемы и суждения. Военная мысль, № 10 2015, 41-49; Антонов С.Г., Гордеев С.В., Климов С.М. & Рыжов Б.С. Модели угроз совместных информационно-технических и информационно-психологических воздействий в гибридных войнах. Информационные войны, № 2(46) 2018, 83-87.

(uprezhdat') strategy.[1279] Notwithstanding all these theoretical ideas, the Minister of Defence Sergei Shoigu claimed in June 2019 that Russia lacked a theory of 'conflicts of the new generation.'[1280]

Before moving on to official strategic planning documents it must be noted that in relation to the interstate struggle there exists a distinct continuum of interstate confrontation in Russian military thinking which is present in the texts analysed above and in the official documents. In relation to war, they can be categorized into the period of no direct military threat, the period of threat, the initial period of war, war proper, and the final stages of war.[1281] In an article from 2005, retired Colonel Iu.E. Donskov and O. G. Nikitin, scholars from the Scientific and Research Test Institute of the Electronic Warfare of Military Educational and Scientific Centre of the Air Force, divided the phases of conflict into the beginning, escalation, crisis and war. Different means of diplomatic, economic, disinformation, EW and computer and finally kinetic means would be used in different phases.[1282] Igor' Popov and M. M. Khamzatov divided the 'military-political situation' into phases of military-political stability, tension, crisis, and military conflict (war).[1283] Igor' Popov has divided the military conflict itself into the preparation period (from hours to months), the active phase of military conflict (which has three subphases i.e. massive aerospace strike, land attack, and consequent operation to destroy enemy forces), and the post-conflict regulation period.[1284] Valeri Gerasimov has presented a somewhat similar vision of the development of modern interstate conflicts which divides interstate conflict into phases of hidden initiation, aggravation, start of conflict actions, crisis, resolution, and post-conflict management.[1285] He has also used the term 'period of threat' to denote a time before open hostilities.[1286]

According to Evgenii Shalamberidze, confrontation is defined as "the actions of the subjects of international relations to resolve their disagreements." This is divided into: peaceful relations where non-violent means of confrontation are used; foreign policy conflict involving the use of non-violent direct and indirect non-military means and indirect military means; and military conflict where all means are used, primarily direct

[1279] Герасимов, Валерий. Векторы развития военной стратегии. Красная звезда 4.3.2019 [Online]. Available: http://redstar.ru/vektory-razvitiya-voennoj-strategii/ [Accessed: 4th March 2019].

[1280] ТАСС. Шойгу заявил, что Россия должна выработать новую теорию ведения войн. ТАСС, 18 июня 2019 [Online]. Available: https://tass.ru/armiya-i-opk/6561643 [Accessed: 2nd July 2019].

[1281] Горбунов, В. Н., Богданов, С. А. О характере вооруженной борьбы в XXI веке. Военная Мысль, № 3 2009, 2-15; Чекинов, С. Г., Богданов, С. А. (2012b) Начальные периоды войн и их влияние на подготовку страны к войне будущего. Военная Мысль, № 12 2012, 14-27; Герасимов 2013; Герасимов 2013; Герасимов 2015; Картаполов 2015.

[1282] Донсков, Ю.Е., Никитин, О. Г. Место и роль специальных информационных операций при разрешении военных конфликтов. Военная мысль, № 6 (2005), 30-34.

[1283] Попов & Хамзатов 2016, 122.

[1284] Попов, Игорь. Военные конфликты: взгляд за горизонт: Технологическая революция в "традиционной" войне. Независимое военное обозрение, № 13 (754) 2013.

[1285] Герасимова 2013a.

[1286] Герасимов 2015. Time period which is usually followed by the beginning of war. "Characterised by an extreme aggravation of the international situation and the confrontation between the probable opponents, the increase in military threats and a sharp activation of direct preparations for war, expansion of arms conflicts." 'Угрожаемый период'. Военного энциклопедического словаря. М.: Воениздат, 2007 [Online]. Available: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=10643@morfDictionary [Accessed: 30th March 2019]. Similar concept is 'a threatening period' or 'period of threat' (ugrozhaemyi period) which is related to military security and has been used officially since 1993 (Известия 1993).

military means.[1287] In the context of information warfare, Manoilo divided state relations into four stages: 'peaceful coexistence' (mirnoe sosushchestvovanie), 'conflict of interests' (stolknovenie interesov) or continuous 'natural rivalry' (estestvennoe sopernichestvo), 'armed confrontation' (vooruzhennaia konfrontatsiia), and 'war' (voina).[1288]

The initial period of war is a distinctly Soviet/Russian concept. According to Chekinov and Bogdanov, it was originally defined in the 1920s–930s as the length of time between the declaration of war and the beginning of fighting between the main forces deployed in a theatre of operations. During this time fighting may occur between border guards and other permanently deployed units covering the mobilization and deployment of the main forces. Later Soviet military theorists concluded that war would begin without the declaration of war with a surprise attack of previously deployed battle-ready formations to achieve the initial strategic goals. Chekinov and Bogdanov claim that the initial period is now preceded by non-military operations and the initial period itself will be the main and decisive period of war.[1289]

On the official side, the Russian military doctrine differentiates the national security situation between peacetime, the time of immediate aggression, and wartime.[1290] Additionally, the armed forces have been given operational requirements based on the categorization of peacetime, times of emergency, times of aggravated military-political and military-strategic situations, and times of war.[1291] The Russian federal law also recognizes the concepts of 'a state of emergency' and 'a state of war' which are both connected to security threats against the state. The former gives the state the authority to restrict the freedom of mass communications, to increase the protection of objects vital to the population, and to manage the use of public communication networks. The latter gives the state the authority to control communication systems. The state has the mandate to mobilize human and material resources, including communications, for war already in peacetime.[1292]

The official and semi-official national security and strategic planning documents have included some aspects of the idea of the interstate struggle. The so-called Ivanov Doctrine of 2004 stated that 'armed struggle' was undergoing change. In short, it subscribed to a vision of high-tech, long-range aerospace warfare, but retained the importance of conventional land forces. According to the doctrine, military power was used as an instrument of foreign policy very frequently and the Armed forces were faced with external, internal, and transborder threats.[1293] The Foreign Policy Concept

[1287] Шаламберидзе 2011a, 23 & 28; Шаламберидзе 2011b, 38-39.

[1288] Манойло et al. 2012, 439.

[1289] Чекинов & Богданов 2012b; Чекинов & Богданов 2015. Cf. ft 753; 'Начальный период войны'. Военного энциклопедического словаря. М.: Воениздат, 2007 [Online]. Available: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=6941@morfDictionary [Accessed: 30th March 2019].

[1290] Указ Президента РФ 2014

[1291] Mil.ru. Задачи Вооруженных Сил Российской Федерации [Online]. Available: https://structure.mil.ru/mission/tasks.htm [Accessed: 28th March 2019].

[1292] Федеральный конституционный закон 2001; Федеральный конституционный закон 1997; Федеральный конституционный закон 2002; Федеральный закон 2003.

[1293] Иванов, Сергей. Вооруженные силы России и ее геополитические приоритеты, 2 февраля 2004 [Online]. Available: https://globalaffairs.ru/number/n_2471 [Accessed: 30th March 2019]; The Defence Ministry of the Russian Federation. The priority tasks of the development of the armed forces of the Russian Federation [Online]. Available: http://red-stars.org/doctrine.pdf [Accessed: 30th March 2019].

of 2008 argues that unilateral actions of some states are a threat to the balance of the world. It also states that the Russian foreign policy should support Russia's influence in the global information space and sphere through public policy.[1294] The National Security Strategy (NSS) of 2009 stated that disagreements between states had intensified. Information confrontation (protivoborstvo) is intensifying which threatens the stability of states. Nevertheless, Russia had survived the crisis of the end of 20th century and was transforming into one of the great world powers.[1295] The military doctrine of 2010 defined armed confrontation (vooruzhennoe protivoborstvo) as consisting of larger-scale, regional, and local wars, and armed conflicts. It mentioned the strengthening of information confrontation and the development of its forces and means to achieve political goals without the use of force. In contrast to information confrontation the document used the term warfare (bor'ba) in relation to armed warfare and terrorism.[1296]

The 2013 Foreign Policy Concept states that the world was transferring towards polycentrism as the West's dominance in the world economy and politics was waning. Global competition was acquiring civilizational dimensions as different political and economic models emerged. 'Soft power' had become a new and potentially dangerous instrument used to infringe on the internal affairs and sovereignty of states. Russia would therefore pursue strategic and regional stability and protect its national and international information security. The most important direction of foreign policy would be to support Russian information influence in the world and the priority direction would be the counties of CIS.[1297] The current Military Doctrine of 2014 states that the world is characterized by global competition, tension, and rivalry between value orientations and developmental models. Military conflict consists of interstate and intrastate use of military power consisting of large-scale armed confrontations (vooruzhennoe protivoborstvo), regional and local wars, and armed conflicts. Information confrontation (informatsionnoe protivoborstvo) is strengthening and its forces and means are developing. Military dangers and threats are shifting into the information space (prostranstvo) and into the internal sphere of Russia. Information and communication technology are being increasingly used against the sovereignty, political independence, and territorial integrity of states and present a threat to global stability. An adversary can operate in the whole depth of information space and affect critical infrastructure and people. Russia will improve the information security system of the Armed Forces, other troops and agencies, develop information cooperation between agencies (including the creation of a unified information space), develop

[1294] Концепция. Концепция внешней политики Российской Федерации от 12 июля 2008 г. N Пр-1440 (утв. 12.07.2008 N Пр-1440) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_85021/ [Accessed: 30th March 2019].

[1295] Указ Президента РФ от 12 мая 2009 года N 537 (2009b). О Стратегии национальной безопасности Российской Федерации до 2020 года Указ Президента Российской Федерации [Online]. Available: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102129631 [Accessed: 21st March 2019].

[1296] Указ Президента РФ от 05.02.2010 N 146 "О Военной доктрине Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_97325/ [Accessed: 30th March 2019].

[1297] Концепция. Концепция внешней политики Российской Федерации (утв. Президентом РФ 12.02.2013) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_142236/ [Accessed: 30th March 2019].

forces and means for information confrontation, and develop an information management system for the Armed forces which will connect weapons control and automated command and control systems from the strategic to the tactical level.[1298]

The NSS of 2015 states that Russia faces threats from the direction of the United States and its allies who deploy multiple types of pressure and challenge Russia's national interests. Global and regional instability has increased and instruments of power have diversified. In the areas near Russia, militarization and an arms race are developing. The information confrontation/struggle (informatsionnoe protivoborstvo) is strengthening as some countries use information and communications technology to manipulate social consciousness and falsify history. There are threats in the information sphere and so the information infrastructure and spiritual-cultural values need to be protected. Information means should be part of the strategic deterrence. Information security in the context of national strategic priorities should be paid special attention in implementing the strategy.[1299] The Foreign Policy Doctrine of 2016 states that contradictions (protivorechiia) continue to increase in the international system as does the role of force. It mentions information security and threats, and the information space and sphere but does not define them. Information is seen as a tool of 'soft power'. Information/communication technology can be used for military-political purposes. According to the Doctrine, Russia takes necessary actions to ensure equitable management of the Internet.[1300]

It is interesting that the Information Security Doctrine of 2016 uses the term 'protivoborstvo' only once and then in the context of military policy and defence when referring to the Armed Forces and means of information warfare as a part of the military use of force. Nevertheless, the document states that Russia has national interests in the information sphere including the constitutional rights of citizens (inc. spiritual-cultural values), resilience of critical information infrastructure, development of the Russian IT industry, public diplomacy, creation of an international system of information security including the protection of Russian sovereignty in the information space. These are threatened by transborder information threats that are used among other things for military and geopolitical goals. The Doctrine divides these threats into information-technological and psychological threats. The Doctrine claims that some states are attempting to use technological superiority to dominate the information space, and because the Internet is not regulated and managed in an equal manner, strategic stability is difficult to achieve.[1301]

To summarize, the interstate struggle or confrontation is a constant theme in Russian strategic thought. Its characteristics have changed but the core idea has stayed recognizably the same: it is the constant zero-sum struggle between great powers, and civilizations or systems grouped around them for power, status, independence and the

[1298] Доктрина. Военная доктрина Российской Федерации. 25 декабря 2014 г., № Пр-2976, 14 & 15 [Online]. Available: http://www.scrf.gov.ru/security/military/document129/ [Accessed: 28th March 2019].

[1299] Указ Президента РФ от 31.12.2015 N 683 "О Стратегии национальной безопасности Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_191669/ [Accessed: 30th March 2019].

[1300] Указ Президента РФ от 30.11.2016 N 640 "Об утверждении Концепции внешней политики Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_ 207990/ [Accessed: 30th March 2019].

[1301] Указ Президента 2016b.

right to exist by any means necessary. The idea of the interstate struggle in the writings of the Russian information war theorists naturally transforms into information struggle. It can be argued that the idea is based on a geopolitical promise of control over globalization, a future eschatological confrontation, and a struggle between systems with the emphasis on historical continuity. There is a shared understanding of the distinct technological and psychological aspects of the information space and their interconnectedness. However, this has not produced a unified terminology or theory on the information struggle.[1302] During the timeframe under analysis the element of information has been perhaps the major addition to the interstate confrontation, and it has, at least in the material analysed here, occupied a somewhat central position. Depending on the writer and the text, information has become either the means, ways or ends of this struggle. However, it is worth noting that the idea of an information confrontation remains a subject of intense discussion in Russian strategic thought.

There are at least two separate meanings for the idea of 'protivoborstvo' present in the material analysed here.[1303] The first is related to the great power struggle conducted as a continuum in all stages of interstate relations. The second is related to the forces, means, forms and methods of conducting warfare in the context of a conflict.[1304] The first is more closely related to strategic cultural thinking, the second is associated with studying and adopting Western ideas. The challenge in analytically separating these two meanings is that throughout the 2000s and 2010s the meaning of war has been broadened by some, mainly civilians, to include non-military and non-violent actions, while some military scholars have pushed back on this formulation. The appearance of the concept of intergovernmental confrontation (mezhgosudarstvennogo protivoborstvo) which highlights intrastate or interagency, i.e. whole-of-state approaches is a resurrection of comprehensive Russian security thinking based partly on Soviet era ideas. The interstate struggle requires the mobilization of all state resources through the vertical of power.[1305] This is not comprehensive security in the sense of broadening the sources and objects of threats, but it is comprehensive in the sense of the means and actors of state power. Most notably, it requires vertical centralised organizations or 'systems.'

By analysing Western theories and military operations, and through the prism of geopolitical and sometimes civilizational confrontation in which globalization is a threat and state sovereignty under attack, the Russian strategic thought has tried to find a way to forecast future wars. The sixth-generation high-tech precision strike warfare of Slipchenko was challenge by those who did not agree with the diminishing role of the conventional ground and nuclear forces. At the same time foreign and domestic

[1302] Соловьев, А.В. Информационная война: теоретико-методологические и практические аспекты. Информационные войны, № 2(18) 2011, 15-22.

[1303] Information struggle and confrontation are different from information warfare. The translation of Russian terms into English is difficult as the Russians seem to use certain terms intentionally to convey certain value-laden messages, i.e. that it is the West that is 'waging war' against Russia. Moreover, the original Western use of the terms around information warfare, starting by calling it warfare, has not lessened this confusion.

[1304] Forces and means refer to troops, weapons and equipment. Forms are formal descriptions of military actions that combine tasks, organization and methods such as strikes, engagement, military action, battle, operations and strategic operations. Methods refer, on the one hand, to ways of using forces, and on the other, to means which differ from service to service and depending on the situation and the commander's intent. (Военного энциклопедического словаря. М.: Воениздат, 2007).

[1305] Julian Cooper and Andrew Monaghan have made similar points considering the development of Russian military mobilization (Cooper 2016; Monaghan 2016).

ideas of netwars, soft power, controlled chaos and 'mutiny wars'[1306] offered a third view. Thus, long before the Western military theorists began to write about Russian hybrid warfare the Russians themselves had analysed the Western way of conducting war in similar terms. This new threat blurred the lines between war and peace, as well as political competition and military confrontation and led to some 'course corrections' by the General Staff and criticism from independent writers. The NCW was embraced and then criticized for being too Western. Hybrid wars were officially adopted and then abandoned, then adopted again. Defensive strategy was first enshrined as morally superior and then abandoned for 'active defence.' There was also a clear tension between emphasising the promises of technology versus spiritual and moral issues—which was a traditional conflict in Russian military thinking.[1307] The core of the problem was the relationship of 'protivoborstvo' and 'voina', and how and by whom the security issues related to them should be handled. Ultimately, information means were widely accepted to have strategic effects either as a destructive power or related to the political objectives of a confrontation. Moreover, the dual military operational-tactical and strategic-geopolitical nature of information confrontation seems to have stabilized.

In the context of the use of information, the distinction between information-technological and information-psychological aspects is conceptually quite clear.[1308] As one comes down from the great political power struggle level to the military strategic, operational and tactical level the importance of the first increases. At this point, it should be noted that those whom previous studies have named as 'holists' define information warfare through its political and political-strategic level objective which is achieved by making the opponent do what you want by whatever means possible primarily by affecting the will of the opponent even during peacetime. However, at least for some Russian theorists, 'systemist' would be a better name for this. They perceive the information struggle as a struggle between systems, perhaps inside an even larger system, and are interested in how the technological and psychological systems affect (control) each other. 'Systemists' emphasise the importance of knowing the opponent and tailoring your own responses accordingly.

Based on the definitions given by different authors, information-technological warfare has been used as a synonym for cyber warfare and its substance and form have similarities to Western ideas. There are differences however, and no single accepted definition exists. Still, military scholars have associated it with counter command and control warfare and the idea of achieving information superiority. Thus, information has become part of military power. Moreover, the idea that information and telecommunications systems are critical for state power and sovereignty was formulated by both Russian civilian and military theorists already in the 2000s.

[1306] This a concept coined by Russian emigrant Evgeni Messner (1891-1975) (Месснера, Е.Э. Хочешь мира, победи мятежевойну! Москва: Военный университет русский путь, 2005).

[1307] Cf. Bukkvoll 2011.

[1308] The Russian emphasis on information-psychological warfare might be a result of the narrative that the Soviet Union fell because of Western information operations or because there was a tradition of psychological warfare in the KGB, ex-members of which have had a major impact on Russian thinking about information warfare. It might also be the result of emphasising morale as an important part of warfare, and it might be connected to the views of geopolitical and civilizational minded theorists who highlight the need to protect 'Russianness' in the face of Western decadence.

Based on the texts discussed here, there has been a distinct and persistent tendency to promote centralized and systematic solutions to the information struggle, warfare and security. There is a shared understanding between civilian and military scholars that the new threat emanating from the Internet and global mass media can and must be controlled through the means of state power. Additionally, this threat must be prevented from materializing and deterred even in peacetime because (technological and psychological) information superiority is a necessary requirement to win future wars. There are differences of opinion as to how this 'system of information security' should be built and what its tasks should be. As time has passed a more versatile, adaptive, distinctly cybernetic, and whole-of-government approach has gathered more support instead of a defensive system controlled by one ministry or agency. Writers with a military background have argued for an offensive role for this system. This is reflected in the recent change in the Russian doctrine characterised by a more aggressive, offensive, and active use of non-violent and violent military power.[1309]

The idea of 'protivoborstvo' was already present in the official documents at the beginning of 2000s. Still the strategic planning process revitalized in 2013-2014 seems to have given the idea more emphasis—it produced multiple documents referring to the geopolitical information confrontation and arguably prioritized its psychological aspect as a national threat. This continuous struggle even during peacetime is aimed at 'information superiority' which would affect the strategic balance. Thus, the new threats born from informatization and globalization were incorporated into the Soviet era balance of power and zero-sum security thinking. The official documents did not directly refer to information power or potential, but science, technology, and the control of information were perceived as something measurable which affected great power relations.

5.3 Strategic deterrence

The Russian idea of strategic deterrence in the Putin era has generated some interest among Western scholars. The term 'deterrence', as it features in the Russian discourse according to previous studies, implies compellence, prevention of the threat or war from materialising, deterrence in peacetime and the use of force during wartime to shape the battlefield, not just threatening the opponent with retaliation or by denying it of its objectives through intolerable risks and costs.[1310] Some previous studies, although recognizing the information struggle or warfare as part of strategic deterrence, have approached the Russian policies and strategy in the information space as inherently offensive.[1311] Pentti Forsström has argued that the current Russian deterrence

[1309] Герасимов 2019.

[1310] Kristin Ven Bruusgard has defined it as "a clustered term used to describe all of the following: activities aimed at containing any threat from materialising against Russia; activities aimed at deterring any direct aggression against Russia; and, lastly, activities focused on coercing an adversary to cede in a confrontation to terms dictated by Russia." (Ven Bruusgaard, Kristin. Russian Strategic Deterrence. Survival, Vol. 58, No.4 (2016), 7-26, 19.) Dimitry Adamsky has argued that the current military strategy of Russia combines three elements. The first is the nuclear component, the second is the integration of non-nuclear, informational, and nuclear types of deterrence and compellence, and third is holistic informational (cyber) operation consisting of cognitive-psychological and digital-technological aspects which merges military and non-military capabilities across nuclear, conventional, and sub-conventional domains. He names this 'cross-domain coercion' to distinguish it from the term 'strategic deterrence'. (Adamsky 2015, 12.)

[1311] The approach has been based on what Russia is doing to others, not on what Russia is doing to information or cyberspace or to protect itself. This 'active' and 'offensive' approach obscures the Russian perception of 'pidäke' is a system consisting of a comprehensive set of ways and means meant for controlling the security situation gradually, preventively and proactively. The means of deterrence have no predetermined order in which they should be used which enables flexibility and surprise. Thus, the border between deterrence and the use of military force has been purposefully faded.[1312] Strategic deterrence has become a unique Russian concept, at least in the eyes of Western scholars. Some of this 'hype' is however based on forgetting that already the Soviets were highly interested in the prevention of war.[1313]

As was noted when analysing the 1990s discussion about the strategic deterrence, the idea had already started to move away from purely strategic *nuclear* deterrence to a wider concept which included multiple means and spaces. Nevertheless, strategic nuclear weapons and the theoretical and practical difference between intimidation (ustrashenie) and deterrence (sderzhivanie) continued all through the 2000s and 2010s. The discussion was primarily related to the U.S.–Russia nuclear arms treaty negotiations and the United States' ballistic missile defence system. These discussions had a highly politized nature.[1314] The problem for Russians was and would also be in the future the United States' strategy which included non-nuclear long-range precision strike weapons and limited ballistic missile defences. Russia could not reduce its strategic nuclear weapons stockpile if the United States could securely perform a decapitating non-nuclear strike from behind its missile defence which would degrade Russia's ability to retaliate. Claims were made that Russia strived for a 'strategic balance' whereas the United States strived for superiority.[1315]

The debate about the nuclear deterrence was renewed in the context of 2010 with the signing of the New START (Strategic Arms Reduction Treaty) between the United States and Russia. As, the Deputy Director of the Institute of Political and Military Analysis Alexander Khramchikhin [1316] wrote in a (only) slightly ironic manner: "nuclear weapons are 'our everything'. A means of deterrence, a factor of prestige, and the only real attribute today, which allows us to be considered a great power."[1317] As long as the Russian armed forces were in a state of decay, strategic nuclear weapons were the only means of deterrence but their usability was highly restricted and they

'deterrence' as a constant struggle and competition – you are never safe because stability is only a theoretical concept. On this cf. Renz, Bettina. Russia and 'hybrid warfare'. Contemporary Politics, Vol.22, No.3 (2016), 283-300; Fink, Anya Loukianova. The Evolving Russian Concept of Strategic Deterrence: Risks and Responses. Arms Control Today, Vol. 47, No. 6 (Jul/Aug 2017), 14-20.

[1312] Forsström 2019.

[1313] Donnelly 1988, 62-63; Scott & Scott 1988, 102-103; Gartoff 1990, 16-17.

[1314] Брезкун, Сергей. Полемика. Подкоп под стратегическую стабильность. ВПК, № 50 за 29 декабр я 2004 года; Арбатов, Алексей. Ядерное сдерживание: реальности и химеры. Независимое военное обозрение, № 17 (377) за 14 мая я 2004 года; Рогова, Сергей, Есин, Виктор, Золотарева, Павел. Эксперты предлагают комплекс мер доверия по стратегическим вооружениям. Независимое военное обозрение, № 24 (384) за 02 июля 2004 года; Arbatov, Alexei, Dvorkin, Vladimir (Eds.) Missile Defense: Confrontation and Cooperation. Moscow: Carnegie Moscow Center, 2013.

[1315] Коробушин, Варфоломей. Метаморфозы стратегического сдерживания. Независимое военное обозрение, № 14 (423) за 15 апреля я 2005 года; Бочаров, Игорь. Парадоксы ядерного сдерживания. Независимое военное обозрение, № 15 (424) за 222 июля я 2005 года.

[1316] The Institute of Political and Military Analysis was created in 1996. It is a non-governmental think thank specialised in geopolitical and ideological research and lobbying mainly related to domestic politics (Иванов 2014).

[1317] Храмчихин, Александр. Иллюзия ядерного сдерживания. ВПК, № 11/2010.

were highly vulnerable to U.S. precision strike weapons.[1318] Retired Major General Vladimir Dvorkin, who has taken part in drafting almost all the major nuclear arms control treaties,[1319] argued in 2010 that strategic stability was based on strategic nuclear equilibrium, which in its turn was based on quantitative and qualitative indicators of the counterforce potential, the potential for retaliation, and the potential of deterrence. The point was that strategic stability was composed of different factors that all could destabilize the situation.[1320] Although people like Dvorkin, Arbatov and others offered a more sophisticated approaches to nuclear deterrence, the quantitative missiles-to-megatons analysis continued on the pages of Russian military journals.[1321] The failure of strategic arms control talks after 2012, the perceived militarization of space, worsened Russia – West relations, and the fear of a massive long-range precision strike seems to have highlighted the importance of the strategic nuclear component of the strategic deterrence between 2015 and 2018.[1322]

Although strategic nuclear weapons were originally seen as the backbone of Russian strategic deterrence, the substance of the idea changed. Makhmut Gareev is one of the main developers of a more comprehensive idea of deterrence. In 2005 he stated that: "In modern conditions, the concept of 'strategic deterrence' implies coordinated and purposeful implementation of all measures (intelligence, counterintelligence, increased combat readiness of strategic and conventional forces if necessary, development of armaments, preparation of TVDs, and training the population and many other measures) so that on the one hand, they reliably deter the threats with the minimum necessary defence sufficiency, and on the other, they do not provoke them."[1323] Basically Gareev claimed that the defence security (oboronnaia bezopasnost') had to be secured through diplomatic, economic, information and other non-military means. The deterrence had to be tailored to all possible military threats which for Gareev were still quite conventional.[1324] Gareev was, of course, not the only one writing about strategic deterrence. For example, researchers from TsVSI GSh VS RF retired Colonels A. L. Khriapin and V. A. Afanas'ev wrote in 2005 that "strategic deterrence is a complex of measures in the political, economic, military and other areas undertaken by the state unilaterally or on a coalition basis, and aimed at signalling to the opposing

[1318] Ibid.

[1319] Дворкин Владимир Зиновьевич. Военного энциклопедического словаря. М.: Воениздат 2007. [Online]. Available: http://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=12996@morfDictionary [Accessed: 1st April 2019].

[1320] Дворкин, Владимир. СНВ на весах стратегической стабильности. Независимое военное обозрение, № 14 за 16 апреля 2010 года

[1321] Бойцов, Маркелл. Калькулятор стратегического сдерживания. Независимое военное обозрение, № 30 за 31 августа 2012 года.

[1322] Arbatov & Dvorkin, 2013; Тадтаев, Георгий. Трамп подписал указ о создании космического командования США, РБК, 18.12.2018 [Online]. Available: https://www.rbc.ru/politics/18/12/2018/5c191a289a79473887d59637 [Accessed: 11th February 2019]; Рыбаченков, Владимир. Стабильность под прицелом. ВПК, № 38 (702) за 4 октября 2017 года; Валеев, Марат, Беломытцев, Александр. Сдерживание неопределенностью. ВПК, № 26 (690) за 12 июля 2017 года; Послание Президента РФ Федеральному Собранию от 01.03.2018 [Online]. Available: http://www.consultant.ru/document/consdoc_ LAW_ 291976/ [Accessed: 27th March 2019].

[1323] Гареев 2005а.

[1324] Ibid.

side the impossibility of achieving military-political goals by force because of the unacceptable consequences of retaliatory action."[1325] They argued that strategic deterrence was based on intimidation (ustrashenie), restraining or limiting (ogranichenie), and coercion (prinuzhdenie). Like Gareev, they too argued for tailored, multivariant and flexible responses but were primarily concerned about military threats.[1326]

For Gareev the greatest threat for Russia was the losing of its great power status which could occur through covert and overt politico-diplomatic, economic, information etc. actions meant to interfere in its internal affairs.[1327] Consequently, in 2008 Gareev proposed a new concept of strategic deterrence, which he saw as an inherently asymmetric response to the challenges Russia was facing.[1328] It was "a complex of interrelated political, diplomatic, information, economic, military and other measures aimed at deterring, reducing, and preventing threats and aggressive actions by any state (or coalition of states) by means of responses that reduce the concerns of the opposite side or threaten it with unacceptable consequences for its actions." It was based upon the defence power of the state derived from the economy and high-technology industry, active politico-diplomatic and information policy, demonstration of military power, intelligence and counterintelligence, military cooperation, protection of airspace and coastal areas with military force, preparation of infrastructure and TVDs, organization of territorial defence, cooperation between security agencies, and peacekeeping and antiterrorist activities.[1329] Gareev's definition was a clear departure from the traditional nuclear weapons-based definitions.

Around the same time as Gareev proposed his idea, V. V. Serebriannikov analysed the difference between the Russian terms of prevention of war (predotvrachshenie voiny) and military-political deterrence (voenno-politicheskoe sderzhivanie). He claimed that deterrence was part of the inhibition of war distinguished by its counterthreat to use military force against a potential threat, whereas prevention aimed at neutralizing the threat before it even become potential or real mainly through nonmilitary means. Serebriannikov claimed that "the prevention of war is a policy of constructing such a common and especially military-political situation (internal and external) which reduces and eliminates military threats, makes the collapse of military aggression unavoidable, establishes the personal legal and moral responsibility of the inspirers and organizers of aggression, and sets up the rejection of war."[1330] In 2009 Colonel V. N. Gorbunov from TsVSI GS and S.A. Bogdanov from TsVSI GSh VS RF offered a more operational and traditional view on strategic deterrence, which stated that a combination of all possible military means including strategic deployment (strategicheskoe razvertyvanoe) must be initiated already during the period of threat so as to deny aerospace and information superiority of the enemy in the initial period

[1325] Хряпин, А. Л., Афанасьев, В. А. Слово юбилярам. Концептуальные основы стратегического сдерживания. Военная мысль, № 1 2005, 8-12.
[1326] Ibid.
[1327] Гареев, М.А. Структура и основное содержание новой военной доктрины. ВПК, № 3 (169) за 24 января 2007 года; Гареев, М.А. Национальные интересы и национальная безопасность россии на современном этапе. Вестник Академии военных наук, №1 (22) 2008, 8-22.
[1328] Гареев, М.А. Стратегическое сдерживание: проблемы и решения. Красная звезда, № 183, 8.10.2008; Гареев, М. А. Проблемы стратегического сдерживания в современных условиях. Военная мысль, № 4 2009, 2-9.
[1329] Ibid.
[1330] Серебрянников 2008.

of war and deter its attack. However, deterrence should be as minimal as possible so as not provoke potential opponents.[1331] It should have deterred the war of 'a new generation' (novoe pokolenie) which consisted of kinetic, electronic, technological and psychological means which would be used at a high tempo and in coordination to destroy the opponent's capability to command its forces, to demoralize its people, and to disrupt its military-industrial complex.[1332]

Although Gareev's formulation seems to have gained wide support, some wanted to reserve the concept of strategic deterrence for the strategic nuclear forces. Accordingly, in 2010, V. V. Matvichuk and A. L. Khriapin from TsVSI argued that strategic deterrence was based on the state's ability to mobilize its conventional and nuclear forces to inflict incommensurable damages to the threating state.[1333] They changed their views in 2015 to conform to Gareev's and divided forces of strategic deterrence into offensive and defensive, nuclear and non-nuclear, global and regional forces and measures into military and non-military measures. However, the primacy of the strategic nuclear deterrence was still paramount.[1334] Others wanted to make the concept of strategic deterrence even wider by including even more spheres of threats and counteraction.[1335]

Unsurprisingly the concept of an information confrontation affected the concept of strategic deterrence. If information weapons had strategic effects, as was argued by many Russian (and Western) information theorists, then they had to be considered when discussing strategic deterrence. The team of Russian military cyber diplomats I. N. Dylevskii, S. A. Komov, S. A. Korotkov, S. V. Rodionov and A. A. Fedorov argued in a 2006 article that 'the leading countries' of the world had decided that the information space was a sphere of military action and, accordingly, it had become the object of a contest over superiority. The writers claimed that the 'weapons of mass effect' defined in the U.S. National Military Strategy of 2004[1336] were aimed at influencing populations across the globe through the 'unified global electronic information space'. They also argued that 'a group of states' impeded the creation of norms restricting the use of these weapons to support their hegemonic aspirations. This led to the conclusion that one of the main tasks of the military policy of Russia in the field of ensuring international information security was the deterrence (sderzhivanie) of

[1331] Горбунов & Богданов 2009.

[1332] Горбунов & Богданов 2009; Горбунов, В. Н., Богданов, С. А. Военно-стратегическое противоборство: формы и способы воздействия на экономический потенциал противника. Военная Мысль, № 12 2007, 50-59.

[1333] Матвичук, В. В., Хряпин, А. Л. Система стратегического сдерживания в новых условиях. Военная мысль, № 1/2010, 11-16.

[1334] Хряпин, А. Л., Калинкин, Д. А., Матвичук, В. В. Стратегическое сдерживание в условиях создания США глобальной системы ПРО и средств глобального удара. Военная мысль, № 1 2015, 18-22.

[1335] Чекинов, С. Г., Богданов, С. А. Стратегическое сдерживание и национальная безопасность России на современном этапе. Военная мысль, № 3 2012, 11-20.

[1336] The definition was based on "chemical, biological, radiological, nuclear, and enhanced high explosive weapons as well as other, more asymmetrical weapons." It can be argued that the Russian writers either misunderstood this definition or purposefully added their own interpretation. (The National Military Strategy of the United States of America. A Strategy for Today; A Vision for Tomorrow, 2004 [Online]. Available: https://www.bits.de/NRANEU/docs/NMS2004.pdf [Accessed: 27th February 2019]).

foreign countries from the possible use of means and methods of waging an "information war" against Russia.[1337]

Throughout the 2000s and 2010s the somewhat same group of authors argued for a similar international cooperation and regulation concerning information weapons as had been developed around weapons of mass destruction.[1338] In 2017 cyber diplomats argued that information weapons affected the strategic stability, and that the General Staff viewed cybersecurity (kiberbezopasnost') as a part of information security. Moreover, the 'cyber deterrence' doctrine adopted by the United States was a threat to Russia. In this context strategic deterrence would include ensuring the resilience (ustoichivost') of strategic nuclear forces and the decision-making related to them from information effects, deterring aggressive information measures, and denying the use of the Internet and mass media to affect the internal affairs of states.[1339] It should be noted that at least Andrei Kokoshin shared the Western view on deterrence which emphasised the 'politico-psychological' impact on the opponent, that is convincing through demonstration or signalling.[1340]

Two interconnected issues are related to the development of the idea of the strategic deterrence: strategic planning and territorial defence. The basics of strategic planning have been discussed above. The idea of strategic deterrence, in the form Gareev has formulated it, is central to the development of strategic planning. According to Gareev, in 1991 the Soviet Union (or Russia) did not have a plan for the time preceding war that would link the activities of various government organs to defend the country.[1341] In 2012 the deficiency was noticed by the leaders of the country and a plan was ordered to be drafted. Gareev argued that this plan would ensure the coordination of the strategic actions of the Armed forces with other law enforcement agencies, the mobilization plan, and a plan for converting the national economy to a state of war. It would include political-diplomatic, economic, information, technological, and psychological measures.[1342] Gareev repeated these arguments up until 2019.[1343] Strategic planning is, thus, partly a tool of strategic deterrence.

[1337] Дылевский И. Н., Комов С. А., Коротков С. В., Родионов С. Н. и Федоров А. В. Военная политика Российской Федерации в области обеспечения международной информационной безопасности. Военная мысль, № 4 2006, 2-7. On diplomats cf. Комов 2009.

[1338] Комов, С. А., Коротков, С. В., Родионов, С. Н. О военных аспектах проблемы международной информационной безопасности. Военная мысль, № 9 2003, 2-5; Дылевский, И. Н., Запивахин, В. О., Комов, С. А., Коротков, С. В., Петрунин, А. Н. Международный режим нераспространения информационного оружия: утопия или реальность? Военная мысль, № 10 2014, 3-12; Базылев, С. И., Дылевский, И. И., Комов, С. А., Петрунин, А. Н. Деятельность Вооруженных Сил Российской Федерации в информационном пространстве: принципы, правила, меры доверия. Военная мысль, № 6 2012, 24-28; Дылевский, И. Н., Запивахин, В. О., Комов, С. А., Коротков, С. В., Кривченко, А. А. О диалектике сдерживания и предотвращения военных конфликтов в информационную эру. Военная мысль, № 7 2016, 3-11.

[1339] Пядышева, Е.Б. (ред.) Приложение к журналу «Международная жизнь»: XI Международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». Гармиш-Партенкирхен, Германия 24–27 апреля 2017 года. Москва: «Международная жизнь», 2017, 98-99.

[1340] Кокошин, А.А. Перспективы развития военной техносферы и будущее войн и небоевого применения военной силы. Вестник академии военных наук, № 2 (67) 2019, 26-29.

[1341] Гареев 2013a, 16.

[1342] Ibid.

[1343] Гареев, М.А. Мобилизация умов Наши руководители должны коренным образом изменить отношение к науке. ВПК, № 12 (676) за 29 марта 2017 года; Гареев 2018; Гареев 2019.

Territorial defence has had an important role in the whole-of-government approach manifested in strategic planning. In the Law on Defence, territorial defence is defined as system of measures for the protection of critical infrastructure, civil society, and the operations of armed forces.[1344] The concept is well established in Russian official documents and law, although it went through a process of clarification in 2017.[1345] It is basically a process or a function which is implemented when a state of war is declared on a territory of the Russian federation. A headquarters of territorial defence is formed as an intergovernmental organ of cooperation. This ensures the upholding of military laws, and the coordination of mobilization, civil defence, and antiterrorism activities. It commands the forces specifically designated for territorial defence and represents federal power on the territory.[1346] It creates 'the platform' upon which the strategic commands operate their forces on Russian territory. The idea of territorial defence is based on the threat of large-scale conventional war and also on the 'colour revolutions' discussed above—it enables a defence in total depth of the nation and society.[1347] Territorial defence is connected to the reorganization of the Armed Forces in 2010 into combined military districts and joint (operational) strategic commands (JSCs) and the creation of the National Guard in 2016.[1348] Although territorial defence might not be a strategic cultural idea in itself, it highlights the importance of geography and defensive depth in the Russian military thinking.

The concept of strategic deterrence appeared in the 2004 Ivanov Doctrine as one of the tasks of the Russian armed forces to guarantee the protection of sovereignty, territorial integrity and other vital national interests of Russia and its allies. It referred to strategic deterrence forces and capabilities which were defined as the ability of strategic nuclear forces to inflict retaliatory damage. It also introduces the concept of de-escalation as "forcing the enemy to halt military action by a threat to deliver or by actual delivery of strikes of varying intensity with reliance on conventional and (or) nuclear weapons."[1349] The Foreign Policy Concept of 2008 did not mention deterrence in relation to Russian activities.[1350] The NSS of 2009 defined strategic deterrence under national defence as "the development and systemic implementation of a complex of interrelated political, diplomatic, military, economic, information and other measures aimed at anticipation or reduction of the threat of destructive actions."[1351] The Military Doctrine of 2010 did not define strategic deterrence but mentioned it in relation to the use of nuclear weapons to deter threats.[1352] The Foreign Policy Concept of 2013

[1344] Федеральный закон от 31.05.1996 N 61-ФЗ (ред. от 3.8.2018) "Об обороне" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_10591/ [Accessed: 29th March 2019]; 'Территориальная оборона'. Военного энциклопедического словаря. М.: Воениздат, 2007. http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=10959@morfDictionary.

[1345] Кардаш, И. Л. О совершенствовании системы территориальной обороны. Военная мысль, № 2 2014, 3-10; Кардаш, И. Л. Новый подход к организации территориальной обороны на региональном уровне. Военная мысль, № 9 2018, 34-40.

[1346] Федеральный закон 1996, Статья 22. Территориальная оборона.

[1347] Фаличев, Олег. Асимметричная война. Борьба с социальным неравенством – главное направление обеспечения безопасности страны. ВПК, № 9 (575) за 11 марта 2015 года; Герасимов 2016; Кардаш 2014 & 2018; Владимиров, Александр. Ты записался ополченцем? Незнание законов партизанской войны не освобождает от ответственности. ВПК, № 34 (649) за 7 сентября 2016 года.

[1348] Cooper 2016, 19-20; Bartles 2011; Grau & Bartles 2018b; Цыганок, Анатолий. Меняется время - меняется и военная доктрина. ВПК, № 43 (209) за 7 ноября 2007 года; Кардаш 2018.

[1349] The Defence Ministry of the Russian Federation 2004.

[1350] Концепция 2008.

[1351] Указ Президента Российской Федерации 2009b.

[1352] Указ Президента Российской Федерации 2010.

mentioned only nuclear deterrence and even that only once.[1353] The 2014 Military Doctrine is a bit confused with its use of terms and mentions nuclear and non-nuclear strategic deterrence. The system of non-nuclear deterrence is defined as "a complex of foreign policy, military and military-technical measures aimed at preventing aggression against the Russian Federation by non-nuclear means."[1354] The NSS of 2015 states that strategic deterrence is part of military policy of the state. It juxtaposes strategic deterrence and prevention of conflicts which seems to indicate they are two different things. Nevertheless, the strategy relates strategic deterrence to interrelated political, military, military-technical, diplomatic, economic, informational and other measures. The military means are based on strategic nuclear deterrence and on conventional military forces which are held in sufficient readiness.[1355] The Foreign Policy Concept of 2016 does not use deterrence in the context of Russian actions.[1356] The 2016 Information Security Doctrine states that to ensure information security in the field of defence the military policy of the Russian federation consists of strategic deterrence and the prevention of conflicts arising from the use of information technologies.[1357]

To summarize. The modern Russian deterrence theory is characterized by the acceptance of the Western theories as the basis of Russian theorizing. There is, however, a tension between the 'American' and 'Russian/Soviet' types of deterrence, where Western deterrence is seen as intimidation and containment and Russian as preventing and deterring. Gareev has been the main proponent of a strategic deterrence understood as a continuum of creating defensive power, preventing threats from materializing, and deterrence through denial and retaliation. This version of strategic deterrence involves all state actors as it is based on the participation of strategic intelligence assets, the military-industrial complex, civilian administration of territorial defence, mobilization organization and other semi-civilian organizations. The inclusive concept of deterrence spanning all environments requires a systemic approach, and perhaps, as some have argued, a new organization to control the multiple security systems. It is also directed against a full-spectrum of threats, including information threats. There is some divergence on the role of information. Some consider it as a threat, some as a sphere or means of strategic deterrence, and some as both.

The current Russian idea of strategic deterrence has two sides which have been in slight competition with one another. The first and traditional version is connected to the strategic nuclear weapons while the newer one is based on a much wider understanding of the tools and domains of deterrence. The understanding that strategic deterrence is a continuum of strategy from peacetime to wartime to neutralize threats, prevent wars and deny objectives using all possible means of statecraft seems to be quite established. Nevertheless, quite often the term of strategic deterrence is reserved for the strategic nuclear forces, and the prevention of conflict is disconnected from deterrence. Arguably, the broadening of the concept might have led to some doctrinal, organizational and resourcing choices which might have caused contention between government organs and the armed forces.

[1353] Концепция 2013.

[1354] Доктрина 2014.

[1355] Указ Президента Российской Федерации 2015.

[1356] Указ Президента Российской Федерации 2016a.

[1357] Указ Президента Российской Федерации 2016b.

Strategic deterrence is inherently connected to strategic stability and the great power struggle. It cannot be understood outside the ideas about the correlation of forces and the constant analysing and forecasting of the balance of power between Russia and the United States (and perhaps also China). Strategic deterrence as a concept has evolved in the 2000s and 2010s to one of the central pillars of Russian military policy. Although its official definition has remained a bit vague, it has materialized in the law and process of strategic planning in 2013-2014. This process incorporates Gareev's and others' ideas of the broader understanding of deterrence—most importantly the idea that wars can be prevented by shaping the Russian security environment through multiple, non-violent means. Most recent definitions include information and cyberspace and their critical systems in the sphere of strategic deterrence. The importance of the ideas of strategic deterrence, strategic planning, and territorial defence stems from the way they arrange current and future military threats, the territorially bound view on security, and the whole-of-state responses on a continuum of interstate struggle. This forms a framework for understanding the thinking of the Russian elites on military security.

5.4 Asymmetric response

The Russian idea of asymmetric actions and responses has lately been an object of interest for Western analysts.[1358] Admittedly, the occupation of Crimea in 2014 by Russia and recent Syrian operations have made Western analysts interested in the Russian military thought about indirect action and asymmetry, and, consequently, something that has been part of traditional Russian thought has been 'rediscovered.'[1359] Some have disputed this interpretations and offered their own views.[1360] More critical assessments have noted that the Russians have sometimes got themselves caught in their own 'asymmetric dreams'.[1361] Many have forgotten that just 15 years ago the whole concept of asymmetry was under heavy criticism by the Western analysts themselves.[1362]

The discussion on asymmetric responses has continued under President Putin from where it had been left under Yeltsin's reign. In 2000, the Director of the Centre for International and Strategic Studies of the Russian-Armenian University Professor Valerii Belous defined asymmetric responses, when discussing the Soviet Union's 1980s policy against American BMD, as creating better offensive strategic nuclear weapons against defensive systems.[1363] When speaking in a military-scientific conference of the

[1358] Kipp 2014; Thomas, Timothy. Russia's Military Strategy and Ukraine: Indirect, Asymmetric—and Putin-Led. The Journal of Slavic Military Studies, Vol. 28, No. 3 (2015), 445-461; Adamsky 2015; Pynnöniemi 2019a & 2019b.

[1359] On this subject Bettina Renz's summary of the debate (Renz 2018).

[1360] Kofman, Michael. Raiding and international brigandry: Russia's strategy for great power competition. War on the Rocks, June 14 2018 [Online]. Available: https://warontherocks.com/2018/06/raiding-and-international-brigandry-russias-strategy-for-great-power-competition/ [Accessed: 3rd January 2019].

[1361] Cooper, Julian. Russia's Invincible Weapons: Today, Tomorrow, Sometime, Never? Changing Character of War Centre, Pembroke College, Oxford [Online]. Available: http://www.ccw.ox.ac.uk/blog/2018/4/30/ russias-invincible-weapons-today-tomorrow-sometime-never [Accessed: 30th October 2018].

[1362] Cf. Blank, Stephen. Rethinking the Concept of Asymmetric Threats in U.S. Strategy, Comparative Strategy, Vol. 23, No. 4-5 (2004), 343-367.

[1363] Алексин, Валерий. Так считает директор Центра международных и стратегических исследований Владимир Белоус. Ответы на американские вызовы имеются. Независимое военное обозрение № 25 (198) 14.07.2000.

Academy of Military Sciences in 2003, General-Lieutenant V. A. Sapozhinskii argued that Russian Armed forces were lagging behind the developed West and they must find forces, means, forms and methods to counter the asymmetric actions of the enemy.[1364] Other speakers in the conference mentioned asymmetry only as a new but useless name for old wars and types of warfare.[1365] By 2006 the Russian military analysts had noticed the Western interest in asymmetric wars and associated these wars with the tsarist era Colonel Evgenii Messner's concept of insurrection or mutiny wars (miatezhvoina). Messner's concept was a collection of different tactics: terror, gangsterism, rebellions, riots and even demonstrations and manifestations aiming at revolution.[1366] Nevertheless, for Russian commentators the war in Chechnya was not interpreted as 'an asymmetric war' or even related to the concept.[1367]

Asymmetry was debated in the context of military reform during the first two terms of Vladimir Putin. The Chief of the General Staff Army General Iurii Baluevskii in 2006 declared that Russia will "reject the principle of symmetry" or numerical parity and build its armed forces based on 'asymmetry'. Because the General did not offer any facts or substance to support his argument the reception of his declaration was somewhat critical.[1368] One commentator ironically pointed out that the whole concept rested on the idea that Russia could create miracle weapons based on identifying the vulnerabilities of the weapons of potential adversaries, creating asymmetric and symmetric weapons through advanced technology, and successfully forecasting the future development of weapons. At the same time, it should avoid direct force-on-force confrontation.[1369] G. Ter-Arutiuniants claimed in 2007 that a new Cold War, which was fought between powers rising from under the weakening Unites States, was by its nature asymmetric. It was a war between civilizations fought with using soft power, terrorism, energy, and nuclear blackmail by weaker states.[1370]

Although the idea of asymmetric responses had not been forgotten in the early 2000s, it was reawakened around 2006–2008 as Vladimir Putin used the concept in his 2006 Annual Statement to the Federal Assembly.[1371] He was perhaps influenced by Andrei Kokoshin, who was an influential academician and politician at that time. In the context of the negotiations on the reductions of strategic nuclear weapons and missile defence, Kokoshin claimed that the strategy of asymmetric response of the Soviet

[1364] Сапожинский, В.А. Взгляды на характер операций (боевых действий) в войнах будущего. Вестник Академии военных наук, №2(3) 2003, 53-57.

[1365] Гареев, М.А. Доклад президента Академии военных наук генерала армии М.А.Гареева. Вестник Академии военных наук, №2(3) 2003, 9-17.

[1366] Маначинский, Александр. Когда слабый побеждает сильного. Независимое военное обозрение N 47 22.12.2006.

[1367] Нечитайло, Дмитрий. "Асимметричная война" исламистов. Независимое военное обозрение № 28 14.8.2006; Сиротинин, Евгений, Криницкий, Юрий. Партизанско-террористические войны в эпоху ядерного сдерживания. Независимое Военное Обозрение, № 20 4.6.2010; Зеленый, В. В. Основные тенденции противодействия терроризму. Военная мысль, № 10 2015, 3-14.

[1368] Колыванов, Георгий. Непонятная асимметрия. Генштаб попытался сказать новое слово в военной науке. Независимое военное обозрение N 4 3.2.2006; Балуевский, Юрий. Генерал армии Юрий Балуевский: Генеральный штаб и задачи военного строительства. Красная звезда, 25.01.2006.

[1369] Растопшин, Михаил. В лабиринте асимметричных ответов. Независимое Военное Обозрение, № 17 1.6.2007.

[1370] Тер-Арутюнянц, Г. Многополярная и асимметричная холодная война. Вестник Академии военных наук, №4(41) 2007.

[1371] Послание Президента РФ Федеральному Собранию от 10.05.2006 [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_60109/#dst0 [Accessed: 27th March 2019]; Иванов 2014.

Union had worked as the United States eventually froze the development of the SDI. According to Kokoshin, the strategy of asymmetric response was based on the idea that the SDI, however complete and efficient, could be bypassed with new weapons and by disrupting the SDI itself, and that the Soviet strategic weapons could be made more secure from a surprise first-strike. Furthermore, Kokoshin argued that parallel to technological solutions, a psychological campaign was launched to turn the American elite against the SDI. Kokoshin has compared the strategy of asymmetric response to Sun Tzu's principle of not doing what the enemy wants or what the enemy does but acting in a way that increases one's own strengths and minimizes the possibilities of the enemy. This principle, he claims, is also found in the works of A. A. Svechin.[1372] Kokoshin's proposals and views on asymmetry were criticized for being simplistic and being based on a model that had already failed once.[1373] Furthermore, his writings were meant to influence current events which apparently worked. For instance, in 2007 when President Vladimir Putin stated that "our response will be asymmetrical, although highly effective" when discussing the United States' missile defence he was explicitly quoting Mikhail Gorbachev from 1986.[1374]

The idea of asymmetric responses eventually reached the Academy of Military Sciences. Gareev had written about an indirect strategy already in 1995 but in 2009 he argued that "With the relative weakness of our economic potential, the main emphasis should be placed on creating asymmetric means and methods of response."[1375] Later, Gareev, for example, promoted the exploitation of weaknesses in C3 systems.[1376] He also connected asymmetric actions to international confrontations and to the so called colour revolutions.[1377] These thoughts led Gareev to conclude that "The Soviet Union had nuclear weapons, these weapons remained, but the Soviet Union did not. Therefore, due attention must be paid to the development of general-purpose forces, including the land forces, air force and navy, and to place the main emphasis on asymmetric means and ways to neutralize the technological superiority of the enemy."[1378] Gareev's views were echoed by Gerasimov who argued that Russia should not just copy and catch up but to work "ahead of the curve" and be in a leading position itself.[1379] In 2015 Gareev argued that to counter the aggression of opponents with

[1372] Кокошин, Андрей. "Асимметричный ответ" vs. "Стратегической оборонной инициативы". Международная жизнь, № 7 - 8, 2007; Кокошин, Андрей. "Звездные войны": ответить асимметрично. Кразная звезда, № 164, 12.9.2007; Кокошин, Андрей. "Звездные войны": как СССР ответил Рейгану. Кразная звезда, № 169, 17.9.2008; Кокошин, Андрей. Асимметричный ответ номер один. Независимое военное обозрение № 24 27.7.2007; Ознобищев, С. К., Потапов, В. Я., Скоков, В. В. Как готовился «асимметричный ответ» на «стратегическую оборонную инициативу» Р. Рейгана. Велихов, Кокошин и другие. М.: Институт стратегических оценок, изд. ЛЕНАНД, 2008

[1373] Кулаков, Александр. Асимметричный ответ не спасет. Независимое военное обозрение N 25 25.7.2008.

[1374] Kremlin.ru. Transcript of press conference with the Russian and foreign media, President of Russia's official web portal, February 1, 2007 [English] [Online]. Available: http://en.kremlin.ru/events/president/ transcripts/24026 [Accessed: 14th February 2019].

[1375] Гареев, М. А. Проблемы стратегического сдерживания в современных условиях. Военная мысль, № 4 2009, 2-9, 6. Also Гареев 2009a.

[1376] Гареев 2013; Гареев 2017b.

[1377] Гареева 2012.

[1378] Гареева 2013c, 4-9, 6.

[1379] Герасимов 2013a, 29.

overwhelming technological superiority and non-contact weapons, Russia had to either develop new weapons or to develop 'operational strategic actions' that would neutralize the advantage of the enemy.[1380]

The idea of an asymmetric response also reached information warfare theorists. Rastorguev, for example, argued that against the efforts to restrict Russia's geopolitical status, Russia's response should be asymmetric which meant the dismantling of the mechanism of self-destruction.[1381] This statement must be understood in the context of Rastorguev's theory of self-destructive systems. An asymmetric response is then an act to remove possible weaknesses in the algorithms of the systems.[1382] Others like Manoilo et al. argued that information was inherently an asymmetric object as it was always changing, and its change reshaped the environment.[1383]

Historical studies produced somewhat anachronistic historical interpretations which included the cruise missiles developed during the Soviet times and the Soviet Navy's blue water fleet programme in the 1970s as asymmetric responses.[1384] On a more diplomatic level, Russia's moratorium of CFE was offered as an asymmetric response.[1385] Russia's permanent representative to NATO Aleksandr Grushko stated in 2016 that Russia would "prepare an asymmetric response" to the increased NATO forces near its borders which would be maximally effective but not extremely costly.[1386] In this context, S. A. Syachev had already proposed in 2009 that in the case an enemy managed to disable Russian strategic forces with a surprise attack, the rapid mobilization of Russian irregular forces against the attacker's land forces could be considered an asymmetric action.[1387] Conversely, strategic nuclear weapons and ballistic missile defences have been a constant source of different interpretations of an asymmetric response.[1388] For example, Alexei Arbatov has associated asymmetry with the idea that the defence against strategic nuclear weapons must be perfect, while offence must succeed to inflict intolerable damage only once .[1389] Asymmetry was also implied when Major General S. V. Kuralenko from the Military Academy of the General Staff pointed out that as warfare had expanded include the air and space, the information systems of air defence, missile defence, and electronic warfare had become decisive.

[1380] Гареев, М.А. В интересах обороноспособности страны. Вестник Академии военных наук 1(50) 2015, 4-9.

[1381] Cited in Ковалев В.И., Коссе Ю.В. "Гудвилл" сша в контексте инициатив по сокращению сяс и проблемы Россиии. Информационные войны, №4 (12) 2009, 10-19, 16.

[1382] Ibid.

[1383] Манойло, Петренко & Фролов 2012.

[1384] Ефремов, Г., Царев, В., Асатуров, С. Владимир Челомей в истории Советского ВМФ. ВПК, № 25 (291) за 1 июля 2009 года; Богданов, Константин. Момент истины для «убийц авианосцев». ВПК, № 46 (362) за 24 ноября 2010 года.

[1385] Фаличев, Олег. Недалеко и до новой "Берлинской стены". ВПК, № 18 (184) за 16 мая 2007 года.

[1386] Мухин, Владимир. Россия и НАТО вышли на дистанцию танковой атаки. Независимая газета, № 65 (6679) 2016.

[1387] Сычёв, С.А. Применение иррегулярных формирований в решении боевых задач. Вестник Академии военных наук, № 4 (29) 2009, 46-48.

[1388] Артамонов, Игор, Рябцев, Роман. Асимметричный ответ России Таковым может стать развитие тактического ядерного оружия малой и сверхмалой мощности. ВПК, № 15 (483) за 17 апреля 2013 года; Сивков, Константин. Глобальный контрудар Способы нейтрализации национальной ПРО США могут быть асимметричными и весьма неординарными. ВПК, № 21 (587) за 10 июня 2015 года; Сивков, Константин. Асимметричный «Сармат» Ракеты средней дальности – оружие малой ценности. ВПК, № 45 (709) за 22 ноября 2017 года.

[1389] Арбатов, Алексей. Стратегические асимметрии и системы ПРО. Независимое Военное Обозрение, № 1 20.1.2012.

He indirectly offered these systems as asymmetric responses of Russia to a technologically superior opponent.[1390]

The idea that electronic warfare could be considered an asymmetric response surfaced from time to time in the Russian debate during the 2000s and 2010s. The importance of EW was at least partly emphasised because of the influence of the American high-tech doctrine and military campaigns—although the Soviet tradition of EW also had an influence.[1391] For example, General-Major L. N. Il'in, and retired Colonels P. A. Dul'nev and V. T. Kobalev have proposed anti-NCW warfare as an asymmetric response to the American technological superiority. It would consist of weapons that can disrupt the command, control and communication systems behind NCW.[1392] In a similar manner I. I. Korolev, V. N. Pavlov and A. V. Ganin, who are representatives of the EW troops, have proposed an 'electromagnetic blockade' as an asymmetric response to NCW.[1393] Electronic warfare combined with aerospace defences has also been proposed as an asymmetric response to the so-called sixth generation of Western warfare.[1394] In contrast to the view that EW is an asymmetric response to NCW, I.N. Vorob'ev and V. A. Kiselev have argued that one of the principles of NCW (in this case understood as a doctrine of command and control) is asymmetry. This sets NCW apart from conventional modern tactics where the guiding principle is 'combat activity' or retaining the initiative.[1395]

The discussion on indirect actions, which had already began in the 1990s, had a direct relationship with the military's understanding of asymmetry. Retired Major General I. N. Vorob'ev and Colonel V. A. Kisilev, both academicians of the Military Education-Training and Research Centre of the Ground Forces (VUNTs SV "OVA VS RF")[1396], wrote in 2006 that because of technological changes, an indirect (nepriamyi) strategy has surpassed the direct strategy of destruction based on material superiority. Modern indirect strategy is based on a large variety of forms and methods and it has manifested as the use of deception (obman), stratagems (khitrost'), and intimidation (ustrashenie) to destroy the enemy without the use of weapons through information superiority. Thus, information-psychological weapons have strategic effects and EW has become an inherent part of all operations.[1397]

[1390] Кураленко, С. В. Тенденции изменения характера вооруженной борьбы в военных конфликтах первой половины XXI века. Военная Мысль, № 11 2012, 40-46.

[1391] Горбачев, Юрий. РЭБ в операциях XX и XXI века. ВПК, № 44 (61) за 17 ноября 2004 года.

[1392] Дульнев, П. А., Ковалев, В. Т., Ильин, Л. Н. Асимметричное противодействие в сетецентрической войне. Военная Мысль, № 10 2011, 3-8.

[1393] Королев, И. И., Павлов, В. Н., Ганин, А. В. Радиоэлектронно-информационная блокада - перспективный способ применения разнородных сил и средств РЭБ. Военная Мысль, № 4 2013, 16-23.

[1394] Лузан, Александр. Воздушно-космическое нападение. В войнах нового поколения резко возрастает роль высокоточного оружия и средств борьбы с ним. Независимое Военное Обозрение, № 10 (846) 20.3.2015.

[1395] Воробьев, И. Н., Киселев, В. А. От современной тактики к тактике сетецентрических действий. Военная Мысль, № 8 2011, 19-27.

[1396] Part of the Combined Arms Academy of the Armed Forces of the Russian Federation after 2009 (Obchshevoiskovaia akademiia Vooruzhennykh Sil Rossiiskoi). The Academy trains officers for the Ground Forces and conducts defence research on various subjects. (ВУНЦ СВ «ОВА ВС РФ» [Online]. Available: http://ova.mil.ru/ [Accessed: 29th March 2019].

[1397] Воробьев, И. Н., Киселев, В. А. Стратегия непрямых действий в новом облике. Военная мысль, № 9 2006, 2-10; Воробьев, И. Н., Киселев, В. А. Военная наука на современном этапе. Военная мысль, № 7 2008, 26-31.

Indirect methods also fascinated the Chief of the Centre for Military Strategic Studies of the General Staff (TsVSI GS) Colonel S. G. Chekinov, and S. A, Bogdanov who wrote in the 2010s that military science had to include indirect and non-military measures in its corpus as interstate confrontation (mezhgosudarstvennoe protivoborstvo) now included them.[1398] Chekinov and Bogdanov seemed to discard the necessary requirement of 'weak against strong.' An asymmetric strategic approach to them was based on non-identical capabilities that enabled the avoidance of direct confrontation and enabled the potential opponent's vulnerabilities to be threatened.[1399] For them indirect measures were inherently associated with asymmetry, military cunning and surprise. The concept also included maskirovka and stratagems.[1400] Furthermore, in 2017 Chekinov and Bogdanov elaborated their views on the role and substance of modern military strategies and claimed that all strategy was asymmetric—a claim that has been made by the Western theorists also, although, as a criticism toward the whole concept of asymmetry.[1401] The scholars argued that Russia must therefore develop its own asymmetric response which should consist of demonstrations, readiness, deterrence, denial and the ability to inflict unacceptable damage to the military and non-military assets of the enemy.[1402]

Perhaps a bit more critical and social-scientific definition of asymmetry has been offered by E. A. Stepanova from the Primakov National Research Institute of World Economy and International Relations.[1403] She has redefined asymmetric war or actions as an asymmetric confrontation (asimmetricheskaia konfrontatsiia) where asymmetry relies on the dialectical relationship of the adversaries instead of one-sided capabilities.[1404] A similar dialectical view was shared by retired Colonel and Professor Iu. V. Krinitskii who has argued that the concepts of asymmetry, superiority in power, and correlation of forces are intertwined. He has claimed that although asymmetry could be achieved through actions on operational-tactical level, on a strategic level it was based on economy and technology and thus it was never cheap. Additionally, asymmetry was never a stable state because an advantage in technology is only temporary.[1405] This temporary nature of asymmetry resonated with Colonel General M. M.

[1398] Чекинов, С. Г., Богданов, С. А. Влияние непрямых действий на характер современной войны. Военная мысль, № 1 2011, 3-13, 13; Чекинов & Богданов 2015b; Чекинов & Богданов 2017.

[1399] Чекинов, С.Г., Богданов, С.А. Влияние асимметричных действий на современную военную безопасность России. Вестник Академии военных наук, № 1 (30) 2010, 46-53.

[1400] Чекинов, С. Г., Богданов, С. А. Военное искусство на начальном этапе XXI столетия: проблемы и суждения. Военная мысль, № 1 2015, 32-43.

[1401] Чекинов, С. Г., Богданов, С. А. Военная стратегия: взгляд в будущее. Военная Мысль, № 11 2016, 3-15, 7; Чекинов & Богданов 2017; Milevski, Lucas. Asymmetry is Strategy, Strategy is Asymmetry. JFQ, Vol. 75, No. 4 (2014), 77-83.

[1402] Чекинов, С. Г., Богданов, С. А. Асимметричные действия по обеспечению военной безопасности России. Военная Мысль, № 3 2010, 13-22.

[1403] The Primakov National Research Institute of World Economy and International Relations (IMEMO) is a federal public institution created in 1956 and functions under RAN. It is a research institution which concentrates on international relations and the world economy and has multiple divisions and a staff of over 500 persons. (Иванов 2014).

[1404] Степанова, Е. А. Асимметричный конфликт как силовая, статусная, идеологическая и структурная асимметрия. Военная Мысль, № 5 2010, 47-54.

[1405] Криницкий, Ю. В. Асимметричные средства и способы ведения войны. Военная Мысль, № 11 2010, 25-30.

Kucheriavyi, the Vice-Governor of St. Petersburg, who defined information asymmetry as a selective, limited response to the aggressive information effects of the enemy with no need to maintain quantitative parity with the opponent.[1406]

By 2015 the General Staff was ready to offer an official definition of asymmetric actions. General-Lieutenant A. V. Kartapalov argued that 'asymmetric actions' would be used in 'a new type' of future wars to level the technological superiority of the enemy. They would be used by weaker adversaries who had limited resources. These actions could be economic, diplomatic, information as well as non-direct and direct military actions aimed at the vulnerabilities of the opponent for maximum effect at the minimum cost to one's own forces and resources. There were no universal asymmetric actions as conflicts differed and opponents adapted to them. Their effectiveness depended on the completeness and timeliness of their implementation which should be achieved through coordination of multi-departmental forces throughout the state organizations. [1407] What Kartapalov was describing was a whole-of-government, state-based approach to asymmetry as a tactical action in peace and wartime, and as such it diverges from the 'asymmetric response' idea of Kokoshin. It is a more traditional definition of asymmetry than some Russian writers have proposed as it concentrates on the means of the weaker side.

Kartapalov's definition did not end the debate. In 2017 A. V. Kiselev claimed that the principles of asymmetric actions include secrecy, the search and identification of weaknesses, the concentration of efforts against the most vulnerable points of the adversary, in addition to the imposition of the desired course of the conflict and will on the adversary. The following of these principles should result in low costs compared to the enemy and superiority or, at least, equality in an armed confrontation.[1408] In 2017 Aleksandr Bartosh managed to combine strategic deterrence, hybrid war and a Russian asymmetric response in a concept that included all the hyped-up terms but did not manage to offer anything beyond a show of loyalty for the official rearmament programme.[1409] Perhaps the latest addition to the Russian debate on asymmetry has been V. V. Selivanov's and Iu. D. Il'in's article where they proposed a methodology to find an asymmetric response to high-technology opponents.[1410] The idea was to avoid a symmetric, costly response which would lead to an arms race and the exhaustion of the economy of the weaker side. Selivanov's and Il'in's model was based on comparing the time-cost-effectiveness values of competing systems.[1411] This 'levelling' (nivelirovanie) of the military-technological superiority of the enemy by locating and

[1406] Кучерявый, Михаил Михайлович. Информационное измерение политики национальной безопасности России в условиях современного глобального мира. Диссертация на соискание ученой степени доктора политических наук по специальности. Санкт-Петербург, 2014, 266.

[1407] Картаполов 2015.

[1408] Киселев, В. А. К каким войнам необходимо готовить Вооруженные Силы России. Военная Мысль, № 3 2017, 37-46.

[1409] Бартош, Александр. Трудно обеспечить безопасность Евразии в условиях "новой холодной войны" Независимое Военное Обозрение, № 30 (961) 18.8.2017.

[1410] Селиванов, В. В., Ильин, Ю. Д. Методические основы формирования асимметричных ответов в военно-техническом противоборстве с высокотехнологичным противником. Военная Мысль, № 9 2019, 33-41.

[1411] Ibid.

striking against its critical strategic objects using creative ways and means is also promoted others.[1412]

The concept of asymmetric response was accepted by many commentators by 2017 as an official Russian strategy against the United States and its allies.[1413] However, none of the official national security and strategic planning documents use the term asymmetric. It can always be argued that with an asymmetric response, even if it had a certain cultural resonance with the positive aspects of Russian traditions like stratagems, creativity and cunning, it was not politically wise to admit that Russia was a weaker side in any geopolitical struggle. After the United States and the European Union imposed sanctions on Russia due to the annexation of Crimea, the asymmetric response became an economic issue. Russian Prime Minister Dmitrii Medvedev, for example, stated that economic sanctions are always political and thus asymmetric.[1414] The economic aspect highlights the issue that there is, as was in the case of strategic deterrence, a noticeable under-current of institutional fighting over resources behind the different formulations of an asymmetric response.

To summarize. The Russian texts analysed here contain multiple meanings of asymmetry and asymmetric response which shows that the Russians have been interested in the idea. Asymmetric response can be described as overcoming an adversary's offensive and defensive systems while at the same time protecting one's own systems. It can be a cost-effective solution and/or an innovative technological breakthrough in the spirit of dialectical weapon–counter-weapon progress. For politicians it might be an economic solution or a new direction in politics such as emphasising regional cooperation. For military scholars it has often meant ways to neutralize an adversary's superiority through technology or creative, innovative action. The substance of this response has depended on the affiliation of the writer as different services, forces and troops have been offered as the asymmetric response. Some of the most vocal proponents have been those claiming that electronic warfare measures and denying the electromagnetic spectrum from the advanced opponent, i.e. the United States would counter the advantages of the NCW. By 2017-2018 the Russian Armed Forces seem to have adopted asymmetry, i.e. exploiting the weaknesses of the opponent, as a part of its official doctrine. Information has had a role in almost all of the definitions of asymmetry proposed in the timeframe of 2000-2018. Clearly, it has been considered as something new or having a disruptive quality, which has made it a variable that could affect the correlation of forces and, thus, everything from the battlefield to the strategic balance. This asymmetric quality of information is applied to both technological and psychological aspects of information.

[1412] Фадеев, А. С., Ничипор, В. И. Военные конфликты современности, перспективы развития способов их ведения. Прямые и непрямые действия в вооруженных конфликтах XXI века. Военная Мысль, № 2 2019, 5-14, 7

[1413] Иванько, Анатолий. Эшелонированная брешь Мысль всегда будет эффективнее самого высокоточного боеприпаса. ВПК, № 12 (627) за 30 марта 2016 года; Казеннов, Сергей, Кумачев, Владимир. Хочешь мира - готовься... к чему? Независимое Военное Обозрение, № 19 29.5.2015; Казеннов, Сергей, Кумачев, Владимир. Ах, если б вам служить на суше... Независимое Военное Обозрение, № 28 7.8.2015; Ивашов, Леонид. Удар Валдая. Выступление президента России на собрании дискуссионного клуба в Сочи стало главной мировой новостью. ВПК, № 41 (705) за 25 октября 2017 года.

[1414] Лысова, Татьяна, Стеркин, Филипп, Харатьян, Кирилл. "Есть вещи пострашнее ограничения поставок". Ведомости, 8.9.2014 [Online]. Available: https://www.vedomosti.ru/newspaper/articles/2014/09/08/est-veschi-postrashnee-ogranicheniya-postavok-dmitrij#ixzz3Ci26r445 [Accessed: 14th February 2019].

An asymmetric response is a prime example of a strategic cultural idea which is carried by epistemic communities and which resurfaces from time to time when the state's external environment calls for it. It is also a good example of how these ideas are made to 'fit' the current needs and environment. The asymmetric response is whatever any individual scholar or lobbyist wants it to be. It holds legitimizing power and as such is contested between different groups—the strategic nuclear weapon and EW professionals serve as an example. It is also offered as a 'deus-ex machina' to rebalance the great power relationship. It is usually a cost-effective but technologically innovative solution offering to replace quantitate with qualitative power. As such, its roots are in the Cold War era correlation of force calculations and in the never ending strive towards strategic parity. However, asymmetric response and asymmetric action should be separated—they are two interconnected but different ideas. The first operates on the political and strategic level while the other is a more tactical and operational concept more tied to the character of war (the borders of which with peace have faded) than strategic stability. Nevertheless, both versions should be understood in the context of 'protivoborstvo', i.e. the continuous struggle to find advantages in the zero-sum game which is international politics. Whereas asymmetric response has been framed as a 'Russian' idea, asymmetric actions were first observed as something Western, but by 2018 were incorporated into the Russian strategic thought.

5.5 Digital sovereignty

As was argued in Chapter 4, the concept of digital sovereignty did not come into being before the 2000s but had its roots in previous Russian ideas about territorial state sovereignty. Its appearance in the 2010s has been noted in previous studies. It has been primarily interpreted as an example of the importance the Russian regime places on sovereignty, state control, and territorial integrity now reflected upon the Internet.[1415] For example, Julian Nocetti has argued that Russia approaches cyberspace as a territory with virtual borders corresponding to physical state borders and state sovereign rights and responsibilities.[1416] Eneken Tikk and Mika Kerttunen have claimed that this sovereignty-based vision of cyberspace has led to a collision between Russian and Western views emphasising human rights and existing international laws.[1417] Moreover, in a 2017 journal article Mari Ristolainen argued that 'digital sovereignty' is a central concept to understanding Russian state cyber security thinking.[1418] She claimed that "Consequently, RuNet has evolved from an alternative social universe to a state-controlled 'safe and secure' digital environment that manifests 'digital sovereignty'."[1419]

[1415] Soldatov, Andrei and Borogan, Irina. Russia's Surveillance State. World Policy Journal, Vol. 30, No. 3 (Fall 2013), 23-30, 29; Soldatov 2017; Vendil Pallin 2017, 17. Here Vendil-Pallin refers to Alena Ledeneva's concept of 'sistema' or clusters of informal networks. Ibid., 28-29; Jaitner & Rantapelkonen 2013, 69.

[1416] Nocetti 2015, 112.

[1417] Eneken & Kerttunen 2017.

[1418] Ristolainen, Mari. Should "RuNet 2020" be taken seriously? Contradictory views about cybersecurity between Russia and the West. Journal of Information Warfare, Vol. 16, No. 4 (2017), 113-131. The article is an updated version of earlier conference paper (Ristolainen 2017a).

[1419] Ristolainen 2017b, 118. Ristolainen, Kukkola and Nikkarila have continued to research the subject of Russian theoretical thought on digital sovereignty. This chapter is based on that research and expands it by introducing new material. Kukkola, Ristolainen & Nikkarila 2019; Ristolainen & Kukkola 2019a.

The Russian understanding of digital sovereignty is intertwined with its cyber norm building efforts which have been spearheaded by a group of people composed of ex-military and ex-KGB/FSB officers, MGIMO academicians and other institutes, and retired or serving diplomats.[1420] These 'cyber diplomats' are essential to understanding the Russian idea of 'digital' or 'information sovereignty'. The previously mentioned Anatolii Strel'tsov belongs to this group and has written about international cyber security norms mainly in the context of the UN GGE process during 2011-2018. His texts are not personal theoretical treatises but arguments for the Russian proposals in the UN and as such represent the official view of the Russian regime.[1421] Their main point is that there is a lack of international rules on the military use of information-communication technology (ICT) and no shared concept of 'information war' or 'weapons' which is an inherently dangerous state of affairs. Strel'tsov's texts highlight the main issues of Russia's cyber diplomacy, that is, the primacy of state sovereignty, the territorial view of cyberspace's infrastructure, and the understanding of information being both psychological and technological. One of the main points of contention here is that Russia pursues the official banning of the 'malicious use of ICT'. It is important to note that 'malicious use' does not mean only destructive use but also denial, manipulation and exploitation. Consequently, in 2014 Andrei Krutskikh and Anatoli Strel'tsov pointed out that Russia had not signed the Council of Europe's Convention on Cybercrime because it presumably allowed unsanctioned access to networks of other countries which violates the sovereignty of the target state.[1422]

Strel'tsov has argued that state dominion (verkhovenstvo) in cyberspace is delineated into three areas: information and telecommunication networks located in the national territory, the ICT means to collect, transfer, store, receive or distribute information, and local or distributed ASUs.[1423] Strel'tsov considers it problematic that things are designated in cyberspace by their address because these addresses do not conform to state borders or designate a physical infrastructure on a state territory and are moreover administrated by international non-governmental organizations with no internationally recognized legal status (i.e. ICANN).[1424] Consequently, Strel'tsov has argued

[1420] For example, beginning from 2007, these people have organized the yearly Russian cyber security conference in Garmisch-Partenkirschen. They know each other, write academic or semi-academic papers together and the most prominent of them belong to the National Association of International Information Security (NAMIB). The group has published multiple books and their bios are included in Комов 2009. Based on the ISTINA database, these people write and publish together (ИСТИНА webpage [Online]. Available: https://istina.msu.ru/ [Accessed: 2nd April 2019]). On NAMIB cf. TACC 2018; Пядышева 2018.

[1421] Крутских, Андрей, Стрельцов, Анатолий. Международное право и проблема обеспечения международной информационной безопасности. Международная жизнь, № 11 (2014); Стрельцов, Анатолий. Основные направления развития международного права вооруженных конфликтов применительно к киберпространству. VIII международный форум по международной информационной безопасности. 21-24 апреля 2014 года. Гармиш-Партенкирхен, Германия, место издания Издательство Московского университета. Москва: 2014, 52-70; Стрельцов, А.А. Адаптация международного права безопасности к информационному пространству. Девятый международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» и Одиннадцатая научная конференция МИКИБ 20–23 апреля 2015 года. Гармиш-Партенкирхен, Германия. М.: 2015, 81-86; Стрельцов, А.А. Применение международного гуманитарного права к вооруженным конфликтам в киберпространстве. Российский ежегодник международного права 2015. Санкт-Петербур: "Россия-Нева", 2015, 152-169; Стрельцов, Анатолий. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности. Журнал Международная жизнь, № 2. 2017.

[1422] Крутских & Стрельцов 2014.

[1423] Крутских & Стрельцов 2014, 155-156.

[1424] Ibid., 156.

that the United States is the only state enjoying sovereignty in cyberspace because it indirectly controls ICANN. To remedy the situation Strel'tsov argues, among other things, for developing an international treaty recognizing state sovereignty in cyberspace, delimiting state borders in cyberspace, and the creation of a map designating a national infrastructure.[1425] In line with this thinking, Strel'tsov argued in 2017 that there is a national ICT segment which is juridically located on Russian territory, and thus under Russian federal state powers. This claim is the basis for the term 'national segment of the Internet' which denotes state sovereignty on the Internet through its infrastructure. Strel'tsov then logically concludes that the state has the right to control the national segment to ensure its security, resilience, and development in accordance with national interests.[1426] In another article Strel'tsov and Anatolii Smirnov[1427], argued that 'the ICT environment' is a widely recognized concept based on a UN GGE report. They then proceed to define this environment—something that the UN GGE report clearly tries to circumvent as it would support Russia's demands for internationally recognized information sovereignty.[1428] Strel'tsov's texts demonstrate an intentional effort to create an intellectual basis for the state claims of authority over the Internet.

Associate professor Elena Zinov'eva from MGIMO[1429] is an interesting scholar because she is connected to Andrei Krutskikh who is one of the central figures of the Russian cyber diplomacy team.[1430] He has co-authored articles with almost all of the leading Russian 'cyber diplomats'—including Anatoli Strel'tsov who was discussed above.[1431] In this group Zinov'eva represents the younger generation. Zinov'eva's basic argument is based on the inherent inequality of globalization and the reactions of authoritarian regimes to the free flow of information. This development creates a divide between 'the info rich' and 'the info poor', or the 'digital divide', and is a source of new types of conflict.[1432] Zino'eva has argued that the multi-stakeholder model of governing the Internet, which Russia has opposed contributes to the 'digital divide'[1433]

[1425] Ibid., 163.

[1426] Стрельцов 2017.

[1427] Smirnov is a Russian diplomat and a leading researcher at the Center of International Information Security and Scientific-Technological politics in the MGIMO.

[1428] The United Nations General Assembly Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174 22 July 2015 [Online]. Available: https://undocs.org/A/70/174 [Accessed: 29th March 2019].

[1429] Zinov'eva has a PhD in Political Science and is an Associate Professor at the Department of World Politics, and Deputy Director of Centre for International Information Security, Science and Technology Policy MGIMO University (Зиновьева Елена Сергеевна. МГИМО Online. Available: https://mgimo.ru/people/zinoveva/ [Accessed: 2nd April 2019]).

[1430] Krutskikh is a Professor at the Department of World Politics, the Director of the Center for International Information Security and Science and Technology Policy, and the vice-chair of the National association of international information security. Krutskikh is a career diplomat and has worked with arms control issues. Zinov'eva's book on Internet governance has been written under the guidance of Krutskikh (Зиновьева, Е. С. Международное управление Интернетом: конфликт и сотрудничество: учеб. Пособие. М.: МГИМО-Университет, 2011.)

[1431] Крутских Андрей Владимирович МГИМО Online. Available: https://mgimo.ru/people/krutskikh-andrey/ [Accessed: 2nd April 2019].

[1432] Зиновьева, Е.С. Международно-политические аспекты развития интернета. Вестник МГИМО-Университета № 4 (31) 2013, 135-140, 139. Also Зиновьева, Е.С. Международное управление интернетом: проблемы, подходы, перспективы. Вестник МГИМО-Университета № 6 (15) 2010, 167-174.

[1433] The 'digital divide' is a concept which was used in the Okinawa Charter on Global Information Society in 2000 (Okinawa Charter on Global Information Society, 2000 [Online]. Available: https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html [Accessed: 2nd April 2019].)

as digitally underdeveloped states do not have the resources to protect their interests.[1434] The borders of state control, sovereignty, and the balance of power in the information sphere are under threat.[1435]Zino'eva has claimed that the current status quo serves the interests of the United States, although her arguments are somewhat contradictory as she claims that the United States does not want to give up its sovereignty in the face of globalization and degrading power position but at the same time claims that Russia (and others) are entitled to their sovereignty and control over the Internet.[1436] Zinov'eva has argued that Russia's place in the global information society is based on its scientific and educational potential, quality of information infrastructure, the level of the development of electronic business and commerce and electronic government. It is noteworthy that these elements can be measured.[1437] Zinov'eva summarized Russian national interests in the information sphere as being based on the respect for state sovereignty, interstate governance of the Internet, and the stability, security, and uninterrupted functioning of the Internet.[1438]

In 2014 Zinov'eva wrote that the interstate confrontation (mezgosudarstvennoe protivoborstvo) had transferred into the information sphere. Accordingly, Russia had expanded its list of information threats from the use of ICT to terrorist, criminal, and military-political ends to include interfering in the internal affairs of states.[1439] She stated that in this context Russia pursued 'the broad understanding' of international information security including technological and politico-ideological aspects, whereas the West pursued only a narrow understanding which was technological and named 'cyber security' (kiberbezopasnost').[1440] Russia has pursued the demilitarization of the information space and the formation of an international normative regime as the basis of international information security.[1441] Zinov'eva also argued in 2016 that information flows draw together culturally similar countries and that the regionalization and Balkanization of the Internet was a natural and beneficial phenomenon resisted by the status quo powers.[1442] She claimed that in this context Russia strives to shape the information space to correspond to the multipolar world order—one polar of which is Russia—and to the idea of 'digital sovereignty'.[1443] This strategy of increased state control she claimed was optimal as, "on the one hand, it provides the openness necessary for the development of Internet business and related industries, and on the other hand, it provides controllability and controllability of the Russian segment of the Internet."[1444] Although Elena Zinov'eva is far from original, her texts offer a glimpse of the changing worldview and ideas, or at least political argumentation, of the 'cyber diplomats'.

[1434] Зиновьева 2010.

[1435] Зиновьева 2013.

[1436] Ibid., 171-172.

[1437] Зиновьева 2011.

[1438] Ibid. Also Зиновьева, Е.С. Глобальное управление Интернетом: российский подход и международная практика. Вестник МГИМО-Университета, № 4 (43) 2015, 111-117.

[1439] Зиновьева, Е.С. Анализ внешнеполитических инициатив РФ в области международной информационной безопасности. Вестник МГИМО-Университета. № 6 (39) 2014, 47-52.

[1440] Ibid., 49.

[1441] Ibid.

[1442] Зиновьева, Е.С. Возможности России в глобальном информационном обществе. Вестник МГИМО-Университета. № 3 (48) 2016, 17-29, 19; Зиновьева, Е.С. Перспективные тенденции формирования международного режима по обеспечению информационной безопасности. № 4 (49) 2016, 235–247

[1443] Ibid., 23.

[1444] Ibid.

The Russian struggle to define international information security and sovereignty is also present in the texts of other cyber diplomats. In 2003 ex-KGB Colonel General Vladislav Sherstiuk[1445] wrote that the globalization of information society did not make the securing of national interests in the information sphere irrelevant. He distinguished the four directions of Russian information security policy as: ensuring citizens' rights to obtain and use information together with preserving moral values and patriotism; securing the information policy, i.e. public relations of the state which requires the regulation and control of mass media; developing domestic information technology; and protecting information and information systems.[1446] In 2009 Sherstiuk defined the Russian position on international information security as based on information security rather than cyber, security. Sherstiuk claimed that the military-political use of information-communication technology included the pursuit of political goals in the interstate struggle on tactical, operational, and strategic levels. This was something that the Western concept of cyber did not allegedly capture. In this context ICT became both the target and the weapon of war and this was the basis for the Russian argument for new international law to regulate its use.[1447]

Beginning from 2003 the Voennaia mysl' has published a string of articles by the 'military contingent' of the Russian cyber diplomacy corps. This group includes colonel S. A. Komov, Colonel I. H. Dylevskii, Major General S. V. Korotkov, Major General S. N. Rodionov, A. V. Fedorov, Colonel S. M. Boiko, V. O. Zapivakhin, A. N. Petrunin, and V. P. El'ias. These articles describe the Russian international norm-building efforts from 1998 onwards. The basic argument and narrative in the early 2000s was that Russia had alerted the world to the threat arising from the malevolent use of ICT, i.e. information weapons, which could affect international stability and security. Russia opposed the efforts of 'some countries' to prepare for information war and sought to approach information weapons as an arms control issue.[1448] The author collective argued that in the timeframe of 2007-2010 the most developed countries would achieve the capability to wage a large-scale war in the information sphere. This would be a civilizational conflict and Russia should protect itself through regional cooperation and by promoting international norms inhibiting the use of information weapons.[1449] They proposed, for example, a joint monitoring system and joint responses to threats in the SCO states' networks to deter geopolitical competitors.[1450] At the heart of the reasoning of the cyber diplomats was the technological superiority of the United States which threatened Russian sovereignty and the larger balance of

[1445] Sherstiuk has made an impressive career in national security. He was the Director of FAPSI from 1998-1999, the First Deputy Secretary of the Security Council of the Russian Federation from 1999-2004, and the Undersecretary of the Security Council from 2004-2010. He is the Director of the Institute of Information Security Problems at the MGU. (Шерстюк, Владислав Петрович. Wikipedia [Online] Available: https://ru.wikipedia.org/wiki/Шерстюк,_Владислав_Петрович [Accessed: 2nd April 2019].)

[1446] Шерстюк, В.П. Актуальные проблемы обеспечения информационной безопасности Российской Федерации. Военная мысль, № 6 2003, 28-32.

[1447] Комов 2009, 112-114

[1448] Комов, Коротков & Родионов 2003.

[1449] Дылевский И. Н., Комов С. А., Короткое СВ., Родионов С. Н., Федоров А. В. Военная политика Российской Федерации в области международной информационной безопасности: региональный аспект. Военная мысль № 2/2007, 32-40, 33.

[1450] Бойко et al. 2010.

power.[1451] The way Dylevskii et al. have used strategic weapons arms control as a basis for their discussion reveals the underlying understanding that international information security is a subject matter for sovereign states and great powers.[1452] By 2015 Dylevskii et al. were ready to admit that Russia had failed to obtain the cooperation of the West in regulating information weapons and recognizing state sovereignty in the information space.[1453] The last article by the military collective in the Voennaia mysl' was published in 2016 and its subject and tone had become defensive and dealt with the deterrence of military conflicts in the information era. Military diplomats argued that the United States' build-up of information weapons necessitated the Russian build-up of national information power (potentsial') to deter possible aggression and conserve the balance of power. [1454]

Sergei Boiko, the Head of the Department of the Security Council of the Russian Federation and a leading expert from the Centre of International Information Security and Science and Technology Policy of the MGIMO, wrote two articles in 2018 which were in effect a continuation of the articles of the cyber diplomats. According to him, Russian cyber diplomacy interests had not changed in 20 years—they still consisted of strategic stability and an equal strategic partnership. However, the conceptual approach had changed somewhat: each state had the sovereign right to independently decide state policy issues concerning the Internet and the right to protect its national segment of the global network including critical infrastructure. Additionally, the emphasis was now on ICT instead of 'information weapons'—the psychological aspects were toned down but still present. These principles would form the basis for Russia's renewed effort to push for a new round of the UN GGE process in 2019.[1455] Consequently, in 2018 Vladislav Sherstiuk used the term 'digital sovereignty' to denote states' sovereign right to manage ICT on their territory and to determine policies in the field of international information security. This sovereignty could be realised through the authentication of users, routing of traffic through designated points, and through virtual borders.[1456] In 2018"digital sovereignty' was finally presented as an official title of a round table discussion at the Russian international cyber security forum of 2018.[1457]

[1451] Дылевский И. Н., Комов С. А., Коротков, С.В., Родионов С. Н., Полякова, Т. А., Федоров А. В. К вопросу о международно-правовой квалификации информационных операций. Военная мысль № 2 2008, 2-10.

[1452] Дылевский et al. 2014.

[1453] Дылевский И. Н., Запивахин, В. О., Комов С. А., Петрунин, А. В., Эльяс, В. П. Военно-политические аспекты государственной политики Российской Федерации в области международной информационной безопасности. Военная мысль № 1 2015, 11-17.

[1454] Дылевский et al. 2016.

[1455] Бойко, Сергей. Формирование системы международной информационной безопасности: российские подходы и инициативы. Международная жизнь, № 5 (2018); Бойко, Сергей. Формирование системы международной информационной безопасности: российские подходы и инициативы. Международная жизнь, №11 (2018).

[1456] Шерстюк 2018.

[1457] Пядышева 2018. The arguments used by cyber diplomats provide one reason for why the Russians officially use the term information instead of cyber and why Russia has not established cyber force but instead information troops. The Russian international norm-building policies require abstaining from the public endorsement of cyber warfare. This is apparent in an interview of Andrei Krutskikh where he effortlessly uses the terms cyber potential, cyber structure, cyber war, cyberattack etc. but then transfers to using 'information' when describing Russian diplomatic efforts. (Крутских, Андрей. Кто владеет Интернетом, тот владеет миром. Международная жизнь, № 10 (2016).)

The Russian information warfare theorists have discussed 'information sovereignty' since the early 2000s. Manoilo referred to 'national segments of the information space' in the context of sovereignty and Manoilo et al. wrote about the control of information infrastructure as a necessary requirement for sovereignty. Griniaev argued that 'virtual state borders in cyberspace' were being erected by states and Panarin wrote about the 'spiritual sovereignty' of Russia.[1458] Nevertheless, although IT-expert Igor Ashmanov, Director of the company Ashmanov and Partners, may not have coined the term 'digital sovereignty' he is the first who has publicly provided a theoretical and systematic analysis of the concept.[1459]

Ashmanov gave a presentation titled 'Information sovereignty—The new reality' at the iForum conference in Kiev in May 2013.[1460] In it Ashmanov listed the 'traditional' forms of sovereignty—military, diplomatic, economic, political and cultural—and argued that a new 'digital sovereignty' had appeared. The traditional forms of sovereignty were eroding because of globalization and informatization, and the loss of digital sovereignty could lead to further loss of other forms of sovereignty. He defined 'digital sovereignty' as the right and possibility of the state to: 1) autonomously and independently determine both domestic and geopolitical national interests in the digital sphere; 2) pursue an independent internal and external information policy; 3) manage own information resources to form the infrastructure of the national information space; 4) guarantee the electronic and information security of the state. Digital sovereignty had two sides: electronic sovereignty and information sovereignty both defined by their resilience against attacks. This type of sovereignty required both electronic and information 'shields' which basically meant domestic programs, operating systems, network equipment, mobile systems, Internet infrastructure, media, social media services, search engines, and a national system for information warfare, and 'ideological services.' Ashmanov argued that a 'cold' information war was already ongoing, and that information dominance was analogous to the air dominance in the previous wars. The United States was the only truly 'digitally sovereign' state in the world—although China was catching up—and it used freedom of speech as a weapon to keep Russia from reaching 'digital sovereignty'. Ashmanov argued that it was impossible for a regional actor like Russia to attain full information sovereignty. Therefore, Russia had to form alliances with CIS countries and China and to build a shield consisting of a system for monitoring the information space, as well as legal regulation, and means of active counterinfluence.[1461]

If one compares Ashmanov's ideas to the ones that were present in the framework of CIS in the timeframe of 2008-2012 it becomes clear that Ashmanov just elaborated ideas that were already circulating amongst security and foreign policy elites of the post-Soviet countries.[1462] This has been argued also by Vladislav Bukharin, a senior

[1458] Манойло 2003, 282; Манойло, Петренко & Фролов 2012; Гриняев 2002; Панарин 2003, 2004 & 2006.

[1459] Макутина, Мария. Цифровой суверенитет. Газета.Ru 19 июня 2013 [Online]. Available: https://www.gazeta.ru/politics/2013/06/19_a_5387077.shtml [Accessed: 28th February 2019].

[1460] Яровая, Майя. Игорь Ашманов: "Сегодня информационное доминирование – это все равно, что господство в воздухе". Ain.ua 01 Мая, 2013 [Online]. Available: https://ain.ua/2013/05/01/igor-ashmanov-segodnya-informacionnoe-dominirovanie-eto-vse-ravno-chto-gospodstvo-v-vozduxe/ [Accessed: 28th February 2019]; Ашманов, Игорь. Информационный суверенитет – новая реальность. 24.04.2013. [Online]. Available: http://eurasian-defence.ru/sites/default/files/doc/ashmanov.pdf [Accessed: 28th February 2019].

[1461] Ibid.

[1462] Cf. Chapter 6.2.

lecturer at the Faculty of Public Administration, at the Department of International Organizations and Problems of Global Governance of Moscow State University. He has claimed that the main analyst of the company Infowatch, N. N. Fedotov, in fact came up with the term in 2010 and that the concept of 'digital' or 'information sovereignty' appeared early on in the Ukrainian and Belorussian official documents, as well as in Chinese documents in the form of 'Internet sovereignty'. Bukharin claimed that for Russia 'digital sovereignty' was more important than 'information sovereignty.' He defined the most important components of technically ensuring national security would be a domestic search engine, social networks, operating system and software, microelectronics, network equipment, a national segment of the Internet, payment systems, autonomous means of protection, cryptographic algorithms and protocols, and a navigation system.[1463] Therefore, Bukharin associated digital sovereignty with the domestic ownership of services and infrastructure and the quality of national information-technological development.

As Bukharin had claimed, the Russians were not the only ones thinking about information or digital sovereignty. In 2016 Russian and Belorussian civilian academics authored a book on information security in the context of CSTO and CIS and proposed multiple definitions for the concept of information sovereignty.[1464] Based on these it would seem that as the Russian and post-Soviet countries' legal experts began to investigate 'information sovereignty' four elements were deemed important: states' rights to determine their interests, to conduct policy, to dispose of resources or to affect the information infrastructure, and to be the (sole) provider of security in the national information/cyberspace.

Anatoli Strel'tsov and Pavel Piliugin[1465], both members of the Russian cyber diplomatic corps, wrote a series of articles on the Internet and sovereignty in 2016-2017. Strel'tsov claimed in 2016 that cyberspace lacked national borders because the network addressing of objects and subjects was unregulated and unconnected to national territories.[1466] Later, Pavel Piliugin and Strel'tsov wrote a joint paper "On the issue of digital sovereignty" in which they approached digital sovereignty through the concept of territorial state sovereignty.[1467] Based on this approach, the inviolability of state borders in cyberspace would be ensured through an international regime designating how borders are crossed. Consequently, Piliugin and Strel'tsov introduced the BGP protocol and its autonomous system of addresses as a tool to control traffic between nations. Furthermore, SDN technology is presented as a method to flexibly control cross-border traffic as the connections of the national ISPs can be shaped from defence lines into borders. Piliugin and Strel'tsov also claimed that anonymity and the

[1463] Бухарин, В.В. Компоненты цифрового суверенитета российской федерации как техническая основа информационной безопасности. Вестник МГИМО университета, № 6(51) 2016, 76-91, 88.

[1464] Вус, М.А., Макаров, О.С. Стратегический вектор обеспечения международной информационной безопасности. СПб.: СПИИРАН. Изд-во «Анатолия», 2016, 34, 47, 105.

[1465] Piliugin is an ex-KGB/FSB computer and cryptography specialist and a senior researcher at the Institute of Problems of Information Security of MGU. (МИЭТ. Педагогический состав: Пилюгин Павел Львович [Online]. Available: https://www.miet.ru/person/50077 [Accessed: 28th February 2019].)

[1466] Стрельцов, Анатолий. Применение международного гуманитарного права к вооруженным конфликтам в киберпространстве. 25.04.2016 [Online]. Available: https://digital.report/konflikt-v-kiber-prostranstve/# [Accessed: 28th February 2019].

[1467] Стрельцов А.А., Пилюгин П.Л. К вопросу о цифровом суверенитете. Информатизация и связь, № 2 2016, 25-30.

problem of attribution could be solved through software solutions, certificates and registers, although this would require national and international agreements.[1468]

In a paper published in 2017 Piliugin continued to propose different ways to understand 'digital borders' based on BGP and SDN technologies.[1469] Piliugin was aware of the high computational and other requirements generated by filtering traffic on a national scale, and thus he proposed a system where the subsystems of the control system would be placed in different parts of the network with less resource intensive systems at the borders and more intensive systems in the depths of the national network. Moreover, incoming traffic would be registered at the border and the subsystems would exchange information about established routes. This would enable national firewall control and the monitoring of traffic, and a centralized control of BGP routing. Strel'tsov wrote in 2017 about 'the segment of Internet' which denoted state sovereignty on the Internet. He argued that sovereignty required state control of borders and the information space itself.[1470] Together in 2018 Piliugin and Strel'tsov stated that the "demarcation" of digital borders could be based on a set of points of contact between digital spaces (autonomous systems) of different states. This would require international agreements which would regulate how and what traffic was routed and where.[1471] The Russian media began to use the term 'digital borders' around 2018, which is a clear indicator that the ideas about delineating the borders of the Russian segment of the Internet had started to spread.[1472]

'Digital sovereignty' has also been analysed from a legal point of view. The first to approach the issue seems to have been V. B. Naumov in 1999.[1473] He argued that the information space has changed international relations because it is a new environment like the sea and air were in their time. As states projected their interests to these new spaces a redefinition of sovereignty was required. Naumov also pointed out that the lack of international norms concerning 'the Internet' would lead to sovereign networks inside the global information space. According to Associate Professor A. A. Efremov, also Senior Researcher of the Centre for Public Administration Technologies at RANEPA, one of the first Russian political scientific definitions of 'information sovereignty' was presented by A. V. Rossoshanskii, Doctor of Law and a member of the Faculty of Law at the University of Saratov State University, in 2011 as the ability and intention to produce, distribute, and consume information and to use information resources based on political interests.[1474] In his 2012 article Ros-

[1468] Ibid.

[1469] Пилюгин П.Л. Проблемы определения границ в информационном пространстве. T-Comm: Телекоммуникации и транспорт. 2017. Том 11. №8, 37-44.

[1470] Стрельцов 2017.

[1471] Пилюгин П.Л., Стрельцов А.А. Проблемы Делимитации и Демаркации Цифровой Границы. XXIII научно-практическая конференция «Комплексная защита информации», 22-24 мая 2018 [Online]. Available: https://kzi.su/files/files/materials2018/13_Pilugin.pdf [Accessed: 28th February 2019].

[1472] Тишина, Юлия. Россия обозначит цифровые границы Власти защитят интернет-пользователей от иностранных силовиков. Коммерсантъ, №181 от 04.10.2018, 1 [Online]. Available: https://www.kommersant.ru/doc/3759627 [Accessed: 28th February 2019].

[1473] Наумов 1999.

[1474] Cited in Ефремов 2017, 209.

soshanskii, however, argued that 'information sovereignty' is a nationally and culturally bound concept so Western liberal notions of the freedom of information might not be applicable to Russia.[1475]

Eferemov also pointed to three articles written by V. S. Polikarpov, E. V. Polikarpova and V. A. Polikarpova in 2014 on 'information sovereignty'. They use Ashmanov's definition of 'digital sovereignty' to argue that the development of ICT and cyberspace have created a new virtual world where states struggle with each other to maintain their sovereignty. The context of this struggle is bound to the United States' failing power position and the rise of challengers.[1476] This connection of sovereignty to the international struggle is also made by others, such as M. M. Kucheriavyi who divided 'information sovereignty' into information-technological, information-psychological, and information-political components.[1477] Kycheriavyi proposes that to secure 'information sovereignty' Russia's information security should be based on, among other things, forming secure national information systems and creating Russia's own information troops, forces and means, and controlling information flows inside the country and those coming from outside.[1478]

Efremov has argued that the concept of information sovereignty was gaining popularity in Russia in 2016-2017 but its definitions were mainly based on threats. He has offered his own legalistic definition of it as "the ability of a state through national and international law to exercise the regulation of a specific information space."[1479] Efremov has also pointed out that 'information sovereignty' cannot be defined nationally because its relationships and technological basis are transnational. Moreover, he has argued that sovereignty cannot be defined based on technological and physical understandings of cyberspace—the information space is a sphere of human relations and activity.[1480] In 2017, Efremov narrowed his definition to 'the state sovereignty in cyberspace' (gosudartsvennyi suverenitet) and distinguished three aspects of sovereignty: state borders, the capability to exercise sovereignty, and the level/quality of sovereignty.[1481] Another legal expert, L. V. Terent'eva, an associate professor at the

[1475] Россошанский, А. В. Информационный суверенитет и свобода слова в контексте политической модернизации в современной России. Серия «Политология. Религиоведение» 2012. № 1 (8), 19–26.

[1476] Поликарпов В.С., Поликарпова, Е.В., Поликарпова, В.А. Информационный суверенитет России, сенсорная революция, социальные сети, интернет и кибервойна. Информационное противодействие угрозам терроризма, № 23 (2014), 272-278; Поликарпов В.С., Поликарпова, Е.В. Новейшие информационно-коммуникационные технологии и информационный суверенитет России. Информационное противодействие угрозам терроризма, № 23 (2014), 279-284; Поликарпов В.С., Поликарпова, Е.В. Проблема информационного суверенитета России. Информационное противодействие угрозам терроризма, № 23 (2014), 285-290.

[1477] Кучерявый, М.М. К осознанию информационного суверенитета в тенденциях глобального информационного пространства. Наука, новые технологии и инновации Кыргызстана № 12, 2015, 22-27; Кучерявый 2014.

[1478] Кучерявый 2015, 24-25.

[1479] Ефремов, А. А. Проблемы реализации государственного суверенитета в информационной сфере. Вестник УрФО № 2(20) / 2016, 54–60, 56.

[1480] Ефремов, А. А. Предложения для включения в проект Рекомендаций Парламентских слушаний «О совершенствовании федерального законодательства по обеспечению информационной безопасности при использовании информационно-коммуникационных технологий для оказания государственных услуг и осуществления межведомственного электронного документооборота» 28.06.2010 [Online]. Available: http://www.ifap.ru/pr/2010/n100622a.pdf [Accessed: 1st May 2019].

[1481] Ефремов 2017.

Moscow State Law University,[1482] argued that the idea of 'information sovereignty' conforms to the traditional Russian view on sovereignty with different horizontal spheres (economic, political etc.) and on the supremacy of the state throughout its territory. She proposed a definition for 'digital sovereignty' which is understood as "The right and the possibility of a national government to autonomously and independently determine both internal and geopolitical national interests in the digital sphere. As well as the state's right to pursue an independent internal and external information policy, to dispose of their own information resources to govern the, and to guarantee the electronic and information security of the state."[1483]

The idea of digital sovereignty is deeply rooted in the concept of information security. However, according to A. A. Paroshin (in 2010) only the Information Security Doctrine of 2000 explicitly mentions information security as the state of protection of Russia's national interests in the information sphere. Nevertheless, multiple documents have linked state security to information technology or the information space—mainly because of threats emanating from technology.[1484] Furthermore, international agreements and foreign policy documents of Russia include their own definitions (cf. Chapter 6). Russia has also pursued joint standards and common normative bases for information security in the framework of CIS and CSTO.[1485] M. A. Vus and O. S. Makarov claim that the Russian definition of information security instead of cyber security has been accepted into the CIS and CSTO lexicon.[1486] Many of the information warfare theorists analysed above have offered their views on or concepts of information security. They are mostly based on the state of protection of the object of security—usually state interests or the information systems and information upholding those interests—or on the measures for securing something. Threats are usually derived from the object of security.[1487]

The authors of the admittedly propagandistic Informatsionnye voiny journal have been very interested in the concept of information security.[1488] They have pointed out

[1482] Терентьева, Л.В. Концепция суверенитета государства в условиях глобализационных и информационно-коммуникационных процессов. Право. Журнал Высшей школы экономики. 2017. № 1, 187–200, 196.

[1483] This is similar to Ashmanov's definition but Terent'eva refers to Поликарпов & Поликарпова 2014.

[1484] Парошин, А. А. Информационная безопасность: стандартизированные термины и понятия. Владивосток: Дальневосточный федеральный университет (ДФУ), 2010.

[1485] Вус & Макаров 2016.

[1486] Ibid., 23. The concept of security must be distinguished from 'information support' (informatsionnoe obespechenie), which is related to public relations and communication, to reputation and image management and to the monitoring of the public opinion. (Петрунин, А. Н. Информационное обеспечение как способ реализации государственной информационной политики в области обороны. Военная мысль, № 8 (2008), 36-44.)

[1487] Стрельцов 2008; Садовничий & Стрельцов 2002; Ноговицын 2009; Тучков Ю.Н. и др. Словарь терминов и определений в области информационной безопасности. 1-е изд Москва: ВАГШ ВС РФ, НИЦ информационной безопасности, 2008; Бачило, И.Л. Информационное право. Учебник 3-е издание. М.: Издательство Юрайт, 2013. The Russian understanding of the concept of security has been analysed, among others, by professor A. S. Malin who distinguishes two versions: "in the broad sense, it is the result of social activities to ensure the security of the individuals, society and the state from external threats, while in the narrow sense it is the state of protection of the vital interests of the individual, society and the state from internal threats." Малин, А.С. Содержание понятия безопасность. вестник академии военных наук, № 4(21) 2007.

[1488] The journal is published by the Academy of Information Self-Defence, an independent organization established in 2007 and sponsored by the Center of Security Studies of the Russian Academy of Sciences and the Academy of Military Sciences. It is connected to such academics as S. P. Rastorguev and V. V. Tsyganov and publishes the journal Information Wars (Informatsionnye voiny) (Иванов 2014).

three important aspects of information security in the Russian understanding. Firstly, that it is an object of a geopolitical and civilizational struggle in the context of globalization. Secondly, that the state must have control over the Internet to win in this struggle. And thirdly, that although spirit, moral and cognition are the target of the information struggle, an information-technological basis is still required for information security and thus sovereignty.[1489]

The concept of cyber security did not manage to break through into the Russian official lexicon, although, in 2013 Professor Iurii Borodakii, an academician of the RAS and a life-long developer of military ASUs in the FGUP Sistemprom, as well as Aleksandr Dobrodeev and Igor' Butysov stated in an article published in a journal connected to the FSB, MoD and FSTEK that cyberspace had become a new environment of interstate confrontation.[1490] They defined cyberspace as a technological environment and cyber security in a philosophical sense as "a property or state of a system to preserve the reliability and functional stability in the context of a modern information confrontation [informatsionnoe protivoborstvo]."[1491] The article was published and the journal was established in a moment when Russia seemed to be on the verge of adopting the concept of cyber security—this moment did not materialise as the draft Cyber Security Strategy floundered and the Russian regime adopted the more inclusive concept of information security.[1492] The tides are, however, turning yet again as 'cyber security' has from 2018 been increasingly used by academicians and even Putin himself.[1493]

The narrative about information threats, security and sovereignty has not been shared by all Russians. There exists an active and critical opposition to the security and military elite's ideas in Russian civil society. The arguments of civil society are mainly based on human rights and the resistance to state control, whereas ICT companies and liberal economists point out that 'digital sovereignty' is bad for the economy.[1494]

[1489] Сергеев 2010; Володенков, С.В. Технологии интернет-коммуникации как фактор обеспечения информационной безопасности современного государства. Информационные войны, № 3(19) 2011, 89-95; Мельников, В.П. Информационная война и современные оружейные технологии. Информационные войны, №3 (43) 2017, 28-35; Лепский В.Е., Мельников А.А., Пойкин А.Е. Информационные войны за доминирование в инновационной сфере россии и на евразийском пространстве. Информационные войны, № 4(36) 2015, 12-20.

[1490] In 2013 a company named Echelon began to publish a journal called 'Voprosy kiberbezopasnosti' (Cybersecurity Issues). What is significant in this journal is that Echelon is accredited as a testing laboratory for the MoD of Russia, FSTEC and the FSB and also functions as a certification centre for the MoD and FSTEC (АО «НПО «Эшелон» [Online]. Available: https://npo-echelon.ru/ [Accessed: 2nd April 2019].)

[1491] Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности xx! века (часть 1). Вопросы кибербезопасности, № 1 (1) 2013, 2-9, 5-6.

[1492] Cf. Chapter 6.

[1493] Шеремет, И.А. Обеспечение кибербезопасности в условиях развития цифровой экономики. Вестник Московского университета. Серия 25. Международные отношения и мировая политика. Т. 11. № 1 (2019), 3-19; Латухина, Кира. Защита цифры Президент призвал вместе бороться с киберугрозой. Российская газета, 8.7.2018 [Online]. Available: https://rg.ru/2018/07/08/putin-nazval-borbu-s-kiberatakami-gosudarstvennoj-zadachej.html [Accessed: 3rd January 2019].

[1494] Агора 2018; Кодачигов, Валерий. Закон Яровой пока не работает: Для его выполнения операторам не хватает документации. Ведомости, 01 октября 2018 [Online]. Available: https://www.vedomosti.ru /technology/articles/2018/10/01/782493-zakon-yarovoi#galleries%2F140737489014365%2Fnormal%2F1 [Accessed: 1st March 2019]; Баленко, Евгения, Галимова, Наталья, Посыпкина, Александра, Балашова, Анна.. Атака изнутри: операторы протестируют закон об устойчивости Рунета. РБК, 8 февраля 2019 [Online]. Available: https://www.rbc.ru/technology_and_media/08/02/2019/5c5c51069a7947bef4503927?from=center_16 [Accessed: 1st March 2019].

Moreover, the 'Sinicization' of the national segment is seen by some as a negative phenomenon.[1495]

State sovereignty is a defining and central element of the Russian political culture and it shows in the national security documents. The 2008 Foreign Policy Concept mentions information threats to sovereignty.[1496] The NSS of 2009 connects sovereignty to national security, and ensuring this security to the spiritual resilience and access to modern information-communication technology.[1497] The Military Doctrine of 2010 acknowledges the need to develop information-technological means to protect the independence and sovereignty of Russia.[1498] The Foreign Policy Concept of 2013 recognises the danger that 'soft power' and information threats pose to sovereignty.[1499] The Military Doctrine of 2014 refers to the use of information and communication technology for military-political ends and against the sovereignty of the state. It defines as military dangers activities conducted to harm the information infrastructure, to destabilize the political situation, and to influence the spiritual values of the people, and emphasises the need to build a system of information security. The Doctrine suggest that the information space is a sphere of military action.[1500] The NSS of 2015 mentions information-technological threats to critical information infrastructure, the threats emanating from the use of telecommunications technology for propaganda purposes, as well as the threats of terrorist or criminal use of information technology. It also points to the vulnerabilities of information infrastructure that could affect economic growth, which is a strategic objective, and the destructive use of information-psychological means against the cultural sovereignty of Russia.[1501] The Foreign Policy Concept of 2016 repeated the points of the NSS, emphasised the respect for sovereignty and mentioned the equitable access to the Internet.[1502] 'Sovereignty in the information space' (suverenitet v informatsionnom prostranstve) was officially mentioned in the 2016 Information Security Doctrine where the task to ensure "the protection of the sovereignty of the Russian Federation in the information space was considered as the main direction of information security and a national interest.[1503] Furthermore, the term 'digital sovereignty' was first used in the 2017 State programme 'The Digital Economy of the Russian Federation'.[1504] The state would protect this sovereignty by conducting autonomous and independent politics to realize its national goals in the information space.[1505]

To summarize. Digital and information sovereignty are parallel concepts although with distinct substances. The idea of information and later digital sovereignty devel-

[1495] Роскомсвобода. «Китаизация» Рунета входит в активную фазу и начнётся с точек обмена трафиком, 18-8-2017 [Online]. Available: https://roskomsvoboda.org/31224/ [Accessed: 1st May 2019]; Роскомсвобода. Цифровая оборона интернета [Online]. Available: https://roskomsvoboda.org/45308/ [Accessed: 1st March 2019].

[1496] Концепция 2008.

[1497] Указ Президента Российской Федерации 2009b.

[1498] Указ Президента РФ 2010.

[1499] Концепция 2013.

[1500] Доктрина 2014.

[1501] Указ Президента РФ 2015.

[1502] Указ Президента РФ 2016a.

[1503] Указ Президента РФ 2016b.

[1504] Распоряжение Правительства РФ 2017.

[1505] Указ Президента РФ 2016b.

oped along two different tracks. The first was external and was based on the understanding that information weapons and operations posed a new kind of threat to the security of the state. The threat was especially acute because the Russian defence and security elites considered Russia to be significantly weaker than its great power rivals in developing and utilizing these weapons. Thus, Russia launched its cyber diplomacy effort in 1997-1998 to contain and regulate this threat. The idea of non-state control of any space was alien to Russian security thinking, and therefore cyberspace and its different elements needed to be controlled. The concept of information sovereignty developed from the state's right to an absence of threat and then to a state's right to control its ICT and thus to the delineation of cyberspace along the lines of state jurisdiction. This version of information sovereignty was probably based on the ideas of those retired and servicing security and military professionals and academicians who took part in the drafting to the first Information Security Doctrine.

The second track of information security is internal and based on the writings of Russian information security and warfare scholars at the turn of the millennium. It naturally draws also from the ideas of territorial state sovereignty, juridical concepts and geopolitics which had wider support amongst the Russian intelligentsia at that time. This information sovereignty is based on the idea that the state has the right and responsibility to control information, creation and use, as well as its flow and substance, inside its borders—like the resources of any other dimension. Additionally, it seems plausible that the Russians were also influenced by the thinking of their counterparts from ex-Soviet countries. Whatever the case, by 2010-2013 the idea was developed to such an extent that it was adopted by the elites, although haltingly. This so-called internal information sovereignty, like the diplomatic version, is based on threats which have changed as time has passed from devastating attacks against the information infrastructure, cyber terrorism, information-psychological operations, and data security to military-political, subversive, terrorist, and criminal operations. These attacks had from the start technological and psychological aspects and, consequently, so did the information sovereignty. Its elements were shaped around the state protection and control of information, as well as the information infrastructure and services, the state's ability to promote domestic information technology research and production, and the ability to protect and cultivate the values, culture and civilization of Russia. As the importance of information technology increased, and society changed, information sovereignty acquired the sub-concepts of electronic, technological and digital sovereignties. This development connected sovereignty to national power as the quality of the information infrastructure and technological-scientific development became sources of power or potential.

The different definitions of information sovereignty proposed by the writers analysed above can be grouped into three categories. The first are the technocratic definitions that are based on the information infrastructure and systems residing in the territory of a state. The second are the judicial definitions, which are based on the regulation of human or societal relationships. The third are political definitions which flow from a certain understanding of state interests and security. The last has been perhaps the most common and includes such elements as the right and ability to determine interests, to conduct internal and external policies, to use national information resources, and to guarantee the security of the national information space. Many of the definitions analysed here follow the supposed Russian legal tradition, which considers sovereignty to be manifested in different spheres but flowing from one source.

Based on the above it can be argued that digital sovereignty developed from sovereignty over the information space to sovereignty in the information space and in the end to information or digital sovereignty, that is, to one of the aspects of state sovereignty. This is based on the interaction of the Russian understanding of territorial state sovereignty and the emergence of cyberspace. Therefore, the idea of inserting sovereignty into cyberspace and the delineation of borders has been quite easy to understand and adopt. The idea of digital and information sovereignty is very much connected to the balance of power thinking. Russia cannot be sovereign if some other state has 'more' sovereignty. Moreover, it resonates with the traditional security and foreign policy thinking and ideas about sovereignty, strategic stability, and great power (derzhavnost'). From the Russian perspective 'digital sovereignty' can then be understood as the extension of the authority and control of a territorial state over and into the national segment of the Internet, which consists of Internet and other network-related ICT systems located on its territory or under its jurisdiction. A wider concept is thus 'information sovereignty' which additionally includes the information residing or flowing through those ICT systems and the interaction of its users.

These definitions demonstrate why it is imperative to control the space and borders of national information space and the national segment of the Internet. The cultural and political aspects of sovereignty also legitimize Russian state actions outside the borders of its information space. Although there might be a dose of Soviet nostalgia mixed into the dream of creating an independent, domestic ICT industry, digital sovereignty has military strategic relevance as it creates a platform for the national information economy which is a national source of power. In the world of ideas, digital sovereignty gathers all the other strategic cultural ideas under its wings.

5.6 Unified information space

The idea of a unified information space (EIP) carried over from the Soviet times into the 1990s and ultimately into the 2010s. This continuity has been noted, among others, by Professor Nikolai Il'in, the Deputy Head of the Special Communications Service (Spetssviazi) of the FSO.[1506] According to him, the first era of the information systems of governmental control was the Soviet era with its central planning systems. During that time some complexes of crisis management situation centres were created. The second era consisted of the years between 1991-2000, which were characterized by the localization of systems. The FAPSI created local centres to collect social-economic data, the construction of national information-telecommunications system began, and federal- and presidential-administration-level situation centres were created. The third and current era is characterized by centralized systems. Il'in describes this complex as a 'state control system' based on geographically distributed management systems at the federal and regional levels and on the unique information

[1506] Ильин Н.И. Эволюция информационных систем государственного управления. Информационные войны №1 (41) 2017, 54-57.

and analytical systems for strategic planning, assessment, and analysis of national security.[1507]

The idea of EIP was established among the defence and security elites as the Armed Forces adopted the Concept of Unified Information Space of the Armed Forces in 2004.[1508] According to A.V. Pankov and S. V. Shevchenko, the EIP of the Armed Forces was defined as "a collection of databases and data banks, technologies of their management and use, information and telecommunication systems, and networks operating on the same principles and general rules to ensure the information based interaction and the exchange of information of the military administration."[1509] Colonel and Professor G. A. Lavrinov and Major A. A. Chumichkin, both members of the Academy of Military Sciences, defined EIP as "in a broad sense […] a specially ordered set of all the information available in the Armed Forces of the Russian Federation, and narrowly as an aggregate of information resources of the RF Armed Forces, organized according to uniform principles and rules of formation, formalization, storage, distribution."[1510] The EIP was, thus, a space with borders, common rules, processes and systems, and standardized information.

Although, the idea of EIP was shared, the discussion of how it should be implemented was not. In 2003 V. V. Baraniuk, a leading researcher at 27th TsNII and the Chief Researcher of the Information Technology Department of TsNII EISU[1511] wrote that the armed forces required a unified information space (edinnoe informatsionnoe prostranstvo) for effective command and control.[1512]. Baraniuk claimed that the information space of the Armed Forces was currently not unified, and he argued for integrating different networks and resources. He divided the definition of EIP into broad and narrow versions which corresponded to Lavrinov's and Chumichkin's definition.[1513] This kind of information space would increase the efficiency (operativnost'), validity, and quality of decisions by providing up-to-date, reliable, timely, and comprehensive information. Baraniuk proposed that the EIP should be constructed based on a model of the Armed Forces command and control system, which consisted of subsystems and information flows, and structural, functional and information components.[1514] Later, Baraniuk together with the Head of the Centre of Information Resources of TsNII EISU I. N. Akhmadishin proposed the creation of the 'Information Service of the Armed Forces' to solve the problems the increased amounts of information and new technology were posing for the command and control system of the

[1507] Ibid., 57.

[1508] Копытко, В. К., Шептура, Владимир. Проблемы построения единого информационного пространства Вооруженных Сил Российской Федерации и возможные пути их решения. Военная мысль, № 10 (2011), 16-26.

[1509] Панков, А. В., Шевченко, С. В. Обоснование роли и формирование концептуальной модели системы интеллектуальной обработки информации в едином информационном пространстве ВС РФ. Известия СПбГЭТУ «ЛЭТИ» № 1/2018, 38-43.

[1510] Лаврино, Г.А., Чумичкин, А.А. Опыт создания единого информационного пространства для решения задач технического оснащения Вооруженных Сил Российской Федерации. Вестник академии военных наук, № 1(26)/2009.

[1511] Рамм, Алексей. На острие экономики и автоматизации Уникальному научно-исследовательскому институту экономики, информатики и систем управления исполняется 45 лет. ВПК, № 19 (537) за 28 мая 2014 года.

[1512] Баранюк, В. В. Единое информационное пространство вс рф: проблемы создания. Военная мысль № 3 (2003), 36-38.

[1513] Ibid., 36.

[1514] Ibid.

Armed Forces.[1515] They argued for a centralized and hierarchical system which would have been extended to the military-industrial complex and all the relevant ministries.[1516]

In 2004 Colonel General E. A. Karpov, Lieutenant General N. I. Burenin and Colonel N. A. Ziuzin argued that information superiority in modern warfare, where troops were spatially distributed and their management was decentralized, required 'a unified military information space' (edinoe voennoe informatsionnoe prostranstvo) to ensure the accuracy and timeliness of information.[1517] According to Karpov, Burenin and Ziuzin, the continuity of EIP could be achieved through multiple redundant communication channels, integration of local and regional and services, and branch networks. Its infrastructure would consist of interconnected computer networks, databases, application programs and subscriber devices, interfaces of weapons and security systems.[1518] This system would be based on sharing information to all participants, it would be 'transparent', and it would be flexible and able to change configuration if the military situation so demanded. What the authors had in mind was similar to the U.S. Defense Information Systems Network (DISN), and they were ready to admit that the Russian Armed forces had nothing like it.[1519] Similarly, ten years later retired General-Lieutenant S. I. Skokov and Senior Lieutenant L. V. Grushka argued that the United States' Global Information Grid gave it technological superiority as it enhanced administration and enabled a constant and flexible modification of their defence network.[1520]

On the civilian side, in 2005 D. Chereskin, G. Smolian and V. Tsygichko argued that Russia had to build a sovereign information and communications infrastructure to ensure the security of the country and its development. To this effect, they presented a National Strategy for Information Development developed by the Institute for System Analysis of the RAS.[1521] According to the strategy, the networks of the ministries and departments should be integrated into a single vertical network supported by a system of distributed databases and a system for identifying and analysing threats. Moreover, Russia needed a single, multi-level, all-Russian information security system. These efforts, and others, would create a unified information space for the country, would ensure Russia's equal participation in the global information society, and guarantee its economic-social development.[1522]

[1515] Ахмадишин, И. Н., Баранюк, В. В. Организационные вопросы создания информационной службы ВС РФ. Военная мысль № 4 (2004), 45-49.

[1516] Ibid., 46.

[1517] Карпов, Е. А., Буренин, Н. И. Зюзин, Н. А. Единое военное информационное пространство: проблемы создания. Военная мысль № 8 (2004), 45.

[1518] Ibid., 47.

[1519] Ibid., 49.

[1520] Скоков, С. И., Грушка, Л. В. Влияние концепции сетецентризма на эволюцию и функционирование системы управления Вооруженными Силами Российской Федерации. Военная мысль, № 12 (2014), 33-41.

[1521] The Institute for System Analysis (FITs IU RAN) is a federal theoretical and applied sciences research institution established in 1976 in the field of informatics, cybernetics, mathematical modelling etc. It is specialized in studying technological, economic and ecological complex systems. In 2014 it was incorporated with two other institutes into the organization of the Federal Research Centre 'Informatics and management' of the RAS. (Институт системного анализа ФИЦ ИУ РАН [Online]. Available: http://www.isa.ru/ index.php [Accessed: 3rd April 2019].)

[1522] Черешкин, Д. С., Смолян, Г. Л., Цыгичко, В. Н. Информационное развитие России – путь к информационному обществу. «Информационные ресурсы России» №1, 2005 [Online]. Available:

The military reform and rearmament programme and the Russian government's renewed efforts to develop the information society and economy around 2008 coincided with a fresh interest in the idea of the EIP. In military journals the concept was used to analyse Western networks despite the fact that Western scholars had not used the term when discussing Western networks.[1523] In the context of Russian military networks, the Chief of the General Staff Iuri Baluevskii argued in 2009 that the Armed Forces were on the threshold of creating a single information space for the Armed Forces.[1524] This view was contested by the Chief of Communication of the Russian Armed forces Evgenii Maichik who claimed that the Russian military still had a long way to go.[1525] The drive to create unified information and telecommunications systems also affected other ministries and forces.[1526] The EIP was also connected to Russian foreign policy as S. M. Boiko et al. proposed that the SCO required a joint monitoring mechanism of communication networks which should include national subsystems interconnected by a special information and telecommunications network with a shared monitoring centre.[1527] The idea of the EIP was also present when M. A. Gareev argued for a unified system of aerospace defence for the country to defend against aerospace attacks in 2007.[1528] Unified systems were also incorporated into the slowly developing common air defence system of the CIS which should have connected the air defence and surveillance assets of Russia and its neighbours to a unified system.[1529] Lastly, the ESU TZ or 'the unified system of command and control of the tactical level' had been under development from the year 2000.[1530] Quite obviously the military saw the EIP as an inherent part of the future armed forces and an element of a network-centric warfare capable force.

The scientists at the 27th TsNII were not the only ones to make a pitch for unified information systems. In 2008 E. A. Perov and A.V. Pereverzev from the 16th

http://www.aselibrary.ru/press_center/journal/irr/2005/number_1/number_1_2/digital_resources515273747787/ [Accessed: 4th March 2019].

[1523] Cf. Молитвин, А. О реализации концепции единого информационного пространства НАТО. Зарубежное военное обозрение, № 1 (2008), 23-27; Азов, В. Концепция создания единой информационно-управляющей структуры ВС США. Зарубежное военное обозрение, № 1 (2003), 3-10; 4. The authoritative texts by Rona, Waltz, Arquilla, Ronfeldt, Libicki, Alberts, Gartzka, Cebrwoski, Smith et al. do not use the term 'unified information space'. Nevertheless, in 2005 the U.S. Joint Chief of Staff published the Net-Centric Operational Environment Joint Integrating Concept, for which Grishkovets, for example, has translated 'network-centric environment' as единое информационное пространство (edinnoe informatsionnoe prostranstvo). (The United States Department of Defence Joint Chiefs of Staff. Net-Centric Operational Environment Joint Integrating Concept, 31 October 2005 [Online]. Available: https://dodcio. defense.gov/Portals/0/Documents/netcentric_jic.pdf [Accessed: 3rd March 2019]; Гришковец, Е. Формирование в США единой информационной инфраструктуры вооруженных сил. Зарубежное военное обозрение, № 3 (2018), 19-2).

[1524] Кедров, Илья. АСУ для оружия будущего. ВПК, № 36 (152) за 20 сентября 2006 года.

[1525] Мейчик, Евгений. На пути к единому телекоммуникационному пространству. Россииское военное обозрение, № 9 (2009), 17-18.

[1526] Мирошников, Алексей. Войска переходят на "цифру". Независимое военное обозрение, № 39 (2009).

[1527] Бойко et al. 2010.

[1528] Гареев 2007.

[1529] Plopsky, Guy. Russia's Big Plans for Air Defense in Eurasia Big plans, indeed, but will they materialize? The Diplomat, April 07, 2017 [Online]. Available: https://thediplomat.com/2017/04/russias-big-plans-for-air-defense-in-eurasia/ [Accessed: 4th March 2019]; Тезиков, Андрей, Моренков, Владислав. АСУ ОС ПВО СНГ: сегодня и завтра. Журнал «Воздушно-космическая оборона» 17 августа, 2014 [Online]. Available: http://www.vko.ru/oruzhie/asu-os-pvo-sng-segodnya-i-zavtra [Accessed: 27th June 2016].

[1530] Старых, Геннадий. ЕСУ ТЗ: время делать следующий шаг. Независимое военное обозрение, 24 февраль 2012.

TsNIII[1531] argued that the communication system of the Russian Armed Forces should be developed into an Integrated Automated Digital Communication System (ob"edinennaia avtomatizirovannaia tsifrovaia sistema sviazi) (OATsSS). OATsSS was defined as "a communication system that is an organizational-technical combination of interconnected, technologically joined, advanced automated communication systems of different command and control levels (while maintaining their chain of command). It would be established by integrating the digital resources of the primary and secondary networks of the participants, and by using modern telecommunications technologies and protocols to format and transfer messages in a digital form."[1532] Perov and Pereverzev claimed that similar system had been attempted during the 1980s with poor results, but now new technology enabled the creation of a system based on a single digital form of messages and uniform algorithms which could be integrated in the common telecommunications space of Russia through standardizes interfaces. OATsSS could be introduced in phases so that the Armed Forces analogical systems could be replaced, and the networks could be connected to the 'Unified network of electronic communications of Russia' in a controlled way.[1533] It should be noted that the concept or at least the acronym OATsSS was, in fact, adopted and is under construction.[1534]

Another concept that has been implemented was proposed by retired Major General V. F. Samokhin, Colonel V. N. Luk'ianchik and Major A. N. Artiushenko from the Military Signal Communications Academy in 2011 who argued that Russian should build 'a military Internet.' It was to be built on the basis of inter-service and interdepartmental communication networks, which were to be digitalized and integrated into a single information space of the RF Armed Forces. This network would be closed, restricted, and technologically autonomous with native DNS and routing services and meant for day-to-day administration in the peacetime and for operational use in wartime. Administratively this network should be based on the organization of military districts. The static backbone network and services were to be complemented by field communications and air and space assets which would enable warfighting based on NCW principles. It would also connect the military to other force structures and agencies.[1535] The 'military Internet' was claimed to be operational in 2016.[1536]

The drive to integrate and unify networks accelerated in the 2010s. The military continued to see the unified information space and NCW as connected and if the Russian Armed Forces were to be reformed based on the principles of NCW, then a unified

[1531] The 16th TsNIII was established in 1923, combined with the 27th TsNII in 2010 and in 2014 again established as a separate institution. It is a research and testing institute for the Armed Forces communication systems and equipment and cooperates with the other institutes of the MoD and the military-industrial complex. (Жужома, Валерий Михайлович. 16 ЦНИИИ МО РФ: история и современность. Связь в Вооруженных Силах Российской Федерации – 2018. Москва: Информационный мост, 2018, 68-70 [Online]. Available: https://army.informost.ru/2018/pdf/29.pdf [Accessed: 4th March 2019].)

[1532] Перов, Е. А., Переверзев, А. В. О перспективной цифровой системе связи Вооруженных Сил Российской Федерации. Военная мысль, № 3 (2008), 7-11, 8.

[1533] Ibid.

[1534] Cf. Chapter 6.

[1535] Самохин, В. Ф., Лукьянчик, В. Н., Артюшенко, А. Н. Перспективы создания военного (боевого) интернета в рамках нового облика ВС РФ. Военная мысль, № 8 (2011), 57-64.

[1536] Зыков, Владимир, Рамм, Алексей. В России появился военный интернет. Закрытый сегмент передачи данных позволяет подразделениям Минобороны безопасно обмениваться секретной информацией. Известия, 19 октября 2016 [Online]. Available: https://iz.ru/news/639221 [Accessed: 18th April 2019].

information space was also required.[1537] According to General Gerasimov, the main directions of communication systems development were the wide use of advanced information telecommunications technologies and the creation of geographically distributed information banks, and the transition from a hierarchical stovepiped control of troops and weapons to a form of distributed network-centric control.[1538] Many Russian proponents of NCW considered the EIP to be a critical component of the concept but were cognizant of the difficulty of integrating the multiple, non-compatible, pipelined, legacy networks of the Russian Armed Forces.[1539]

The basics of the EIP concept were still being discussed in the late 2010s. Major General E. B. Khachenko, Colonel V. G. Ivanov and Professor V. N. Luk'ianchik from the Military Signal Communications Academy (St. Petersburg) wrote in 2018 that the EIP of the Armed Forces required a multi-level territorially distributed or zonal communication system covering the entire territory of the Russian Federation capable to ensure the continuous exchange and processing of information between command posts of all levels.[1540] The networks and systems of Russian abroad-deployed forces should become separate fragments of such a system. The system would have land-, sea-, air-, and space-based echelons of communications systems with static, reserve, field, and mobile components.[1541] The interesting point here is that the EIP is extended outside the territorial borders of the Russian federation and that it was envisioned to be divided into separate zones.

The integrating characteristics of the EIP became more pronounced as the Russian environment changed. It was proposed in the context of the military reform that an the EIP could connect all the authorities responsible for the procurement of weapons, the users of the weapon systems, research institutions, and the OPK.[1542] Moreover, a vertical and horizontal national security command structure should be created based on shared information networks and the ASUs of all power ministries and security agencies to respond to new military and non-military threats.[1543] Consequently, the military required an all-encompassing, automated command and control system. It would consist of a decision-making support system, an information-communication system and a system to acquire and store information.[1544] In 2018 Colonel V. A. Skiba

[1537] Гареева 2014; Герасимов 2018; Харченко, Е. Б. Проблемы безопасности инфокоммуникационных систем Вооруженных Сил Российской Федерации. Военная мысль, № 11 (2014), 14-19).

[1538] Герасимов, Валерий Васильевич. Приоритеты развития системы вооружения Вооруженных Сил Российской Федерации. Федеральный справочник. Оборонно-промышленный комплекс России, Том № 10, 2014, 117-120 [Online]. Available: http://federalbook.ru/files/OPK/Soderjanie/OPK-10/III/ Gerasimov.pdf [Accessed: 5th March 2019].

[1539] Воробьев & Киселев 2011; Дульнев, Ковалев & Ильин 2011; Чаднов, А. П. Роль военных сетевых технологий Вооруженных Сил Российской Федерации при создании и боевом применении высокотехнологичных систем вооружения, военной и специальной техники нового поколения. Военная мысль, № 7 (2018), 33-39, 34; Копытко & Шептура 2011; Шептура, Владимир. Единое информационное пространство ВС РФ. Защита и безопасность, № 2 (2016), 32-34; Панков & Шевченко 2018; Лаврино & Чумичкин 2009.

[1540] Харченко, Е. Б., Иванов, В. Г., Лукьянчик, В. Н. Научно-теоретические положения по построению технической основы системы управления Вооруженными Силами Российской Федерации. Военная мысль, № 8 (2018), 46-53.

[1541] Ibid.

[1542] Лаврино & Чумичкин 2009.

[1543] Чекинов & Богданов 2015a.

[1544] Выговский, И. И., Давыдов, А. Е. Направления совершенствования организации автоматизированного управления в военной сфере. Военная мысль, № 9 (2017), 37-42.

provided a technological concept for these ideas. It was a national command and control system for all military and non-military forces (a unified, interconnected system of military and state administration (EUSAPU)) which would be based on leased civilian networks, military networks (OATsSS), cloud services, data centres, SDN technology, VPNs and virtualized solutions. SDN technology could be used to ensure the combat resilience of the services provided by the networks and data centres.[1545]

Similarly to Skiba, a group of Russian scientists from federal ICT corporations offered a clear tribute to Soviet cybernetists in 2017 when they proposed to create a nationwide decision support system of automated management systems of complex organizational and technical objects for cosmonautics, nuclear energy, ecology, logistics, military applications, etc. These systems offer prognoses and optimal solutions.[1546] As I. V. Professor Solov'ev and Associate Professor C. M. Zlobin of the Military Academy of the General Staff argued in 2018, the rise of new centres of power and the intensified competition between them required better information cooperation between the elements of the military organization of the state.[1547] Against this background it is not surprising that a group of scholars from the 4th TsNII[1548] of the MoD proposed that to counter information-psychological and technological actions exploiting the vulnerabilities of information-telecommunications and information systems in the context of 'hybrid war', a system to monitor and prevent attacks must be built to protect Russian sovereignty.[1549] The EIP was thus transforming from an information sharing network to the 'information security system' envisioned by the Russian information warfare theorists.

As the military reform initiated in 2009 by the Defence Minister Anatoli Serdiukov progressed, the new command structure required new command, control, and communications solutions.[1550] The forces of different branches and services were subordinated directly under the command of the military districts and joint strategic commands (OSK).[1551] Moreover, the reorganization of territorial defence and its 'whole-of-government' approach required new ways to share information and to command forces under different agencies.[1552] These needs were recognized by Major General Major P. N. Kriazhev, a professor at the Military Training and Research Centre of the Ground Forces, who wrote in 2011 that automated control systems must be interconnected both vertically (at the strategic, operational-strategic, operational, and

[1545] Скиба, В. А. Синтез информационно-коммуникационного пространства эргатических систем военного назначения. Военная мысль, № 11 (2018), 39-48, 41.

[1546] Автамонов П.Н., Немыкин С.А., Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. Методологические и методические основы разработки и внедрения интегрированных систем поддержки принятия решений (СППР) в АСУ объектами военно-государственного управления. Информационные войны №1 (41) 2017, 39-48.

[1547] Соловьев, И. В., Злобин, С. М. Политика межведомственного взаимодействия - важнейшее направление решения задач обороны государства. Военная мысль № 7 (2018), 15-20.

[1548] The 4th TsNII is one of the largest scientific institutions of the MoD and conducts research in the area of strategic nuclear weapons and missiles. (Mil.ru. 4-й Центральный научно-исследовательский институт Министерства обороны Российской Федерации [Online]. Available: http://ens.mil.ru/science/SRI/ infrmation.htm?id=10807%40morfOrgScience [Accessed: 4th April 2019].)

[1549] Антонов et al. 2018.

[1550] Giles, Keir. A New Phase in Russian Military Transformation, The Journal of Slavic Military Studies, Vol. 27 No.1 (2014), 147-162.

[1551] Кряжев, П. Н. Развитие военно-административной территориальной структуры Вооруженных Сил Российской Федерации. Военная мысль № 11 (2011), 30-42.

[1552] Ibid.; Кардаш 2014; Кардаш 2018.

tactical level) and horizontally (at the inter-service, and interdepartmental level) and that they should enable the mutual exchange of information between all military and security authorities. Moreover, they should enable a smooth transition from peacetime management to wartime operational command and control in any conditions.[1553] Four years later General Gerasimov demanded that the network described by Kriazhev should be constructed, and that it should enable centralized and unbroken command and control as far as the operational-tactical level, and be able to function under difficult conditions and enemy influence.[1554] Some even argued that the electromagnetic sphere should be taken under centralized and vertical control.[1555]

The uses envisioned for the EIP transcended purely military-operational issues. The EIP was to be a platform upon which a complex of systems for automated collection, processing and modification of information would be built to help manage the military-industrial complex by connecting different ministries, agencies and companies.[1556] This could, for example, be a 'unified information space for the military-technological policies of the MoD' (EIP VTP RF) which would enable more efficient management of state weapons procurement programmes.[1557] Some argued that special purpose networks of the military and security services should be physically and logically separated from the common telecommunications networks.[1558] The principles of open communication networks were not acceptable for managing special networks and therefore a centralized ASU of these networks was required.[1559] These ideas have found purchase as a closed management network of the OPK is being built.[1560]

The establishment of the National Defence Management Centre (NDMC) in 2014 was a reflection of the above-mentioned ideas. It is meant to be a command centre for the Security Council, the General Staff and other federal organs in all situations and phases of conflict. According to A. P. Shabanov, a leading researcher at the Institute of the Problems of Informatics at RAN, the NDMC enables a nation-wide system of information-analytics ,which in its turn supports the management of many

[1553] Кряжев 2011, 40. Cf. also Хомутов, А. В. Опыт и перспективы использования концепции единой информационно-коммуникационной сети в управлении войсками. Военная мысль № 11 (2015), 17-22; Раскин, А.В. Некоторые подходы по созданию единого информационно-управляющего пространства разнородных группировок войск (СИЛ). Информационные войны № 4(40) 2016, 2-5.

[1554] Герасимов 2015, 12.

[1555] Горбачев, Юрий. Борьба в электронном пространстве усиливается. Независимое военное обозрение, № 3 (2015).

[1556] Боков, С.И., Воронков, О.В, Чупринов, А.А. Основные принципы методологии формирования единой информационно-поисковой и аналитической системы управления развитием вооружения, военной и специальной техники. Вооружение и экономика 3 (36) / 2016 г, 54-58.

[1557] Боков, С. И., Желтухин, П. С., Пьянков, А. А. Основные подходы к созданию единого информационного пространства военно-технической политики Российской Федерации. Военная мысль, № 4 (2018), 5-12.

[1558] Харченко, Е.Б., Сазыкин, А.М., Лысенков, Ю.Н. Вопросы кибербезопасности инфокоммуникационных систем специального назначения. Известия Российской Академии Ракетных и Артиллерийских Наук 97 (2017), 38-47; Независимая газета. Российские системы связи остаются уязвимыми. Независимая газета, 07 августа 2013 [Online]. Available: http://www.ng.ru/editorial/2013-08-07/2_red.html [Accessed: 6th March 2019].

[1559] Макаренко, С. И. Перспективы и проблемные вопросы развития сетей связи специального назначения. Системы управления, связи и безопасности №2. 2017, 18-68.

[1560] Зыков, Владимир, Рамм, Алексей. У оборонных предприятий появится свой интернет. По защищенной сети будет передаваться засекреченная техническая документация. Известия, 31 октября 2016 [Online]. Available: https://iz.ru/news/641528 [Accessed: 18th April 2019].

other spheres of life than just the national defence.[1561] The ideas behind the establishment of the NDMC have also guided the construction of centralized and integrated aerospace defence and early-warning radar and satellite networks.[1562] It would seem that despite the construction of the NDMC, the creation of the EIP for the Armed Forces has advanced slowly and ineffectually. Moreover, the national EIP is being independently constructed by different government agencies. Therefore, Lieutenant General A. Ia Cherysh and Colonel V. V. Popov have proposed the construction of an EIP based on the NDMC which would integrate all the different networks, standards, and technologies of the power ministries.[1563]

The EIP is not exclusively a military concept, reserved for the military or offered only as a solution to military or security problems. The EIP has been extensively deployed to define information networks, abstract or real, that unify subjects and objects of information and services and is a virtual reality of social relationships.[1564] The EIP could have been a hierarchical administrative system of databases to collect information for the management of the society.[1565] More modestly and concretely, it was to be a national public electronic system of documentation and services—similar to the electronic government concepts formulated in other parts of the world in the early 2000s.[1566] To summarize, already in 2004 Professors S. V. Konovchenko and A. G. Kiselev could argue that the concept of a 'unified information space' was being used from multiple perspectives: geopolitical, information-noonspherical, social-information, and social relations.[1567]

Practical solutions for the EIP were proposed also on the civilian side, for example by the Federal Information and Management Research Centre of the RAS (FITs IU RAN).[1568] In 2015 A. A. Zatsarinnyi and E. V. Kiselev published a series of articles

[1561] Шабанов, А.П. Технология информационной поддержки аналитических структур ситуационных центров государственных организаций. Информационные войны № 1(41) 2017, 33-38; Герасимов, В.В. Опыт стратегического руководства в Великой Отечественной войне и организация единого управления обороной страны в современных условиях. Вестник Академии военных наук, 2(51) 2015, 5-15.

[1562] Miasnikov, Eugene. The air-space threat to Russia. In Arbatov, Alexei and Dvorkin, Vladimir (Eds.) Missile Defense: Confrontation and Cooperation. Moscow: Carnegie Moscow Center, 2013, 121-146; Чельцов, Борис. Вспомнив тернистый путь, подумаем о будущем. ВПК, № 13 (329) за 7 апреля 2010 года; Соколов, Анатолий. Новый космический щит России. Русская Планета, 18 ноября 2015 [Online]. Available: http://rusplt.ru/society/novyiy-kosmicheskiy-schit-rossii-19771.html [Accessed: 5th March 2019]; Майбуров, Д. Г., Иконников, О. В. Развитие теоретических положений информационного обеспечения управления отражением ударов средств воздушно-космического нападения противника. Военная мысль № 9 (2018), 48-53.

[1563] Черныш, А. Я., Попов, В. В. Эволюции теории и практики единого информационного пространства и первоочередных мерах по его развитию в интересах повышения эффективности управления национальной обороной Российской Федерации. Военная мысль № 9 (2019), 47-54.

[1564] Пителинский, К.В. Интернет: Единое информационное пространство, экономический инструмент, виртуальная реальность и учебный процесс. Межотраслевая информационная служба. 2006. № 3, 63-71.

[1565] Коровкин С.Д. Единое информационное пространство органов государственной власти. Компетентность. 2007. № 2 (43), 26-37.

[1566] Ицкович, Б.С. Формируя единое информационное пространствою Железнодорожный транспорт. 2011. № 5., 60-61; Симушков, А.М. Единое информационное пространство в транспортной логистикею Железнодорожный транспорт. 2009. № 10, 46-47.

[1567] Коновченко С.В., Киселев А.Г. Информационная политика в России. Монография. М., РАГС, 2004.

[1568] The Federal Information and Management Research Centre of the RAS (FITs IU RAN) was created in 2014 by combining five institutes doing theoretical and applied research in the field of informatics. Its research about the creation of the EIP of the Russian Federation which they called 'a mega system'. The mega system consisted of multiple systems of coordination, control and management which would be used to support strategic planning, centralization of scientific-technological development, and monitoring of national security. Technologically, Zatsarinnyi's and Kiselev's system would been based on federal and regional data centres that would exchange information in a protected environment outside the Internet and would access the Internet through one controlled gateway. Information exchange would be conducted through the already existing System of Electronic Interagency Cooperation (CMEV)—or federal governmental intranet—and there would be monitored and protected gateways between open, confidential, and secret (closed) resources.[1569] In fact, what Zatsarinnyi and Kiselev were describing in theory was being already built (cf. Chapter 6).

The ideas connected to the EIP were also carried over to the cyber and information-technological security issues. By 2011 the Russians were just as worried about the vulnerabilities of critical infrastructure as the rest of the world.[1570] For example, A. V. Kortokov and E. S. Zinob'eva argued that because critical infrastructure is the key to public order, economic stability and national security of states, the protection of critical infrastructure falls within the competence of the state.[1571] They argued that the information infrastructure should be included in the Russian definition of critical infrastructure and objects.[1572] In 2015 the FSB declared that it would create a National Coordination Centre for Computer Incidents (NKTsKI) which was described as a unified, centralized, geographically distributed complex to respond to computer incidents.[1573] Russia also adopted laws concerning the CII in 2017 (cf. Chapter 6). Consequently, A. A. Sidak, for example, proposed that a segmented and layered information security system should be built. The layers consisted of perimeter protection, data network protection, server protection, protection of automated workstations, protection of application services, and data protection. The segments and layers should form a national system of CII protection.[1574]

The parallel or applied concept of the EIP, 'the national segment of the Internet' (natsional'nyi segment Interneta), appeared in academic and journalistic sources long

covers, for example, information-telecommunication networks, big data and artificial intelligence. (Федеральный исследовательский центр «Информатика и управление» Российской Академии Наук (ФИЦ ИУ РАН) [Online]. Available: http://www.frccsc.ru/ [Accessed: 3rd April 2019]).

[1569] Зацаринный, А. А., Кисилев, Э. В. Некоторые подходы к формированию нормативно-технической базы единого информационного пространства России в части информационных ресурсов. Информатика и управление, Том 25 № 1 (2015), 155-167; Зацаринный, А. А., Кисилев, Э. В. Некоторые подходы к формированию нормативно-технической базы в части требований к архитектурному построению информационных систем организаций - участников единого информационного пространства России. Информатика и управление, Том 25 № 3 (2015), 161-178; Зацаринный, А. А., Кисилев, Э. В. Некоторые подходы к формированию обобщенной архитектуры информационных систем организаций - участников единого информационного пространства России. Информатика и управление, Том 25 № 4 (2015), 114-127.

[1570] Pynnöniemi 2012.

[1571] Коротков А.В., Зиновьева Е.С. Безопасность критических информационных инфраструктур в международном гуманитарном праве. Вестник МГИМО-университета, №4(19) 2011, 154-162.

[1572] Ibid., 157.

[1573] ВПК. Кибербезопасность страны – дело всенародное. ВПК, № 11 (577) за 25 марта 2015 года.

[1574] Сидак, А.А. Вопросы структуризации автоматизированных систем при организации защиты информации. Информационные войны №1 (45) 2018, 88-90; Сидак, А.А. Применение метода анализа иерархии при определении критических процессов для категорирования объектов критической информационной инфраструктуры Российской Федерации. Информационные войны №2 (46) 2018, 79-82.

before it was introduced officially (cf. below). Even on the official side it appeared first outside of Russia. For example, the Model Law on the Basics of Internet Regulation adopted by the Inter-Parliamentary Assembly of the CIS used the concept of a national segment of the Internet in 2011 and defined it based on DNS country code top-level domains.[1575] The concept of the national segment was used in Belorussia in 2010 when the President gave an edict (ukaz) titled, 'On Measures to Improve the Use of the National Segment of the Internet'. It defined this segment as "a set of information networks, systems and resources connected to the Internet, located on the territory of the Republic of Belarus and (or) using the hierarchical names of the national segment of the Internet."[1576] The roots of the Russian use of the concept of the national segment seem to reside in the idea that the Internet can be divided based on language, technology (primarily DNS ccTLDs), and governance.[1577] In the unofficial Russian use, the concept of the national segment seems to have originally referred to the governance of the country code top-level domains of the DNS system and of the IP -address blocks.[1578] Possibly because of the technological framing of the issue, the concept of the national segment does not really appear in the Russian military journals. Nevertheless, the military was familiar with the concept of the national segment of the Internet at least from 2009 onwards.[1579]

The concept of the national segment of the Internet is connected to the emergence of the RuNet concept, or the Russian Internet. There is no agreed definition of RuNet.[1580] Neither is there a definite point of time when RuNet appeared. For example, in 2003 Iu. Iu. Perfilev proposed to define it either as the collection of telecommunications networks in Russia, the collection of all information resources related to the domain zones of .ru and .su, or the collection of all Russian language information resources.[1581] Nevertheless, it was given a semi-official status as RuNet and awards were given in 2004. The 'RuNet award', i.e. 'a national award for the contribution to the development of the Russian segment of the Internet' is an annual award for the best initiatives, applications, and companies issued by the Federal Agency of Press

[1575] СНГ. Модельный закон «Об основах регулирования Интернета» Межпарламентская Ассамблея государств – участников Содружества Независимых Государств, Приложение к постановлению МПА СНГ от 16.05.2011 г. № 36-9 [Online]. Available: http://www.cikrf.ru/international/docs/mpa_modzakon. html [Accessed: 3rd April 2019].

[1576] Указ Президента РБ № 60 от 01.02.2010 "О мерах по совершенствованию использования национального сегмента сети Интернет" [Online]. Available: https://belzakon.net/Законодательство/ Указ_Президента_РБ/2010/3321/скачать [Accessed: 2nd April 2019].

[1577] Горошко, Е.И. Современные Интернет-коммуникации: структура и основные характеристики. М.: Наука, Флинта, 2012. [Online]. Available: http://www.textology.ru/article.aspx?aId=232 [Accessed: 7th March 2019].

[1578] Белов, Сергей. Интернет по-русски. Российская газета, 10.11.2009 [Online]. Available: https://rg.ru/2009/11/10/rf.html [Accessed: 7th March 2019]; Рузин, Андрей. Интернет: Россия у критической черты, CNews.ru 08.04.2004 [Online]. Available: http://www.cnews.ru/articles/internet_ rossiya_u_kriticheskoj_cherty [Accessed: 7th March 2019]; Lenta.ru. Зона.ru вошла в десятку самых активных национальных сегментов интернета. Lenta.ru, 31 марта 2004 [Online]. Available: https://lenta.ru/news/2004/03/31/domen/ [Accessed: 7th March 2019]; Info.nic.ru. Система доменных имен. Российский сегмент. Технические подробности, 11.4.2005 [Online]. Available: https://info.nic.ru/st/11/out_954.shtml [Accessed: 3rd April 2019].

[1579] Самохин, Лукьянчик & Артюшенко 2011; Голышко А. В., Князев К. Г. NGN: Российский сегмент. Электросвязь, № 12 2009.

[1580] Wikipedia. Рунет (термин) [Online]. Available: https://ru.wikipedia.org/wiki/ Рунет_(термин) [Accessed: 7th March 2019].

[1581] Перфильев 2003.

and Mass Communication (Rospechat).[1582] As Ristolainen and Kukkola have argued, 'RuNet' represents the 'sociocultural basis' for 'the Russian segment of the Internet'.[1583] According Ristolainen, RuNet refers to a relatively closed, online environment that is based on the Russian language but includes also a social aspect—a Russian way of doing things.[1584] RuNet has also been defined by Gorny as "a totality of information, communications and activities which occur on the Internet, mostly in the Russian language, no matter where the resources and users are physically located, and which are somehow linked to Russian culture and Russian cultural identity."[1585] RuNet forms a 'RuNet community' that provides a sense of belonging to its members through the use of common Russian language social media, news and search engine services, most of which are Russian in origin.[1586] According to Andrei Soldatov, since 2012 RuNet has become a more political and also securitized space as the Russian state has sought to control it through legislation and censorship.[1587]

The 'unified information space' did not appear in the 2004 Ivanov Doctrine but it was implicitly mentioned in the 2009 NSS which stated that information security threats would be prevented by creating a unified information-telecommunications support system for the needs of national security.[1588] Concomitantly, Associate Professor Nikolai Sergeev of the RARAN claimed that the 2009 NSS ordered the creation of a national, hierarchical, distributed and specialized system or 'information management system' (informatsionno-upravliaiuchshaia sistema) which consisted of 'information-analytical centres' (informatsionno-analiticheskie tsentry) to counter information threats and especially Western 'network-centric warfare'. This vertical system should be supported by a horizontal one which connects government organizations to society's structures.[1589] The Military Doctrine of 2010 mentions 'a unified information field of the Armed Forces and other military forces' which would be created and would form a part of the information space of the Russian Federation. It also mentions 'information management' or 'command and control' systems which would be integrated with the automated command and control systems, weapon systems, and military command systems of all levels.[1590] The 2014 Military Doctrine was as sparse on the EIP as the previous ones had been. It noted that the Armed Forces had to improve its unified information space as part of the information space of the Russian Federation.[1591] The 2015 NSS used the term 'single' or 'unified' (edinyi) much more freely. It identified a single or unified transportation space, cultural space, system for emergency situations, and system for preventing crimes. It did not use the terms 'EIP' or the 'national segment of the Internet'.[1592] The Information Security Doctrine of 2016 introduced the concept of 'the national segment of the Internet' by

[1582] РИА Новости. История развития Рунета. Справка, 30 сентября 2009 [Online]. Available: https://ria.ru/20090930/186873799.html [Accessed: 7th March 2019].

[1583] Ristolainen, Mari and Kukkola, Juha. Closed, safe and secure – the Russian sense of information security. In Benson & McAlaney 2019, 53-71.

[1584] Ristolainen 2017a & 2017b.

[1585] Gorny, Eugene. A Creative History of the Russian Internet. Studies in Internet Creativity., Berlin: DVM Verlag Dr. Muller, 2009, 27.

[1586] Vendil Pallin 2017; Ristolainen 2017a & 2017b; Ristolainen & Kukkola 2019a.

[1587] Soldatov 2017b.

[1588] Указ Президента Российской Федерации 2009b.

[1589] Sergeev 2010.

[1590] Указ Президента РФ 2010.

[1591] Доктрина 2014.

[1592] Указ Президента РФ 2015.

stating that, "The main directions of ensuring information security in the field of strategic stability and equal strategic partnership are: [...] the development of a national system for managing the Russian segment of the Internet."[1593] The Doctrine did not use the concept of the EIP. It only referred to the 'unified network of electronic communications of the Russian Federation' the resilience and uninterrupted functioning of which should be ensured in peacetime, in times of threat and during the times of war. Although this is a clear reference to a legal concept it is also related to the concept of the information infrastructure of the Russian Federation, which is defined to reside on the territory and/or under the jurisdiction of Russia.[1594] The foreign policy documents did not really touch upon the subject of the EIP more than has been already discussed in the context of the interstate struggle and digital sovereignty, and it was already noted that the concept of the national segment of the Internet was used in CIS documents.

To summarize. The idea of a unified information space has two aspects: civilian and military. The civilian aspect has been analysed here less extensively than the military one, but it can be argued that they both share the same characteristics of vertical control and horizontal integration, centralization, and delimitation of borders. The EIP is not merely a space but a system of integrated and standardized communication networks and data resources, a system of security and management, and a system of operational, political, social and/or economic control and management. The reference point of the EIP of the Armed Forces was consistently the Western or more precisely the doctrinal and technological development of the United States. In some cases, the EIP is simply understood as a shared information space or a network in the context of NCW. However, it should be noted that the Russian understanding of the EIP differs somewhat from the American one because it is connected to the idea of territorial and total defence. It encompasses all forces (military and other), national leadership, economy, and society. It is geographically bound. It is not originally based on a globally projected military network meant for expeditionary operations—although that was envisioned as an end-state. Thus, it might be understood as a vertically and horizontally integrated system of systems enabling total situation awareness and control over the Armed Forces and the state. The EIP as a concept is also a tool for forcing the 'power vertical' onto cyberspace as the separated networks of different ministries and agencies are collected under one management system. Consequently, it can be argued that the EIP, with its multiple variations between different academic communities, is based on both the Soviet era idea of EIP and on the analysis and adaptation of Western, mainly American theory and practice of NCW.

Nevertheless, the EIP, in its civilian or military versions, is not some mystic all-encompassing concept. On the most basic level, the EIP is a common information network shared by users. For many of the military journalists it is just a catchword which points to an information network that provides total situation awareness and control to commanders or top administrators. Furthermore, many texts use the EIP as a synonym for WAN or corporate networks that are mostly based on international standards and technologies and there is nothing particularly Russian about them. Still, many in the military have used the EIP to conceptualize an operational, organizational, and

[1593] Указ Президента РФ 2016b.

[1594] Федеральный закон 2003.

technological system of unified information resources and ASUs which should be operational from peacetime to wartime and be organized around the Armed Forces command structure. The OATsSS is a one proof that these ideas have been put into practise.

Although they are connected concepts in many ways, RuNet and the EIP should not be confused. The EIP refers to a defined space which becomes delineated and controlled through state power whereas RuNet is a socio-cultural phenomenon which has arisen from below and through the spontaneous interaction of individuals, communities and commercial interests. The official transformation of 'the unified information space' to 'the national segment of the Internet' around the time of the drafting of the 2016 Information Security Doctrine is indicative of the how the information space was brought into more direct contact with state sovereignty and national security interests. There was a clear interaction with the elites and the epistemic communities as the EIP was debated during the 2000s and 2010s and some ideas were eventually put into action. Various institutes and individual scholars offered their views on the subject, and it can be argued that these views were usually more grandiose than the ones presented in the official strategic level documents or what really materialized.

5.7 Information superiority

Information superiority was a central concept in the Russian understanding of the information struggle and war already in the early 2000s. The Russians quite intensely followed the Western doctrinal debates about IW and borrowed concepts from it.[1595] Consequently, an information security specialist Sergei Griniaev could argue in the early 2000s that information superiority is the ability to collect, process and distribute a continuous stream of information about the situation, and to prevent an adversary from doing the same. It can also be defined as the ability to designate and maintain a pace of operations that surpasses any opponent's possible pace, thus allowing the protagonist to dominate, remain unpredictable, and act ahead of the opponent throughout the duration of the confrontation. This is based on a real understanding of the situation.[1596] Grinaev, among others, was basically introducing Western ideas to the Russian speaking audience.[1597] However, as was already noted above, information warfare had distinct technological and psychological aspects for Russians and so information superiority also had two aspects. Here I will concentrate on the technological part.[1598]

[1595] Стародубцев, Ю. И., Бухарин, В. В., Семенов, С. С. Техносферная война. Военная мысль, № 7 (2012), 22-31; Шеремет, Игорь. Компьютеризация как путь к победе в вооруженной борьбе. Концепция "сетецентричной войны" и особенности ее практической реализации. Независимое военное обозрение» №43 (2005); Печуров, С.Л. Англо-саксонская модель военной реформы: история и современность. М.: Издательство Московского университета, 2015; Попов, Игорь. Сете-центрическая война Пентагона. Независимое Военное Обозрение, № 9 (2004).

[1596] Гриняев, Сергей. Война в четвертой сфере. Превосходство в киберпространстве будет определять победу в конфликтах XXI века. Независимое военное обозрение N 42 (215) 10.11.2000; Гриняев 2004, 101.

[1597] Гриняев 2004; Донсков, Ю. Е., Фомин, В. В. Информационное превосходство: пути реализации в операциях. Военная мысль, № 11 (2003), 57-61.

[1598] Some Russian commentators conflated 'netwars' to 'network-centric warfare' and thus the social and psychological aspects are sometimes difficult to separate from the technological aspects. Джерелиевский, Борис. Сетевые войны. ВПК, № 45 (112) за 30 ноября 2005 года; Медведко, Леонид. Под эгидой Соединенных Штатов. ВПК, № 10 (226) за 12 марта 2008 года; Грачева, Татьяна. Наставники плохих парней – На

In addition to Griniaev, Fedorova and Tsygichko have claimed that information superiority based on the capability to acquire more information, to process it faster, and to make more efficiently decisions, will decide future wars.[1599] Panarin has claimed that states fight in the unified global information space for information superiority.[1600] Manoilo et al. defined information superiority as the ability to collect, process and distribute an uninterrupted information flow of the situation, while at the same time denying the same from the enemy and doing it faster than the enemy.[1601] Vorob'ev and Kiselev argued that the enemy could be destroyed without weapons through information superiority and Nogovitsyn claimed that victory in modern war without information superiority was impossible.[1602] Moreover, Gorbunov and Bogdanov argued that information superiority had to be acquired already in peacetime.[1603] Generals Karpov, Burenin and Ziuzin understood information superiority as the ability to obtain more truthful and accurate data on the situation than the adversary and to obtain it faster and, moreover, the ability to utilize this advantage in commanding forces.[1604] These views hardly differ from their Western versions.

Information superiority was connected to informatization which was defined, for example, as an organised process of "collecting, transmitting, processing, storing, and using information in order to create and use information resources to increase the effectiveness of the Armed Forces and meet the information needs of the military officials."[1605] Informatization was accompanied by the concept of digitalization, which meant updating analogue communication systems and ASUs with modern technology.[1606] In this context, the feeling that Russia was lagging further and further behind the United States was prevalent.[1607] It was also understood that superiority was not only about technology but also required doctrinal and organizational changes in the hierarchical and commander-centred traditions of the Russian Armed Forces.[1608] Nevertheless, domestic or "Russian" solutions were proposed from the start—as were reinterpreted Western concepts.[1609] In 2005, for example, retired Major General Igor Sheremet, a professor, member of RAN and member of the Military Industrial Com-

политическую войну Пентагон рекрутирует отщепенцев и предателей. ВПК, № 46 (612) за 2 декабря 2015 года.

[1599] Федорова & Цигичко 2001.

[1600] Панарин 2003.

[1601] Manoilo 2003.

[1602] Воробьев & Киселев 2006; Ноговицын 2009a & 2009b.

[1603] Горбунов & Богданов 2009.

[1604] Карпов, Буренин & Зюзин 2004.

[1605] Иванов, А.А. Информатизация вооруженных сил. Информатизация Вооруженных Сил: проблемы и пути их решения. Военная мысль, № 2 (2000).

[1606] Петров, Алексей, Ианин, Алексей, Карпачев, Сергей. Спасение – в цифре! Цифровизация – основной фронт мировой конкуренции. ВПК, № 31 (695) за 16 августа 2017 года; Акулинчев, А. Б. Проблемы цифровизации военных сетей связи и пути их решения. Военная мысль, № 9 (2006), 76-80; Самохин, Лукьянчик & Артюшенко 2011; Перов, Е. А., Переверзев, А. В. Проблемы цифровизации военных сетей связи и пути их решения. Военная мысль, № 9 (2006), 76-80.

[1607] Ibid. Долгополов, А. В., Богданов, С. А. Эволюция форм и способов ведения вооруженной борьбы в сетецентрических условиях. Военная мысль, № 2 (2011), 49-58; Первов, А.В. Сетецентрическая война в воздушно-космическом пространстве: миф или реальность. Вестник Академии военных наук, № 2 (31) 2010, 80-83.

[1608] Ibid. Кондратьев, Александр. Новые возможности для нового облика. ВПК, № 45 (311) за 18 ноября 2009 года.

[1609] An example of the latter Cf. Казарьян, Б. И. Операции, боевые действия, сетецентричная война. Военная мысль, № 2 (2010), 25-37.

mission under the Government of the Russian Federation and the Board of the Military Industrial Complex of Russia, proposed that Russia should adopt the concept of NCW as a system of mean and anti-means and should not concentrate on separate technologies of networking, sensors etc.[1610] The early Russian theorists were also very aware of the fact that the concept of command and control of the NCW did not follow traditional hierarchical, vertical models with tight, unbroken control of the commander over his subordinates.[1611] M. M. Khamzatov, for example, argued implicitly that the self-synchronization of units did not mean self-control but the ability to share capabilities to achieve the objectives ordered from above in tight cooperation with all the other TVD forces.[1612]

In the early 2000s electronic warfare specialists argued that EW combined with computer attacks, disinformation, and kinetic strikes would provide information superiority in the initial phase of war. Thus, the role of information systems and networks built already in peacetime was decisive. Air defence specialists argued for the integration of all air defence assets, sensors, network and weapon platforms, to achieve information superiority through improved speed, more comprehensive information, and secrecy. However, most specialists were at least a little sceptical of such "American ideas."[1613] The debates about the role of various services, branches and troops in relation to information superiority, NCW and IW in general among the military should be understood in the context of the military reform and competition for resources. The concept of NCW was officially adopted as a guideline in the so-called Serdiukov reforms in 2008.[1614]

One of the foremost Russian military theorists of NCW is Professor Aleksandr Kondratev of the Academy of Military Sciences. Kondratev has extensively studied the Western concept of the NCW and its implementation and argued that the development of information technology had led from a platform-centric to a network-centric form of warfare which offered synergistic effects.[1615] Kondratev disputed the claim that the system of NCW had anything to do with the Soviet concepts of RUK and ROK—they were instruments of non-contact war. Russia had to comprehensively overhaul its doctrines, organizations and military-industrial complex if it wanted to

[1610] Шеремет 2005.

[1611] Ibid.; Попов 2004; Горбачев, Ю. Е. Сетецентрическая война: миф или реальность? Военная мысль, № 1 (2006), 66-76; Хамзатов, М. М. Влияние концепции сетецентрической войны на характер современных операций. Военная мысль, № 7 (2006), 13-17; Раскин, А. В., Пеляк, В. С. Сетецентрическая война - война информационной цивилизации. Военная мысль, № 4 (2008), 78-80; Буренок, Василий. Базис сетецентрических войн – опережение, интеллект, инновации... Независимое военное обозрение, № 12 (2010).

[1612] Хамзатов 2006, 15-16.

[1613] Донсков & Фомин 2003; Донсков & Никитин 2005; Горбачев 2004; Горбачев 2006; Фролов, Николай. Главный ТВД будущего. ВПК, № 48 (214) за 12 декабря 2007 года; Чельцов, Б. Ф. Уточнение подходов к созданию системы воздушно-космической обороны государства в условиях сетецентричных войн будущего. Военная мысль, № 9 (2008), 2-10; Чельцов, Б. Ф. Проблемы создания сетецентрической системы управления войсками, силами и средствами ВКО. Вестник Академии военных наук, № 4 (37) 2011, 56-63.

[1614] Макаренко, С.И., Бережнов, А.Н. Перспективы использования сетецентрических технологий управления боевыми действиями и проблемы их внедрения в вооруженных силах Российской Федерации. Вестник Академии военных наук, № 4 (37) 2011, 64-68; Kjellén, Jonas. Russian Electronic Warfare: Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces. FOI, 2018 [Online]. Available: https://www.foi.se/rest-api/report/FOI-R--4625--SE [Accessed: 9th March 2019]; Esin, Viktor. Russia's air-space force and armaments program. In Arbatov & Dvorkin 2013, 147-166.

[1615] Кондратьев 2009.

achieve the benefits of NCW. [1616] Kondratev's views were challenged by Colonel V. I. Vypasniak from the 27th TsNII of MoD who saw a direct connection between the NCW and RUK/ROK and he argued for vertically and centrally controlled systems.[1617] Somewhat similarly, retired Major General V. F. Samokhin, Colonel V. N. Luk'ianchik and Major A. N. Artiushenko claimed in 2011 that the basic military-administrative unit of the Russian AF was the military district and NCW should be applied on this basis. The Russian EIP should connect the territorial nodes of command and control though digitalized systems.[1618] Nevertheless, as an article by retired Lieutenant-Colonels V. A. Knizhitskii and V. E: Zav'ialov and Lieutenant-Colonel S. M. Savarenkov showed, new 'universal' ideas of command and control penetrated Russian military thought.[1619] The authors basically introduced the U.S./NATO Guidelines for Operations as a more flexible and reactive 'algorithm of command and control' without referring any Western sources.[1620]

In 2010 Vasii Burenok argued that information superiority was not about the amount of information but instead about the achievement of a deeper awareness and understanding of the situation, a more accurate understanding of the advantages and disadvantages of the enemy. It was also the ability to form a plan based on this awareness, to immediately communicate decisions to subordinates, and to monitor and control their implementation.[1621] Basically, Burenok transformed the concept of NCW to correspond to the Russian understanding of command and control and updated it with the results of earlier Western self-criticism. Thus, he criticised those Russian views that saw automatization and technology as the essence of a network-centric war and over-emphasised the meaning of time. For Burenok the human component, i.e. the professionalism of subordinate commanders was a critical factor.[1622] This importance of the human, social and psychological aspects was shared by others.[1623]

Iurii Borodakii, a lecturer at the Military Academy of the General Staff and a member of the Scientific Council of the Security Council of RF also attempted to combine Russian theories of command and control and Western ideas of NCW.[1624] According

[1616] Ibid., 96.

[1617] Выпасняк, В. И. О реализации сетецентрических принципов управления силами и средствами вооруженной борьбы в операциях (боевых действиях). Военная мысль, № 12 (2009), 23-30, 27.

[1618] Самохин, Лукьянчик & Артюшенко 2011.

[1619] Кижицкий, В. А., Завьялов, В. Е., Саваренков, С. М. Об уточнении содержания терминов "организация" и "управление" в терминологической системе теории военного управления. Военная мысль, № 10 (2014), 59-64.

[1620] North Atlantic Treaty Organization (NATO). An Introduction to Operations Planning at the Operational Level - A summary of the Allied command operations comprehensive operations planning directive, 4 Oct 13 [Online]. Available: http://www.act.nato.int/images/stories/events/2016/sfpdpe/copd_v20_summary.pdf [Accessed: 10th March 2019].

[1621] Буренок 2010.

[1622] Ibid.

[1623] Попов, Игорь. Сетецентрическая война. Красная звезда, № 169 (2012); Зиновьев В.Н., Колдунов А.И., Груздев Н.В. Перспективы применения информационных сетей в военном деле. Информационные войны, №1 (33) 2015, 37-40, 40.

[1624] Бородакий, Ю.В. Информатизация вооруженных сил. Развитие методологических основ построения информационно-управляющих систем военного назначения. Военная мысль, № 6 (2009), 33-41; Бородакий Ю. В., Боговик А. В., Курносов В. И., Лободинский Ю. В., Масановец В. В., Паращук И. Б. Основы теории управления в системах специального назначения. М.: Управление делами Президента Российской Федерации, 2008.

to him and others[1625] 'the Russian version of OODA-loop' consisted of monitoring, analysing, forecasting the situation, making decision, commanding forces, making plans, coordinating actions, preparing forces, organizing support for them, and subsequently controlling the implementation of orders.[1626] This 'loop' was seen by some to be based on the principles of resilience (ustoichivost'), continuity (nepreryvnost'), efficiency (operativnost'), secrecy and expediency (validity) and undivided and centralised control.[1627]

In connection to NCW, Chekinov and Bogdanov have argued that military activities should be carried out with increasing intensity in time and space which will deprive the enemy of initiative and freedom of manoeuvre. However, as they understand military activities as three-dimensional (ob"emnyi) and having electronic, economic, psychological, informational and kinetic (force) effects, their definition of technological and psychological information superiority emphasizes deception and obfuscation. Consequently, they argue that information superiority demands the integration of all state agencies in a unified system.[1628] Others have also associated the principles of NCW to the way the defence of the state had to be organized and argued that this required tight cooperation between all "49 agencies and ministries" which would form the basis for national system of command and control.[1629]

By 2011, Russian IW and NCW thinking had achieved a state of self-reflection and adaptation. Professor A. V. Kopylov analysed the Western criticism towards the concept of NCW and argued that knowing the weaknesses of NCW enabled an opponent to use them to its advantage and also allowed the Russian Armed Forces to avoid some of the problems the United States had faced when implementing NCW. V. I. Kovalev, G. G. Magnitskii and Iu. A. Matvinenko repeated this view in 2015 and argued that Russia did not have to prepare for a war dictated by the United States. They viewed the NCW as based largely on technology and if Russia could not afford it then NCW would be 'a mental trap'.[1630] Similar ideas had been voiced already in 2008 by A. V. Raskin and V. S. Peliak who argued that information parity could be achieved by influencing the global information networks that enabled the United

[1625] For other who use the 'cycle of command' cf. Грудинин, И.В., Майбуров, Д.Г. Содержание и структура категории «информационно-управленческий ресурс отражения удара средств воздушно-космического нападения противника». Вестник академии военных наук, № 1 (62) 2018, 104-111; Выпасняк, В.И., Тиханычев, О.В. Автоматизированные системы управления войсками (силами): тенденции, методы и перспективы развития. Вестник академии военных наук, № 4 (29) 2009, 61-69.

[1626] The Soviet and Russian concept of command and control (upravlenie voiskami (silami)) has stayed essentially unchanged and was defined in the Military Encyclopaedia of 2007 as "the purposeful activity of the command [...] to maintain constant combat and mobilization readiness of troops (forces), prepare them for operations (combat actions) and lead them in carrying out assigned tasks." (Управление войсками (силами). Военного энциклопедического словаря. М.: Воениздат, 2007 [Online]. Available: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=10705@morfDictionary [Accessed: 10th March 2019]; Рипенко, Ю. Б., Волков, А. Б. О терминологии в теории управления войсками (силами) и уставных документах. Военная мысль, № 8 (2014), 10-18, 11.)

[1627] Анисимов, Е. Г., Анисимов, В. Г., Солохов, И. В. Проблемы научно-методического обеспечения межведомственного информационного взаимодействия. Военная мысль, № 12 (2017), 45-51; Бытьев, А.В., Смирнова, Л.А. К вопросу о научном понятии «военное управление». Вестник академии военных наук № 1 (66) 2019, 43-49.

[1628] Чекинов & Богданов 2015b.

[1629] Скоков & Грушка 2014, 41.

[1630] Ковалев, В.И., Малинецкий, Г.Г., Матвиенко, Ю.А. Концепция «сетецентрической» войны для армии России: «множитель силы» или ментальная ловушка? Вестник Академии военных наук, 2(51) 2015, 94-100.

States and its allies to fight according to NCW principles.[1631] Subsequently, Iu. I. Starodubtsev, V. V. Bukharin and S. S. Semenov from the Military Academy of Signal Corps proposed an alternative approach on NCW based on Russian cybernetic theories about ASUs which basically characterized the future warfare as warfare between systems.[1632] In 2013 Russian scholars V. I. Kovalev and Iu. A. Matvinenko from the Academy of Military Sciences argued that NCW was not about new forms and methods of warfare, or a new paradigm of war, but a functional concept based on the principles of command and control of forces and means and thus it might not work against a well-prepared state.[1633]

The dialectical approach present in the above mentioned arguments was 'operationalized' by I. I. Korolev, V. N. Pavlov and A. V. Ganin in 2013 who argued that information superiority could be blocked by a 'radio electronic information blockade' which would be a complex, multifunctional and adaptive system of EW.[1634] The idea was further developed in 2017 when researchers from NIII EW VUNTs (re)introduced the concept of command and control warfare. In this context superiority was defined as an advantage in the effectiveness and efficiency of command and control in relation to a certain situation and opponent and the ability to use EW as a tool of counter-C2 warfare.[1635] Information superiority was thus replaced by command and control superiority.

An additional aspect of information superiority was based on the Russian interpretation of 'netwars' and 'network wars' as wars conducted by horizontally organized forces that were geographically dispersed, connected by global information networks and controlled through them.[1636] This approach tended to incorporate the concept of 'network-centric warfare' into itself by transforming the term to mean a warfare using and targeting all-kinds of networks, primarily social, with mostly non-military non-direct means.[1637] These ideas gave information superiority its distinct information-psychological and perhaps even social aspect.[1638] The element of great power competition in informatization meant that information superiority would not only be used in a military-operational context. Therefore, both civilian and military commentators argued that Russia needed an information policy that would enable Russia to counter the technological-scientific and psychological information superiority of its potential

[1631] Раскин & Пеляк 2008.

[1632] Стародубцев, Бухарин & Семенов 2012.

[1633] Ковалёв В.И., Матвиенко Ю.А. «Сетецентрическая» война как новая парадигма вооружённой борьбы. Информационные войны №2 (26) 2013, 2-9; Ковалев, Виктор, Малинецкий, Георгий, Матвиенко, Юрий. Концепция «сетецентрической» войны для армии России: «множитель силы» или ментальная ловушка? Экономические стратегии № 5/2013, 40-51.

[1634] Королев, Павлов & Ганин 2013; Донсков, Ю. Е., Морареску, А. Л., Беседин, П. Н. Завоевание превосходства в управлении как цель применения войск радиоэлектронной борьбы в операциях объединения Сухопутных войск. Военная мысль, № 1 (2018), 28-32. Also, Донсков, Беседин & Ботнев 2017.

[1635] Донсков, Ю. Е., Беседин, П. Н., Ботнев, А. К. Превосходство в управлении - обязательный фактор реализации основных закономерностей оперативного искусства. Военная мысль, № 11 (2017), 28-31;. Донсков, Морареску & Беседин 2018.

[1636] Раскин, А. В., Пеляк, В. С. К вопросу о сетевой войне. Военная мысль, № 3 (2005), 21-27.

[1637] Герасимов, Н. Н., Шакирова, Е. Ю. Социально-сетецентрические войны современности: реальность информационной эпохи. Военная мысль, № 10 (2017), 79-87.

[1638] Савин, Л. В. Сетецентричная и сетевая война. Введение в концепцию. Москва: Евразииское движение, 2011; Татаринов, В.В. Элементы сетецентрической защиты. Вестник Академии военных наук, № 1 (42) 2013.

adversaries even in peacetime.[1639] Thus the concept became part of the great power competition

The connection between kibernetik ideas and the Western NCW doctrine was not lost to Russian commentators and scholars.[1640] By 2012 the leading Russian NCW theorist Aleksandr Kondrat'ev argued the West had, if not stolen, then at least borrowed the ideas of Marshal Ogarkov.[1641] Petr Cherkassin claimed that, firstly, NATO had stolen the Soviet 'Maneuvr' automated command and control system and, secondly, that Western systems were developed for aggressive, offensive actions—contrary to Russian defensive needs.[1642] Others claimed that the Russian Evgeni Messner (1891-1975) was the true creator of networked warfare.[1643] Furthermore, some argued that the American concepts contained nothing new, and that people remained at the heart of military action, not machines.[1644] Military historian Vasilii Mikriukov even managed to thrice change his views on NCW until he finally argued on a Russian theory of command and control.[1645]

The 2004 'Ivanov Doctrine' notices the importance which foreign armed forces place on information superiority and is clearly designed to guide the Russian Armed Forces in the same direction.[1646] However, in later documents the emphasis of NCW and information superiority is more muted. The term of superiority was used in the NSS of 2009 and the Military Doctrines of 2010 and 2014 in connection to the great power competition and strategic weapon systems, and the "politics of some leading countries directed at the achievement of superiority in the military sphere."[1647] Superiority on land, at sea and in space, in addition to strategic surprise and the resilience of state and military command and control, were seen as decisive factors in achieving military objectives in war.[1648] The 2015 NSS omitted the term altogether.[1649] Neither was it used in official foreign policy documents. The Information Security Doctrine of 2016 noted information superiority only implicitly arguing that "the state of information security in the field of strategic stability and equal strategic partnership is characterized

[1639] Прудников, Д. П. Государственная информационная политика в области обороны: исходное определение. Военная мысль, № 3 (2008), 43-48; Базылев et al. 2012; Бородакий, Добродеев & Бутусов 2013.

[1640] Ковалёв & Матвиенко 2013.

[1641] Кондратьев, Александр. Мнение: информатизация по-российски. ВПК, 18 января 2012 [Online]. Available: https://vpk-news.ru/news/224 [Accessed: 8th March 2019].

[1642] Черкашин, Петр. Сетецентрические веяния. Замыслы советского генштаба реализуются под новым названием в пентагоне. ВПК, № 45 (758) за 20 ноября 2018 года. It should be noted that a myth was built around a story that the U.S. and NATO had acquired (stolen) the system after the Warsaw bloc fell and were shocked to discover that the system would have enabled Soviet Union to destroy NATO forces in three days without the use of nuclear weapons. (Мясников, Виктор. Путин нацеливает армию на интернет. Независимое военное обозрение, № 22 (2010).)

[1643] Александров, Михаил. Сетецентрические войны будущего и подготовка государства к их отражению. Взгляды русского военного теоретика Е. Э. Месснера. Обозреватель–observer, Ноябрь 2016 г. № 11 (322) 109-118; Месснер 2005.

[1644] Костарев, С. В., Ефремов, О. Ю., Зверев, С. Э. Концепция сетецентрических войн в свете доктрины "Единый взгляд 2020". Военная мысль, № 1 (2014), 58-64.

[1645] Микрюков, Василий. Нездоровый сетецентризм. Отечественная военная наука находится в плену у западных догматов. ВПК, № 8 (672) за 1 марта 2017 года.

[1646] The Defence Ministry of the Russian Federation 2004.

[1647] Указ Президента РФ 2015.

[1648] Указ Президента РФ 2010; Доктрина 2014.

[1649] Указ Президента РФ 2015.

by the desire of individual states to use technological superiority to dominate the information space."[1650] However, the document made it explicitly clear that differences in information-technological and psychological capabilities between states were strategic issue of balance of power.

To summarize. Information superiority is a central concept and idea for understanding the importance the Russian military and security scholars and elites have placed on information warfare. In the timeframe of 2000-2018 the interest in information superiority was based on the need to reform the Russian Armed Forces, and the theory of NCW seemed to offer a successful and proven way to achieve it. The defence and security elites bought into these ideas, which was apparent in the objectives of the Serdiukov's military reform. By the 2010s, Russian scholars were quite familiar with the NCW and its Western self-criticism and, consequently, began themselves to approach the NCW more critically. This led to the further study and development of the idea of information superiority on the one hand and to the study of the vulnerabilities of the NCW solutions on the other hand. The result was, firstly, an emphasis of knowledge, understanding, and efficiency of command and control, instead of the quantity and speed of information. Secondly, the Russians began to develop counter-NCW theories around 2008-2012. From 2013-2014 onwards the idea of information superiority and the principles of NCW appeared in the context of strategic planning, mobilization and state security. Thus, they had ascended from the tactical level to the strategic and subsequently acquired an increasingly Russian outlook with the emphasis of centralized control and vertical and horizontal synchronization. The ideas of information superiority and the EIP were therefore more and more intertwined.

The chronology presented above is a simplification of a complex process. It has included heated debates about the nature of the NCW and the relevancy of information superiority in winning a war. The NCW was variously described in terms of means and methods, or as tactics, a doctrine or theory of command and control, philosophy or a paradigm. The concept of information superiority is important for Russians because it seems to explain why the West has been militarily so successful, and what the West did to the Soviet Union and was doing to Russia and other countries, and so offered an explanation and solutions for future warfare and the broader interstate struggle. Later, this approach developed into criticism towards adopting Western concepts in Russian military thought. Information superiority as a real phenomenon was not disputed but the NCW's applicability to the Russian way of conducting war was. Moreover, 'netwars' and Western concepts altogether were seen by some as an insidious political technology to subvert the Russian society and weaken its military.

There is also a geopolitical version of information superiority and the NCW. This version points to an important Russian idea: Information superiority is not only about the quality or speed of the flow of information, it is more about the result of the ability to manipulate the adversary already during the time of peace. Superiority is as much about processes as it is about space—superiority over the minds of the people over certain territory or at least the ability to influence an important segment of that population. Thus, information superiority is not only about information. It has technological and psychological aspects and political, social, economic and military effects.

[1650] Указ Президента РФ 2016b.

It can appear on any level of political and military action from international politics down to tactical warfighting level. Moreover, this superiority is based on scientific, technological, economic and spiritual potential, and the ability to control information.

Information superiority is related to the Soviet and Russian theory of command and control. This is apparent in the way the Russian theory of the cycle of command was compared with Boyd's theories. Information superiority is also related to other strategic cultural ideas. It is connected to the interstate struggle as it is seen as something that the main competitor or adversary is striving to achieve already in peacetime. From this follows that information superiority, its denial or conquest, becomes part of strategic deterrence. Moreover, the strategy of denial is connected to the control of the EIP and the national segment. Ultimately, as Russian scholars admit that Russia is weaker than the United States in information technology, an asymmetric response is required. The last two ideas of information-technological warfare and automated command and control systems give substance to the means and ways information superiority can be achieved.

5.8 Information-technological warfare

The examination of previous studies and the analysis of other strategic cultural ideas above and in Chapter 4 has shown that the Russian understanding of information warfare has two aspects: technological and psychological. It was also established that the means and objectives of information warfare change depending on the state of interstate relations and the level of analysis from military tactical to geostrategic. Here the idea of information-technological warfare in all its variants is analysed more exhaustively.

Russian ideas on information-technological warfare were well developed by the end of the millennium. An article in 'Vobrosy Bezopasnosti' (Issues of security) in 2000 claimed that the creation of a unified global information space had generated concerns that 'information-cybernetic technologies' would be used to attain foreign policy and military objectives, and that they opened up the prospect of a new arms race.[1651] The article claims that information weapons were first used in the Gulf War and it provides a list of information-technological weapons such as computer viruses, logic bombs, means of suppressing telecommunications networks and the falsification of information, and supply-chain attacks. Information weapons were "designed to achieve information superiority, as well as to damage information, information resources, processes and systems; to improve traditional weapons and to create new types of weapons and military equipment deployed for direct military impact against the enemy; to incapacitate civilian objects and life support systems; to disorganize public administration; to organize economic chaos and sabotage; to damage national financial systems based on information and computer networks; and to influence the population psychologically in order to socially destabilize society." According to the article, the properties of information weapons were, among others, universality, radicalism of effects, and accessibility. These are economical, their use is easily disguised, and the identity of the user is hidden. They are not affected by geographical distances or state borders,

[1651] Вопросы Безопасности. Информационное оружие: постановка проблемы и пути решения. Вопросы Безопасности, № 3 (2000).

and they can be used in secret without a declaration of war and even without the target knowing it is under attack. They are also difficult to counter. Information weapons, the article claims, change the character of military conflicts, may destabilize the strategic stability, and empower criminals and terrorists (non-state actors).[1652] The article could very well have been written by the leading Western cyber warfare theorists of the time.

Professor Vitalii Tsygichko voiced similar alarmism when he argued in 2004 in an article named "Weapons akin to nuclear"[1653] that the interaction of informatization, globalization, and geopolitical developments were creating new global threats. Tsygichko claimed the American experts believed that information-technological weapons would provide an advantage over those countries that do not have them. Moreover, the weapons would enable the termination of a confrontation even before active kinetic hostilities. Accordingly, Tsygichko claimed that information weapons could therefore be used as weapons of mass destruction, for pressuring, and for deterrence like nuclear weapons.[1654] These arguments were also were akin to the contemporary Western views.

By 2008 the Military Academy of the General Staff had collected and produced at least one public dictionary of information (cyber) terms. In it information-technological effects/actions/influence (vozdeistvie) was defined as "a complex of computer programs (software) and radio-electronic means, aimed at manipulating the functioning of information-technological objects and also at suspending (hindering) their activity or putting them out of order for a defined period of time."[1655] Objects included information-telecommunications systems and communications networks, industrial systems, and other services. Information-technological weapons could be used against equipment (tekhnika) and were divided to strategic (state resources – strategic operation), operational (operation at the TVD level) and tactical (combat action level) weapons.[1656] However, the definitions of the General Staff were not publicly used by the Russian Ministry of Defence.[1657]

A less 'kinetic' view was offered by retired Colonel Professor V. I. Lutovinov from the Russian Presidential Academy of Public Administration, later RANEPA, who argued in 2009 that information-technological means belonged to the strategy of indirect actions.[1658] In his view the strategy would be applied in the opening of hostilities, in covert operations, and in the securing of defence secrets. These functions were the responsibility of the SVR, FSB and GRU. Lutovinov defined the objectives and tasks of IW to include collecting information about the adversary, disrupting enemy plans and command and control systems, planting disinformation, protecting information resources, and neutralizing the information resources of the adversary on strategic,

[1652] Ibid.

[1653] Цыгичко, Виталий. Оружие сродни ядерному. ВПК, № 42 (59) за 3 ноября 2004 года.

[1654] Ibid.

[1655] Тучков 2008, 50.

[1656] Ibid.

[1657] Министерство обороны Российской Федерации. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве, 2011 [Online]. Available: http://ens.mil.ru/files/morf/Strategy.doc [Accessed: 30th January 2019].

[1658] Лутовинов, В. И. Развитие и использование невоенных мер для укрепления военной безопасности Российской Федерации. Военная мысль, № 5 (2009), 2-12.

operational and tactical level to gain information superiority.[1659] Basically Lutovinov argued that information-technological operations belonged to the secret services and the special forces.

The interest in the foreign use of cyber concepts became acute when the United States created its Cyber Command in 2010 and subsequently adopted the Department of Defense Strategy for Operating in Cyberspace in 2011.[1660] Basically, the Russians were trying to understand the concepts used by their great power competitor. Ultimately, their understanding of the subject was not so different—they just avoided the word cyber and wrote about information-technological warfare and information space.[1661] This was apparent in a round-table discussion of cyber security experts organized in 2013 by Nezavisimaia Gazeta.[1662] M. V. Iakushev from the PIR Centre argued that cyberspace was related to the electronic environment and digital signals, and conflict in cyberspace consisted of state or state-proxy actions in cyberspace which would lead to physical destruction or death. An independent military expert D. N. Kandaurov defined cybernetic warfare (protivoborstvo) in terms of computer (apparatno-programmyi)[1663] attacks on computerized military and civilian systems of ASUs, aimed at disrupting their normal functioning. M. M. Khazmatov argued that cyber means and operations could decide the result of a conflict if the target did not have defensive capabilities. However, no war could be conducted through cyberspace alone. I. M. Popov argued against understanding cyberspace as a new ‘theatre of military action’ as it should be understood only in terms of computers connected by networks used to accumulate, store and circulate data. Popov argued that actions in networks were characterized by their high tempo, possibly non-destructive effects and non-attribution, unrestricted scope of effects, unpredictability of enemy actions, and the threat of catastrophic effects.[1664] Cyber terms were clearly familiar to these experts and their rejection of the concept of a cyber war reflected the thinking of the Western theorists. Furthermore, at least some Russian scholars by the 2010s were ready to accept that information-technological actions had primarily enabling and supporting effects through information superiority, instead of direct strategic effects.[1665] This did not, however, mean that Russia and the West would or could officially agree upon information and cyber security terms.[1666]

[1659] Ibid., 4-8.

[1660] The U.S. Cyber Command. U.S. Cyber Command History [Online] Available: https://www.cybercom.mil/About/History/ [Accessed: 3rd May 2019]; The United States Department of Defence. Department of Defense Strategy for Operating in Cyberspace, July 2011 [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf [Accessed: 13th March 2019].

[1661] Паршин, С. А., Гобачев, Ю. Е., Кожанов, Ю. А. Кибервойны – реальная угроза национальной безопасности? М.: КРАСАНД, 2011; Чекинов & Богданов 2012a; Макаренко & Чукляев 2014.

[1662] Независимое военное обозрение. Война в киберпространстве: уроки и выводы для России. Круглый стол в редакции “Независимого военного обозрения”. Независимое военное обозрение. № 46 (787) 2013 [Online]. Available: http://nvo.ng.ru/concepts/2013-12-13/1_war.html [Accessed: 4th April 2019].

[1663] The Russian term ‘apparatno-programmyi’ is usually translated into English as ‘software and hardware’. This is not in fact accurate as the term refers to a elements such as BIOS chips, processors, industrial control systems, and telecommunication equipment. It is more akin to programmed hardware than software as such.

[1664] Ibid.

[1665] Горбачев, Юрий. Кибервойна уже идет. Независимое военное обозрение, № 13 (754) 2013.

[1666] The confusion over terminology is evident in the efforts to find common ground between the American and Russian use of different terms and concepts (Godwin et al. 2014). Western efforts to define cyber warfare issues, i.e. the Tallinn Manual, which was published in 2013, was mostly received by the Russians negatively as a ‘NATO document’. (Кранс, Максим. Кибероружие в арсенале НАТО. Независимое военное обозрение, № 21 (762) 2013.).

The above examined debates were taking place in a time when the Russian government had begun to discuss of the necessity of creating cyber troops. The idea was first voiced by vice-premier Dmitrii Rogozin in the March of 2012. In 2013 Interfax reported that a Russian Cyber Command would be created in 2014 as a new branch of the Armed Forces "for operations in the virtual space both in peacetime and in wartime."[1667] The issue of cyber or information troops was debated amongst military scholars. Major General and Professor Vladimir Zolotarev argued that a new kind of troops were needed because new 'information-network war' aimed at transferring defender's strategically important resources to the geopolitical aggressor. This type of war would be fought in geographic, economic, ideological and network dimensions and the main task was to hinder access to reliable and truthful information.[1668] Zolotarev's views were supported, among others, by Konstantin Sivkov who argued that because IW was a complex issue it required a systematic approach—not such a fragmented approach as the U.S. was taking by creating a separate military command. On the contrary, Russia required a unified, centralized organ of information warfare command, i.e. the General Staff of Information Security of Russian Federation under the Information Security Ministry.[1669]

In 2014 Major General Igor' Sheremet summarized the developments of the 'global information infrastructure' over the last twenty years.[1670] He claimed that the evolved infosphere now exposed 'the technosphere' and 'the anthroposphere' to new threats as it connected everything to everything. Sheremet divided information security into technological and psychological areas, the former of which he also called cybernetic. Cyber security was defined as "the safety of the material and information objects of the technosphere, that is, their protection from threats realized through the use of special information technologies for destruction or for the illegal use of these objects." In this context, states were trying to affect each other's information infrastructure while protecting their own. Sheremet conceded that Russia was lagging other world powers in technology, but it could catch up. Russia should protect its own technosphere's resilience (ustoichivost') and security by continuously monitoring the technosphere and identifying and neutralizing threats. It should also ensure the manageability (upravliaemost') of the state institutions and the population in the case of systemic destruction of critical infrastructure. Sheremet argued that these tasks, in the form of a 'mega-project' ensuring the resilience and security of the Russian technosphere should be given to the Ministry of Defence.[1671] Later in 2019 Sheremet wrote about the 'cyber threats' threatening Russian 'socio-technological systems' which could cause a catastrophic fall of society, financial collapse, and a change in military-technological parity—just like the use of nuclear weapons. Russia would only be saved

[1667] Независимое военное обозрение. В бой идет новый род войск. Кибероперации приравняли к нанесению ядерного удара. Независимое военное обозрение, № 7 (938) 2017.

[1668] Золотарев, Владимир. Психологическая война уже в киберпространстве. Войска информационных операций способны обойтись без применения военной силы. ВПК, № 16 (484) за 24 апреля 2013 года; Золотарев 2013a.

[1669] Сивков, Константин. Хуже иприта Информационные средства ведения борьбы уже можно приравнивать к оружию массового поражения. ВПК, № 31 (499) за 14 августа 2013 года; Сивков, Константин. Четвертое измерение войны. Каким должен быть Генеральный штаб информационной безопасности. ВПК, № 39 (752) за 9 октября 2018 года.

[1670] Шеремет 2014a.

[1671] Шеремет, Игорь. Киберугрозы России растут — часть II. Ситуация в этой области изменяется в лучшую сторону гораздо медленнее, чем того требует развитие геополитической обстановки. № 6 (524) за 19 февраля 2014 года.

through fully domestic hardware and software production and by creating a new 'class of cybertariatom', that is, a digital age working class.[1672]

As has been seen in previous chapters, many Russian scholars took a more systematic approach to the information threats than just creating new troops and weapons to answer new threats. This became more evident during and after 2014. One of the more ambitious and theoretical models of society's information security system was presented by V. V. Tsyganov and Iu. G. Bochkareva in 2014. They defined it as "a hierarchical adaptive self-organizing system with two types of functions: the adaptive management of public safety objects and the development of public safety subjects through self-organization."[1673] This system would have multiple levels and subsystems. It would have adaptive subsystems that would enable it to react to changes in the environment and functional subsystems that would enable it to react to different threats.[1674] In effect Tsyganov's and Bochkarev's model would have transformed the Russian state into a cybernetic system for controlling public security.

V. K. Novikov, a professor of the RVSN Academy offered a more philosophical approach.[1675] He argued that information permeated everything and thus information warfare (bor'ba) was a confrontation in peace and war time between two or more sides (systems) that try to attack the opponent's information resources while protecting their own information resources. Novikov divided the weapons used in this warfare into information technological, psychological, and reconnaissance. The first group included means of radio suppression (EW), functional destruction (EW, EMP, laser, 'special program-technical means'), changing the conditions of radio wave propagation, and electromagnetic degradation.[1676] Another systematic approach was offered by S. I. Makarenko, an associate professor at the Department of Networks and Communication Systems of Space Systems and a professor of the Academy of Military Sciences, who in 2017 described his vision of information conflict as a dynamic model of a bidirectional information conflict. It consisted of two (or more) multilevel organization-technical systems which tried to affect each other through information-telecommunications space with hardware-software and radioelectric means. The systems had subsystems of surveillance and observation, control, action (vozdeistvie), and information, and they used surveillance, capturing of resources, and blocking of resources to affect each other in constant struggle.[1677]

The cyber or information-technological issues discussed among the military scholars were not limited to direct warfare. Supply-chain vulnerabilities were highlighted by the researchers from the 18th TsNII of the MoD[1678] and Internet anonymizers and

[1672] Шеремет 2019.
[1673] Цыганов & Бочкарева 2014, 65.
[1674] Ibid.
[1675] Новиков, В. К. Информационное оружие – оружие современных и будущих войн. М.: Горячая линия-Телеком, 2013.
[1676] Ibid.
[1677] Макаренко, С. И. Динамическая модель двунаправленного информационного конфликта с учетом возможностей сторон по наблюдению, захвату и блокировке ресурса. Системы управления, связи и безопасности №1 (2017), 60-97.
[1678] The 18th TsNII specialises in the research of protected and secret communications, satellite and long-range communications and polymaterials. (Петелин, Герман, Баринов, Владимир. Разведка Минобороны требует от ученых неустойку в 30 млн рублей. Главное разведывательное управление отстаивает в суде свои права. Известия, 15 марта 2013 [Online]. Available: https://iz.ru/news/546680 [Accessed: 5th April 2019];

crypto currencies were seen by some as a part of the U.S. State department policy of the Freedom of the Internet[1679]—which was aimed at keeping other states open and vulnerable to American influences. The new technologies had the power to change the balance of power.[1680] By 2012 the Russians were debating the protection of industrial control systems from cyber-attacks. For example, professor Iu. A. Matvinenko of the AVN wrote an article on the subjects by using only Russian language sources on critical infrastructure protection. He defined a 'cyber strike' as a weapon for information-psychological operations to destabilize the target state for geopolitical purposes. The strike had psychological components such as disinformation and PR campaigns and technological components to penetrate and affect automated industrial control systems.[1681] Despite the growing shared understanding of the need to protect the CII, the lack of official terminology and unresponsive Russian government policies were criticized in 2013-2016.[1682]

The basic concepts of Russian IW thought created in the 1990s survived into the 2010s. A. A. Bartosh repeated the views of Tsymbal in 2016 as he categorized information war into broad and narrow variants where the latter was military confrontation in the information sphere targeting information infrastructure.[1683] Moreover, Professor I. A. Kryglova, a senior research fellow from RAS, argued in 2016 that a new form of geopolitical information warfare had appeared and it was directed against the information security of the state. It consisted of information-technological actions against information-technological systems and, conversely, their protection, and information-psychological actions against the psyche of elites and the population and their protection. Information-technological warfare is part of military operations and used against communication networks and centres to disorganize the command and control of the enemy and suppress its will to fight.[1684]

Kryglova's article highlights the Russian way of defining information warfare through 'who is doing what to whom'. Thus, the concept of information-technological warfare

Балыбин, С.В., Белов, Е.Н., Федорец, В.Н. Информационная безопасность военной техники, использующей интегральные схемы иностранного производства. Военная мысль № 12 (2011), 11-21).

[1679] The President of the United States. International strategy for cyberspace: Prosperity, Security, and Openness in a Networked World, 2011 [Online]. Available: https://obamawhitehouse.archives.gov/sites/default/files/ rss_viewer/international_strategy_for_cyberspace.pdf [Accessed: 14th March 2019].

[1680] Роговский, Евгений. Новое кибероружие. Станут ли электронные деньги средством поражения. Независимое военное обозрение, № 8 (796) 2014.

[1681] Матвиенко Ю.А. Комплексная информационная атака типа «киберстачка» на промышленную автоматизированную систему: анатомия явления и подходы к защите. Информационные войны №1 (21) 2012, 85-94.

[1682] Борисов, Сергей. СОИБ. Безопасность критической информационной инфраструктуры (КСИИ), 13 Августа, 2013 [Online]. Available: https://www.securitylab.ru/blog/personal/sborisov/32175.php [Accessed: 14th March 2019]; Калашников, А. О. Управление информационными рисками объектов критической информационной инфраструктуры Российской Федерации. Вопросы кибербезопасности №3(4) 2014, 35-41; Муравник В.Б., Захаренков А.И., Добродеев А.Ю. Некоторые предложения по подходу и порядку реализации политики и стратегии импортозамещения в интересах национальной безопасности и укрепления обороноспособности Российской Федерации. Вопросы кибербезопасности №1(14) 2016, 2-8; Массель Л.В., Воропай Н.И., Сендеров С.М., Массель А.Г. Киберопасность как одна из стратегических угроз энергетической безопасности России. Вопросы кибербезопасности №4(17) 2016, 2-10.

[1683] Бартош, А.А. Адаптивные стратегии информационной войны (Часть 1). Вестник академии военных наук, № 2 (55) 2016, 85-93; Thomas 2001.

[1684] Крылова, И.А. Информационные войны и безопасность России. Информационные войны №3 (39) 2016, 63-70.

is used when discussing Russian information or cybernetic theory, and cyber warfare when discussing American strategies, concepts, and actions.[1685] Thus in contrast to Kryglova, Vorob'ev and Kiselev argued that the West could use 'cyberspace' for electronic invasion into Russia by using destructive attacks against networks, systems, and information. They claimed that warfare in 'cyberspace' was a new level of military confrontation, now in the electronic sphere, and the United States had for same time strengthened its superiority in 'cyberspace.'[1686]

Others used the cyber-prefix more objectively. Retired General-Lieutenant B. I. Kuznetsov, Colonel Iu. E. Donskov and Lieutenant-Colonel O. G. Nikitin from the Institute of EW of the Gagarin Air Force Academy claimed, "Cyberspace is an integral part and the material basis of another, more general, information space."[1687] Cyberspace consisted of infrastructure and information circulating in it and as an element or dimension of the battlespace (boevoe prostranstvo) it defined new forms and methods of battle and thus would influence the processes of battle, for example, by affecting command and control.[1688] In 2011 Colonel P.I. Antonovich, an associate professor of the Faculty of EW of the Combined Arms Academy of the Armed Forces of the Russian Federation, argued that cyberspace was a virtual space because it described systems which were not altogether material.[1689] Cyber-attack was an action against cybernetic systems, information resources or information infrastructure and a weapon gained its effectiveness through the vulnerability of the target.[1690] Although Antonovich offered a definition of cyber war he argued that it was a theoretical construct and in real life it would be better to talk about military actions is cyberspace or cybernetic warfare (protivoborstvo).[1691]

The idea that cyber warfare involved ASUs was expressed by Professor B. I. Vypasniak from the Academy of Military Sciences, and O. V. Tikhanychev and V. R. Gakhov from the 27th TsNII of the MoD.[1692] They listed kinetic (ognevoi), radio electronic, and cyber threats as the means of damaging ASUs. These means could materialize through backdoors, cyber sabotage (intentional actions by personnel), and remote attacks using software, EW, kinetic effects, exotic weapons, and hacking through networks.[1693] V. V. Kabernik from MGIMO also used ASUs in defining different types of cyber weapons. He distinguished four types based on their complexity and autonomy.[1694] Clearly by 2013 Russian scholars were becoming more systematic in their analysis of information-technological means of warfare but also closer to the

[1685] Cf. Тихонов, М.Н., Богословский, М.М. Кибернетические войны и информационная безопасность. Атомная стратегия, № 104 (2015), 15-20; Гриняев 2000; Паршин, Гобачев & Кожанов 2011; Иванов, Владимир. Армия США готовится к кибервойне. Независимое военное обозрение, № 6 (984) 2018; Дылевский, И. Н., Комов, С. А., Коротков, С. В., Петрунин, А. Н. Операции в киберпространстве: вопросы теории, политики и права. Военная мысль, № 8 (2011), 72-78.

[1686] Воробьев, И. Н., Киселев, В. А. Киберпространство как сфера непрямого вооруженного противоборства. Военная мысль, № 12 (2014), 21-28, 25.

[1687] Кузнецов, В. И., Донсков, Ю. Е., Никитин, О. Г. К вопросу о роли и месте киберпространства в современных боевых действиях. Военная мысль № 3 (2014), 13-17, 15.

[1688] Ibid.

[1689] Антонович, П. И. О сущности и содержании кибервойны. Военная мысль, № 7 (2011), 39-46.

[1690] Ibid., 42.

[1691] Ibid., 45.

[1692] Выпасняк, В.И., Тиханычев, О.В., Гахов, В.Р. Кибер-угрозы автоматизированным системам управления. Вестник Академии военных наук, № 1 (42) 2013, 103-109.

[1693] Ibid., 108.

[1694] Каберник, В.В. Проблемы классификации кибероружия. MGIMO 2 (29) 2013, 72-78.

way the English-speaking cyber security specialists defined and categorized cyber threats.

The way the idea of information-technological warfare is formulated is fundamental to the discussion about who should be responsible for it. As was noted in Chapter 4 EW troops were put forth as a one possible candidate at least in wartime.[1695] EW was connected to IW in Russian military thinking early on through the potential to affect command and control communications as both the weapon and target systems became more complicated.[1696] EW was 'fitted' to the new theories of IW. For example, Makarenko defined modern NCW to consist of electronic warfare and information confrontation where the latter was further divided into psychological and technological aspects.[1697] For others, EW was about reconnaissance, warfare, and maskirovka (deception). Therefore, the general argument was that the concept of information could be attached to the target list of EW troops and thus they could be transformed to cyber troops able to acquire information superiority.[1698]

The concept of resilience of (critical) information infrastructure has appeared in many of the sources analysed in this and the previous chapter and is central to understanding the defensive side of information-technological warfare.[1699] In Chapter 4 it was argued that the Russian term 'ustoichivost'' could be translated to mean resilience or resiliency—both are derived from the adjective 'resilient'.[1700] It was also noted that 'ustoichivost'' was one of the four requirements for command and control, others being continuity, efficiency, and secrecy. Furthermore, the Information Security Doctrine of 2016 states that one of national interests of Russia is "the ensuring of resilient (ustoichivost') and uninterrupted (bespereboinoi) functioning of the information infrastructure, primarily the critical information infrastructure of the Russian Federation [...] and the unified telecommunications network of the Russian Federation, in peacetime, during the immediate threat of aggression and in wartime."[1701]

[1695] The theoretical ruminations about EW, IW and cyber must be understood in the context of the EW troops trying to strengthen their position in the Armed Forces. Cf. Никитин, О. Г. Направления повышения эффективности организации боевого применения войск радиоэлектронной борьбы в операциях объединений Сухопутных войск. Военная мысль, № 5 (2017), 23-29; Андреев, В. В., Никитин, О. Г., Марасанов, А. В. Особенности методического обеспечения обоснования состава органов управления разнородными силами и средствами радиоэлектронной борьбы объединений Сухопутных войск. Военная мысль, № 6 (2017), 51-54.

[1696] Горбачев 2004.

[1697] Макаренко, С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. СПб.: Науко-емкие технологии, 2017.

[1698] At least according to the "year books" of EW troops they had not been tasked with cyber or information-technical tasks by 2018 (Ласточкинб Ю. И. (ред.) Радиоэлектронная борьба в Вооруженных Силах Российской Федерации – 2018. Москва: Информационный мост, 2018 [Online]. Available: https://reb.informost.ru/2018/sod.php [Accessed: 14th March 2019]). On the arguments cf. Ильин, А. П. Шакин, Д. Н. К вопросу о месте радиоэлектронной разведки, радиоэлектронной борьбы и радиоэлектронной маскировки в информационной борьбе. Военная мысль, № 1 (2008), 25-30; Кузнецов, В. И., Донсков, Ю. Е., Коробейников, А. С. О соотношении категорий "радиоэлектронная борьба" и "информационная борьба". Военная мысль, № 3 (2013), 14-20; Балыбин, В. А., Донсков, Ю. Е., Бойко, А. А. О терминологии в области радиоэлектронной борьбы в условиях современного информационного противоборства. Военная мысль, № 9 (2013), 28-32; Горбачев 2013.

[1699] Федорова & Цигичко 2001, 11-13; Дербин 2007 & 2009; Расторгуев 2014, 73-77; Стрельцов 2015, 163.

[1700] Resilience. Oxford Dictionary. [Online]. Available: https://en.oxforddictionaries.com/definition/resilience [Accessed: 15th March 2019]; Resilience. The Cambridge Dictionary [Online]. Available: https://dictionary.cambridge.org/dictionary/english/resilience?q=resiliency [Accessed: 15th March 2019]. In this thesis I will use the form resilience.

[1701] Указ Президента РФ 2016b.

Makhutov et al. have defined ‘ustoichivost” in the context of critical infrastructure as follows: “A system that is resilient (ustoichivyi) to extreme influences must meet the following requirements: survivability, (zhivuchest’), i.e. the ability to function and to a certain extent perform the prescribed functions in the presence of local damage arising from extreme influences; redundancy, (izbytochnost’), i.e. the availability of redundant links, alternative load transfer routes and redundant elements that may be involved in an emergency situation; resource availability, (resursoobespechennost’), i.e. availability of resources in the system that can be used in case of extreme exposure; the ability to quickly recover, (sposobnost’ k bystromu vosstanovleniiu) determined by the interval of time during which damage can be repaired, that is, to restore the system and reach the nominal level.”[1702] A more formal definition can be found in the Russian national standard on risk management which states that the resilience of an organization is its ability to adapt in a complex and changeable environment.[1703]

In 2016 representatives from the PIR Centre and the Information Security Institute of MGU used a trinity of Russian terms—stabilnost’, bezopasnost’ and otkazoustoichivost’—to refer to the Western concepts of stability, security and resilience when writing about Internet governance.[1704] The definition of resilience is taken from ICANN and is “the capacity of a system to effectively withstand/tolerate/survive malicious attacks and other disruptive events without disruption or cessation of service.”[1705] The writers do not explain where they derive the term ‘otkazoustoichivost” from although it has similarities to concepts of dependability (nadezhnost’), reliability (bezotkaznost’) and durability (zhivuchest’).[1706] The Russian national standard ГОСТ Р 56111-2014 defines ‘otkazoustoichivost” in English as “failure-related durability[1707] and ГОСТ 28806-90 defines it as “fault tolerance”.[1708] Accordingly, it can be argued that neither ‘ustoichivost” or ‘otkazoustoichivost” truly capture the Western definitions but they are similar enough to denote the same idea of preparing for, withstanding and recovering from an outside negative influence on a system. However, Igor Sheremet has used the term ‘ustoichivost” to denote the English terms of sustainability and resilience and argued that in the context of ‘sociotechnical systems’ and digital economy resilience means the ability of a system to fulfil its function under a successful cyber-attack. Sheremets’ definition allows for a certain degradation of services until the attack has been neutralized.[1709]

Both Military Doctrines of 2010 and 2014 recognized the importance of the information infrastructure and information technology in the military sphere but do not explicitly discuss information-technological warfare. Nevertheless, a comparison of

[1702] Махутов, Н.А., Резников, Д.О., Петров, В.П. Особенности обеспечения безопасности критических Инфраструктур. Безопасность в техносфере, №1 (январь–февраль), 2014, 3-14.

[1703] ГОСТ Р 51897-2011. Менеджмент риска. Термины и определения. Дата введения 2012-12-01 [Online]. Available: http://docs.cntd.ru/document/gost-r-51897-2011 [Accessed: 15th March 2019].

[1704] Медриш, М.А. (ред.) Стабильность, безопасность, отказоустойчивость глобальной инфраструктуры Интернета: технические и правовые вопросы. Москва - Лос Анджелес: ПИР-Цеитр, 2016, 17-18.

[1705] Ibid., 18.

[1706] Ibid., 19.

[1707] ГОСТ Р 56111-2014. Интегрированная логистическая поддержка экспортируемой продукции военного назначения [Online]. Available: http://cals.ru/sites/default/files/downloads/56111_.pdf [Accessed: 15th March 2019].

[1708] ГОСТ 28806-90. Качество программных средств. Термины и определения [Online]. Available: https://meganorm.ru/Data2/1/4294825/4294825913.pdf [Accessed: 15th March 2019].

[1709] Шеремет 2019, 9-10.

these two documents makes it clear that the more recent one emphasizes the military aspects of information technology and expresses the need for cooperation with allies. Both documents associate information technology with deterrence and both express concern for the vulnerability of systems of management and command and control. Russia is thus presented as a non-aggressive defender. It is noteworthy that these documents do not make the explicit difference between technological and psychological information warfare—which the 2004 Ivanov Doctrine did.[1710] The 2009 NSS is quite explicit in stating that threats to the national information-telecommunications infrastructure and critical objects of infrastructure are threats to national interests.[1711] The 2015 NSS makes the same points with more emphasis. It also connects information technology to national security and interests which is understandable in the context of Western sanctions. The 2015 Strategy is perhaps more 'psychologically' than 'technologically' oriented. The 2013 Foreign Policy Concept states as one of its priorities the strengthening of international security to counter threats in the information space arising from the hostile use of ICT.[1712] The 2016 Foreign Policy Concept follows the same lines although it emphasises the "equitable internationalization of the control of the information-telecommunications network Internet."[1713] Perhaps more important in the international context than the Foreign Policy Concepts are the Basics of Government Policy in the Area of International Information Security adopted in 2013 which clearly states that information technology is an issue of strategic parity and, therefore, the hostile use of information and communication technology is a threat to Russia.[1714]

The Information Security Doctrine of 2016 states that one of the basic negative factors influencing information security, which is a part of national security, is the use of information-technological actions (vozdeistvie) for military purposes. Information technology can be used to inflict damage to the sovereignty, territorial integrity, and social and political stability of Russia. Other states can use their technological superiority to dominate the information space. One of the strategic goals of the Russian federation is the protection of the CII which can be affected by information-technological means. For the defence of the country a system of information security will be created, and it will be built on the principles of vertical and centralized control. Although the Doctrine does not explicitly define information-technological and psychological aspects of IW, it is clearly built upon them and uses both terms.[1715]

To summarize. The idea of information-technological warfare is very much related to the idea of interstate (information) confrontation. Therefore, the discussion here should be approached in the context of the material analysed in Chapter 5.2. It is quite possible that the categorization of information warfare or struggle into technological and psychological aspects comes from the ex-KGB and FSB people who served during the Cold War in various cryptography and signal intelligence positions and taught

[1710] Указ Президента РФ 2010; Доктрина 2014; The Defence Ministry of the Russian Federation 2004.

[1711] Указ Президента Российской Федерации 2009.

[1712] Концепция 2013.

[1713] Указ Президента РФ 2016a.

[1714] Основы. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (Утверждены Президентом Российской Федерации В.Путиным 24 июля 2013 г., № Пр-1753) [Online]. Available: http://www.scrf.gov.ru/security/ information/document114/ [Accessed: 30th March 2019]..

[1715] Указ Президента РФ 2016b.

at security service and military academies. At least the categorization appears early-on in their texts and ends up in official documents which have been partly drafted by them. A direct connection is, of course, difficult to prove.

Information-technological activities and warfare are partly defined by their psychological counterpart which includes mass media, social media, and the Internet as a means. Psychological warfare often uses technological means, but an inverse relationship is not so common. Arguably, the psychological aspect is almost always present in the texts of the Russian IW scholars and it is more directly connected to the political goals of modern and future confrontation or war than its technological counterpart—thus the technological aspect is slightly secondary to the psychological. Both are rooted in the rise of the information society but also to the Soviet past—the psychological aspect is related to the theories of reflexive control, deception, and maskirovka, and the technological aspect to reconnaissance strike and fire complexes (RUK/ROK), command and control warfare, and EW. Computers and computer networks were incorporated into the technological aspects and social media and the Internet to the psychological aspects when the information revolution really kicked-off in the 1990s.

The Russian debate on information-technological warfare draws heavily on Western and particularly American concepts and theories. The early views were quite like the 'strategic cyber war' ideas of, for example, the RAND Corporation and Gregory J. Rattray.[1716] Furthermore, the Russians later discarded the idea of cyber war like their Western counterparts and concentrated on analysing different information-technological means, forms and effects, which might be used in warfare but also outside of it. Ideas about defence migrated towards cybernetic systems theories whereas ideas about offensive concentrated on categories of different attacks. By the end of 2010s these included kinetic (precision), software, hacking, electromagnetic, EMP, laser and other exotic means of attack. Thus, the idea of information-technological warfare is much broader than its Western counterpart of cyber warfare. Moreover, the divide between offensive and defensive measures is not as black-and-white as perhaps in the Western thinking (up until late 2010s). Many Russian scholars see information warfare as an interaction between systems during peace and wartime where offensive and defensive actions are difficult to separate. However, military sources have been quite consistent in arguing that information-technological warfare and means have an explicit role in the context of actual warfare. These means are directed against the will, decision-making capabilities, infrastructure, and armed forces of the opponent to achieve different effects in different phases of confrontation depending on the objectives.

The problem, and perhaps a source of confusion, is that the discussion about information-technological threats and the responses to them has been affected by geopolitical theories and ideologies on the one hand and institutional battles for authority and resources on the other. Cyber (technological) events have been interpreted through the lens of great power competition and an anti-globalization ethos. Therefore, the proposed solutions to threats have combined the technological and psychological aspects with political, economic, military and cultural elements and the results

[1716] Molander, Riddile & Wilson 1996; Rattray 2001.

have been things like 'information troops' and 'national information security systems.' Even if this use of an all-encompassing concept of information is a version of double-talk and deception on the part of the Russian authorities, it still leaves even Russian scholars and experts confused about the real state of the Russian information-technological capabilities. This confusion is exacerbated by the 'politically correct' use of the term cyber and information depending on whose operations a particular scholar is writing about. Whereas cyber is the work of 'the adversary', information confrontation is an interactive state-to-state relationship in which Russia, as a great power, takes part even if reluctantly. Thus, although many Russian scholars have conceded that the United States had acquired temporary dominion or superiority in cyberspace, they did not recommend passive defence. The use of weapons should be varied and flexible. Defence should be built upon the resilience, continuity, efficiency and secrecy which would guarantee the information-technological foundation for information superiority.

5.9 Automated command and control systems

The concept of an automated management or command and control system has retained its relevancy in the Putin era. The Military Encyclopaedia of 2001 offers a definition for the automation of command and control (avtomatizatsiia upravleniia voiskami/silami) (ASUV(S)) and definitions for its sub-concepts automated system of command and control of battle systems (weapons) (avtomatizirovannaia sistema upravleniia boevymi sredstvami) (ASU BS), automated systems of command and control of communication (avtomatizirovannaia sistema upravleniia sviazi) (ASS or ASUS), and automated systems of command and control of troops (avtomatizirovannaia sistema upravleniia voiskami/silami) (ASUV). Basically, automation means the use of computers in the process of command and control, i.e. gathering information, making decisions, giving orders, making plans, and controlling the implementation of tasks.[1717]

The ASUV is a complex man-machine system based on the collecting, processing and transmitting information to enable the efficient control of its objects, that is, troops, forces, weapon systems etc. through the use of calculating machines, i.e. computers and special technologies. This system is supposed to increase the efficiency (operativnost'), reliability (nadezhnost'), flexibility (gibkost') and secrecy (skrytnost') of the process of command and control. Efficiency is defined by speed, reliability by continuity of control, flexibility by the ability to quickly adapt to changes in the organization and secrecy by confidentiality of information.[1718] The ASUS is part of ASUV and an aggregate of interconnected automated networks, nodes, lines of communication and systems of command and control organized according to single or unified plan to enable the command and control of troops.[1719] The ASU BS is defined as a man-

[1717] Горкин, А. П., Золотарев, В. А., Карев, В. М., Манилов, В.Л., Милованов, В. И. Военный энциклопедический словарь в двух томах. Москва: Большая Российская энциклопедия, 2001, 27.

[1718] Ibid., 29.

[1719] This system operates based on the principles of constant readiness (postoiannaia gotovnost'), survivability (zhivuchest'), noise immunity (pomekhoustoichvost'), reliability (nadezhnost'), throughput (propusknaia sposobnost'), reconnaissance-resistance (razvedzachshichshennost'), mimic resistance (imitostoikost'), mobility (mobil'nost'), timeliness (svoevremennost'), and secrecy (skrytyi) and reliable (dostovernyi) transmission of information. Ibid., 28.

machine system which is based on computational technology to collected information for optimization of primarily fire control resolutions.[1720]

These definitions have basically been retained in the current 2007 version of the Military Encyclopaedia.[1721] ASUV is defined as an organizational-technological complex of technical means designed to increase the effectiveness of control by automating the basic processes of command and control. It collects information about the situation (friendly and enemy), offers decision-making support, transmits orders and collects information of their implementation.[1722] The definition of ASUS uses the term 'core or backbone network' instead of single or unified plan and highlights the modern capabilities of the system. The principles of operation have changed to constant readiness, stability, mobility, high bandwidth, secrecy and security of communication. The ASS of AF RF is supposed to be based in the future on the Integrated Automated Digital Communication System (OATsSS).[1723] The definition of ASU BS now includes a mention of the capability to manage groups of weapon systems on the tactical, operational, operational-strategic and strategic level including long-range precision weapons. Its principles are efficiency, reliability, noise resistance and survivability.[1724] ASUs are much more than computers and networks. They are complex systems with inherent rules and principles connected to their organizational and hierarchical environment. ASUs have a predetermined, goal-oriented and contextual functionality. [1725]

The ASU concept also has civilian definitions. It is defined in the government standards as "a system consisting of personnel and a complex of automation equipment for personnel's activities, or implementing information technology for the performance of set functions."[1726] The type of the system depends on its purpose and the system consists of multiple subsystems designed for different functions. The Great Encyclopaedic Dictionary defines an automated system of management as "a set of mathematical methods, technical means (computers, communication devices, infor-

[1720] Ibid., 28.

[1721] Автоматизация управления войсками. Военного энциклопедического словаря. М.: Воениздат, 2007 [Online]. Available: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=2639@morfDictionary [March 17th 2019].

[1722] Автоматизированная система управления войсками (силами). Военного энциклопедического словаря. М.: Воениздат, 2007 [Online]. Available: http://encyclopedia.mil.ru/encyclopedia/dictionary/ details.htm?id=2643@morfDictionary [March 17th 2019].

[1723] Автоматизированная система связи. Военного энциклопедического словаря. М.: Воениздат, 2007 [Online]. Available: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=2640@morfDictionary [March 17th 2019].

[1724] Автоматизированная система управления боевыми средствами. Военного энциклопедического словаря. М.: Воениздат, 2007 [Online]. Available: http://encyclopedia.mil.ru/encyclopedia/dictionary/ details.htm?id=2642@morfDictionary [March 17th 2019].

[1725] Автоматизированная система управления войсками и оружием (АСУ В и О). Соловцов, Н. Е., Шлычков, В. Р. (Общ. ред.) Энциклопедия ракетных войск стратегического назначения. М-во обороны РФ. М.: Белгород, 2009 [Online]. Available: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id =12536@morfDictionary [March 17th 2019]; Буренка В.М (Общ. ред.) Толковый словарь в области военного управления, связи и информационных технологий: Военно-теоретический труд. М.: РАРАН, 2017, 11-12.

[1726] ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. 1992-01-01 [Online]. Available: http://docs.cntd.ru/document/gost-34-003-90 [March 17th 2019].

mation display devices, etc.) and organizational complexes ensuring rational management of a complex object (process) in accordance with a given goal."[1727] The Law on the Security of the Critical Information Infrastructure of the Russian Federation defines ASU as "a set of software and hardware designed to control technological and (or) production equipment (control devices) and the processes they produce, as well as to manage such equipment and processes."[1728] Thus, in the realm of cyber security, ASUs are a hypernym for all controlling devices, functions and processes with various amounts of autonomy to achieve a given task. ASUs are still very much rooted in the cybernetic and systems analytic thinking.

The discussion about ASUs continued in the military journals during the Putin era and arguably was intensified when Serdiukov's military reform and rearmament program began to gather steam. Between 2001-2002 Colonel I. A. Grachev, Vice-Director of 27th TsNII, authored or co-authored multiple articles under the title 'Informatization of the Armed Forces'.[1729] He argued that information technology (IT) should enable the unity of control both vertically and horizontally. Intellectualization of information management should make command and control more efficient in the ever more complex situation—this included analysing, modelling and forecasting situations. Grachev conceptualized special mathematical and programmatic support (system) for troops which should support the whole cycle of command and control including forecasting if required on all levels of command. The system should have been tailored according to the organization using it and should be built on a functionally hierarchical modular basis. Grachev's ideas show how Russian military scholars were adapting to the information era but still hanging on to the Soviet era dreams of integrated systems that would be able to 'scientifically' forecast the future. Grachev' articles also reveal how there were many similarities between ASUs and American automated battle-management systems despite dissimilar and foreign terms.[1730]

In 2006 Captain of 1st rank V. R Grin' proposed a conceptual approach to efficiently develop ASUVs. He argued that the ASUVs consisted of technological, programmatic (software), mathematical, information, linguistic, ergonomic support, and information protection tools.[1731] Grin basically defined ASUVs through subsystems, principles, and goals. His article points to official technical Russian military standards adopted in 2005-2006, which show that the Armed Forces were actively engaged in conceptualizing modern ASUs. Later, in 2012, Grin' together with Iu. H. Golubev and A. V.

[1727] Автоматизированная система управления. Прохоров, А. М. (Гл. ред.) Большой энциклопедический словарь, 2000 [Online]. Available: https://dic.academic.ru/contents.nsf/enc3p/ [March 17th 2019].

[1728] Федеральный закон 2017.

[1729] Грачев, И. А., Каргин, В. Н. Информатизация вооруженных сил. информационные технологии в автоматизированных системах военного назначения. Военная мысль, № 6 (2001), 19-22; Грачев, И. А. Информатизация вооруженных сил. к вопросу об информационно-методической согласованности моделей военных действий. Военная мысль, № 2 (2002), 53-57; Грачев, И. А. Принципы построения специального математического и программного обеспечения АСУ войсками (силами). Военная мысль, № 6 (2002), 64-68.

[1730] For the American views at the turn of the millennium cf. Ullman, Harlan K. and Wade, James P. (eds.) Shock and Awe - Achieving Rapid Dominance. Washington: National Defence University, 1996; Khalilzad, Zalmay and M., White, John P. (eds.) The Changing Role of Information in Warfare. Santa Monica: RAND, 1999; Alberts, David S., Garstka, John J., Hayes, Richard E. and Signori, David A. Understanding Information Age Warfare. Washington, D.C.: CCRP, 2001. On the comparison of the Russian ESU TZ and American FBCB2 cf. Богданов, Попов & Иванов 2014; Выпасняк &Тиханычев 2009.

[1731] Гринь, В.Р. Информатизация вооруженных сил. Качество и безопасность автоматизированных систем управления войсками (силами): единство целого и частного. Военная мысль, № 12(2006), 26-31.

Shrialov, all from the 27th TsNII, argued that the introduction of 'information' to the scientific lexicon had muddled previous theoretical and technological terms and concepts. The concept of ASU as a closed system with fixed requirements of automation was not suited for a network-centric environment. Grin' et al. wanted to replace the concept of ASU, with the concept of information infrastructure which signified the reality that all command and control is now dependent on information technology with horizontal networks and uniform rules.[1732] A similar worry about the terms and concepts was expressed in 2011 by a group of researchers from TsNII EISU[1733] who argued that from the 1960s to the 1980s Russia had already had ASUs and now the same mistakes were being repeated, i.e. each service and branch was creating its own incompatible systems.[1734]

The issue Grachev and others were writing about had already been noted by the Russian MoD as the 2000 Military Doctrine and the Actual Tasks of the Development of the AF RF in 2003 required the development of automated systems of command and control.[1735] The deplorable state of the Russian Armed Forces vis-á-vis the United States was also noted by the commentators and this was considered to be a critical vulnerability.[1736] As the interest in ASUs and ASSs grew so did the number of articles about their Soviet and Russian era history.[1737] By 2010 then-Prime Minister Putin took a personal interest in the development of ASUVs as their development had not met expectations during the last ten years.[1738] Consequently, the Director of the Military Academy of the GS General-Lieutenant Anrdei Tret'iak was ready in 2012 to admit that the transfer to new ASUs had no scientific basis and was difficult because the systems of services and branches were not interoperable.[1739] Around 2015 the problems of creating interoperable ASUs for the Armed Forces were still openly discussed but not after that.[1740]

[1732] Ibid., 51.

[1733] The Central Research Institute for the Economics of Informatics and Management Systems (TsNII EISU) was established in 1969 to research and support the management of the OPK. It was transferred in 2010 from the Ministry of Industry and Trade of the Russian Federation to the Ministry of Defence. Currently its main task is officially to develop the technical base for the systems of command and control of the Armed Forces (ASU TOSU VS). (ЦНИИ ЭИСУ [Online]. Available: http://cniieisu.ru/ [Accessed: 5th April 2019]).

[1734] Толмачев, А.П., Баранюк, В.В., Тютюнников, Н.Н. Информационное обеспечение управления Вооруженными силами Российской Федерации. Вестник академии военных наук, № 3 (36) 2011, 102-105.

[1735] Военная доктрина Российской Федерации 2000 г. (Шаклеина 2002); Красная звезда 2003.

[1736] Красная звезда. Актуальные задачи развития вооруженных сил Российской Федерации. Красная звезда, 11 октября 2003; Растопшин, Михаил. Как управлять войсками и оружием? ВПК, № 22 (39) за 16 июня 2004 года; Маслов, Алексей. Чтобы нейтрализовать военные угрозы. ВПК, № 7 (223) за 20 февраля 2008 года; Постников, Александр. Время "автоматизированных" войн. Независимое военное обозрение, № 1 (2010).

[1737] Безель, Яков. Этапы развития АСУ авиацией и ПВО. Воздушно-космическая сфера, № 4 (2014), 23-27; Моренков, Владислав, Тезиков, Андрей. Исторический аспект развития АСУ ПВО. Воздушно-космическая сфера, № 1 (2015), 59-64.

[1738] Мясников 2010.

[1739] Фаличев, Олег. Интервью начальника академии Генштаба А. Третьяка. ВПК, 10 декабря 2012 [Online]. Available: https://vpk-news.ru/articles/13536 [Accessed: 18th March 2019].

[1740] Иванов, Валерий. Поршневое управление. Чтобы достичь прорыва в разработке межвидовой АСУ, Минобороны должно сделать ставку не на кустарей, а на государственниковвпк. ВПК, № 33 (599) 2-8 сентября 2015 года; Павлов, Вячеслав. «СКАЙНЕТ», которого нет. Создание автоматизированной системы управления Вооруженных сил РФ – залог победы в современной войне. ВПК, № 39 (605) 14 –20 октября 2015 года.

Practical problems did not stop theoretical work. In 2013 V. V. Kolodiazhnyi, Iu. E. Kuleshov and H. P. Shekhovtsov, provided a concept of a three-dimensional structure of command and control composed of hierarchy, services and functions. This structure was combined with the cycles of preparing for military action, conducting military action, and fighting, from which they derived three circuits of command and control with different interconnected functions. Kolodiazhnyi et al. then argued that their model gave theoretical grounds for creating at least two distinct ASUs, i.e. a decision-support system and battle command and control system.[1741] On a more 'strategic level' in 2012 professor V. I. Orlianskii, retired Colonel P. A. Dul'nev and Colonel A. N. Kostenko VUNTs RF argued that the creation of the EIP of the AF RF was necessary for the further development of command and control and for the adoption of 'network-centric' warfare. They argued that the EIP was not a space as such, but an instrument of real-time command and control created through unified databases, networks, command posts, common C2 software and information—a Universal Automated Command and Control System (UASUV). This system could be used to command anything from a battle up to a whole conflict. Despite utilizing elements of NCW, it is clear Orlianskii et al. refuted the ideas of NCW and instead preferred a unified, hierarchical command.[1742] Based on the above ideas, it would seem that the ideas of the EIP and ASU began to coalesce into a comprehensive cybernetic system at least in the minds of some military specialists.

In 2014 Iu. Ia. Bobkov and N. N. Tiutiunnikov, both former employees of the 27th TsNII and currently employed by the private sector, wrote a book called Conceptual basis of building an ASU for the Ground Forces of the AF RF.[1743] Bobkov and Tiutiunnikov argued that Zhukov and Ogarkov had discovered the principles of NCW but that the American model of NCW was not suitable for Russia: it was considered offensive in nature.[1744] Russia had its own theory of command and control based on the cybernetic theoretical work done in the 1970s which would provide a theoretical base for Russian NCW.[1745] Bobkov and Tiutiunnikov proposed, in addition to an asymmetric response (cf. above), that ASUVs should be developed as integrated systems of systems operating in automated or automatic modes. This meant that the EIP of the AF should, in principle, be an integrated ASUV with weapons, forces, and sensors. This EIP/ASUV should be based on multiple reserve communication channels, command posts and strategic-operational countermeasures, i.e. missiles, UAVs and EW capabilities.[1746] Despite their criticism, Bobkov's and Tiutiunnikov's vision was based on the United States' Global Information and Control Network not some imaginary 'Skynet.'[1747]

[1741] Колодяжный, В.В., Кулешов, Ю.Е., Шеховцов, Н.П. Методический подход к совершенствованию автоматизации управления войсками: информационный аспект. Вестник академии военных наук, № 1 (42) 2013, 109-115.

[1742] Орлянский, В. И., Дульнев, П. А., Костенко, А. Н. Универсальная автоматизированная система управления войсками - принципиальное условие успешного ведения сетецентрических войн. Военная мысль, № 12 (2012), 12-20, 18.

[1743] Бобков, Ю. Я., Тютюнников, Н. Н. Концептуальные основы постарения АСУ Сухопутными войсками ВС РФ. М.: Палеотип, 2014.

[1744] Ibid., 27-28.

[1745] Ibid., 31.

[1746] Ibid.

[1747] The replication of the GICN was supported by the military-industrial complex. Скокова, С.И. Сетецентрическая система управления ВС РФ и необходимые меры по ускорению развития АСУ войсками (силами). Вестник академии военных наук, № 1 (46) 2014, 52-54, 52.

S. V. Morozov, O. A. Kudrenko and R. S. Dolin took a more operational-strategic level approach and analysed the requirements of the ASU and EIP of a military district. They noted, among other things, that it should be able to integrate the information resources of the troops (units) in a changing environment where centralized data centres were out of reach. Moreover, it should also enable the exchange of information with other military and security forces (agencies). Morozov et al. used the phrase 'centralized and noncentralized automated command and control' as an expression for the fact that their EIP did not include NCW-type self-synchronizing semi-independent units.[1748] Others also had grandiose visions of ASUs and the EIP, for example, for repulsing aerospace attacks on an operational-strategic level.[1749] On a tactical level, the ESU TZ ASU was defined by others as a multifunctional distributed system built on a single information and technical basis, observing the principles of hierarchy, i.e. compliance with the organizational and staff structures of a tactical unit, openness and simplicity.[1750]

In 2015 a group of scholars from the 27th TsNII proposed a concept for building an information infrastructure for the ASU of the whole Armed Forces which they named a 'corporative automated information system' (KAIS).[1751] It would support territorially separated transmission networks and data centres and be able to flexibly change its functions from peacetime, to times of threat and to wartime. This system of systems should be built on the modern principles of data management (cloud) and virtualized user environments. Its subsystems would consist of computational complexes, data storage, and systems of information security, physical security and maintenance. The KAIS would have a central data centre for providing common AF RF services and its reserve (warm) and secure (cold) nodes and a regional data centre would provide services for regional force groups. The main and reserve data centres should be geographically separated but connected with high-bandwidth connections—making the system disaster-proof. Like the OATsSS concept of E. A. Perov and A.V. Pereverzev, the KAIS concept may have influenced the way the Russian military is now constructing its networks (cf. Chapter 6).

In 2017, M. O. Bets, V. A. Kiselenko and C. C. Orlov claimed that under the Main Directorate for the Development of Information and Telecommunications Technology of the MoD, there already existed a functional Territorially Distributed Disaster-Proof Centre of Data Processing for the AF RF (TrKTsOD VS RF), which was based on cloud-technology and geographically distributed data-centres.[1752] Bets et al. called it 'our fortress in cyberspace' which through the EIP enabled the achievement of information superiority. This 'military cloud' could in the future include quantum

[1748] Морозов, С. В., Кудренко, О. А., Долин, Р. С. Основные направления развития автоматизированных систем управления военного округа. Военная мысль № 4 (2018), 29-34.

[1749] Грудинин & Майбуров 2018.

[1750] Анохин, Д. В., Зинатуллин, И. Р., Царелунга, В. В., Сафонов, В. В. О совершенствовании программного обеспечения Единой системы управления тактического звена. Военная мысль, № 4 (2018), 21-28.

[1751] Козичев, В. Н., Каргин, В. Н., Ширманов, А. В., Голошев, С. П. Перспективы создания корпоративных автоматизированных информационных систем военного назначения. Военная мысль, № 20 (2015), 19-32.

[1752] Бец, М.О., Киселенко, В.А., Орлов, С.С. Перспективные технологические направления для развития и совершенствования облачной информационной инфраструктуры Вооруженных сил Российской Федерации. Вестник академии военных наук, № 4 (61) 2017, 74-82.

computers, more advanced tools for managing big data etc.[1753] According to the MoD, this network of military district-based data centres should be operational by 2020.[1754]

People from civilian institutions also had ideas about ASUs in the military or national security contexts. Professor Elena Veduta, Head of the Department of Strategic Planning and Economic Policy for the Faculty of Public Administration of MGU, for example, argued that Russia must avoid the Soviet mistakes of the OGSU but that the 'kibernetik' ideas were in themselves still useful and Russia had the chance to create a kibernetik economy by harnessing the digital revolution and its massive amounts of data.[1755] The Soviet roots behind the 'sovereign Internet' draft law were also noted by the Russian Internet ombudsman Dmitrii Marinichev.[1756] A group of engineers and scholars proposed in 2017 that an automated system of management of decision-making support for complex organizational-technological systems (SPPR ASU SOTO) should be created. It would basically be a national-level military and security monitoring, modelling, forecasting and decision support system. According to the group, Russia would have to create this system if it wanted to remain an independent state.[1757] In a similar nation-level approach, a group of professors and associate professors from the Krasnodar Higher Military Academy presented three different classifications for protecting national information infrastructure. These included: moving physically away from the opponent, controlling impact channels, and controlling the information streams. They judged the first to be outdated in the context of information societies, the second always to lag behind the attacker, and the third to be the most promising. It would be based on some sort of system-to-systems of communications.[1758] Around 2018 intelligent information systems and language processing had entered the discussions on automated systems.[1759] AI could, according to Vasili Burenok, offer adaptability, self-learning and intuition in comparison to static algorithms of ASUs.[1760] Kokoshin has argued that AI could enhance ISR capabilities, situation analysis, filtering of disinformation and even the ability to detect imminent

[1753] Ibid., 76.

[1754] Круглов, Александр, Рамм, Алексей, Степовой, Богдан. Минобороны создает военное облачное хранилище Армия получит распределенную сеть для обработки секретных и служебных данных. Известия, 5 июня 2018 [Online]. Available: https://iz.ru/751658/aleksandr-kruglov-aleksei-ramm-bogdan-stepovoi/minoborony-sozdaet-voennoe-oblachnoe-khranilishche [Accessed: 5th April 2019].

[1755] Ведута, Елена. Цифровая экономика приведет к экономической киберсистеме. Международная жизнь, № 10/2017.

[1756] Cf. Chapter 6. Нелюбин, Николай. От «суверенного Интернета» нет пользы никому. Это просто кипячение океана. Фонтанки.ру 8 января 2019 [Online]. Available: https://www.fontanka.ru/2019/01/08/014/ [Accessed: 5th April 2019].

[1757] Автамонов П.Н., Немыкин С.А., Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. Методологические и методические основы разработки и внедрения интегрированных систем поддержки принятия решений (СППР) в асу объектами военно-государственного управления. Информационные войны №1 (41) 2017, 39-48.

[1758] Maximov R.V., Krupenin A.V., Sharifullin S.R., Sokolovsky S.P. Innovative Development of Tools and Technologies to Ensure the Russian Information Security and Core Protective Guidelines. Вопросы кибербезопасности №1(29) 2014, 10-17.

[1759] Быстров, И. И., Козичев, В.Н., Ширманов, А.В. Концептуальные вопросы создания интеллектуальных информационных систем обработки неструктурированной информации в автоматизированных системах военного назначения. Вестник академии военных наук, № 3 (64) 2018, 114-121; Быстров, И. И., Козичев, В. Н., Ширманов, А. В. Автоматизированная обработка неструктурированной информации в перспективных автоматизированных системах военного назначения: концептуальные основы. Военная мысль № 8 (2018), 54-64.

[1760] Буренок, Василий. США создают для военных нужд искусственный разум нового поколения. чем ответит Россия? ВПК, № 37 (701) за 27 сентября 2017 года.

surprise attacks. Thus, the military-political leadership would be guaranteed maximal situation awareness.[1761]

Official and public national security documents rarely refer directly to ASUs. The Military Doctrine of 2009 mentions the increasing efficiency of command and control as a result of the transition from a strictly vertical command and control system to a global network of automated control systems. It also notes "the creation of basic information management systems and their integration with weapons control systems and complexes of automation equipment for command and control of organs of strategic, operational-strategic, operational, operational-tactical and tactical levels."[1762] The 2014 Military Doctrine repeated the need to create automated systems and stated that one of the characteristics of modern military conflicts was "the increasing centralization and automation of command and control of troops and weapons as a result of the transition from a strictly vertical control system to global networked automated systems of command and control of troops (forces) and weapons."[1763] The Information Security Doctrine of 2016 mentions as one of directions of the national information security the improvement of the automated command and control systems of the military.[1764] Arguably, ASUs have a distinct presence and role in the national security documents as integral instruments of national power.

To summarize. ASUs, ASSs and ASUVs are inherently Soviet and Russian concepts. They make concrete the idea of systemic and centralized control of complex systems. As has been shown in Chapter 4 and here, these systems could be military, economic or societal. Arguably, the ASUs and cybernetic ideas behind them have influenced the Russian civilian and military thought on information security issues emphasising centralization, systemization and hierarchy. As the theory dictates, there must be a subject of control to affect the object of control through various sub-systems and feedback channels to achieve designated goal.

ASUs have been conceptualized as tools but also as infrastructure and later as universal systems combining control mechanisms with the space in which they are used. Their function is based on the automation of parts of the 'cycle of command' but not on displacing humans from the loop, yet. The concept of AIs and related technologies is just starting to penetrate the discussions in the military journals and information security communities in Russia. It is conceivable that this new technology will change the whole concept of ASUs and perhaps even lead to their rejection. Thus, ASUs have been seen in the texts analysed here as a Russian solution to NCW, but their applicability has also been questioned. Perhaps the most contested issue has been the relationship between the EIP and ASUs, as the former has incorporated ever more elements into itself and the latter has perhaps suffered from its legacy definitions which are hard to combine with modern ICT concepts. The essence of the Russian theory on ASUs, in contrast to NCW, was expressed in terms of its Soviet roots as a 'cycle of command and control' and a systemic and/or cybernetic approach. It can be argued that the whole idea of ASUs is implicitly centralized and vertical. They are meant as a support for the commander who makes the decisions. ASUs provide forecasts

[1761] Кокошин 2019.
[1762] Указ Президента РФ 2010.
[1763] Доктрина 2014.
[1764] Указ Президента РФ 2016b.

but are at best only semi-automated. Creativity is a trait and property of the human commander.

ASUs are also inherently connected to the function and tasks of the organization they are tailored to support and the environment in which they are supposed to operate. Therefore, ASUs are not purely technological concepts, and because of this they shape the environment in which they are deployed. Moreover, they are connected to the historical principles of command: efficiency, readiness, stability, reliability, secrecy and, flexibility and mobility. Thus the principles of ASUs and the 'cycle of command' form a self-replicating triangle. ASUs affect the way in which command and control is organized and have perhaps increased the tendency to emphasise resilience and continuity as a factor of information superiority instead of speed and totality of information. The idea of ASUs influences the idea of EIP which thus becomes a system-of-systems, i.e. a space created, maintained and controlled by automated systems. This entity can be protected by moving away it away from the threat, removing the source of the threat, controlling information channels including setting barriers, controlling information itself, and through self-modification.

5.10 Cyber power and the life of strategic cultural ideas

Based on the above analysis of strategic cultural ideas it can be argued that although the Russians do not use the terms of cyberspace, cyber power or cyber warfare they have an understanding and concepts for these real phenomena. Below I offer one interpretation of this understanding. I start by first examining the relationship of the Russians concepts of military power, policy, strategy and doctrine, so that I can interpret cyber/information-technological issues through them.

The current version of the Military Dictionary defines military power as "(defence power, defence might), the power of state (a coalition of states), its ability to influence other political actors, the system of international relations through indirect (through demonstration) or direct use of the means of armed violence, and the successful conduct of armed warfare."[1765] This power is based on the geopolitical situation of the state, its territory and population, and the ability to mobilize material and immaterial resources. Potential, according to V. V. Kirillov, consists of the material and spiritual resources that might be mobilized. Potential has different forms such as military, scientific, economic etc. The relationship between potential and power is one between opportunity and actualization.[1766] Military policy is related to potential and power and is defined in the Military Doctrine as "the activity of the state in organizing and implementing defence and ensuring the security of the Russian Federation, and also the interests of its allies." It includes deterrence, prevention of military conflicts, development of the armed forces, and increasing the mobilization readiness of the country.[1767] Military policy is related to countering both internal and external threats to

[1765] 'Военная мощь'. Военный энцикаопедический словарь. М.: Воениздат, 2007 [Online]. Available: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=4337@morfDictionary [Accessed: 5th April 2019].

[1766] Кириллов, В. В. Военная мощь государства: сущность, структура, проблемы. Военная мысль, № 9 (2005), 2-12.

[1767] Доктрина 2014.

independence, integrity, and sovereignty of the state, and to the sustainment and development of the military organization of the state.[1768] Strategy has been quite consistently defined as the highest part of the military art and the practice of preparing the country and armed forces to war, of planning the conduct of war and strategic operations through and conducting those operations with a later addition of preventing war. Strategy has interactive relationship with politics and doctrine.[1769] Doctrine is a codified and relatively compulsory guidance based on the laws of military science and the analysis of current and future politico-social and technological situation.[1770]

To summarize then, military potential consists of all material and spiritual resources that can be mobilized as military power through a state's military policy. Strategy utilizes military power by planning, organizing, and conducting the use of force by utilizing forces, means, forms and methods. Military policy builds potential and creates possibilities for taking action, whereas military strategy plans the actual conversion to power and enables the use of that power as force if necessary. Doctrine provides guidance on preparing for war and on conducting it. The substance of policy and strategy arguably overlap and the adoption of the above discussed concept of strategic planning might have been an effort to address this issue.

No commonly accepted or widely shared Russian concept of information or cyber power is available in open sources. Russian scholars have, nevertheless, provided some definitions. Rastorguev mentions the potential resources of systems to affect each other.[1771] The power of state (state understood as a system) is defined by the quantity of its elements and their functional possibilities and the capability of the system to reproduce itself. Despite his formal logical and mathematical approach, Rastorguev emphasized the importance of creativity.[1772] Kruglov argued that only through the management of information, intellectual potential, and other resources better than potential rivals, could a state prevail.[1773] Tsyganov and Bukharin are more interested in controlling systems of information confrontation than power or potential. Still, in the context of cybernetic models, control is power.[1774] Panarin mentions information-psychological potential of a nation and defines it as the ability to control information flows and to create a civilization. He also mentions scientific-technological, intellectual, and creative potential, among others.[1775] Makhmut Gareev has emphasized the unity of people and moral forces in addition to the technological and scientific potential of the state.[1776]

[1768] 'Военная политика'. Рогозин, Д. О. (общ. Ред.) Война и мир в терминах и определениях [Online]. Available: http://www.voina-i-mir.ru/article/64 [Accessed: 5th April 2019].

[1769] 'Стратегия'. Гречкоб А. А., Огарков, Н. В. (Гл. ред.) Советская Военная Энциклопедия, Том. 7(8). М.: Военное издательство Министерства обороны СССР, 1976—1980, 556; 'Стратегия'. Военный энциклопедический словарь в 2 томах (ВЭС). / Редкол.: А. П. Горкин, В. А. Золотарев, В. М. Карев и др. М: Большая Российская энциклопедия; Рипол классик, 2001, 607-608; 'Стратегия' Военный энцикаопедический словарь. М.: Воениздат, 2007 [Online]. Available: http://encyclopedia.mil.ru/ encyclopedia/dictionary/details.htm?id=10395@morfDictionary [Accessed: 5th April 2019].

[1770] Lalu 2014, 331; Forsströn 2019; 'Военная доктрин'. Рогозин, Д. О. (общ. Ред.) Война и мир в терминах и определениях [Online]. Available: http://www.voina-i-mir.ru/article/74 [Accessed: 5th April 2019].

[1771] Расторгуев 1999, 144.

[1772] Ibid., 169; Расторгуев 2014, 24.

[1773] Круглов 2006 & 2006.

[1774] Цыганов & Бухарин; Бухарин & Цыганов.

[1775] Панарин 2003 & 2006.

[1776] Гареев 2016, 2017a, 2017b & 2018.

Manoilo et al. mention information-communication potential which enables information imperialism. This potential consists of intellectual, technological, spiritual and scientific potential, but also the ability to manipulate information in relation to others.[1777] For Novikov the ability of systems to influence each other was based on resources, i.e. capabilities to manipulate information.[1778] Griniaev approaches information potential through a geopolitical lens and argues that it is something that can be measured and compared and translated into power rivalling nuclear and conventional military power. This potential must be created already during peacetime and mobilized into power very rapidly if a war is to be won because information superiority will be a decisive factor in future wars.[1779] Rastorguev and Manoilo refer to V. N. Ustinov who seems to have been one of the first modern-era Russians to write about information power. According to secondary sources, Ustinov saw information war as the use of information and information technology against military and civilian cybernetic systems. Power would thus be based on information and information technology.[1780] The cyber diplomats of the MGIMO considered Russia's place in the global information society to be based on scientific and educational potential, quality of information infrastructure, the level of the development of electronic business and commerce, and electronic government. These were all measurable qualities.[1781] The strategic planning documents of the Russian Federation also acknowledge the importance of developing the scientific-technological, economic, human and spiritual resources of the state and thus the potential of information power.

Power is an abstract idea. If one would attempt to form some sort of synthesis of the Russian idea of cyber or information power based on the ideas analysed above it would include at least the following elements: power is control over systems, flows, information and the opponent; power is continuity, effectiveness, efficiency, resilience (reliability and stability), flexibility and secrecy; and power is scientific, technological, creative, spiritual, economic, and human potential. It has a function, principles and resources. This power is state power. It is both an end and means, as the protection of state interests, especially sovereignty, has been the paramount principle of the Russian foreign and security policy from the late 1990s. Power is relative and measurable, with value only in relation to the power of others and it is inherently volatile as it can be undermined, negated, and changed through creativity and technology. Power is not directly proportional to material resources or spent wealth because asymmetry can be created through human will, innovation, and the forever changing substance of information itself. Power has both a qualitative and quantitative character. Thus, power is always in flux and the interstate information struggle is a permanent feature of great power relations. Absolute parity is a mirage but stability and balance as a condition can be achieved. Therefore, the Russian understanding of information power is decidedly material and corresponds to the theoretical definition of power

[1777] Манойло, Петренко & Фролов 2012, 80 & 107.
[1778] Новиков 2013, 51.
[1779] Гриняев 2004, 13.
[1780] Сативалдыев Р. Ш. Противодействие информационной войне как предметное содержание информационной функции государства. Правовая жизнь, Январь – март 2017, № 1 (17) [Online]. Available: http://www.tnu.tj/Hayoti%20huquqi/PZh_1_2017.pdf [Accessed: 16th March 2019]. Original cf. Устинов В. Н. Информационная мощь в стратегии национальной безопасности и проблемы информатизации российского общества. РИСИ. М., 1996.
[1781] Зиновьева 2011

proposed in Chapter 2 and 3. Information-technical (cyber) power is a component of information power, more material, more connected to technology.

The Russian views on cyberspace are much clearer than on power. Cyberspace is viewed as an information infrastructure composed of information, systems, and resources and sometimes of users—although then it is a sphere of action and not a space. It is penetrated by power, the relationships of subjects and objects. It is as material as electromagnetic emissions can be and, thus, has borders. It forms the basis of the information space, which includes the substance of information, human minds and societies. It is sometimes called information-telecommunications space to highlight its most important function which is the transfer of information. The Russian understanding of this space and its principles and laws are very similar to those proposed by foreign scholars.

The Russian understanding of information warfare is ambivalent. As previous studies have shown, and the analysis in this chapter has confirmed that the Russian view of information-technological warfare is very similar to Western understandings of cyber warfare. Nevertheless, computer attacks are only one element of information-technological warfare—electronic warfare, exotic weapons, and kinetic force directed against information systems are also included. Cybernetic ideas and systems theory give the Russian approach to cyber warfare its distinct character as does the distinction between geopolitical information confrontation and operational-tactical warfare. Yet, the intentional use of different terms should not obfuscate the fact that the reality of cyberspace is the same for all who operate in it.

Neither official nor unofficial Russian sources refer to the concept of a cyber strategy. The Information Security Doctrine of 2016 is the closest official document to such an effect. It defines threats, interests, general objectives, and organizational responsibilities but it does not prepare or plan, or 'do' anything in that regard. Russian cyber strategy is part of the strategic planning process, and its implementation is dispersed into multiple processes and documents as will be demonstrated in the next chapter. It is inherently connected to the wider information sphere, and the creation of economic, technological and even cultural power—and guided by the Russian understanding of the strategic environment and its threats.

What then can be said about the change and continuity of the strategic cultural ideas? The interstate and class struggle have changed from there Soviet era ideological forms to a geopolitical great power issue, and the information struggle has become one of its main manifestations. Based on official documents and statements it has retained its place in the minds of the Russian elites quite persistently—perhaps excluding short periods in the late 1980s and early 1990s. The Western ideas of deterrence were introduced to Russia in the 1990s through civilian academicians and they were accepted as part of the national security thinking by 2000. Nevertheless, they have also morphed into strategic deterrence—to an almost grand-strategy-like national policy concept. This has been promoted by the military from 2006-2008 onwards and it involves all spheres of life and the whole state and society and it has contributed to the evolution of the whole-of-state strategic planning. Preserving the balance of power and stability, prevention of war, deterrence, and defence now form a systematic, although sometimes, ambivalent group of ideas defining the interests of the state.

The asymmetric response was discovered in 1986 and then rediscovered multiple times as a tool to balance Russia's obvious weaknesses in the peer to peer competition. Its roots are arguably in the Russian tradition of stratagems and cunningness. Its cost-effective, measure to counter measure dialectic has remained the same, but its means and methods have changed with the character of war. Although scholars have offered different applications of asymmetric responses from the late 1990s, the elites have employed the idea more sparingly. Asymmetry has acquired two distinct manifestations: tactical and operational actions and strategic and national responses. Both have found substance in indirectness, creativity, information, and technology. Although, asymmetry has become a semi-official part of military doctrine it has not yet become an accepted part of the codified language of strategic planning.

Digital or information sovereignty was developed after 1999 from the idea of territorial state sovereignty which has roots in the Soviet era and beyond. It has changed from sovereignty over the information space to sovereignty in the information space and in the end to information or digital sovereignty. The concept had become by 2017 an officially recognized, although poorly defined, aspect of state sovereignty. Sovereignty has been tied to the concept of the national segment of the Internet which has developed into the territorial basis of digital sovereignty. The RuNet has become its socio-cultural reflection. Digital sovereignty is Russia's response to the global quest to define cyberspace.

The unified information space was first introduced in the late 1950s as a Soviet kibernetik dream. During the 1990s it rapidly changed from an idea of open and shared information flows to technological and organizational concepts of building the national information space. The elites (re)adopted the idea of EIP already in the mid-1990s but it has been resurrected and redefined multiple times after that. It has retained its roots in the cybernetic dreams of the Soviet scientists but also incorporated modern concepts and technologies which have their own rules and principles of information management. Both its military and civilian versions are based on vertical control and horizontal integration, centralization, and delimitation of borders. Its latest incarnations from the early 2000s onwards include visions involving a system of systems for controlling the national information space as part of digital sovereignty.

The idea of information superiority was already discussed by the Soviet military theorists in the 1970s and 1980s—although its substance was a bit different than it is today. Since 1991, information superiority has become a central concept in Russian security thinking explaining why things are as they are. However, it has also offered solutions for changing the balance of power at least from 2006–2008 onwards in the context of the military reform. It has, perhaps more than any other idea analysed here, changed the way Russians perceive competition, warfare, and power in the international system. Therefore, it also has two interconnected manifestations: one related to warfare and the other to interstate struggle. Information superiority was accepted by the military as a defining principle quite early in the 2000s but in national strategic documents it did not appear until 2016.

The distinction between information-technological and psychological warfare was an almost instinctive definition offered by the Russian academicians in the early 1990s. After that, these aspects have retained their distinct natures but have also changed with the times. Information-technological warfare has interacted with the Western ideas of NCW, CII and cyber warfare. It has perhaps been left in the shadow of psychological ends, ways, and means but has also developed its own distinct Russian character with a definite role in achieving politico-military goals. The distinction between the psychological and technological aspect has been accepted and used by the elites from 2000 onwards although the umbrella term of information warfare or confrontation has been more popular.

Perhaps the most consistent and constant idea has been the ASU. The idea was developed during the Soviet times and different concepts built around it are still in use. It has required an official status and has been defined in the official state standards. ASU's cybernetic heritage has affected other ideas by producing ideas about systems versus systems warfare and a system of systems in the information space. However, the ASUs themselves are now facing flexible, self-controlling, mutating, deep learning AIs which might doom the idea into the dust bin of history—or create a basis for new scientific breakthroughs based on a Russian way of thinking.

The ideas analysed above have been quite widely shared in the texts of officials, officers, academicians, and journalists representing different institutions. Thus, it can be argued that there is a group of people sharing a certain set of common ideas. Nevertheless, these people do not have the same interests or agendas. The Academy of Military Sciences strives to set guidelines to the military academic discussion about military theory and has some latitude in proposing new ideas but is nevertheless under the oversight of the General Staff. The Centre for Military Strategic Studies of the General Staff and the Military Academy of the General Staff and its departments with their mandates on strategic planning and forecasting represent a more official view on military security issues. In this context their representatives can and will take contrary views on certain issues proposed by retired officers and academicians. The different TsNII(I)s of the MoD usually pursue more limited agendas and quite often their researchers promote solutions to problems that would bring resources to their institutions. Similarly, the military training centres and academies of various services and branches have their own agendas but also take part in the more general discussions. Although there are many institutions, the group of officers and scholars writing about strategic issues is rather small.

The non-military authors and scholars publishing in various civilian and military journals form a network, but it is highly suspect as to whether they form any sort of community with professional ethos, values or agendas. Nevertheless, there are some groups that can be called communities such as the ex-KGB information and cryptography professionals including Rastorguev, Manoilo, and Strel'tsov. Another group of Russian military and cyber diplomats is tightly connected to this group. There is some evidence to support the claim that the group of information security specialists which was formed around 1995-1997 under the Security Council has, in fact, formed a very influential community, some members of which have become part of the elite. This group is now established institutionally as the NAMIB. Moreover, many of the so-called civilian academicians working in civilian research institutions have military backgrounds. Thus, the Russian information security academia is highly penetrated by ex-military and ex-special services personnel, which might explain some of commonality of the shared ideas. Another explanation is the prevalence of systems theoretic thinking in Russian academia.

Based on the analysis of journals, monographs and national security documents between 2000–2018 it can be argued that the strategic cultural ideas of the communities have reached the elites. However, it is possible that the ideas had already been held by the elites and that the communities might have been echoing the ideas of the regime to gain resources. The early discussion about information warfare before the initiation of the 1998 UN norm-building initiative and the adoption of the first Putin era national security documents in 2000 was perhaps the purist example of an epistemic community offering ideas to the elites. However, many of those who took part in the discussions represented security elites themselves or were ex-members in academic guises. After the 2000 Information Security Doctrine had made information warfare and threats a legitimate subject of national security discussions, Russian civilian and military scholars produced large amounts of literature on the subject. Their ideas were reflected in the 2009-2010 national security documents and more strongly in 2014-2016 strategic planning documents. However, many of the writers concentrated on providing substance to the basic ideas that had been adopted already in 2000 and not so much on arguing for completely new ideas or radical changes. Every political system has its own characteristics, and the way in which ideas move between the academia and the decision-making elite points to a certain characteristic of the Russian system. Some of these will be examined in the next chapter.

6

THE RUSSIAN NATIONAL SEGMENT OF THE INTERNET

This chapter examines the Russian policies concerning cyberspace. It continues to provide answers to the thesis' research problem's analytical part by asking: How have the strategic environment and strategic cultural ideas given reason to the Russian strategy of shaping and controlling a part of cyberspace into a national segment of the Internet? I begin with an analysis of the environment in which the Russian security and military policy decision-makers have operated between 2000 and 2019. Firstly, I analyse how the Russian segment of Internet has developed, and then I explore the wider international environment and its cyber security aspects to gain an understanding of the Russian elite's strategic environment to demonstrate that there was a real and significant change in its nature during the time period under analysis. Secondly, I examine the different actors taking part in the process of making and implementing strategy to better understand how Russian cyber strategy is made. I will also examine the international treatises and the early policies and laws of 2000–2011 to understand how Russian elites tried to manage cyber and information issues before 2012. Thirdly, I will analyse the strategies, policies and laws that have been formed by the Russian government to tackle the new security issues brought forth by the changes in the strategic environment after 2011. Fourthly, I will examine the civilian and military information systems and networks that the Russian regime is building or directing the private sector to build. Fifthly, I will present a model of the Russian national segment of the Internet as a system of systems in a continuum of interstate relations to understand how a closed national network could function.

My main argument throughout this chapter is that in the 2011–2012 period and then again in 2014 the Russian elites perceived a clear, new, and threatening change in Russia's international environment which required 'fitting' new and old strategic cultural ideas to find ways to reasonably answer the new challenges. This has led to a reasonable adoption of policies and laws which will form a national segment of the Internet that can be considered as a manifestation of a theoretical closed national network. This national segment is Russia's answer, which has distinct Soviet roots, to the challenges of digitalization and the threats emanating from cyberspace.

6.1 The environment

The development of the Internet in Russia and the birth of RuNet were discussed briefly in Chapter 5. This chapter will examine the penetration of the Internet and its services amongst Russian society, the development of the information infrastructure and services, and the importance of digital economy between 2000–2019. Then Russia's position in the international system is examined in order to understand how the Russian decision-making elites might have perceived the strategic environment between 2000–2019. This analysis is complemented with an analysis of the developments in the cyberspace. The chapter ends with a discussion on whether there is enough evidence to argue that a change in Russia's environment required the fitting of new and old ideas and if the strategic cultural ideas examined in Chapters 4 and 5 helped the elite to make sense of the situations and thus guided it towards reasonable solutions.

6.1.1 Development of the Russian Internet and the information society

The Russian Internet was born out of a territorially disconnected group of networks operated by scientific institutions, small IT companies, and regional telecom operators during the 1990s and began to really develop only after the economic crisis of 1998.[1782] The penetration (percentage of users of the Internet in the population) of the Internet in 2000 was only 2.1% and the Internet had just spread to cover most of the big cities and mainly the European part of Russia.[1783] However, the Russian Internet began to develop rapidly so that in 2007 the penetration was approximately 20.8%, and then in 2008 it was 25%, in 2009 33%, 2010 37%, 2011 44%, 2012 53 %, 2013 57%, 2014 67%, 2015 70%, 2016 71%, 2017 73% and in 2018 it was 75.4%.[1784] Thus, the fastest growth rate was experienced from 2001–2008 but the use of the Internet became socially and politically significant only since 2011–2012. In 2000 Russia was behind almost all the advanced industrial countries in the usage of the Internet and by 2018 it was still behind the Western countries and China, where the penetration is around 90%.[1785] Russia has followed global trends in the mobile use of the Internet which covered 59% of the population in 2017 or 73 million people and the number of those using just the mobile Internet surpassed desktop users in 2017. Around 50–60% of the population depending on the region have a desktop computer or a mobile phone.[1786] Mobile phones began to spread in Russia around 2011–2013.[1787] Russians seem to rely more on mobile data connections than on fixed broad-band connections, the development of which has stalled after 2010–2012.[1788]

The first and still functioning Russian non-state conference on the Internet—the Russian Internet Forum—was convened in 1997.[1789] Although the Rambler.ru search engine was launched in 1996, the first online store (Ozon) had opened in 1998, the email

[1782] Перфилев 2003, 44-45.

[1783] Internet World Statistics [Online]. Available: https://www.internetworldstats.com/euro/ru.htm [Accessed: 10th April 2019]; Перфилев 2003, 48, 53.

[1784] GfK. Исследование GfK: Проникновение Интернета в России, 15 января 2019 [Online]. Available: https://www.gfk.com/ru/insaity/press-release/issledovanie-gfk-proniknovenie-interneta-v-rossii-1/ [Accessed: 10th April 2019]; ФОМ. Интернет в России: динамика проникновения. Зима 2017–2018 гг., 04 Апреля 2018г [Online]. Available: https://fom.ru/SMI-i-internet/13999 [Accessed: 10th April 2019].

[1785] РАЭК. Интернет в России в 2017 году: Состояние, тенденции и перспективы развития. М.: Типография «Форвард Принт», 2018 [Online]. Available: http://www.fapmc.ru/rospechat/activities/ reports/2018/teleradio/main/custom/0/0/file.pdf [Accessed: 10th April 2019].

[1786] РАЭК. Экономика Рунета 2018. РАЭК, 2019 [Online]. Available: https://raec.ru/upload/files/ruec_booklet.pdf [Accessed: 12th April 2019].

[1787] РАЭК. Экономика Рунета 2015–2016 [Online]. Available: http://files.runet-id.com/2016/presentation-research/presentations/EconomicaRunetaItogy2016.pdf [Accessed: 10th April 2019].

[1788] Федеральная служба государственной статистики. ониторинг развития информационного общества в Российской Федерации [Online]. Available: http://www.gks.ru/wps/wcm/connect/rosstat_main/ rosstat/ru/statistics/science_and_innovations/it_technology/ [Accessed: 10th April 2019]; Mediascope. Аудитория интернета, 21.11.2018 [Online]. Available: https://mediascope.net/upload/iblock/ea0/ RIW2018_I-Ishunkina_21.11.2018.pdf [Accessed: 10th April 2019].

[1789] Wikipedia. Российский интернет-форум. Wikipedia [Online]. Available: https://ru.wikipedia.org/wiki/ Российский_интернет-форум [Accessed: 10th April 2019].

service Mail.ru started in 1998, and the first Internet magazine Lenta.ru had begun to operate in 1999, at the beginning of the 2000s Internet news services and the online economy were still a marginal phenomenon in Russia. They began to develop rapidly around 2001.[1790] The Yeltsin era oligarchs tried to take advantage of this development but failed as the Putin regime turned against their media empires.[1791] Andrei Soldatov has argued that after Putin met with the leaders of the Internet companies in 1999 a kind of unofficial non-intervention policy between the Internet companies and the regime was agreed. Moreover, the Internet companies managed to block or modify bills directed against Internet freedoms. This arrangement was broken when Putin took a more critical view of the Internet in 2014.[1792]

Around 2010 over 90% of Russians got their news from the television. Thus, John Dunn has argued that the Internet was left outside state control because it served a minority of the population, functioned as a politico-social safety-valve, and promised social and economic benefits for the state.[1793]According to Levada, in 2018 73% of Russians declared that they got their news from TV but the share of Internet webpages and social network was 65% combined (multiple answers were permitted in the survey) and their importance has continuously risen since 2013.[1794] Peterson has claimed that at least until around 2005 the Internet remained a largely apolitical space, so the government had no significant incentive to control it and the IT industry was able to defend its independency.[1795] There is some proof that Russian state television and the Internet currently live in a symbiosis where television sets the agenda and the Internet provides a platform for further discussion and the dissemination of ideas.[1796] Although, social media's challenge to television's monopoly of the news is intensifying, its main impact has been in connecting people from the early 2010s.[1797]

Google and Facebook entered Russia in 2006, the same year that the Yandex search engine was launched.[1798] The Russian social media platforms competed successfully with primarily English-language services and LiveJournal (1999), Ondoklassniki (2006), and VKontankt (2006) had established their pre-eminence by 2012.[1799] This pre-eminence of Russian language social media has been one of the building blocks of the RuNet phenomenon.[1800] Nevertheless, in 2017–2018 Russians quite frequently

[1790] Sodatov & Borogan 2015; Peterson, D. J. Russia and the Information Revolution. Santa Monica: RAND, 2005; Susiluoto 2006; РИА Новости. История развития российского Интернета. Справка, 19 сентября 2011 [Online]. Available: https://ria.ru/20110919/439857350.html [Accessed: 24th March 2019].

[1791] РИА Новости 2011.

[1792] Soldatov 2017.

[1793] Dunn, John A. Lottizzazione Russian Style: Russia's Two-tier Media System, Europe-Asia Studies, Vol.66 No. 9 (2014), 1425-1451.

[1794] ЛЕВАДА-ЦЕНТР. Общественное мнение-2018 [Online]. Available: https://www.levada.ru/cp/wp-content/uploads/2019/03/OM-2018.pdf [Accessed: 26th April 2019].

[1795] Peterson 2005.

[1796] Cottiero, Christina, Kucharski, Katherine, Olimpieva, Evgenia and Orttung, Robert W. War of words: the impact of Russian state television on the Russian Internet, Nationalities Papers, Vol.43, No.4 (2015), 533-555.

[1797] Remmer, Vladimir. The Role of Internet Based Social Networks in Russian Protest Movement Mobilization, Central European Journal of International and Security Studies, Vol. 11, No. 1 (2017), 104-135; ВЦИОМ. А если без интернета?! [Online]. Available: https://wciom.ru/index.php?id=236&uid=116148 [Accessed: 12th April 2019].

[1798] РИА Новости 2011.

[1799] Roesen, Tine and Zvereva, Vera. Social network sites on the Runet. Exploring social communication. In Gorham, Michael S., Lunde, Ingunn and Paulsen, Amrtin (eds.) Digital Russia: The Language, Culture and Politics of New Media Communication. London & New York: Routledge, 2014, 72-86.

[1800] Ristolainen 2017b.

used international services like Google, Twitter, WhatsApp, YouTube, Instagram, Facebook and Wikipedia.[1801] Moreover, the Google Chrome browser (54.5%) and Android OS (49.5%) by far dominate other browsers and OSs.[1802] Chinese social media platforms or browsers are not used in Russia. At least according to LiveInternet, visits from Russian IP -addresses are directed predominantly to Russian language webpages.[1803] Thus, the social media or content sharing aspect of RuNet is technologically not as insular as the idea of RuNet would suggest. Further isolation is favoured by the Kremlin as Putin has, for example, called for the creation of a Russian alternative to Wikipedia.[1804]

Despite its promising start, the IT crisis of 2000 negatively affected the developing Russian Internet industry.[1805] The development of information society seemed to need government support. The Russian government was, however, a bit slow to react to the development needs.[1806] By 2002 the Russian government began to develop strategies on the development of informatization and the electronic government of Russia, and in 2004 the Premii Runet prizes were first awarded. The first prize was given for the development of 'the Russian segment of Internet'.[1807] These early state-led efforts largely failed because of corruption, state-centrism, utopianism, and the lack of leadership.[1808] Not until President Dmitri Medvedev embraced the Internet in 2008–2009 did things start to move forward.[1809] Based on advertisement data, the commercialization of the Internet began around 2011 but it would take additional seven years before the Internet would catch up with television.[1810] According to RAEK's estimations, which are perhaps somewhat optimistic, the share of the Internet economy of the Russian GDP was 1% in 2011, 1.3% in 2012, 1.6% in 2013, 2.2% in 2014 and 2.4% in 2015, and 2.42% in 2017.[1811] In 2018 RAEK decided not to calculate the share of Internet economy but still announced a total of 5.1% of GDP.[1812] In 2018 the Internet

[1801] Mediascope 2018; Alexa. Top Sites in Russia [Online]. Available: https://www.alexa.com/topsites/countries/RU [Accessed: 12th April 2019]; LiveInternet. Statistics – Summary, 5th December 2019 [Online]. https://www.liveinternet.ru/stat/ru/internet/summary.html [Accessed: 5th December 2019]; РАЭК 2019.

[1802] LiveInternet. Statistics – OS, 5th December 2019 [Online]. Available https://www.liveinternet.ru/stat/ru/internet/oses.html [Accessed: 5th December 2019].

[1803] Ibid.

[1804] Роскомсвобода. Большая российская энциклопедия не станет полноценной заменой Википедии, 7.11.2019 [Online]. Available: https://roskomsvoboda.org/51846/ [Accessed: 5th January 2020].

[1805] РИА Новости 2011.

[1806] Ibid.

[1807] Постановление Правительства РФ от 28.01.2002 N 65 (ред. от 09.06.2010) "О федеральной целевой программе "Электронная Россия (2002 - 2010 годы)" [Online]. Available: http://www.consultant.ru/ document/cons_doc_LAW_90180/ [Accessed: 10th April 2019]; Федеральное агентство по печати и массовым коммуникациям приказ от 18 июля 2005 г. № 106 "О проведении открытого конкурса на выполнение работ по подготовке и проведению Второго Конкурса на присуждение ежегодной Национальной премии за вклад в развитие российского сегмента сети Интернет «ПРЕМИЯ РУНЕТА - 2005»" [Online]. Available: http://www.fapmc.ru/rospechat/docs/documents/order/2005/07/fap106.html [Accessed: 11th April 2019].

[1808] Peterson 2005; Susiluoto 2006.

[1809] РИА Новости 2011; Soldatov 2017; Budnitsky, Stanislav and Jia, Lianrui. Branding Internet sovereignty: Digital media and the Chinese–Russian cyber alliance. European Journal of Cultural Studies, Special Issue, 2018, 1-20.

[1810] Ассоциация Коммуникационных Агентств России. Объём рекламного рынка России в 2000-2018 гг. [Online]. Available: http://www.akarussia.ru/node/7849 [Accessed: 11th April 2019].

[1811] РАЭК 2016.

[1812] РАЭК 2019; РАЭК. Рунет подвел итоги года, 13 Декабря 2018 [Online]. Available: https://raec.ru/live/raec-news/10766/ [Accessed: 11th April 2019].

economy was estimated to be worth of 3.9 trillion roubles.[1813] For comparison, Russian arms sales in 2018 were worth 19$ billion and energy revenues were expected to be around 129$ billion from the export of oil and 49$ billion from the export of natural gas.[1814]

The Russian ICT industry has not been able to develop a popular domestic operating-system,[1815] although in 2012 Yandex launched its own browser which has gained around 10-12% share of the searches done in the Russian segment of Internet.[1816] The state has actively supported the domestic IT industry against foreign competition.[1817] The President's Internet ombudsman German Klimenko has even hinted that Microsoft would have to 'leave' Russia because of the restrictions the U.S. government has imposed on the cyber security firm Kaspersky.[1818] Despite efforts to develop the Russian digital economy it has been reliant mostly on Western software and hardware. After 2017 domestic and Chinese software solutions have increased their market share as the IT sector has become the most rapidly growing sector in the Russian economy.[1819] RAEK noted that in 2018 the 'common legislative vector' continues to be prohibitive to the Internet economy and referred to the legal regulations which began around 2012-2013.[1820] The state has tried to support the domestic online economy against the growing influence of foreign companies and Russian banks and Internet companies have allied to finance and establish Russian online market platforms.[1821]

[1813] РАЭК 2019.

[1814] Moscow Times. Russia's Arms Exporter Sold $19Bln Worth of Weapons in 2018, Official Says. Moscow Times 1.11.2018. [Online] Available: https://www.themoscowtimes.com/2018/11/01/russias-arms-exporter-sold-19-billion-worth-weapons-2018-ceo-says-a63380 [Accessed: 12th April 2019]; ПРАЙМ. Доходы РФ от экспорта нефти в 2018 году выросли на 38%, от газа - на 28,8%. ПРАЙМ, 06 Февраля 2019 [Online]. Available: https://1prime.ru/energy/20190206/829687892.html [Accessed: 12th April 2019].

[1815] As Ristolainen has pointed out, the Minister of Telecommunications Nikolai Nikiforov proposed the idea of creating national OS already in 2012 but the idea did not achieve support. (Ristolainen 2017a & 2017b).

[1816] LiveInternet. Statistics – Browsers, 5th December 2019 [Online]. Available https://www.liveinternet.ru/stat/ru/internet/browsers.html [Accessed: 12th April 2019].

[1817] Воейков, Денис. Почему Реестр российского ПО так и не смог запустить в стране импортозамещение. CNews, 24.04.2018 [Online]. Available: http://www.cnews.ru/news/top/2018-04-24_pochemu_reestr_rossijskogo_po_tak_i_ne_smog_zapustit [Accessed: 12th April 2019]; РБК. На Форуме «Российский софт» обсудили национальную кибербезопасность. РБК, 30 Апреля 2019 [Online]. Available: http://presscentr.rbc.ru/page5701909html [Accessed: 17th May 2019]; Жукова, Кристин, Новый, Владислав, Скоробогатько, Денис. Sailfish вносят в бюджет. Государство получило оценки стоимости перехода чиновников на отечественную ОС. Коммерсантъ, №138 от 06.08.2018 [Online]. Available: https://www.kommersant.ru/doc/3706552?from=four_tech [Accessed: 12th April 2019].

[1818] Коммерсантъ. Герман Клименко допустил ограничение работы Microsoft в России. Коммерсантъ, 29.05.2018 [Online]. Available: https://www.kommersant.ru/doc/3643881 [Accessed: 12th April 2019].

[1819] Юзбекова, Ирина. Россия уменьшит зависимость от Америки с помощью серверов из Китая. РБК, 18 августа 2014 [Online]. Available: https://www.rbc.ru/economics/18/08/2014/5424c895cbb-20f353dbe0370 [Accessed: 3rd May 2019]; Жукова, Кристина. Российский софт отключают от заграницы. Требования к отечественному ПО ужесточают в деталях. Газета "Коммерсантъ" №229 от 12.12.2018, стр. 7 [Online]. Available: https://www.kommersant.ru/doc/3827670?from=main_11 [Accessed: 3rd May 2019]; Коломыченко, Мария, Посыпкина, Александра. Иностранным производителям телеком-оборудования решили дать послабление. РБК, 22 января 2018 [Online]. Available:
https://www.rbc.ru/technology_and_media/22/01/2018/5a608cfd9a79477ebc3b3e7f [Accessed: 3rd May 2019].

[1820] РАЭК 2019.

[1821] КонсультантПлюс. К 2025 году Минпромторг России планирует довести долю электронной торговли в общем объеме торговли до 20 процентов, 18.10.2017 [Online]. Available: http://www.consultant.ru/law/hotdocs/51181.html/ [Accessed: 12th April 2019]; АКИТ. Исследование рынка Интернет-торговли в России. Результаты 1 полугодия 2017 года, 28 синтября 2017 [Online]. Available: http://www.akit.ru/ исследование-рынка-интернет-торговл/ [Accessed: 12th April 2019].

The possibilities of a crypto currency have been intensely debated in the Russian media and the government and the Bank of Russia have considered how to regulate them and/or to incorporate them into the official Russian economy.[1822]

The trend of state-led and state-centric innovation policy has affected the whole ICT sector. For example, the techno-park Skolkovo was established by the state in 2011 to copy the success of the Silicon Valley.[1823] It has, however, been called a failure by people involved in the project.[1824] Skolkovo has been subsequently divided into regional centres.[1825] The concept was repeated in 2017 when the state created the Era technology park in Anap for innovative military scientific-technological research, where by 2020, 2000 scientists should be working. In principle Era is supposed to combine civilian and military scientific research with the practical experience and resources of the companies of the military-industrial complex.[1826] The Russian regime has also created the Russian Foundation for Advanced Research Projects in the Defence Industry to mimic the success of the United States DARPA in 2012.[1827] Despite all these state-led efforts, Internet ombudsman Klimenko noted in 2018 that although Russian software was good, everything from the interface level downwards was 'bad'.[1828]

Vendil Pallin has examined the state-ownership of Russian Internet companies after 2013 and argues that in 2014 the largest companies providing Internet infrastructure and services were directly state owned or owned by people connected to the regime.[1829] She makes the same claim about some of most popular Russian websites and social services.[1830] In addition to controlling the Internet and wider ICT industry through ownership, the state uses soft takeovers to transfer companies to trusted ol-

[1822] Известия. Путин считает, что криптовалюты несут с собой серьезные риски. Известия, 10 октября 2017 [Online]. Available: https://iz.ru/656864/2017-10-10/putin-schitaet-chto-kriptovaliuty-nesut-s-soboi-sereznye-riski [Accessed: 12th April 2019]; Аношин, Иван, Петухова, Людмила. Биткоин от дилера: почему россияне не купят криптовалюту без посредника. РВК, 25 января 2018 [Online]. Available: https://www.rbc.ru/money/25/01/2018/5a699d3a9a79471460896e07?from=center_5 [Accessed: 12th April 2019].

[1823] Soldatov & Borogan 2015, 132; Budnitsky & Jia 2018, 12; Susiluoto 2006.

[1824] Сухова, Светлана. "Пропагандой выиграть нельзя. Доминированием в технологиях — можно". Журнал "Огонёк" №40 от 10.10.2016 [Online]. Available: https://www.kommersant.ru/doc/3106914 [Accessed: 11th April 2019

[1825] Едовина, Татьяна "Сколково" обретет всероссийский масштаб Компании из регионов получат льготы и сервисы центра. Газета "Коммерсантъ" №73 от 26.04.2018 [Online]. Available: https://www.kommersant.ru/doc/3614096 [Accessed: 11th April 2019].

[1826] ТАСС. Минобороны РФ увеличит число научных рот в 2018 году. ТАСС, 30 марша 2018 [Online]. Available: https://tass.ru/armiya-i-opk/5080737 [Accessed: 11th April 2019]; ТАСС Путин посетит в Анапе новый военный технополис и проведет итоговое совещание по "оборонке". ТАСС, 21 ноября 2018 [Online]. Available: https://tass.ru/armiya-i-opk/5819998 [Accessed: 11th April 2019]; Сидоркова, Инна. Военное «Сколково»: зачем Шойгу строит технополис в Анапе. РВК, 13 марша 2018 [Online]. Available: https://www.rbc.ru/politics/13/03/2018/5a9e82869a7947860d0516ca [Accessed: 11th April 2019]; Буренок, Василий. Интеллект по призыву. ВПК, № 46 (710) за 29 ноября 2017 года [Online]. Available: https://www.vpk-news.ru/articles/40134 [Accessed: 7th July 2019].

[1827] Коммерсантъ. Госдума приняла законопроект о Фонде перспективных оборонных исследований. Коммерсантъ, 28 сентября 2012 [Online]. Available: https://www.vedomosti.ru/technology/news/2012/09/28/gosduma_prinyala_zakonoproekt_o_fonde_perspektivnyh [Accessed: 17th May 2019].

[1828] Коммерсантъ 2018.

[1829] Vendil Pallin 2017, 22.

[1830] Ibid., 24-27; Soldatov 2017.

igarchs and applies indirect pressure and non-transparent negotiations to affect Internet media companies' policies.[1831] For example, in 2019 a draft law on restricting foreign ownership of Internet resources was first introduced but then withdrawn after the governance structure of Yandex was reformed to enable better control by the Kremlin.[1832] Thus, it can be argued that by 2019 the state presence in and influence on the Internet and IT industry was significant.

The Russian segment of the Internet was unofficially born on April 7, 1994 when the .ru Internet country code top-level domain (ccTLD) for the Russian Federation was introduced.[1833] Later in 2009 the state supported the creation of the .рф domain in addition to .ru and in 2010 approximately three million .ru and 700,000 .рф domain names were registered. By 2019 these figures were five million and 779,500 respectively.[1834] Currently, the Coordination Centre of National Domain of Internet functions as the administrator of the national top-level domains of .ru and .рф and accredits the registrars of these domains. Between 2001–2010 the Coordination Centre created official relations with IANA and ICANN as Russia's representative and with the Ministry of Telecommunications and Mass Media (Minkomsviaz') to establish its position as the national administrator of ccTLDs. In 2010 it also signed an agreement with the autonomous company Technical Centre Internet (TTsI) on the technical operation of the registration system and domain name registries.[1835] TTsI operates two primary ccTLD name servers for .ru, .рф, .su, .дети, and .tatar in Moscow and Saint Petersburg and has subcontracted a network of secondary DNS servers. This network is geographically located in 8 federal districts (okrug) and partly outside Russia.[1836] In 2015 the Minkomsviaz' became a participant organization in the Coordination Centre.[1837] In January 2018 the Coordination Centre relinquished its mandate to operate national domain servers for the state-owned telecommunications company Rostelekom which acquired the TTsI.[1838] This was done in order to ensure "the reliability, stability and resilience of the registry."[1839] Rostelekom had already in 2017 acquired the Safedata group which has the controlling stake in MSK-IX, the first and most important IXP in Russia.[1840] MSK-IX operates a network of 11 .ru and .рф domain name servers in Russia, (Moscow, St. Petersburg, Rostov-na-Donu, Stavropol', Samara, Kazan, Ekaterinburg, Novosibirsk, Vladivostok) and 18 in Europe, Asia, and

[1831] Vendil Pallin., 24-25.

[1832] Seddon, Max. Inside the deal between the Kremlin and Russia's top search engine. Financial Times, December 5th 2019 [Online]. Available: https://www.ft.com/content/dce2e23c-15c5-11ea-8d73-6303645ac406 [Accessed; 5th January 2020].

[1833] Федеральное агентство по печати и массовым коммуникациям. Российскому национальному домену «.RU» исполнилось 25 лет. 08 апреля 2019 [Online]. Available: http://www.fapmc.ru/rospechat/newsandevents/newsagency/2019/04/item4.html [Accessed: 10th April 2019].

[1834] Технический центр Интернет. [Online]. Available: https://statdom.ru/ [Accessed: 10th April 2019].

[1835] Координационный центр национального домена сети Интернет [Online]. Available: https://cctld.ru/ru/about/history.php [Accessed: 10th April 2019].

[1836] Технический центр Интернет 2019.

[1837] Координационный центр национального домена сети Интернет 2019.

[1838] Балашова, Анна, Канаев, Петр. «Ростелеком» стал оператором реестра доменов .ru и.рф. 23 января 2018 [Online]. Available: https://www.rbc.ru/technology_and_media/23/01/2018/5a675ab29a79473a98-2cd704?from=main [Accessed: 10th April 2019].

[1839] Ростелеком. Функции Технического центра Интернет передаются компании «РТК – Центр обработки данных» 24.1.2018 [Online]. Available: http://www.rtk-dc.ru/press/rostelekom-v-voronezhe-prinyal-uchastie-v-kruglom-stole-po-voprosam-bezopasnosti-detey-v-internete8/ [Accessed: 10th April 2019].

[1840] Королев, Игорь. «Ростелеком» поглотил «сердце Рунета». CNews, 06.03.2017 [Online]. Available: http://www.cnews.ru/news/top/2017-03-06_rostelekom_poglotil_serdtse_runeta [Accessed: 10th April 2019].

North and South Africa for the TTsI.[1841] Russia got its first root name server (F) in 2003 and in 2012 an L -server.[1842] Despite the slow start, in spring of 2019 there were 12 root name servers physically located in Russia (Novosibirsk, Ekaterinburg, Moscow, and St. Petersburg) which were operated by ICANN, RIPE NCC, Internet Systems Consortium, Inc., Verisign, Inc., NASA Ames Research Centre, and Netnod.[1843] Arguably, Russia has managed to acquire a reasonable amount of root and ccTLD servers to enable the stability of its networks.[1844] The Russian state now directly or indirectly controls the national segment of the domain name system which is in accordance with the plans laid out by the Minister of Telecommunications Nikolai Nikiforov in 2015.[1845]

The physical infrastructure of the national segment of the Internet has been founded on the national telecommunications network of the Soviet Union. This network consisted of spoke-and-wheel-like constellations around the main population centres along the main railroad lines. The system was complemented by satellite and HF-radio communications in the northern regions and submarine cables to Sakhalin, Kamchatka and Magadan.[1846] Currently, according to publicly available data, the physical infrastructure and ownership of the Russian Internet is the following. In 2018 the length of the backbone network of Rostelekom was 500,000 km and it had cross-border fibre-optic links to Azerbaijan, Belarus, China, Estonia, Finland, Georgia, Japan, Kazakhstan, Latvia, Lithuania, Mongolia, Poland and Ukraine. Its backbone was connected to the domestic MSK-IX and foreign IXPs. The joint stock company (JSC) MTS had 213,000 km of network and it had cross-border connections to Belarus, Finland, Germany, Netherlands, Sweden, Ukraine, and the United Kingdom. Its backbone was connected to the domestic MSK-IX and foreign IXPs. Vimpelcom (Beeline/VEON) had 183,370 km of network which had cross-border connections to Azerbaijan, Germany, Kazakhstan, Netherlands, Sweden and Ukraine. Its backbone is connected to foreign IXPs as it is a multinational telecommunications company. JSC Megafon had 121,100 km of network which had cross-border connections to Azerbaijan, Belarus, Estonia, Kazakhstan, Latvia, Lithuania, Mongolia and Ukraine. Its backbone was connected to the domestic MSK-IX and foreign IXPs. TransTeleKom (TTK), which is part of the Russian Railways, had 78,000 km of network which had cross-border connections to Abkhazia, Azerbaijan, Belarus, China, Estonia, Finland, Japan, Kazakhstan, Latvia, Lithuania, Mongolia, North Korea, Poland, and Ukraine. Its backbone was connected to the domestic MSK-IX and foreign IXPs. The

[1841] MSK-IX. [Online]. Available: https://www.msk-ix.ru/dns/ [Accessed: 10th April 2019].

[1842] CNews. В Москве создан первый корневой сервер имен. CNews, 19.11.2003 [Online]. Available: http://www.cnews.ru/news/line/v_moskve_sozdan_pervyj_kornevoj_server_imen [Accessed: 10th April 2019]; Благовещенский, Антон. В России установлен корневой DNS-сервер. Российская газета, 04.04.2012 [Online]. Available: https://rg.ru/2012/04/04/server-site-anons.html [Accessed: 10th April 2019].

[1843] Root-servers.org [Online]. Available: https://root-servers.org/ [Accessed: 10th April 2019].

[1844] RIPE NCC. Russia Country Report, April 2019 [Online]. Available: https://labs.ripe.net/country-reports/russia-country-report/view [Accessed: 11th April 2019].

[1845] Голицына, Анастасия, Серьгина, Елизавета. Министр связи предложит правительству взять рунет под контроль. Ведомости, 26 марта 2015 [Online]. Available: https://www.vedomosti.ru/technology/ articles/2015/03/26/ministr-svyazi-predlozhit-gosudarstvu-vzyat-runet-pod-kontrol [Accessed: 11th April 2019].

[1846] Перфилев 2003, 56; Росич 2005; Черная, Н.Д. Сети связи. Конспект лекций для студентов заочного отделения Специальности 210406 и 210406у "Сети связи и системы коммутации". Самара, 2008.

rest of the ISPs operate much smaller networks, have only one or two foreign connections, and are mainly connected to domestic IXP networks.[1847] An exception is JSC RetnNet which is a multinational European company with headquarters in the United Kingdom. Its network basically forms a physical and logical peninsula inside the Russian Internet.[1848] According to the Russian self-declared Tier 1 ISPs, the Russian segment of Internet is highly interconnected.[1849]

Russian IXPs are also quite well interconnected.[1850] Based on the cable connections which mainly follow railroads and major highways, and the location of the IXPs, the main nexuses West of Volga are St Petersburg, Moscow, Voronezh, Belgorod, Volgograd, Rostov-na-Donu, Krasnodar, Sochi and Saratov, and east of Volga Kazan, Samara, Perm, Ufa, Ekaterinburg, Chelyabinsk, Tyumen, Kurgan, Omsk, Novosibirsk, Khabarovsk and Vladivostok. Since the 1990s the network has gained resilience as two parallel backbone lines of have been constructed from east to west. Moreover, on the logical level the Russian networks are highly interconnected inside Russian and into Europe. On a physical level there are multiple connections to the Caucasus and Central-Asia although countries in these regions have very limited networks and provide limited global connectivity. On the IXP-level in the east, China and Hong-Kong are the main thoroughfares.[1851] Data on IXPs and cable connections does not, however, tell the whole picture as Tier 1 and 2 ISPs do not always publicly share data on their commercial connections.

There have been plans on the cross-border and international level from 2012 to build a network between the BRICS countries by constructing a submarine cable exclusively between them, although this project seems to have stalled.[1852] Russia is also planning

[1847] The main national ones are: MSK-IX (St.Petersburg, Rostov-na-Donu, Stavropol', Samara, Kazan, Yekaterinburg, Novosibirsk, Vladivostok, Riga), Data-IX (St. Petersburg, Moscow, Samara, Ufa, Yekaterinburg, Chelyabinsk, Khabarovsk, Astana, Kiev, Kharkov, Odessa, Helsinki, Stockholm, Amsterdam, Frankfurt), Red-IX (Irkutsk, Krasnoyarsk, Novosibirsk), CLOUD-IX (St. Petersburg, Moscow, Voronezh, Ekaterinburg), W-IX (Moscow, St. Petersburg, Omsk, Perm', Chelyabinsk , Kiev, Voronezh, Samara, Cheboksary, Kazan, Novosibirsk, Tiumen', Jekaterinburg, Vladimir, Ufa, Frankfurt, Amsterdam, Stockholm, Paris, London, Kiev, Copenhagen), Global-IX (St. Petersburg, Moscow, Stocholm, Helsinki), Piter-IX (St. Petersburg, Moscow, Tallinn). The main local IXPs are: Crimea-IX, EKT-IX (Ekaterinburg), NSK-IX, OMSK-IX (Omsk), TSK-IX (Tomsk), SIBIR-IX (Krasnoyarsk), SMR-IX, SPB-IX, SFO-IX, YAR-IX (Yaroslava), KZN-IX, NN-IX (Nizhniy Novgorod), RND-IX, STW-IX, RB-IX (Ufa), EURASIA-IX (Moscow), SEA-IX (Krasnodar), ULN-IX (Ulyanovsk), VLV-IX, Dataline-IX (Moscow).. Стандард. "Магистральные сети связи в России", Стандард № 9 (188) September 2018 [Online]. Available: https://www.comnews.ru/standart/issue/400 [Accessed: 11th April 2019]; Internet Exchange Map [Online]. Available: https://www.internetexchangemap. com/ [Accessed: 14th April 2019]; PCH Packet Clearing House [Online]. Available: https://www.pch.net/ ixp/dir#!mt-zoom=%5B2.8284271247461907%2C-0.5148480778834943%2C0.06895898910116116%5D [Accessed: 15th April 2019]; ДВДМ.РУ Internet exchange (точки обмена трафиком) https://www.dwdm.ru/ wiki/19 [Accessed: 15th April 2019].
[1848] RETN. Networkmap [Online]. Available: https://retn.net/networkmap/ [Accessed: 11th April 2019]; RIPE NCC 2019.
[1849] ОГО АДЭ. Отчет о фактическом состоянии маршрутизации внутрироссийского трафика через зарубежные сети, 30 ноября 2017 [Online]. Available: http://www.rans.ru/images/news/Traffic_30112017.pdf [Accessed: 5th January 2019].
[1850] ru.map-ix.net [Online]. Available: http://ru.map-ix.net/home [Accessed: 15th April 2019].
[1851] Submarine Cable Map 2018; Кибердемократ. Как можно снизить цены на интернет в Кыргызстане - «Элкат» 11.03.2013 [Online]. Available: http://kiber.akipress.org/news:189 [Accessed: 15th April 2019]; Ростелеком. Магистральная сеть связи [Online]. Available: https://www.company.rt.ru/about/net/ magistr/# [Accessed: 15th April 2019]; Murmanlink. Магистральная сеть [Online]. Available: https:// murmanlink.ru/magistralnaya-set/ [Accessed: 15th April 2019].
[1852] Lee, S. International Reactions to U.S. Cybersecurity Policy: The BRICS undersea cable. Washington: Henry M. Jackson School of International Studies, 2016; Трифонова, Екатерина. Россия предложила разделить

to build an Artic sea cable for military use which would connect Severomorsk and Vladivostok. At the same time Finland and some other countries are planning a similar civilian cable.[1853] Additionally, the CIS has adopted a declaration to create 'a unified information space', although this project too has faced difficulties and is very much uncompleted.[1854] There are also ambitious plans for massive LEO Internet satellite constellations, 5G networks, and Smart Cities.[1855] Many of the state-led projects were in a state of negotiation in the autumn of 2019.[1856] Some more critical voices have claimed that the new infrastructure is being built upon the basis of legacy networks and the regions outside of the main population centres were not being developed.[1857] However, official and semi-official statistics claim that the telecommunications infrastructure is in a relatively good condition across the country.[1858]

Based on the 2019 RIPE NCC report, approximately 3 percent of Russian internal traffic was routed outside its borders in 2019 and that traffic went mainly to Western Europe. Moreover, Russian entities had registered 6,228 ASNs which makes the national segment's connectivity quite robust with many different paths of traffic—at least on the logical level. Russia holds 45.5 million IPv4 addresses from RIPE NCC which are distributed amongst 1927 Local Internet Registries. There were multiple connections between Russian and foreign ASs which supports the claim that there is no monopoly on international IP connectivity.[1859] Russian ASs are highly connected but there are a few central ones. According to one site, the BGP IPv4 neighbourhoods are concentrated in the St. Petersburg and Moscow areas with Rostelekom, TransTeleCom, MegaFon and MTS with the greatest number of neighbours. Southern Russia (Voronezh, Krasnodar, Rostov, Rostov-na-Donu, Tambov, Vladikavkaz), the Volga region (Saratov, Kazan, Samara), the Urals (Perm', Ekaterinburg, Tiumen), Siberia (Nizhnevartovsk, Barnaul, Novosibirsk, Irkutsk) and the Far East (Vladivostok) form their own clusters. ASs registered in St. Petersburg and Moscow offer the most cross-border connections with Voronezh, Rostov, Vladikavkaz, Ekaterinburg, Nizhnevartovsk, Barnaul and Chita following.[1860] Based on cable maps, IXP locations, and BGP routing data, it would seem that the triangle of Nizhnevartovsk, Surgut, and

интернет. Независимая газета, 1 декабря 2017 [Online]. Available: http://www.ng.ru/politics/2017-12-01/3_7127_internet.html [Accessed: 15th April 2019].

[1853] Murdoch-Gibson, Sebastian. Finland's Arctic Data Cable Set to Disrupt Global Connectivity. Asia Pacific Foundation of Canada, June 19, 2018 [Online]. Available: https://www.asiapacific.ca/blog/finlands-arctic-data-cable-set-disrupt-global-connectivity [Accessed: 15th April 2019]; Nilsen, Thomas. Russia plans to lay trans-Arctic fiber cable linking military installations. The Independent Barents Observer April 24, 2018 [Online]. Available: https://thebarentsobserver.com/en/security/2018/04/russia-slated-lay-military-trans-arctic-fibre-cable [Accessed: 15th April 2019].

[1854] Сурма, И.В. Единое информационное пространство СНГ: 20 лет спустя. Вопросы безопасности, № 5 (2015), 41-58.

[1855] Cf. Chapter 6.2.4 & 6.3.1.

[1856] Шмырова, Валерия . «Цифровая экономика» исполняет бюджет хуже всех нацпрограмм, потому что обо всем советуется с бизнесом. CNews, 11.11.2019 [Online]. Available: https://cnews.ru/news/top/2019-11-08_tsifrovaya_ekonomika_ispolnyaet [Accessed: 5th January 2020].

[1857] Хатунцева Е.А., Хатунцев А.Б. Анализ основных тенденций развития сетей связи на телекоммуникационном рынке России. T-Comm: Телекоммуникации и транспорт, Том 10. №7. 2016, 71-74.

[1858] Федеральное агентство по печати и массовым коммуникациям. Интернет в России в 2018 году: состояние, тенденции и перспективы развития [Online]. Available: https://raec.ru/upload/files/190617-fpmk-2019.pdf [Accessed: 5th January 2019]; InfraOne Research. Инфраструктура России: Индекс Развития 2019 [Online]. Available: https://bit.ly/2Fiz4GW [Accessed: 5th January 2020].

[1859] RIPE NCC 2019.

[1860] Runet connectivity [Online]. Available: https://www.ididb.ru/en/runet/bgp.html [Accessed: 15th April 2019].

Noiabrusk in Northern Siberia is a hub for Internet services—although Moscow is clearly the nexus of the Russian Internet infrastructure.

The largest mobile network operators in Russia are MTS (owned by Sistema and oligarch Vladimir Evtushenkov), MegaFon (owned by the USM Group and oligarch Alisher Usmanov), Beeline (owned by VimpelCom) and Tele2 (owned by Rostelecom).[1861] Based on data from the Ministry of Telecommunications in 2019, 2G and 3G networks of every company except Tele2 covered all the big cities and transportation routes in Russia. Tele2 lacked coverage in parts of the Far Eastern regions. 4G coverage was sparser and more concentrated on population centres and western parts of Russia. Only MegaFon and MTS provided service in Novaia Zemlia.[1862] Despite the official statistics, according to (even) Roskomnadzor there was in 2017 a stretch of 400 km in Siberia and the Far East where none of the four mobile operators provided coverage. The problems with mobile connectivity continued in the Far East in 2018.[1863] It should be noted that much of Russia is uninhabited and, therefore, there is no need for fixed telecommunications.

Cloud data storage and services have developed quite rapidly in recent years but according to some sources there is a real gap between supply and demand.[1864] Currently, according to RAEK the biggest data centre providers are Rostelekom with 19 centres on Russian territory (Moscow, Sochi, Novosibirsk, Nizhnii Novgorod, Krasnodar, Ekaterinburg, Stavropol', Kaliningrad, Chelyabinsk, Kazan, Khabarovsk, Ryazan), DataLine with 7 (Moscow), Linxdata-centre with 2 (Moscow, St. Petersburg), Ixcellerate with 1 (Moscow), and Selectel with 6 (Moscow, St. Petersburg, Leningradskii oblast).[1865] In 2018 Yandex launched its own cloud service platform.[1866] Russian private data servers are concentrated in Moscow or the Western part of Russia and it has been left to Rostelekom to establish a nation-wide network of data centres.[1867] There seems to be some cooperation between state corporations to secure connectivity, capacity, and energy-supply for the most critical data-centres, although private companies are, at least in principle, invited to construct data centres providing state services.[1868]

[1861] Wikipedia. Список операторов сотовой связи [Online]. Available: https://ru.wikipedia.org/wiki/ Список_операторов_сотовой_связи#Россия [Accessed: 14th April 2019].

[1862] Минкомсвязь. Качество связи [Online]. Available: https://geo.minsvyaz.ru/#/-1/-1/12/60.16689199-9990966/24.943592000000006/4 [Accessed: 14th April 2019].

[1863] Казарновский, Павел, Демченко, Наталья. Роскомнадзор назвал федеральные трассы с худшей мобильной связью. РВК, 25 декабря 2018 [Online]. Available: https://www.rbc.ru/society/25/12/2017/5a40d9739a794727e1779fd2 [Accessed: 14th April 2019]; Дубов, Григорий, Костина, Екатерина. В Роскомнадзоре ответили на слова Пескова о сотовой связи во Владивостоке. РБК, 12 сентября 2018 [Online]. Available: https://www.rbc.ru/society/12/09/2018/5b994abb9a79473eda33153f?from=main [Accessed: 14th April 2019].

[1864] Балашова. Анна. Мало места большим данным: почему Москву ждет дефицит мощностей. РВК, 06 ноября 2018 [Online]. Available: https://www.rbc.ru/technology_and_media/06/11/2018/5bdc45019a-79472ab0ecdbc2?from=center_2 [Accessed: 14th April 2019].

[1865] РАЭК 2019.

[1866] ТАСС. "Яндекс" запускает собственную облачную платформу. ТАСС, 5 сентября 2018 [Online]. Available: https://tass.ru/ekonomika/5523570 [Accessed: 14th April 2019].

[1867] CNews. Крупнейшие поставщики услуг ЦОД в России 2017. CNews 24.12.2018 [Online]. Available: http://www.cnews.ru/reviews/cloud2018/review_table/6df1a7366926feb538d10f26888ff71d6f0ff9cd [Accessed: 15th April 2019].

[1868] Кантышев, Павел. «Росэнергоатом» начал строить крупный дата-центр. Проектом займется близкая к «Ростелекому» компания. Ведомости, 08 апреля 2015 [Online]. Available: https://www.vedomosti.ru/technology/articles/2015/04/08/rosenergoatom-nachal-stroit-krupnii-data-tsentr [Accessed: 21st April 2019];

Overall, the Russian segment of Internet has been classified as highly resilient to outside interference as it is internally comprehensively interconnected and has multiple physical and logical connections across its borders.[1869] By 2019 over eighty decisions to build ground telecommunications lines from Russia to neighbouring countries had been made.[1870] According to Oleg Demidov and Alena Makhukova the real number could be somewhere around 150-200.[1871] They also claim that the resilience of the national segment was proven by the state level cyber exercise conducted in 2014, although the state ultimately claimed contrary results.[1872]

The information infrastructure and services described above form the basis for 'the information-telecommunications network Internet' of Russia which is recognized by the Russian federal law as part of the Unified Network of Electronic Communications of the Russian Federation. The component parts of this network are the public communication network, separated communication networks (private and closed networks), technical communication networks (industrial management networks), and special networks (networks of government organs including the Armed Forces).[1873] For the sake of clarity the component parts of this network and the different public and governmental information systems are examined in Chapter 6.3.

6.1.2 Development of the international environment

This Chapter will explore Russia's strategic environment in the period between 2000-2018. The main argument will be that in 2011-2014 Russian elites perceived a clear, new and threatening change in Russia's international environment which required the 'fitting' of new and old strategic cultural ideas to find ways to reasonably answer to the new challenges.

There is widespread view among Western scholars of Russian foreign policy that the contours and directions of Russia's foreign policy (RFP) after the Cold War must be analysed in relation to the West or more precisely to the United States.[1874] This approach has produced a view according to which the RFP has been influenced in different times by the 'Westernist' or 'Atlanticist', Statist, and Nationalist or Civilizational

Жукова, Кристина, Скоробогатько, Денис. Гособлако выведут на рынок. IT-системам органов власти подберут операторов. Коммерсантъ, № 68 от 17.04.2019 [Online]. Available: https://www.kommersant.ru/doc/3946062?from=main_12 [Accessed: 21st April 2019].

[1869] This is stated by RIPE NCC 2019; Qrator Labs. 2019 National Internet Segments Reliability Research & Report, 5th September 2019 [Online]. Available: https://habr.com/en/company/qrator/blog/466287/ [Accessed: 5th January 2019].

[1870] Роскомнадзор. Выданные и аннулированные разрешения на строительство, реконструкцию, проведение изыскательских работ для проектирования и ликвидацию сухопутных линий связи при пересечении государственной границы Российской Федерации и на приграничной территории 14.01.2019 [Online]. Available: http://rkn.gov.ru/communication/register/p191/ [Accessed: 18th April 2019].

[1871] Демидов, Олег, Махукова, Алёна. Инфраструктура Интернета в контексте регулирования жизненно важных услуг и критических информационных инфраструктур: обзор международного и российского опыта. CIIP Research, 2016 [Online]. Available: http://s.siteapi.org/808b25df7dd28c9.ru/docs/bf57c0ebec178d0c74fdc875e6ca39925397fd1e.pdf [Accessed: 18th April 2019].

[1872] Демидов & Махукова 2016.

[1873] Федеральный закон 2003.

[1874] Mankoff 2012; Kanet, Roger E. and Piet, Rémi (eds.) Shifting Priorities in Russia's Foreign and Security Policy. Surrey: Ashgate Publishing Limited, 2014; Gvosdev & Marsh 2014; Lo 2015; Tsygankov 2016; Cadier & Light 2015; Donaldson, Robert H. and Nadkarni, Vidya. The Foreign Policy of Russia. Changing Systems, Enduring Interests (6th ed.) New York & London: Routledge, 2019.

schools of thought. Based on the changing fortunes of these schools different chronologies and narratives of RFP have been presented.[1875] I will base my approach on these previous observations, although I will not limit myself purely to the Russia – West relationship as the RFP has been 'multidirectional' at least from the period of Foreign and the Prime Minister Evgenii Primakov (1996—1999).[1876]

Previous studies have given multiple reasons for why the RFP has developed after 2000 as it has.[1877] Continuity is a consistent theme. Before Putin came to power, Russia's relationship with the United States and NATO had soured which produced Evgeni Primakov's foreign policy based on 'multipolarism' or Eurasianism. This was based on the understanding and vision that Russia could not rely on the West's help in reforming itself and would yet again seek the status of a great power to which it was entitled, and thus had 'privileged interests' in Eurasia and Post-Soviet countries. For this reason it would pursue a world based on multiple poles of power in opposition to perceived American unilateralism and hegemony. Primakov thus put the national interest at the centre of the RFP.[1878] When Putin came to power first as prime minister in 1999 and then as President in the spring of 2000 he continued with Primakov's policy—influenced by Western policies, domestic politics, Chechen terrorism, and his own background in the KGB and FSB.[1879]

However, when Vladimir Putin and the new American President George Bush Jr. met in the summer of 2001 and especially after Putin pledged Russia's support for the United States' War against Terror after 9/11 the Russia – U.S. relationship changed dramatically. Western scholars have argued that this turn in Putin's policy was driven by the understanding that by jumping on the bandwagon with the U.S. Russia could pursue its national interests. These included: the fight against Islamist extremism in the Caucasus and Central Asia; economic recovery through integration with the world economy as the U.S. helped Russia to gain access to the G8 and WTO; strategic weapon reductions which were necessary because Russia did not have the resources to keep up parity with the U.S., and the legitimation of great power status through bilateral and equal cooperation with the United States. Putin thus conducted a pragmatic and strategic choice.[1880] The 2001–2002 partnership produced the Strategic Offensive Reductions Treaty (SORT) and enabled the U.S. to withdraw from the Anti-Ballistic Missile Treaty without much opposition from Russia.[1881] This was against Russia's long-term interests, as Russia tried to connect the issues of ballistic missile

[1875] Andrei Tsygankov has defined the RFP based on three distinct traditions or identities, the influence of which has alternated: 'Westernist' which is based on imitation of and belonging to the West and conducting reforms to such effect; Statist which emphasises sovereignty, the centrality of state, the importance to counter external threats and balancing of power; and Civilizational which is based on distinct Russian values, aggressiveness and messianism (Tsygankov 2016, 4-9). Cf. also Donaldson & Nadkarni 2019; Lo 2015; Mankoff 2012; Gvosdev & Marsh 2014; Legvold, Robert. Return to Cold War. Cambridge: Polity Press, 2016; Light, Margot. Foreign Policy Thinking. In Malcolm et al. 1996, 33-100.

[1876] Mankoff 2012; Gvosdev & Marsh 2014.

[1877] For the most recent summaries cf. Tsygankov 2018; Kanet, Roger E. Routledge Handbook of Russian Security. London and New York: Routledge, 2019.

[1878] Tsygankov 2016, 97-101; Donaldson & Nadkarni 2019, 125; Gvosdev & Marsh 2014, 80-83; Mankoff 2012, 95-97; Kuchins, Andrew C. Mismatched Partners: US-Russia Relations after the Cold War. In Cadier & Light 2015, 117-137; Berryman, John. "Fear and Loathing" in the Kremlin. In Kanet & Piet 2014, 51-71).

[1879] Donaldson & Nadkarni 2019, 125; Myers 2015.

[1880] Mankoff 2012; Gvosdev & Marsh 2014; Lo 2015; Tsygankov 2016; Donalson & Nadkarni 2019.

[1881] Gvosdev & Marsh 2014, 86–87.

defence and strategic weapon's reductions to entice the United States to renounce its missile defence plans and thus to preserve strategic parity, restrain U.S. global hegemony, and preserve Russia's status as a nuclear super power.[1882] The partnership also enabled the establishment of the NATO-Russia Council which gave Russia more influence in NATO than the arguably failed Permanent Joint Council (1997–2002) as Russia could take part, within limits, in the internal discussions of NATO.[1883]

There are multiple reasons why Putin's 'strategic choice' failed to produce persistent change and they all contributed to the downward spiral of the Russia–U.S. relationship from late 2002 onwards. Firstly, the United States ignored Russia's economic, status and military interests in attacking Iraq in 2003.[1884] Secondly, the second round of NATO enlargement began in 2002 and was completed in 2004 despite semi-official promises given to Russia in the 1990s to not to expand the alliance. Furthermore, Ukraine and Georgia entered intensified dialogue with NATO in 2005-2006, although they were not ultimately offered membership in 2008.[1885] This brought NATO to the borders of Russia and showed that the NATO-Russia Council did not really give Russia any power to influence NATO decision-making. For the Russian military this meant that the Western military alliance was again a legitimate and potential adversary.[1886] Thirdly, the Bush administration revived the ballistic missile defence programme which Russian military considered a direct threat to its strategic deterrence and great power status.[1887] The issue became even more divisive as the U.S. stated in 2006 that it would deploy parts of the system in Europe and began negotiations with Poland and the Czech Republic in 2007 and concluded agreements with them in 2008.[1888] Fourthly, the Russian regime and the Armed Forces interpreted the so-called 'colour revolutions' in Georgia (2003), Ukraine (2004) and Kyrgyzstan (2005) as Western efforts of regime change under the umbrella of democratization in the Russian sphere of interests. This view was enhanced by the United States' increased military presence in the Caucasus and Central Asia which resonated with nationalistic and civilizational ideas that Russia was yet again being encircled and contained.[1889]
Fifthly, the Russian economy began to recover between 2003–2007 as a result of high energy prices. With a recovering economy also came a more assertive foreign policy as Russia was able to pay off its foreign debts and was able to conduct independent

[1882] Donalson & Nadkarni 2019, 382–383, 406.

[1883] Smith, Martin A. A bumpy road to an unknown destination? NATO-Russia relations, 1991–2002, European Security, Vol. 11, No.4 (2002), 59-77; Gvosdev & Marsh 2014, 101-102; Donaldson & Nadkarni 2019, 262-264.

[1884] Bouldin 2004; Mankoff 2012, 107-108; Gvosdev & Marsh 2014, 87-88; Kuchins 2015; Donalson & Nadkarni 2019, 388-392.

[1885] Blank & Weitz 2010; Mankoff 2012; Gvosdev & Marsh 2014, 100-101; Tsygankov 2016, 108; Donaldson & Nadkarni 2019; NATO. Enlargement [Online]. Available: https://www.nato.int/cps/en/natolive/topics_49212.htm# [Accessed: 29th April 2019].

[1886] Blank 2010.

[1887] Cimbala, Stephen J. The New Nuclear Disorder: Challenges to Deterrence and Strategy. London & New York: Routledge, 2015.

[1888] Lewis, George N. U.S. BMD Evolution Before 2000. In Arbatov & Dvorkin 2013, 51-70; Blank 2008.

[1889] Jackson 2002; Mankoff 2012, 103-104; Donaldson & Nadkarni 2019; Berryman 2014; Tsygankov 2016, 178; Nikitina, Yulia. The "Color Revolutions" and "Arab Spring" in Russian Official Discourse. Connections, Vol. 14, No. 1 (Winter 2014), 87-104; Blank 2010. Whatever the Russian interpretations were, according to Jeffrey Mankoff, the U.S. actively supported the pro-Western Victor Yuschenko in the Ukraine 2004 elections while the Russians botched their own operation to sabotage his campaign. Moreover, the U.S. did eventually position forces in Georgia, Uzbekistan and Kyrgyzstan officially as part of the War on Terror. (Mankoff 2012).

policy in its near-abroad.[1890] Russia began to more vigorously pursue its energy interests by acquiring pipelines and assets in Post-Soviet countries which collided with the United States' interests which had sought access to Russian and Eurasian energy markets.[1891] Moreover, Russia engaged in natural gas price negotiations and even coercion by disconnecting natural gas exports to Ukraine in 2006, 2007 and 2009. This caused a diplomatic backlash from Europe which was dependent on the gas transiting through Ukraine and Belarus.[1892]

Sixthly, the war between Russia and Georgia in August 2008 demonstrated that Russia was willing to use force to protect its interest.[1893] It also pushed forward the long-awaited military reform which (re)started in 2008 and, together with the state armament program initiated in 2010 (GPV 2020), managed to produce a significant change in the Russian Armed Forces' fighting capability by 2014.[1894] And seventhly, various Russian human right violations, fraudulent elections and authoritarian domestic politics were constantly criticized by the United States, the European Union, the Council of Europe and the OSCE unceasingly from the 1990s.[1895] This was a somewhat self-fulfilling process and led to further 'great power assertiveness', mistrust towards the West's 'democratizing' tendencies. It intensified conservative and nationalist domestic policies in Russia and produced policies like 'sovereign democracy' which basically called for freedom from outside influence and control, national control of strategic resources, and state-driven modernization.[1896] Moreover, the Soviet past began to be rehabilitated by Putin which led to consternation in Russia and in the West.[1897] Russian assertiveness was most visibly present in Putin's speech at the Munich Conference on Security Policy in February 2007 in which he argued that the United States mistakenly thinks that it operates in a unipolar world and disregards the basic principles of international law.[1898] Putin's speech produced the first debate about the new Cold War.[1899]

Although Dmitri Medvedev became president before the war with Georgia in May 2008, his term was ultimately characterised by the 'Reset' policy of the Obama administration, the pursuance of economic modernization after 2008–2009 financial crisis, which hit Russia hard, and the search for alternative foreign and economic policy

[1890] The causality of energy incomes to aggressive foreign policy has been challenged, cf. Weber, Yaval. Petro politics. In Tsyganov, Andrei P. Routledge Handbook of Russian Foreign Policy. London and New York: Routledge, 2018, 99-117.

[1891] Mankoff 2012, 32; Gvosdev & Marsh 2014, 86-87; Kuchins 2015; Donaldson & Nadkarni 2019, 158-159; Myers 2015, 281-282.

[1892] Mankoff 2012, 147; Donaldson & Nadkarni 2019, 158–159, 184-192.

[1893] Mankoff 2012, 114; Renz 2018, 144–146.

[1894] Connolly, Richard and Boulégue, Mathiue. Russia's New State Armament Programme. Implications for the Russian Armed Forces and Military Capabilities to 2027. Chatham House Research Paper, May 2018 [Online]. Available: https://www.chathamhouse.org/sites/default/files/publications/research/2018-05-10-russia-state-armament-programme-connolly-boulegue-final.pdf [Accessed: 29th April 2019]; Persson, Gudrun (ed.) Russian Military Capability in a Ten-Year Perspective – 2016. FOI, 2016 [Online]. Available: https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4326--SE [Accessed: 29th April 2019].

[1895] Kuchins 2015; Myers 2015; Tsygankov 2016; Donaldson & Nadkarni 2019.

[1896] Lo 2015, 31-32; Mankoff 2012, 81-82.

[1897] Lee 2015, 207-208.

[1898] Legvold 2016, 105.

[1899] Monaghan, Andrew. 'An enemy at the gates' or 'from victory to victory'? Russian foreign policy. International Affairs, Vol.84, No.4 (2008), 717–733.

directions in China and Eurasia. With hindsight it is easy to argue that although Vladimir Putin stepped aside to become the prime minister his influence on RFP remained strong. However, during Medvedev's term in 2008–2012 this was not so self-evident.[1900] The 'Reset' managed to produce the new START treaty (2010), provided Russian support for a new UNSC resolution against Iran's nuclear program, and overflight permission for the U.S. Afghanistan supply flights. Russia got its WTO membership, freeze on Ukraine's and Georgia's NATO membership process, and peaceful elections in Ukraine which brought to power pro-Russian Yanukovych, and less criticism about Russia's democratic deficiencies but, ultimately, little else.[1901] Medvedev's 2008 proposal on a new European security architecture was practically pushed aside by NATO and the United States.[1902] Economic cooperation on energy or high technology between Russia and the U.S. stalled and remained competitive. The issue of ballistic missile defence was not solved. The 'Reset' did not bring about the convergence of values, threats or interests. Moreover, there was internal political resistance to it in both countries.[1903] However, the Russian economy did recover from the 2008 crisis and performed relatively well up until 2012—2013. Still, the Russian economy remained depended own energy incomes, and structural reforms and modernization were not successful.[1904]

In 2011-2012 the relationship between Russia and the United States turned for the worse. There were multiple reasons, although as Donaldson and Nadkarni have argued, the 'Reset' had only been a tactical measure on both sides and antagonistic interests from 2003-2008 had remained under the surface.[1905] The United States and many European countries were disappointed as Putin declared that he would seek a third term as president. Consequently, the demonstrations first against the fraudulent Duma elections in 2011 and then against Putin in 2012 were supported, at least in spirit, by the West.[1906] Furthermore, the Arab spring, i.e. the demonstrations and revolutions which began in the Middle-East and North Africa in 2011 raised multiple threats to Russia. It was perceived as a Western attempt to spread democracy—not altogether without proof.[1907] It threatened to give power to extremist Islamic groups and increase terrorism. It affected Russian economic interests and threatened authoritarian political leaders which had been ready to do business with Russia. Moreover, the West was ready to bypass Russian interests in handling the issues raised by the events and, thus, marginalize Russia and its status.[1908] Russia considered its fears validated as NATO helped to remove Muammar Gaddafi from power in Libya. As Russia with the support of China vetoed any similar resolutions in 2011–2012 against Bashir

[1900] Lo 2015, 177.

[1901] Gvosdev & Marsh 2014, 93-94; Tsygankov 2016, 215-216; Donaldson & Nadkarni 2019, 426.

[1902] Tsygankov 2016, 217.

[1903] Mankoff 2012, 123; Gvosdev & Marsh 2014, 95.

[1904] Oxenstierna, Susanne. The Russian Economy: Can Growth be Restored within the Economic System? FOI, 2014 [Online]. Available: https://www.foi.se/report-search/pdf?fileName=D:%5CReportSearch-%5CFiles%5C7b0d3cb7-e080-447f-a4e5-2b49d669543f.pdf [Accessed: 3rd May 2019].

[1905] Donaldson & Nadkarni 2019, 426.

[1906] Donaldson & Nadkarni 2019, 426.

[1907] McCarthy, Daniel R. Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet. Foreign Policy Analysis, Volume 7, Issue 1, January 2011, Pages 89–111; Griffiths, James. The Great Firewall of China: How to Build and Control an Alternative Version of the Internet. London: Zed Books Ltd., 2019.

[1908] Donaldson & Nadkarni 2019, 331-333.

al-Assad's regime in Syria, relations with the West became strained.[1909] In December 2011 Dmitri Rogozin claimed that the United States had influenced the uprisings in North-Africa and was waiting for Russia to become weak to do the same to it.[1910]

Putin's 2012 election campaign emphasised Russia's great power status, its Eurasian character, and was quite critical of the West.[1911] Consequently, Russia was used as a threat in the United States' 2012 presidential campaigns, and U.S.–Russia relations soured.[1912] The U.S. Congress passed the Magnistky Act which sanctioned Russian officials based on alleged human rights violations. Russia responded with its own sanctions.[1913] In this heightened state of political rhetoric, the new laws that Russia began to draft and adopt restricting political freedoms in the name of national security were seen as a proof of Putin's inherent authoritarian tendencies.[1914] The way in which Putin presented himself as the defender of national values versus Western depravity and decadence did not lessen the criticism.[1915]

In 2012 Putin was faced with multiple foreign policy problems compounded with demonstrations directed against him, worsening economic performance and an economy still reliant on energy exports, a decaying infrastructure, income inequality and poor public health and burdened by promises of increased social and military spending. Moreover, the United Russia party had been weakened after the election scandal of 2011.[1916] The situation did not get better in 2013 although there were some promising developments and the demonstrations ended in the summer of 2012 after they had been suppressed with a combination of new laws, media manipulation and police operations.[1917] Russia managed to mediate a deal to remove chemical weapons from Syria and took constructive part in the negotiations concerning the Iran nuclear programme.[1918] Arguably, in both cases Russia tried to protect Syria and Iran from the U.S. use of force. The revelations of Edward Snowden on NSA's cyber espionage programme and his consequent flight to Russia in the summer of 2013 gave Putin the chance to present himself as a defender of the freedom of speech.[1919]

When the revolution in Ukraine reached its zenith in February 2014 Russia offered sanctuary for the ex-president, did not acknowledge the interim government, occupied and annexed Crimea, and instigated and supported an uprising in the Eastern parts of Ukraine.[1920] The 2014 change of government in Ukraine was portrayed by the

[1909] Gvosdev & Marsh 2014 313; Averre, Derek. Russia, the Middle East and Syria Conflict. In Kanet 2019, 399–409.

[1910] Donalson & Nadkarni 2019, 426.

[1911] Donaldson & Nadkarni 2019; Lo 2015; Tsygankov 2016.

[1912] Lo 2015, 174–177.

[1913] Cadier & Light 2015, 2; Lo 2013, 176.; Donaldson & Nadkarni 2019, 387.

[1914] Gvosdev & Marsh 2014, 95; Kuchins 2015; Roberts, Karl. The United States. In Tsygankov 2018, 237-253, 247; Stoner, Kathryn E. and McFaul, Michael A. Russian security policy towards the US. In Kanet, 2019, 242-256, 246.

[1915] Trenin, Dmitri. Russian Foreign Policy as Exercise in Nation Building. In Cadier & Light 2015, 30–41.

[1916] Donalson & Nadkarni 2019, 427.

[1917] Treisman 2018.

[1918] Donalson & Nadkarni 2019.

[1919] Soldatov & Borogan 2015.

[1920] McDermott, Roger, N. Brothers Disunited: Russia's Use of Military Power in Ukraine, FMSO, Kansas, 2015; Norberg & Westerlund 2016; Jonsson & Seely 2015; Legvold 2016; Donaldson & Nadkarni 2019.

Russian politicians and media as an unconstitutional coup d'état engineered by extremist and anti-Russian forces.[1921] Although Russia participated in mediating the two ceasefire agreements (Minsk I and II) it has unofficially and covertly supported the Donbass rebels against Ukraine's Armed Forces.[1922] The United States and the European Union have imposed multiple economic and financial sanctions against Russian companies and individuals—to which Russia has countered with its own sanctions.[1923] Moreover, NATO adopted the Readiness Action Plan and the Enhanced Forward Presence policy to enhance its military readiness and deterrence against the possible military threat from Russia.[1924] Furthermore, the EU has adopted the Joint Framework on countering hybrid threats and NATO and EU have agreed to cooperate in the fight against hybrid threats.[1925]

In the autumn of 2015 Russia sent military forces to support the Syrian regime against the rebels and has protected President al-Assad from the Western demands for regime change.[1926] Western accusations of Russia's interference in elections, of covert support for far-right parties, and of other diversionary actions and information warfare in 2015–2018 have further eroded the Russia–West relationship.[1927] Moreover, the Russian economy suffered from a slump and the sanctions in 2014–2015, and its recovery has been slow.[1928] The economic and financial isolation from the West (and Ukraine) has especially hit the high-technology sector.[1929] The import substitution programmes devised to help the economy have been criticised for transferring state resources to non-profitable and rent-addicted sectors.[1930] In 2018 the director of the Federal antimonopoly service called Russian economy 'semi-feudal'.[1931] The Russian economy appeared to stagnate in early 2019 despite government investments through Putin's twelve national projects.[1932] These projects emphasising the 'hand control' of the head of state were accompanied by the discreet normalization of the Stalinist past.[1933]

[1921] Donalson & Nadkarni 2019, 434.

[1922] McDermott 2015; Norberg & Westerlund 2016; Jonsson & Seely 2015.

[1923] Gutterman, Ivan and Grojec, Wojtek. A Timeline of All Russia-Related Sanctions. RFE/RL, September 19, 2018 [Online]. Available: https://www.rferl.org/a/russia-sanctions-timeline/29477179.html [Accessed: 30th April 2019].

[1924] Connolly, Gerald E. NATO @ 70: Why the Alliance Remains Indispensable. NATO Parliamentary Assembly, Report, 12th October 2019 [Online]. Available: https://www.nato-pa.int/document/2019-nato70-why-alliance-remains-indispensable-146-pctr-19-e-rev1-fin [Accessed: 5th January 2020].

[1925] European Parliament. Countering hybrid threats: EU-NATO cooperation. Briefing, March 2017 [Online]. Available: http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf [Accessed: 30th April 2019].

[1926] Lund, Aron. Syria's Civil War. Government Victory of Frozen Conflict. FOI, December 2018 [Online]. Available: https://www.foi.se/rest-api/report/FOI-R--4640--SE [Accessed: 30th April 2019].

[1927] Polyakova, Alina and Boyer, Spencer P. The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition. Washington: The Brookings Institution, 2018 [Online]. Available: https://www.brookings.edu/wp-content/uploads/2018/03/fp_20180316_future_political_warfare.pdf [Accessed: 30th April 2019].

[1928] BOFIT. Venäjä-tilastot [Russia statistics] [Online]. Available: https://www.bofit.fi/fi/seuranta/tilastot/venaja-tilastot/ [Accessed: 30th April 2019].

[1929] Monaghan 2017, 36.

[1930] Ibid.

[1931] Артемьев, Игорь. Экономику России назвали полуфеодальной. Lenta.ru, 25 сентября 2018 [Online]. Available: https://lenta.ru/news/2018/09/25/half_feodal/ [Accessed: 3rd May 2019].

[1932] Aris, Ben. The Russian Economy is Stagnating. GDP growth since the start of the year has been well below forecasts. Moscow Times, May 28, 2019 [Online]. Available: https://www.themoscowtimes.com/2019/05/27/the-russian-economy-is-stagnating-a65760 [Accessed:28th May 2019].

[1933] Братерский, Александр. Путинский взгляд на советских вождей. Газета, 16.6.2017 [Online]. Available: https://www.gazeta.ru/politics/2017/06/17_a_10721567.shtml [Accessed: 11th January 2020].

On the military strategic front, Russia has been unable to stop the deployment of the elements of ballistic missile defence system to Turkey, Germany, Romania and Poland and to the maritime areas near its borders.[1934] The election of the new American President Donald Trump has not brought aid to Russia's situation. The U.S. has accused Russia officially of interfering in its elections, withdrew from the INF treaty in 2018, has declined to cooperate with Russia in the Middle-East, and has accused Russia of interfering in the situation in Venezuela.[1935] Russian military spending has risen between 2011 and 2017 from 3.5% GDP to 5.5% GDP although it fell back to 3.5% GDP in 2018 and it has become the second or third biggest arms exporter. The military expenditure of the U.S. and China have also grown at the same time.[1936] Moreover, both the United States and Russia are modernizing their strategic nuclear weapons, and Russia has introduced new weapons systems to demonstrate the capability to strike the United States.[1937] All this has produced a second debate on the new Cold War.[1938]

The reasons for Russia's actions and its regime's interpretations of the international environment cannot be understood only in the context of the Russia–West relationship.[1939] Russia tried half-heartedly to manage the Post-Soviet space through the Collective Security Treaty (1992) which, however, provided little concrete collective action or cooperation in the 1990s. The treaty was updated to the Collective Security Treaty Organization (CSTO) in 2002 on the initiative of Russia and now includes Russia, Armenia, Belarus, Kazakhstan, Kyrgyzstan and Tajikistan. The CSTO's tasks have developed from the mid to late 2000s to include promoting regional stabilization, addressing non-traditional threats like terrorism, separatism and extremism, and

[1934] Arms Control Association. The European Phased Adaptive Approach at a Glance. January 2019 [Online]. Available: https://www.armscontrol.org/factsheets/Phasedadaptiveapproach [Accessed: 30th April 2019].

[1935] Dennis, Steven T., Brody, Ben and Frier, Sarah. Russia's Bid to Help Trump Revealed as Much Wider Than Once Known. Bloomberg, December 17, 2018 [Online]. Available: https://www.bloomberg.com/news/ articles/2018-12-17/russia-waged-vast-pro-trump-social-media-plan-senate-panel-told?srnd=politics-vp [Accessed: 30th April 2019]; Engel, Eliot and Smith, Adam. US pulling out of the INF treaty rewards Putin, hurts NATO. CNN, February 2, 2019 [Online]. Available: https://edition.cnn.com/2019/02/01/opinions/us-pulling-out-of-the-inf-treaty-rewards-putin-hurts-nato-engel-smith/index.html?no-st=1556603190 [Accessed: 20th April 2019]; Schmitt, Eric and Gibbons-Neff, Thomas. American-Russian Relations in Syria? Less Rosy Than Trump and Putin Claim. New York Times, July 17, 2018 [Online]. Available: https://www. nytimes.com/2018/07/17/world/middleeast/american-russian-military-syria.html [Accessed: 30th April 2019]; The White House. Statement by National Security Advisor Ambassador John Bolton on Venezuela, March 29, 2019 [Online]. Available: https://www.whitehouse.gov/briefings-statements/statement-national-security-advisor-ambassador-john-bolton-venezuela-2/ [Accessed: 18th May 2019].

[1936] During the same time period the U.S. military spending has fallen from 4.5% to near 3% of GDP but in absolute numbers rose in 2012 to 731$ billion to fall sharply but then increasing again to 649$ billion in 2018. China's military spending has been a steady approximately 2% of GDP but total spending has risen from 108$ in 2008 to 249$ billion in 2018. (Legvold 2016; Lo 2015, 166; SIPRI. SIPRI Military Expenditure Database 1949-2018 [Online]. Available: https://www.sipri.org/databases/milex [Accessed: 3rd May 2019]; Oxenstierna, Susanne. Russia's Economy and Military Expenditures. In Kanet 2019, 97-108; BOFIT. Growth in Chinese and Russian arms exports lags growth of other major arms suppliers. BOFIT WEEKLY 2019/11 [Online]. Available: https://www.bofit.fi/en/monitoring/weekly/2019/vw201911_5/ [Accessed: 3rd May 2019]; Kruglov, Alexander. Business booming for Russia's arms trader. Asia Times, April 22, 2019 [Online]. Available: https://www.asiatimes.com/2019/04/article/business-booming-for-russias-arms-traders/ [Accessed: 3rd May 2019].

[1937] Kristensen, Hans M. and Norris, Robert S. Russian nuclear forces, 2018. Bulletin of The Atomic Scientists, 2018 Vol. 74, No 3 (2018), 185–195; Kristensen, Hans M. and Korda, Matt. Russian nuclear forces, 2019. Bulletin of the Atomic Scientists, Vol. 75, No. 2 (2019), 73-84.

[1938] Legvold 2016.

[1939] Mankoff 2012.

providing security guarantees to its members in the event of a conventional war. Furthermore, it has annual exercises, rapid deployment and anti-terrorist forces, and a collective air defence system—at least on paper. For Russia, in addition to creating a Russia-centred normative security zone, the CSTO legitimizes its military presence, and thus a buffer zone, in Post-Soviet countries, especially Central Asia. It also enables force projection and offers balancing tools towards the United States and China. However, practice has shown that Russia's ability to control the organization and receive its member states' political support has been limited in the 2010s.[1940]

After the 2008 financial crisis Russia began to genuinely develop the economic relationship with Post-Soviet countries. A customs union between Russia, Belarus and Kazakhstan was established in 2010.[1941] Consequently, Putin adopted Eurasian economic integration in his 2011–2012 election campaign, and an economic integration road-map was developed in 2013. The creation of the Eurasian Economic Union (EEU) was confirmed by Russia, Belarus and Kazakhstan in May 2014. The EEU was launched in January 2015 and Armenia and Kyrgyzstan joined the same year. However, the EEU has not been able promote trade between its members and has been hindered by internal disputes.[1942] Ukraine's decision to not join the EEU has been a major complication.[1943] By analysts, the EEU project has been variously described as neo-imperial, pseudo multilateralism, new regionalism, and a vehicle of great power geo-economic competition.[1944]

The CSTO and EEU projects are related to Russia's so-called pivots to the East which, according to Natasha Kuhrt, there have been at least three: in 2009, 2012 and 2014. She argues that these pivots have been more reactions to events than voluntary choices and have concentrated on China. Moreover, they have resulted in partnerships more than alliances as Russia has lacked other options. Identity, status and economics have all driven Russia's approach to China.[1945] China's economic and military rise was still viewed suspiciously by the elite during Putin's first term although energy cooperation began to influence the relationship and by Putin's second term the cooperation grew even more important.[1946] During Medvedev's term voicing the idea

[1940] Deyermond, Ruth. The Collective Security Treaty Organization. In Tsyganov 2018, 421–429; Gvosdev & Marsh 2014, 169; Donaldson & Nadkarini 2019, 179–180.

[1941] Cadier, David. Policies towards the Post-Soviet Space: The Eurasian Economic Union as an Attempt to Develop Russia's Structural Power? Cadier & Light 2015, 156-174, 171; Donaldson & Nadkarni 2019, 177-178.

[1942] Molchanov, Mikhail A. The Eurasian Economic Union. In Tsyganov 2018, 410–420; Gvosdev & Marsh 2014, 169; Donaldson & Nadkarini 2019, 197.

[1943] Lo 1995, 184-192; Donaldson & Nadkarni 2019, 184-192.

[1944] Molchanov 2018; Lo 2015, 80-81; Arakelyan, Lilia A. The Soviet Union is Dead: Long Live the Eurasian Union. Kanet & Piet 2014, 141-161; Cadier 2015, 171; de Haas, Marcel. Relations of Central Asia with the Shanghai Cooperation Organization and the Collective Security Treaty Organization. The Journal of Slavic Military Studies, Vol.30, No.1 (2017), 1-16. Although every relationship which Russia has with its neighbours is different, the union-state established in 1999 with Belarus is special because, in principle, it enables the unification of the two ethnically very similar countries. However, the relationship has been strained for various reasons and Belarus has approached the European Union – and also China – to balance Russia, although only haltingly. (Preiherman, Yauheni. Belarus and Russia Dispute the Fundamentals of Their Relationship. Eurasian Daily Monitor, January 15, 2019 [Online]. Available: https://jamestown.org/program/belarus-and-russia-dispute-the-fundamentals-of-their-relationship/ [Accessed: 3rd May 2019]).

[1945] Kurth, Natasha. Asia-Pacific and China. In Tsyganov 2018, 254–268.

[1946] Tsygankov 2016, 153–154, 198–199; Gvosdev & Marsh 2014, 141. China was semi-officially acknowledged as a conventional enemy by Chief of the Ground Forces General Staff Lieutenant-General Sergei Skokov. He was dismissed as part of a group of generals in 2011 who were made to resign or resigned themselves because they opposed the way in which the reforms were conducted (Коновалов, Сергей. Генеральский демарш.

that China poses a military threat become a taboo.[1947] In 2018 China was Russia's largest single trade partner but the exports were almost inclusively energy and the relationship is not economically optimal for Russia.[1948] Although Russia's military co-operation with China goes back to the mid-2000s, starting from 2012, China–Russia military relations have deepened with more military contacts and more complex military exercises, and interestingly, increasingly less arms exports from Russia to China.[1949]

The Shanghai Cooperation Organization which was established in 2001 is an integral part of Russia's strategy towards China.[1950] Russia began to resist the United States' presence in Central Asia by mobilising the support of the SCO from 2005 onwards and by 2014 had managed to facilitate the removal of U.S. forces from ex-Soviet Central Asian countries.[1951] Russia's fears of the United States' influence were at least partly legitimate as the United States' declared policy was to promote "freedom through reform" in Central Asia.[1952] On the other hand, Russia may have promoted the institutionalization of the SCO and the enlargement of its membership pool to counter China. Initially, the SCO had a security emphasis on combating terrorism, separatism and extremism but its agenda has grown to include information security and more importantly economics, which is China's priority. Consequently, Russian efforts to use the organization as a political tool have been constrained and eclipsed by the ever-increasing Chinese influence in the Central Asia.[1953]

Russia has also promoted the BRICS from 2006 as an alternative forum for the West dominated G-8, G-20, IMF and World Bank. Its first summit was organized in 2008.[1954] Bobo Lo argues that the BRICS is an effort to realize Putin's idea of the multipolar world, but the organization and its members lack the real resources to truly bring such an order into existence. Moreover, they do not represent any like-minded community of states in any sense.[1955] However weak the BRICS might be as an organization it still offers Russia a platform in which and from which to promote and co-ordinate its ideas in other international frameworks.[1956]

Независимое военное обозрение, 5 июля 2011 [Online]. Available: http://nvo.ng.ru/nvo/2011-07-05/1_demarsh.html [Accessed: 30th April 2019]; Rangsimaporn, Paradorn. Russian Elite Perceptions of the Russo-Chinese 'Strategic Partnership' (1996-2001). Slovo, Vol. 18, No. 2, (Autumn 2006), 129-145.

[1947] Kurth 2018.

[1948] Donaldson & Nadkarni 2019, 300; Barkanov, Boris. Natural gas. In Tsygankov 2018, 138-152.

[1949] Meick, Ethan. China-Russia Military-to-Military Relations: Moving Toward a Higher Level of Cooperation. U.S.-China Economic and Security Review Commission, March 20, 2017 [Online]. Available: https://www.uscc.gov/sites/default/files/Research/China-Russia%20Mil-Mil%20Relations%20Moving%20Toward%20Higher%20Level%20of%20Cooperation.pdf [Accessed: 30th April 2019]; Juola, Cristina D. Venäjän puolustusteollinen yhteistyö Kiinan ja Intian kanssa 2010-luvulla. [Russia's military-industrial cooperation with China and India in the 2010s] Maanpuolustuskorkeakoulu Sotataidon laitos, Julkaisusarja 3: Työpapereita nro 9 [Online]. Available: http://www.doria.fi/bitstream/handle/10024/164170/181108_VENR_J_kiina_venaja_intia_juola_web.pdf?sequence=1&isAllowed=y [Accessed: 30th April 2019].

[1950] Donaldson & Nadkarni 2019.

[1951] Donaldson & Nadkarni 2019, 226.

[1952] Fried, Daniel. A Strategy for Central Asia. Statement Before the Subcommittee on the Middle East and Central Asia of the House International Relations Committee. Washington, DC. October 27, 2005 [Online]. Available: https://2001-2009.state.gov/p/eur/rls/rm/55766.htm [Accessed: 27th April 2019].

[1953] Herd, Graeme P. The Battle of ideas, Concepts and Geopolitical Projects in Central Asia: Implications for Russo-Chinese Relations? In Kanet & Piet 2014, 183-203.

[1954] Gvosdev & Marsh 2014, 387.

[1955] Lo 2015, 77-80.

[1956] Tsygankov 2018; Gvosdev &Marsh 2014, 389-390.

The crisis in the relations between Russia and the United States, NATO and the EU is related to the above discussed integration projects of Russia and to their collision with Western integration projects.[1957] In brief, the EU's European neighbourhood policy and the Eastern Partnership Programme offered to post-Soviet countries threatened Russian political and economic interests. Moreover, the possibility of Ukraine's and Georgia's NATO membership was unacceptable for Russia.[1958] The resultant crisis has been argued to have been either a result of the EU's arrogance, Putin's personality, Russian elites' deep-seated fear of regime change, or the West's intentional disregard of Russia's security interests.[1959] Be that as it may, aggressive foreign policy secured support for the faltering regime as Putin's approval rating shot above 80% in 2014.[1960] Additionally, according to Levada, it stayed there until May 2018 after which it has declined to 63% in March 2019.[1961]

6.1.3 Development of cyberspace

Cyberspace is part of Russia's strategic environment and its security. This means that normative and technological developments need to be considered when examining the situations in which the Russian elites have operated. Previous studies have argued that the Russian elites were caught off-guard by the development of the Internet as a new political information channel in 2011. The regime reacted based on domestic interests and authoritarian instincts and began to force the Russian Internet under state control.[1962] However, domestic issues and political control are only one part of the puzzle. As I demonstrated in Chapter 3.2.2 the development of cyberspace including its ICT, cryptography, use of outer space, digitalization of infrastructure, governance issues, and all the new related threats challenged states' sovereignty, their ability to provide security, and the overall balance of power.

Already in the late 1990s the Russian security services were undoubtedly aware of the risks the Internet posed to Russia's national security. The United States government was openly discussing cyber threats to its national infrastructure and the NSA was developing secret cyber offensive capabilities by 1996.[1963] The Clinton administration adopted Presidential Decision Directive/NSC-63 in 1998 which stated: "I [President Clinton] intend that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber-attacks on our critical infrastructures, including especially our cyber systems."[1964] Between 1997–1999 the U.S. Armed Forces and the CIA used cyber capabilities against Russia's allies the Serbs

[1957] On the phases of this relationship cf. Forsberg, Tuomas and Haukkala, Hiski. The European Union. In Tsyganov 2018, 269-281.

[1958] Legvold 2015; Cadier 2015; Donalson & Nadkarni 2019, 184-192.

[1959] Rieker, Pernille and Gjerde, Kristian Lundby. The EU, Russia and the potential for dialogue – different readings of the crisis in Ukraine. European Security, Vol. 25, No. 3 (2016), 304-325; Legvold 2016, 118-199; Trenin 2014; Mearsheimer, John J. "Why the Ukraine Crisis Is the West's Fault," Foreign Affairs, September/October 2014, 77-89.

[1960] Donalson & Nadkarni 2019, 433-435.

[1961] Levada. Putin's approval rating [Online]. Available: https://www.levada.ru/en/ratings/ [Accessed: 27th April 2019].

[1962] Nocetti 2018, 182–198; Soldatov & Borogan 2015; Treisman, Daniel (ed.) The New Autocracy: Information, Politics, and Policy in Putin's Russia. Washington, D.C.: Brookings Institution Press, 2018.

[1963] Kaplan 2016, 47-49.

[1964] The White House Washington. Presidential decision directive/NSC-63, May 22, 1998 [Online]. Available: https://fas.org/irp/offdocs/pdd/pdd-63.htm [Accessed: 1st May 2019].

in the former Yugoslavia.[1965] The Russians themselves were already hacking the U.S. DoD networks—an incident which became to be known as the Moonlight Maze.[1966] This breach lead Deputy Secretary of Defense John Hamre to claim in 1999 that the United States was in a "cyberwar."[1967]

Between 2000 and 2007 most state-level cyber activity seems to have concentrated on espionage although this is difficult to know for sure as the only data available for scholars comes from primarily public Western sources.[1968] China activated its operations around 2000 and began to use the Internet for industrial espionage to secure its national development to such a magnitude that the U.S. began to complain about it in 2006–2007.[1969] Cyber criminality became an international threat.[1970] From a Russian point of view the Chechen rebels' presence on the Internet posed a threat, as did the possibility that other radical Muslim groups in Russia or Central Asia might use the Internet to gather global support.[1971] Importantly, the United States DoD and NSA cyber forces went through multiple reorganizations in an effort to find the right balance between espionage, cyber defence, and offensive operations—a process that Russia quite probably monitored.[1972]

The threats and possibilities inherent in the development of cyberspace produced international cooperation, or at least efforts to that effect such as the Budapest Convention of Cyber Crime, which was adopted quickly after 9/11. However, Russia and China have not signed it and have criticized it.[1973] The United Nations ITU created the World Summit on Information Security (WSIS) in 2001 and the Working Group on Internet Governance (WGIG) in 2003 to operate between the summits (2003, 2005). The ITU's approach to Internet governance set certain developing countries, (including Russia which argued multilaterally for a state governed Internet) against ICANN, IETF, W3C and the multi-stakeholder model promoted by the United States.[1974] In 2006 the Internet Governance Forum (IGF) was established as a multi-stakeholder open discussion forum with no regulatory functions. Its latest session was held in Paris in 2018.[1975] Another arena for developing Internet governance norms

[1965] Kaplan 2016, 113-118.

[1966] Kaplan 2016, 78-88; Rid 2016, 316-322.

[1967] Rid 2016, 329.

[1968] This is apparent from, for example, the CSIS's list of Significant Cyber Incidents and the CFR's Cyber Operations Tracker (Center for Strategic and International Studies 2018; Council on Foreign Relations 2018).

[1969] Kaplan 2016, 222–223; Inkster 2016, 71-75; Valeriano, Jensen & Maness 2018.

[1970] United Nations Office on Drugs and Crime. Comprehensive Study on Cybercrime, Draft—February 2013 [Online]. Available: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [Accessed: 1st May 2019].

[1971] Carr 2012; Rantapelkonen, J. Psykologiset operaatiot. Propagandasta informaatio-operaatioihin. [Psychological operations. From propaganda to information operations]. Maanpuolustuskorkeakoulu Taktiikan laitos, Julkaisusarja 1 Taktiikan tutkimuksia N:o 1/2002. Helsinki: Edita.

[1972] Kaplan 2016. For 'eyewitness accounts' cf. CSIS. Cyber From The Start podcast, multiple episodes [Online]. Available: https://www.csis.org/podcasts/cyber-start [Accessed: 28th May 2019].

[1973] Drake, Cerf & Kleinwächter 2016; The Russian claim that the Budapest Convention article 32(b) breaches sovereignty is controversial (Clough, Jonathan. A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization. Monash University Law Review, Vol. 40, No. 3 (2014), 698-736).

[1974] Cogburn, Derrick L. The Multiple Logics of Post-Snowden Restructuring of Internet Governance. In Musiani et al. 2016, 25-45.

[1975] Cogburn 2016; IGF. The Internet of Trust. Thirteenth Internet Governance Forum (IGF) 12 - 14 November 2018 Paris, France [Online]. Available: http://www.intgovforum.org/multilingual/index.php?q=filedepot_download/6037/1555 [Accessed: 2nd May 2019].

have been the working groups of the UN GGE process beginning from 2004/2005. They have approached cyber security as a disarmament issue.[1976]

Somewhere around 2006–2007 more serious and militarized state-to-state cyber-attacks began to surface or were at least made public.[1977] Before this, the U.S. had probably used offensive cyber measures against Iraq in 2003 and against Islamist extremist from 2001 onwards.[1978] There is evidence and even acknowledgements on this and it was also a real belief held by the Russian and Chinese elites.[1979] Quite probably the U.S. together with Israel initiated the Stuxnet or Operation Olympic Games in 2006 (which was discovered in 2010). Israel allegedly used cyber tools in its attack against Syrian air defences in 2007. Russian state sponsored hackers managed to cause major disturbances in Estonian financial and public services in 2007, and Russia allegedly used cyber-attacks against the Georgian government and media in 2008.[1980] These operations raised fears of catastrophic attacks against national infrastructure and the infrastructure of the Internet itself—a resource that state economies were becoming ever more reliant on.[1981]

Between 2006–2009 the United State adopted the National Infrastructure Protection Plan, the Comprehensive National Cyber Security Initiative, and the DoD National Military Strategy for Cyberspace Operations and chose to militarize cyber issues by designating cyberspace as a military domain. The U.S. Cyber Command was established in June 2009.[1982] This militarization was arguably a Western led process as China and Russia did not really discuss these issues in public and concentrated on criticizing the U.S. while at the same time advancing their own espionage operations.[1983] The establishment of the U.S. Cyber Command forced all other states to take a similar action, choose some other strategy to secure their national cyber security, or do nothing. The United States also led the discussion on securing critical infrastructure and how to establish public-private partnerships to do it, although its own success was not exemplary.[1984] In addition to the threats emanating from the military steps taken by the United States, the Russian information society had developed to a phase where cyber criminality had started to become a domestic problem and awareness of infrastructural threats also increased.[1985]

[1976] Osula & Rõigas 2016.

[1977] Libicki 2016, 6; Valeriano & Maness 2015.

[1978] Kaplan 2016, 158-160.

[1979] Thomas 2005; Inkster 2015.

[1980] Libicki 2015; Kaplan 2016; Rid 2016; Valeriano, Jensen & Maness 2018.

[1981] Kramer, Starr, Stuart & Wentz 2009; Valeriano, Jensen & Maness 2018.

[1982] Kramer, Starr & Wentz 2009; Dombrowski & Demchak 2014; Kaplan 2016.

[1983] Soldatov & Borogan 2015; Inkster 2016; Office of the National Counterintelligence Executive. Foreign Spies Stealing US Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, October 2011 [Online]. Available: https://www.dni.gov/files/NCSC/ documents/Regulations/Foreign_Economic_Collection_2011.pdf [Accessed: 29th May 2019]. On the timeline and relationships between different cyber operations cf. Valeriano & Maness 2015; Valeriano, Jensen & Maness 2018.

[1984] Kaplan 2016; Marks, Joseph. Obama's Cyber Legacy. Defence One, January 18, 2017 [Online]. Available: https://www.defenseone.com/threats/2017/01/obamas-cyber-legacy/134629/?oref=d-river [Accessed: 3rd May 2019].

[1985] Symantec. Symantec Global Internet Security Threat Report Trends for 2009. Online]. Available: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf [Accessed: 1st May 2019]; Tadviser. Киберпреступность и киберконфликты: Россия [Online]. Available: http://www.tadviser.ru/a/240126 [Accessed: 1st May 2019]; Pynnöniemi 2012;

The other rising great power, China, had built up its Internet censorship system called the Golden Shield or the Great Firewall of China already in 1996–2006.[1986] Between 2009 and 2013 China significantly increased the censorship of social media and pushed foreign, mainly Western Internet companies, out of the Chinese markets. The Communist party was partly suppressing national minorities who had discovered social media and partly establishing rules of national self-censorship concerning all Chinese.[1987] By 2015 the Chinese Internet was tightly under government control, and censorship was pervasive.[1988] This arguably provided Russia with an example to follow as the Arab Spring and the demonstrations of 2011–2012 began.

Before the Arab spring of 2011, the Iranian Green revolution of 2009 gave a glimpse into how the social media could be used to organize support for a regime change.[1989] Consequently, the Arab Spring had its cyberspace dimensions as cyber means were first used to support the revolutions but then used to cut their wings as authoritarian countries began to 'switch off' mobile and Internet services in the event of demonstrations.[1990] The 'shut down' of the Internet was not a new phenomenon but gained popularity as a measure of political control in the 2010s. The idea had already been discussed even in the United States in 2010, although it was ultimately discarded.[1991] Additionally, the importance of protecting the critical (information) infrastructure increased. In 2012 ENISA reported that cyber-attack methods and tools had reached such a maturity that they could be used for cyber warfare and that the threats against critical infrastructures were on the rise.[1992] The fear of cyber attacks against industrial control systems with possibly catastrophic consequences increased as Stuxnet, Shamoon and then the attacks against the Ukraine's electricity networks occurred in 2015 and 2016.[1993]

Before the war in Ukraine and the alleged Russian cyber operations against the political systems and critical infrastructure of the West—and other major cyber incidents like NotPetya etc. which were blamed on Russia with or without evidence—there was an effort to build bilateral regimes of cyber security between the United States, China and Russia.[1994] After the revelations by Edward Snowden about the massive U.S. cyber espionage campaigns in 2013 and the downturn in West–Russia relations in 2014 the efforts faltered. However, in the midst of the Snowden affair the Obama administration agreed to establish a 'cyber-hotline' and increase cooperation between national

Pynnöniemi, Katri and Busygina, Irina. Critical infrastructure protection and Russia's hybrid regime, European Security, Vol.22, No.4 (2013), 559-575.

[1986] Inkster 2016; Lindsay, Cheung & Reveron 2015

[1987] Griffiths, James. The Great Firewall of China: How to Build and Control an Alternative Version of the Internet. London: Zed Books Ltd., 2019, 183-184.

[1988] Inkster 2015; Griffiths 2019.

[1989] Griffiths 2019, 110-111.

[1990] Vargas-Leon 2016.

[1991] Zittrain, Jonathan and Sauter, Molly. Will the U.S. get an Internet "kill switch"? MIT Technology Review, March 4, 2011 [Online]. Available: https://www.technologyreview.com/s/423196/will-the-us-get-an-internet-kill-switch/ [Accessed: 3rd May 2019].

[1992] ENISA. ENISA Threat Landscape Responding to the Evolving Threat Environment [Deliverable – 2012-09-28] [Online]. Available: https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape/at_ download/fullReport [Accessed: 1st May 2019].

[1993] O'Neil, William D. Cyberspace and Infrastructure. In Kramer et al. 2009, 113-146; Harrop, Wayne and Matteson, Ashley. Cyber Resilience: A Review of Critical National Infrastructure and Cyber-Security Protection Measures Applied in the UK an USA The White House. In Lemieux 2015, 149–166.

[1994] Cf. Sanger 2018; Valeriano, Jensen & Maness 2018; Maurer 2018; CSIS 2018; CFR 2019.

CERTs with Russia.[1995] Additionally, in 2015 Obama was able to push the Chinese to conclude an agreement on restricting economic cyber espionage and establish a hotline for handling incidents.[1996] Russian efforts towards a similar or deeper pact have fallen flat.[1997] In fact, after the Obama–Xi agreement, Chinese cyber-attacks against Russia increased significantly in 2016–2017 and were directed against Russia's South-Asian diplomatic efforts and arms sales and also against industrial targets in Russia.[1998] This happened despite the signing of the Russia–China information security agreement in 2015 which forbid computer attacks against information resources between the states.[1999]

The militarization of cyberspace was completed in the latter half of the 2010s. In 2014 NATO included cyber-attacks in its collective defence clause and in 2016 recognized cyberspace as a domain of military operations. In 2018 it established a Cyberspace Operations Centre.[2000] In 2015 China established its own military cyber force under the Strategic Support Forces.[2001] Countries over the world followed the United States' and NATO's example.[2002] In 2017 USCYBERCOM was elevated to a unified combatant command and in 2018 it achieved 'full operating capability' with 133 teams of the Cyber Mission Force operational.[2003] In the autumn of 2018 President Trump relaxed the constraints on conducting offensive cyber operations and the U.S. DoD adopted a doctrine of forward cyber defence even outside open conflicts.[2004] However, already

[1995] The White House. Fact sheet: U.S.-Russian Cooperation on Information and Communications Technology Security. June 17, 2013 [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol [Accessed: 1st May 2019].

[1996] Sanger 2018, 121-123; Tucker, Patrick. China Is Still Stealing America's Business Secrets, US Officials Say. Defense One, July 26, 2018 [Online]. Available: https://www.defenseone.com/technology/2018/07/china-still-stealing-americas-business-secrets-us-officials-say/150086/ [Accessed: 1st May 2019].

[1997] Grisby, Alex. Russia Wants a Deal with the United States on Cyber Issues. Why Does Washington Keep Saying No? CFR, August 27, 2018 [Online]. Available: https://www.cfr.org/blog/russia-wants-deal-united-states-cyber-issues-why-does-washington-keep-saying-no [Accessed: 1st May 2019].

[1998] Lenta.ru. Китайские хакеры стали в два раза чаще атаковать стратегические объекты России. Lenta.ru, 26 августа 2016 [Online]. Available: https://lenta.ru/news/2016/08/26/hacker_china_rus/ [Accessed: 25th May 2019]; Холявко, Анна. «Лаборатория Касперского» назвала мишени китайских хакеров в России. Эксперты фиксируют их возросшую активность. Ведомости, 06 декабря 2017 [Online]. Available: https://www.vedomosti.ru/technology/articles/2017/12/06/744343-hakeri-atakuyut-rossiiskie-gosudarstvennie-strukturi [Accessed: 25th May 2019].

[1999] Правительство Российской Федерации. Соглашение между Правительством Российской Федерацией и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности, от 30 апреля 2015 г. N 788-р [Online]. Available: http://static.government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf [Accessed: 26th February 2019].

[2000] Brent, Laura. NATO's role in cyberspace. NATO Review, February 12th, 2019 [Online]. https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm [Accessed: 1st May 2019].

[2001] DIA. China Military Power. Modernizing a Force to Fight and Win, 2019 [Online]. Available: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf [Accessed: 1st May 2019].

[2002] UNIDIR. The Cyber Index. International Security Trends and Realities. New York and Geneva: United Nations, 2013 [Online]. Available: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf [Accessed: 1st May 2019]; Pernik, Piret. Preparing for Cyber Conflict. Case Studies of Cyber Command. RKK ICDS, December 2018 [Online]. Available: https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf [Accessed: 1st May 2019].

[2003] The U.S. Cyber Command 2019.

[2004] The White House. National Cyber Strategy of the United States of America, September 2018 [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [Accessed: 3rd May 2019]; The United States Department of Defence 2018; Rudesill, Dakota S. Trump's Secret in 2016 it was revealed that the USCYBERCOM had planned a massive cyber operation called 'Nitro Zeus' against Iran.[2005] There is also evidence that the U.S. has used its new capabilities against state and non-state actors during the Obama era and has continued to do so under President Trump.[2006] This development was noticed in Russia.[2007]

The evolution of cyber warfare happened while the UN GGE process first showed great promise in 2009–2013 but then faced mounting problems and contradictions and failed altogether in 2016–2017. Russia's and China's efforts to form international consensus on banning cyber-weapons and transferring the control of the Internet to states failed.[2008] Furthermore, in 2012 the ITU organized the World Conference on International Telecommunications (WCIT) in Dubai where Russia, China and some other states tried unsuccessful to push through state-centred Internet governance. Moreover, the SCO sponsored international cyber security treaties also failed to gain traction in the United Nations in 2011 and 2015.[2009] The latest 'information sovereignty based' norm-building effort in the context of the UN by Russia (and China) was initiated in the autumn of 2018 and has produce a new UN GGE round, an alternative forum Open-Ended Working Group (OEWG) and UN committee decision on drafting a new cybercrime treaty. A clear change is that this effort is not only parried by countries supporting non-sovereignty-based models but is also being challenged with counter proposals. The Russian and Chinese proposals have been mainly supported by developing semi-authoritarian or authoritarian states.[2010] In addition to these state-led norm-building efforts, private companies and think tanks have put forth their own initiatives in the last couple of years.[2011]

New threats to the information infrastructure upholding cyberspace and national ICT systems have developed or become more acute in the 2010s. First, China, Russia and the United States have advanced their anti-satellite programmes and the United States

Order on Pulling the Cyber Trigger. Lawfare, August 29, 2018 [Online]. Available: https://www. lawfareblog.com/trumps-secret-order-pulling-cyber-trigger [Accessed: 3rd May 2019].

[2005] Sanger 2018.

[2006] Valeriano, Jensen & Maness 2018; Sanger 2018; Nakashima, Ellen. U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms. The Washington Post, February 27, 2019 [Online]. Available: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?utm_term=.08c7444b6474 [Accessed: 3rd May 2019].

[2007] RT. Чем может угрожать России активность американских военных в киберпространстве. Рамблер 28 февраля 2019 [Online]. Available: https://news.rambler.ru/other/41794660/?utm_content=rnews&utm_medium=read_more&utm_source=copylink [Accessed: 28th February 2019]; Иванов 2018.

[2008] Tikk & Kerttunen 2017.

[2009] Cogburn 2016; McKune, Sarah. An Analysis of the International Code of Conduct for Information Security. The CitizenLab, September 28, 2015 [Online]. Available: https://citizenlab.ca/2015/09/international-code-of-conduct/ [Accessed: 2nd May 2019]; Kavanagh 2017.

[2010] Sherman, Justin and Raymond, Mark. The U.N. passed a Russia-backed cybercrime resolution. That's not good news for Internet freedom. Washington Post, 4th December 2019 [Online]. Available: https://www. washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/ [Accessed: 5th January 2020].

[2011] Hinck, Garrett. Private-Sector Initiatives for Cyber Norms: A Summary. Lawfare, June 25, 2018 [Online]. Available: https://www.lawfareblog.com/private-sector-cyber-norm-initiatives-summary [Accessed: 2nd May 2019].

established the Space Command in 2018. These developments have put space stationed Internet infrastructure under military threat.[2012] Second, modern societies and militaries have become dependent on easily jammed satellite navigation systems and time-services.[2013] Third, the growth of IoT infrastructure and the sophistication of exploitation methods has enabled the launching of massive DDoS attacks that can knock out parts of the Internet infrastructure—not to mention a single country's DNS system.[2014] Fourth, the infrastructure of the Internet can itself be weaponised through the manipulation of BGP routing, which can lead to the dropping of traffic or its rerouting through hostile networks.[2015] Fifth, the increased tensions between great powers in the latter half of the 2010s has made supply-chain attacks a critical national security issue which is evident in the way in which foreign IT companies have fallen under sanctions and restrictions.[2016] Sixth, the advances in artificial intelligence, quantum computing and cryptography, and blockchain based technologies all might have disruptive effects on the balance of power in cyberspace. The problem for Russia is that, at least according to one study, it is not among the forerunners in developing and deploying these technologies.[2017] Seventh, in April 2016 the Russian elites became the object of an Internet leak for the first time as the Panama papers revealed information about the corruption of Vladimir Putin and people close to him.[2018] This was followed in 2019 by the "The Dark Side of the Kremlin" file released by human right advocacy groups.[2019] Eighth, data localization and the possible access of foreign security services to governmental, corporate, and personal data has become a national security issue, as has the question of using foreign cloud servers and other extraterritorial technology for critical services of societies.[2020] Lastly ninth, old threats have not

[2012] Sankaran, Jaganath. Limits of the Chinese Anti-satellite Threat to the United States. Strategic Studies Quarterly, Vol. 8, No. 4 (WINTER 2014), 19-46; Rose, Frank A. Re-establishing U.S. Space Command is a great idea. Brookings, January 7, 2019 [Online]. Available: https://www.brookings.edu/blog/order-from-chaos/2019/01/07/re-establishing-u-s-space-command-is-a-great-idea/ [Accessed: 1st May 2019].

[2013] Burgess, Matt. To protect Putin, Russia is spoofing GPS signals on a massive scale. Wired, March 27, 2019 [Online]. Available: https://www.wired.co.uk/article/russia-gps-spoofing [Accessed: 1st May 2019].

[2014] Sozeri 2015; Cloudflare. Famous DDoS Attacks. The Largest DDoS Attacks Of All Time [Online]. Available: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/ [Accessed: 1st May 2019].

[2015] Jonker, Mattjis, Pras, Aiko, Dainotti, Alberto and Sperotto, Anna. A First Joint Look at DoS Attacks and BGP Blackholing in the Wild. IMC '18, October 31-November 2, 2018, Boston, MA, USA [Online]. Available: http://www.caida.org/publications/papers/2018/dos_attacks_and_bgp/dos_attacks_and_bgp.pdf [Accessed: 1st May 2019].

[2016] Levite, Ariel. ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies. Carnegie Endowment for International Peace, October 4th 2019 [Online]. Available: https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974 [Accessed: 5th January 2020].

[2017] KPMG. The Changing Landscape of Disruptive Technologies. Tech hubs forging new paths to outpace the competition [Online]. Available: https://info.kpmg.us/content/dam/info/en/techinnovation/pdf/2018/tech-hubs-forging-new-paths.pdf [Accessed: 2nd May 2019]; Bendett, Samuel and Kania, Elsa B. A new Sino-Russian high-tech partnership. Authoritarian innovation in an era of great-power rivalry. ASPI Policy brief Report No. 22/2019.

[2018] Luhn, Alec and Harding, Luke. Putin dismisses Panama Papers as an attempt to destabilise Russia. Guardian, April 7th, 2016 [Online]. Available: https://www.theguardian.com/news/2016/apr/07/putin-dismisses-panama-papers-as-an-attempt-to-destabilise-russia [Accessed: 1st May 2019].

[2019] Shane, Scott. Huge Trove of Leaked Russian Documents Is Published by Transparency Advocates. New York Times, January 25th, 2019 [Online]. Available: https://www.nytimes.com/2019/01/25/world/europe/russian-documents-leaked-ddosecrets.html [Accessed: 1st May 2019]. Also a smaller leak in 2017 Cf. Newman, Lily Hay. A fishy WikiLeaks dump targets Russia for a change. Wired, September 20, 2017 [Online]. Available: https://www.wired.com/story/wikileaks-spy-files-russia/ [Accessed: 1st May 2019].

[2020] Тишина 2018; Захарцев, Алексей. Федеральный антивирус: Защитникам виртуального мира требуется помощь государства- ВПК, № 3-4 (618-619) за 3 февраля 2016 года [Online]. Available: https:// vpk-news.ru/articles/28996 [Accessed: 28th February 2019].

gone away as the amount of cyber-crime, including more sophisticated attacks, has steadily increased. In 2016 the General Persecutor of the RF estimated the damages from cybercrime to be 0.25% of GDP.[2021] Vladimir Putin himself has stated that cyber-attacks against the government have increased: in 2014–2015 there were a little more than one and a half thousand, in 2016 there were 12 thousand, in 2017 - about 12.5 thousand, and in 2018 - already 17 thousand.[2022] Of course, these declarations must be approached in the political context of the state policies analysed below.

Now that Russia's international and cyber environment have been examined, it is time to answer the question of whether the Russian strategic environment changed during the 2000s and 2010s in a way that required the Russian elites to reach for new ideas or rediscover old ones which might then have influenced or given reason for adopting particular policies. Arguably, the mid and late 1990s were the period when cyberspace as a part Russia's strategic environment was born. At that point it did not present itself as a critical national security issue even though the Russian security services understood its potential for both offensive and defensive purposes. The exception was the information warfare against the Chechen separatists, but it was a piecemeal effort constituting of persecuting individual websites and disseminating counter-propaganda mainly through other mediums than the Internet.[2023]

During the 2000s and 2010s Russian domestic information technology research and hardware and software development and production lagged significantly behind the United States and increasingly that of China, and Russia became almost totally reliant on foreign technology. The United States' perceived control over the Internet, its technological superiority and the eventual establishment of the Cyber Command affected the strategic balance unfavourably for Russia. As Russia's own information economy and society developed it was faced with the same problem of securing the critical information infrastructure, which maintained critical state, economic, and societal services, as it did for everybody else. Moreover, the Internet was becoming a social medium, enhancing the effects of globalization on Russian political and cultural spheres. The first 'new Cold War' in 2004-2009 was certainly a change for the worse in Russia's security environment, although this was not because of new and unseen threats emerging. As its economy recovered, Russia began to challenge the roles, values, and norms that had been imposed upon it after the Soviet Union collapsed. Because the Internet's influence was still marginal, these developments did not produce any significant efforts to control or shape the national cyberspace or its content by the Russian regime.

Yet, in 2008-2009 as Russia 'pivoted to the East' it is quite possible that in the context of different economic forums, in the CSTO and the SCO there was an exchange of ideas and convergence of interests on the issues of information security. Perhaps more critically, although Russia's economy recovered quickly in 2009-2012,

[2021] Сухаренко, Александр. Кибертеррористов вычислят с ГосСОПКА. Независимая газета, 23.12.2016 [Online]. Available: http://www.ng.ru/ideas/2016-12-23/5_6893_kiber.html [Accessed: 1st May 2019].

[2022] Латухина, Кира. Барьер для шпиона. Владимир Путин призвал ФСБ защитить Россию от кибернаступления. RG.ru, 6 марта 2019 [Online]. Available: https://rg.ru/2019/03/06/putin-prizval-fsb-zashchitit-rossiiu-ot-kibernastupleniia.html [Accessed: 28th May 2019].

[2023] On Chechenia Cf. Thomas 2005; Berger 2010.

Medvedev (in fact Putin's government) failed in reforming the Russian 'digital' economy. At the same time, the great power balance was changing. In the contest between a rising China and the status quo United States, Russia chose to ally itself with China which shared a similar authoritarian political system and compatible values. Moreover, as was noted above, the U.S. 'Reset' policy was only a tactical move and the underlying interest-conflicts between Russia and the United States remained.

The way in which the militarization of cyberspace advanced and the Internet began to challenge the state-controlled media as a source of information in Russia also affected the foundations of the Russian security environment. It is probable that the military reform and the rearmament programme that began in 2008-2011 heightened the sensitivity of the Russian defence and security elites to the performance gap between Russia and the U.S.—and increasingly China. Ever faster developing information technology with its potentially disruptive effects and the possibility for rapid impacts on the balance of power made it imperative to enhance the domestic technological base. More so as the efforts to control the United States through arms control negotiations disguised as 'information security norm-building' repeatedly failed. The failure of the Russian initiative in the 2012 WCIT in Dubai demonstrated that international sovereignty-based cyber security was unattainable through global agreements. Russia had to go ahead and make sovereignty a norm through its own actions and regional agreements.

Around 2011–2012 the Internet had reached a significant portion of the Russian urban population, and arguably the 2011 Arab spring was an event that changed the calculus of the Russian elite.[2024] It highlighted the power of social media and heightened the tensions between the 'interventionist' and 'democratizing' West and the 'sovereignty-respecting' and 'great-power status seeking' Russia (and China). However, there was nothing new in the threat of regime change or the Russian vision on the multipolar world order. Moreover, the grounds for fearing a 'colour revolution' quickly faded as the Arab spring largely fizzled out by the end of 2012 and the demonstrations inside Russia were over by the summer of 2012. More importantly, Putin had clearly decided to develop the Russian 'pivot to the East' even before the demonstrations of 2011-2012 occurred. He built his re-election campaign on great-powerness, Eurasian alliances and he chose to retain his anti-Western stance even after the demonstrations had been suppressed.[2025] As the United States was withdrawing from Iraq and Afghanistan and itself 'pivoted to the East' to counter the rising China, the Russian military was regaining its strength. Thus, the global balance of military power was rapidly changing. This is not to argue that the Arab spring had no genuine effect, only that it was a prelude, not the defining moment.

Geopolitical great power rivalry intensified in 2013 and the Snowden case forced states all around the world to take a good look at their national cyber security. The Russian economy began to falter just as the European Union was drawing Ukraine (and Georgia) away from Russia's sphere of influence. Consequently, the real change

[2024] Nocetti 2015; Soldatov 2017; Treisman 2019.

[2025] Fernandes, Sandra. Putin's Foreign Policy towards Europe: Evolving Trends of an (Un)Avoidable Relationship. In Kanet & Piet 2014, 13-34, 26-27.

in Russian international environment occurred in 2014, first, as the result of the revolution in Ukraine, and then with the diplomatic and economic confrontation with the West, which is still ongoing. By 2015 Russia had ended up with a latent conflict with the United States, NATO and European Union with little support from its so-called allies from CSTO or SCO, while its military reform was still uncompleted. Moreover, Russia's economic decline and the use of force against Ukraine had undermined its Eurasian integration policies. Thus, Russia's security and economic environment changed drastically to the worse. Moreover, the Russian digital economy was facing a triple crisis: intense competition from foreign companies, sanctions restricting financing and cooperation, and weak domestic markets. Through Russian and Western reactions and counter reactions the militarization of cyberspace accelerated and information became weaponized in state-to-state relationships, and Russia was under threat of further sanctions from the U.S., NATO and the EU. Thus, the cyberspace had in fact become more dangerous for Russia at the same time as it has become reliant on foreign IT technology. Russia's policies during 2015–2019 testify to this as it has tried to eliminate its technological vulnerabilities and build up its stagnating technological-scientific power base.

Together with everything noted above, an American administration led by President Trump which clearly strives to rid itself from binding and unbeneficial international agreements, has made Russia's strategic environment quite fluid.[2026] Its vulnerability is increased by its slowly recovering economy, micro-level protests to the cuts on social benefits, and the dipping approval ratings of Putin and his party. It can thus be argued that the Russian elites have been looking for ideas after the spring of 2014 that might provide answers to Russia's current situation which has been characterised by the perceived change in the balance of power, multiple outside and inside security threats, economic problems, and the forced reorientation to Eurasia and Asia—in addition to the need to control a society penetrated by the Internet. The Russian elite became acutely aware of the changes in the cyberspace between 2011-2012, particularly in the Internet, and most importantly of its effects on national security throughout the wider information space. This increased the demand for new and old ideas as the elite searched for creative and innovative ways to make sense of the confusing and threatening environment from domestic epistemic communities but perhaps also from foreign sources. However, the true shift in the strategic environment necessitating novel policies and strategic choices happened in 2014. A new or at least updated strategy to confront the threats in and from cyber and information space was needed.

6.2 Policies and ideas

This chapter analyses the strategies, policies, and laws that have been adopted by the Russian regime to tackle the new security issues brought forth by the development of the international environment and the Internet in the period of 2000–2019. I will start by examining the national actors involved in developing, selecting, and implementing policies to understand how and through what kind of instruments cyberspace is shaped by the Russian state, and how cyber strategy is made and to examine how

[2026] Wolf, Zachary B. and Carman, JoElla. Here are all the treaties and agreements Trump has abandoned. CNN, February 1, 2019 [Online]. Available: https://edition.cnn.com/2019/02/01/politics/nuclear-treaty-trump/index.html [Accessed: 8th July 2019].

ideas are transferred between the elites and epistemic communities. The second part of this chapter examines the international treatises Russia has either advocated or adopted concerning cyber and information security during 2000–2019. The third part examines the strategies, policies, and laws developed and adopted in the period of 2000–2011 to give context for the next chapter. Throughout these parts I analyse how the strategic cultural ideas examined in Chapter 5 resonate with the adopted strategies, policies, and laws.

6.2.1 Decision-making elites and institutions

Russian security, defence and foreign policy behaviour has been explained through multiple different theories and variables—many of them domestic.[2027] Russia has been variously described as authoritarian state, a Neo-Soviet Union, a 'KGB state', a kleptocracy and an 'informational autocracy'.[2028] Some have found persistent features like patron-client nomenclature, administrative silos, lack of investment, directly government led strategic projects, non-transparency, lack of responsibility, and emphasis on campaigns and projects instead of development.[2029] However, Russia's political system has changed between 2000–2019 and thus any single theory describing the Russian political system under Putin will fail to capture the whole picture, which has changed over time.[2030] Keeping that in mind I shall limit myself here to examining the current main Russian public and private decision-making elites or institutions, in short those actors taking part in developing and implementing policies towards the Russian national segment of the Internet. The actors and their responsibilities towards different networks of the Russian national segment are presented in Table I.[2031] The categorization of actors is based on mandates and functions as indicated by the references in the table. The categorization of the networks is based on Russian law. Public Internet refers to the 'information-telecommunications network Internet' defined by the Russian federal law. Government networks and the military Internet are different types of special networks also defined be law. Critical information infrastructure is a regulatory category central to understanding Russian national cyber security. Corporate

[2027] Cf. Lo 2015; Cadier & Light 2016; Oliker 2017; Tsygankov 2018; Donaldson & Nadkarni 2019; Kanet 2019.

[2028] The debate about the Russian authoritarian nature is ongoing. Perhaps the most prominent Western scholar on the Russian domestic political system Richard Sakwa has labelled Russia 'soft authoritarian' but he has also pointed out that designating Russia to be authoritarian and 'the West' liberal democratic is a gross simplification and a political act (Sakwa, Richard. Dualism at Home and abroad: Russian Foreign Policy Neo-Revisionism and Bi-continentalism. Cadier & Light 2015, 65-79). Also cf. Treisman 2018; Pomerantsev, Peter and Weiss, Michael. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. New York: The Institute of Modern Russia, Inc., 2014; Oliker, Olega: Putinism, Populism and the Defence of Liberal Democracy, Survival, Vol.59, No. 1, February – March 2017, 7-24.

[2029] Porfiriev & Simons 2016.

[2030] On this change cf. Marten 2017; Soldatov, Andrei. From the "New Nobility" to the KGB. Russian Politics and Law, Vol. 55, No. 2 (2017), 133-146; Soldatov, Andrei and Rochlitz, Michael. The Siloviki in Russian Politics. In Treisman et al. 2018, 79-103; Konyshev, Valery and Sergunin, Alexander. Military. In Tsyganov 2018, 168-181; Herspring, Dale R. Vladimir Putin and Military Reform in Russia, European Security, Vol.14, No.1 (2005), 137-155; Vendil 2001; Mankoff 2012; Gvosdev & Marsh 2014; Bacon, Edwin. Security Council and decision-making. In Kanet 2019, 119-130; Pomeranz, William E. Law and the Russian State- Russia's Legal Evolution from Peter the Great to Vladimir Putin. London and New York: Bloomsburym 2019, 164-165; Noble, Ben and Schulmann, Ekaterina. Not Just a Rubber Stamp. Parliament and Lawmaking. In Treisman 2018, 47-78; Monaghan 2017; Renz 2018; Golts, Aleksandr. Military Reform and Militarism in Russia. Washington, D.C.: The Jamestown Foundation, 2019.

[2031] For a somewhat similar survey cf. Carr 2012; Nocetti 2015; Vendil Pallin 2019, 203-213.

networks refer to 'separated networks' administered by non-governmental entities and possibly connected to the common telecommunications network.[2032]

Table I. The Russian National segment of the Internet: Actors, Networks and Responsibilities[2033]

Actors	**Networks**				
	Public Internet	***Government networks***	***Military Internet***	***Critical information infrastructure***	***Corporate networks***
The President of the Russian Federation	SP AL	SP AL	SP AL	SP AL	SP AL
The Security Council	SP C DL&DP	SP C DL&DP	SP C DL&DP	SP C DL&DP	SP C DL&DP
The Federal Assembly	DL&AL	DL&AL	DL&AL	DL&AL	DL&AL
The Ministry of Digital Development, Communications and Mass Media of the Russian Federation	DL&DP IP NR	DL&DP IP NR			NR
Rozkomnadzor	NSC CM TC	NSC CM TC			NSC (TC)
Rossviaz'	TD TC PC RA	TD TC PC RA			
Rospechat'	IP RA				
ANO Tsifrovaia Ekonomika	C DP	C DP			C DP
The Ministry of Foreign Affairs	IP CD				
Think tanks and other forums	CD DP TD	DP	DP	DP	DP TD
The Ministry of Defence and the Armed Forces	CD C	C	DP&IP RA NR TC CL CS		
The Federal Service for Technical and Export Control	NR CL	NR CL	NR CL	NR NSC CL	CL
The Defence-Industrial Complex			TD PC SS		
Ministry of Interior (Directorate K)	LE	LE			LE

[2032] Федеральный закон 2003; Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 18.03.2019) "Об информации, информационных технологиях и о защите информации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_61798/ [Accessed: 8th May 2019]; Федеральный закон 2017a.

[2033] Abbreviations: Strategic planning (SP), Coordination (C), Drafting laws (DL), Drafting policies (DP), Adopting laws (AL), Implementing policies (IP), Normative regulation (NR), Normative supervision and control (NSC), Cyber diplomacy (CD), Content monitoring (CM), Technical control (TC), Providing connectivity (PC), Technical development (TD), Resource administration (RA), Cyber security and incident response (CS) RU-CERT(a), GOV-CERT(b), Military SOCs (c), FSB (d), CERT-GIB / Private SOCs FIN-CERT (e), Certification and licences (CL), Systems and Services (SS), Law enforcement (LE).

Actors	**Networks**				
	Public Internet	***Government networks***	***Military Internet***	***Critical information infrastructure***	***Corporate networks***
Ministry of Industry and Trade and the Ministry of Economic Development	DP&IP	DP&IP			DP&IP
The Federal Security Service	LE CM CL	LE CM CL	LE CM CL	C LE CL TC CS(d)	LE CL
The Federal Protective Service		TC PC CS SS			
Computer Emergency Response Teams	CS(a)	CS(b)	CS(c)	CS(d)	CS (e)
Coordination Centre of National Domain of Internet and Technical Centre Internet	TC PC	TC PC			PC
State and private Internet Service Providers	PC (TC)	PC	PC	PC (TC)	PC
State and private software and hardware companies	SS TD	SS TD	SS TD	SS TD	SS TD
”The civil society”	CM				

The President of the Russian Federation by the constitution and through Vladimir Putin’s personal power and through the political system is the highest decision-maker of Russian security, defence and foreign policy.[2034] He approves all federal laws and has veto powers which have not been challenged after 2011.[2035] This does not mean that he is omnipotent or a dictator, but he can, if he so chooses, ‘manually control’ issues he deems to be important.[2036] He takes part in the strategic planning process as the Head of the Security Council, by influencing the legislative system through the presidential administration and the United Russia party, by issuing strategic directives like the May Edicts, by controlling the executive system through constitutional and personal power.[2037] During his third and fourth term, Putin has relied more on semi-formal gatherings or working groups and presidential advisers and representatives like: the Internet Ombudsman Dmitrii Marinichev, the Presidential Adviser on the Development on the Internet German Klimenko, and the Presidential Adviser on International Cooperation in the Area of Information Security Andrei Krutskikh.[2038]

[2034] Mankoff 2012, 55; Gvosdev & Marsh 2014, 34–36; Lo 2015, 7; Trenin 2015.

[2035] Pomeranz 2019.

[2036] Monaghan 2017; Treisman 2019.

[2037] Sakwa 2015; Lee 2015; Oliker 2017; Monaghan 2017; Treisman 2019.

[2038] Soldatov 2017; Monaghan 2017; Treisman 2019; Pomeranz 2019; Левченко, Григорий. Интернет-омбудсмен и советник Путина открестились от защиты пользователей Сети. Republic, 11 января 2016 [Online]. Available: https://republic.ru/posts/62291 [Accessed: 8th May 2019]; Указ Президента РФ 2018a; Посольство России в Республике Гана. Статья спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, Посла по особым поручениям МИД России А.В.Крутских, опубликованная в газете "Коммерсант" 27 марта 2019 года [Online]. Available: https://ghana.mid.ru/ru/press-centre/news/statya_spetspredstavitelya_prezidenta_rossiyskoy_federatsii_po_voprosam_mezhdunarodnogo_sotrudniches/ [Accessed: 8th May 2019].

The Security Council of the Russian Federation has the overall responsibility for the strategic planning process.[2039] It is headed by the president and has approximately 30 permanent and ordinary members including the prime minister, heads of key ministries, head of the presidential administration, head of the Armed Forces, security services, speakers of the Duma and Federal Council, and regional presidential representatives. The Security Council has a secretariat headed by the ex-FSB Director and friend of Vladimir Putin, Nikolai Patrushev.[2040] The Security Council functions as a national security coordination instrument at the highest level. It formulates policies, strategies and law drafts, monitors the national security situation and exercises oversight over the federal and regional executive power.[2041] As Edwin Bacon has noted, the Security Council blurs the lines between the constitutional separation of powers.[2042] The Security Council does much of its work through inter-departmental commissions, one of which is the Inter-Departmental Commission of Information Security. It analyses and forecasts the information security situation in Russia, makes policy proposals for the Security Council and takes part in the strategic planning process. The Commission together with the Scientific Council of the Security Council has taken part in the formulation of the Digital Economy programme and the debates on information threats against Russia.[2043] The membership of the Commission includes presidential representatives, representatives of ministries, security services (FSB, SVR, FSO), the military, the national guard, the federal agencies related to information security (Roskomnadzor, Rossviaz', Rospechat'), the FSTEK, and representatives from Gasprom, Rosneft, Rosatom, and Sberbank among others.[2044] The Scientific Council provides overall scientific-methodological support for the Security Council and its memberships includes 150 academicians from the leading think tanks and universities including: V. M. Burenok, S. N. Griniaev, S. G. Chekinov, A. A. Kokoshin, A. V. Krutskikh, A. V. Serzhantov and many representatives from the scientific military

[2039] Cf. Chapter 5; Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 05.10.2015) "О безопасности" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_108546/ [Accessed: 6th May 2019]; Указ Президента РФ от 06.05.2011 N 590 (ред. от 25.07.2014) "Вопросы Совета Безопасности Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_113807/ [Accessed: 6th May 2019]; Vendil 2001; Bacon 2019.

[2040] Указ Президента РФ от 25.05.2012 N 715 (ред. от 18.02.2019) "Об утверждении состава Совета Безопасности Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_130204/ [Accessed: 8th May 2019].

[2041] Указ Президента РФ от 06.05.2011 N 590 (ред. от 25.07.2014) "Вопросы Совета Безопасности Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_ LAW_113807/ [Accessed: 6th May 2019].

[2042] Bacon 2019.

[2043] Указ Президента РФ от 20 октября 1993 г. N 1686 "О совершенствовании деятельности межведомственных комиссий Совета безопасности Российской Федерации" [Online]. Available: https://base.garant.ru/5348225/ [Accessed: 8th May 2019]; Совет Безопасности РФ. Вопросы информационной безопасности при реализации национальной программы «Цифровая экономика России» обсуждены экспертами Совета Безопасности РФ. 29 октября 2018 года [Online]. Available: http://www.scrf.gov.ru/news/allnews/2493/ [Accessed: 8th May 2019]; Совет Безопасности РФ. В аппарате Совета Безопасности РФ рассмотрены вопросы развития цифровой экономики с точки зрения обеспечения национальной безопасности. 30 июня 2017 года [Online]. Available: http://www.scrf.gov.ru/news/allnews/2245/ [Accessed: 8th May 2019].

[2044] Указ Президента РФ от 10 ноября 2018 г. N 648 "Об утверждении состава Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям" [Online]. Available: https://base.garant.ru/72100350/ [Accessed: 8th May 2019].

institutions.[2045] The Security Council and its Committees have had a decisive role in how Russian information security has developed.[2046]

The role of the Bicameral Federal Assembly, i.e. the State Duma and the Federal Council in the area of information or cyber security is mainly limited to drafting and approving laws and offering a platform for "elite battleground" on issues concerning rents and power.[2047] Although many laws affecting the national segment of the Internet are proposed by seemingly independent parliamentarians, they are more often than not based on the guidance of the Presidential Administration, the Security Council, the government or corporation lobbyists.[2048] Donaldson and Nadkarni argue that under the Putin regime the parliament may have shaped the tone, tactics, and political climate through discussion but not its directions.[2049]

The Ministry of Digital Development, Communications and Mass Media (in short Minkomsviaz') is a federal executive organ responsible for, among other things, the development and implementation of state policy and regulatory framework in the field of information technology, telecommunications, radio spectrum, the Internet, and the provision of public services in the field of information technology. Basically, Minkomsviaz' has the power to regulate public telecommunications and government networks, including the content and some aspects of security, and it administers certificates of electronic signatures and regulates their providers. It is also responsible for forming 'a unified information space' in the territory of CIS countries. Minkomsviaz' takes part in mobilization and civil defence if so ordered.[2050] Minkomsviaz' is the ministry responsible for the national programme of the Digital Economy which is one of national programmes based on Putin's May Edicts 2018.[2051] It also maintains the register of Russian produced software (Unified Register of Russian Programs for Electronic Computers and Databases) and may in the future with some other ministries manage a register of Russian produced hardware.[2052] Federal

[2045] Указ Президента РФ 2011; Указ Президента РФ от 29 декабря 2018 г. № 771 "Состав научного совета при Совете Безопасности Российской Федерации" [Online]. Available: http://www.scrf.gov.ru/about/NS_spis_organ/sost_NS/ [Accessed: 8th May 2019].

[2046] Cf. Chapter 4.1.

[2047] Noble & Schulmann 2018.

[2048] Treisman 2019; Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) [Online]. Available: https://base.garant.ru/10103000/ [Accessed: 6th May 2019]; Sakwa 2008.

[2049] Donaldson & Nadkarni 2019, 152-253.

[2050] Постановление Правительства РФ от 02.06.2008 N 418 (ред. от 07.02.2019) "О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_77387/ [Accessed: 8th May 2019]; Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1 (последняя редакция) [Online]. Available: http:// www.consultant.ru/document/cons_doc_LAW_2481/ [Accessed: 8th May 2019]; Федеральный закон 2006.

[2051] Президиум Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 24 декабря 2018 года "Паспорт национальной программы «Цифровая экономика Российской Федерации»." [Online]. Available: http://static.government.ru/media/files/ urKHm0gTPPnzJlaKw3M5cNLo6gczMkPF.pdf [Accessed: 7th January 2020]; Правительство Российской Федерации. Заседание президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, 24 декабря 2018 [Online]. Available: http://government.ru/news/ 35168/ [Accessed: 8th May 2019].

[2052] On the register cf. Chapter 6.3.1. These are the Ministry of Industry and Trade of the Russian Federation, Ministry of Economic Development of the Russian Federation, and the Federal Antimonopoly Agency. (Федеральный закон 2006; Кодачигов, Валерий. В России появится реестр отечественного телеком-оборудования. Реестр отечественного софта уже три года ведет Минкомсвязи. Ведомости, 14 января 2019 agencies under Minkomsviaz' are responsible for the control and censorship of the Russian segment of Internet. The Ministry has been headed by Igor' Shchegolev (2008–2012), Nikolai Nikiforov (2012–2018), Konstantin Noskov (2018–2019) and Maksut Shadaev (2020–).[2053] In addition to Noskov, from 2018 to 2020 Vice-Premier Maksim Akimov has been responsible for transportation, communications, and digital economy.[2054] Akimov's position is a clear indication of the primacy the Kremlin sets for the controlling and developing of the national segment. He was replaced in January 2020 by Viktoriia Abramchenko.

Rozkomnadzor or the Federal Service for Supervision of Communications, Information Technology and Mass Media is the federal executive body responsible for, among other things, monitoring and supervising the mass media and electronic mass communications, information technologies and communications, the compliance of the processing of personal data with the requirements of the legislation of the Russian Federation, and the functions of organizing radio frequency service. Roskomnadzor's powers extend to the so-called special networks if they affect the routing of public networks. Moreover, it manages the Register of Information Dissemination Organizers (ORI) which defines the status of Russian ISPs and Internet content providers in the context of the laws regulating the Internet.[2055] Additionally, it maintains the register of blocked Internet resources, i.e. the Unified register of domain names, websites on the Internet and network addresses that identify Internet sites containing information the distribution of which is prohibited in the Russian Federation. The register obliges ISPs to block access to designated resources within a day of the promulgation of an order. Resources can be added to the register by Rozkomnadzor based on law or through a court decision.[2056] Rozkomnadzor will be responsible for the system for ensuring the resilience, security and integrity of the Russian segment of the Internet beginning from December 2019.[2057] This is a definite change in its responsibilities as it becomes a national security operator instead of being a supervisory and regulatory organ of state power. Under Roskomnadzor operates the Radio Frequency Service or Federal State Unitary Enterprise "Main Radio Frequency Centre" which has been allegedly responsible for monitoring the traffic of the national segment since 2014–2015 to ensure the compliance of the ISPs with the Unified Register. The Service will most probably operate the "Centre for monitoring and management of public telecommunications network" which will be used to disconnect the Russian segment of Internet from the global Internet if necessary.[2058]

[Online]. Available: https://www.vedomosti.ru/technology/articles/2019/01/14/791362-reestr-otechestvennogo [Accessed: 8th May 2019]).

[2053] Википедия. Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Online]. Available: https://ru.wikipedia.org/wiki/ Министерство_цифрового_развития,_связи_и_массовых_коммуникаций_Российской_Федерации [Accessed: 8th May 2019].

[2054] Ведомости. Кто вошел в новое правительство. Полный список. Десять вице-премьеров и двадцать один министр. Ведомости, 18 мая 2018 [Online]. Available: https://www.vedomosti.ru/economics/articles/2018/05/18/768949-pravitelstvo-polnii-spisok [Accessed: 8th May 219].

[2055] Постановление Правительства РФ от 16.03.2009 N 228 (ред. от 28.02.2019) "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций" (вместе с "Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций") [Online]. Available: https://base.garant.ru/195117/ [Accessed: 6th May 2019].

[2056] Федеральный закон 2006.

[2057] Федеральный закон 2019.

[2058] Голунов, Иван, Горбачев, Александр, Туровский, Даниил. «Симона» в поисках мата и порно «Медуза» выяснила, как работают сотрудники Роскомнадзора, которые занимаются цензурой в СМИ. И

Rossviaz' or the Federal Communications Agency is the federal executive body responsible for managing state property and providing public services in the field of telecommunications including communication networks and satellite services. It is responsible for managing the public telecommunications network of the RF during emergency situations.[2059] The satellite fleet is operated by Kosmicheskaia sviaz' company and consists of 12 satellites.[2060] Emergency communications are offered by the Federal State Budgetary Organization "Industry Expertise Centre for Monitoring and Development in the Sphere of Info-Communication Technologies" for example through TETRA networks.[2061] Furthermore, the SORM system was and is still developed by the FGUP TsNIIS under Rossviaz'.[2062] The convergence of mobile communications and data traffic further promotes Rossviaz's role.[2063]

Rospechat' or the Federal Agency for Press and Mass Communications is a federal agency which manages state property in the field of press, mass media and mass communications including computer networks. It implements state information policy, for example, through the control of the main television channels and by supporting various patriotic events like the Premiia Runeta competition.[2064]

The autonomous non-commercial organization (ANO) Digital Economy is one of the institutions created for the implementation of the national programme of the Digital Economy. Its main function is the coordination between the government and the state and private businesses. It monitors the development of the program, forms workgroups, comments on law drafts and participates in the goal setting of the program. It is led by people from the leading Russian ICT companies.[2065] Although it has no authority to allocate resources, it does provide a platform for debate and feedback

сколько это стоит. Meduza, 8 декабря 2017 [Online]. Available: https://meduza.io/feature/2017/12/08/ simona-v-poiskah-mata-i-porno [Accessed: 15th May 2019]; Роскомсвобода. Суверенное регулирование продолжает обрастать «нормативками». Роскомсвобода, 21.6.2019 [Online]. Available: https://roskomsvoboda.org/47728/ [Accessed: 8th July 2019].

[2059] Постановление Правительства РФ от 30.06.2004 N 320 (ред. от 25.09.2018) "Об утверждении Положения о Федеральном агентстве связи" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_48289/ [Accessed: 8th May 2019].

[2060] Космическая связь. Спутниковая группировка. [Online]. Available: https://www.rscc.ru/space/seriya-ekspress-am/ekspress-am44-11-zd/ [Accessed: 8th May 2019].

[2061] ФГБУ Центр МИР ИТ. Устав ФГБУ Центр МИР ИТ, 22.6.2016 [Online]. Available: http://centrmirit.ru/wp-content/uploads/2017/07/Ustav-FGBU-TSentr-MIR-IT.pdf [Accessed: 8th May 2019]; Ландышв, Юлия. Ростове монтируют новую систему связи для чемпионата мира по футболу. Современная радиосеть позволит надежно общаться тысячам волонтеров. Комсомольская Правда, 20 апреля 2018 [Online]. Available: https://www.rostov.kp.ru/online/news/3091086/ [Accessed: 8th May 2019].

[2062] Центральный научно-исследовательский институт связи. СОРМ [Online]. Available: https://zniis.ru/focus/sorm [Accessed: 8th May 2019].

[2063] Маркелов, Роман. В России предложили ввести платную регистрацию мобильных устройств. RG.ru, 25 января 2019 [Online]. Available: https://rg.ru/2019/01/25/v-rossii-predlozhili-vvesti-platnuiu-registraciiu-mobilnyh-ustrojstv.html [Accessed: 8th May 2019].

[2064] Постановление Правительства РФ от 17.06.2004 N 292 (ред. от 25.09.2018) "О Федеральном агентстве по печати и массовым коммуникациям" [Online]. Available: https://base.garant.ru/187125/ [Accessed: 22 January 2018]; Федеральное агентство по печати и массовым коммуникациям. Итоги премии Рунета 2017, 24 ноября 2017 [Online]. Available: http://www.fapmc.ru/rospechat/newsandevents/newsagency/2017/11/item20.html [Accessed: 8th May 2019].

[2065] Постановление Правительства РФ от 2 марта 2019 г. N 234 "О системе управления реализацией национальной программы "Цифровая экономика Российской Федерации" [Online]. Available: https://base.garant.ru/72190034/ [Accessed: 6th May 2019]; АНО «Цифровая Экономика». Наблюдательный совет АНО «Цифровая экономика» назвал законопроекты, которые требуют приоритетного одобрения Госдумой, 04.12.2018 [Online]. Available: https://data-economy.ru/04122018 [Accessed: 6th May 2019].

and it its officially connected to the government. In addition to the ANO Digital Economy there are also investment and financing tools like the Internet Initiatives Development Fund (FRII) which channels energy-revenues into the ICT sector,[2066] and government–private business forums like the Internet Development Institute (IRI).[2067] The Russian Union of Industrialists and Entrepreneurs (RSPP) also has a Committee of Digital Economy chaired by the President of Rostelekom.[2068] Because venture-capitalism is poorly developed in Russia, these organizations facilitate the process of allocating state resources to national projects.[2069]

The Ministry of Foreign Affairs (MFA) has a distinct role in the international cyber norm-building effort of the Russian regime.[2070] It must be noted that the MoD also has a role in this process as do some representatives from the security services. However, official international negotiations are conducted in the framework of the United Nations which is the territory of the MFA.[2071] Because the MFA does not conduct independent policy its main function in the context of information security is the advancement of Russian national interests by promoting Russian ideas about information security.[2072] To these ends, it in 2019 established the 42nd Department of International Information Security. It is headed by Andrei Krutskikh, a founding member of NAMIB and a career diplomat.[2073]

Independent, semi-independent, and subordinate think tanks and domestic and international forums provide a platform for developing technologies and policies related to the control and development of the national segment of the Internet.[2074] These think tanks include, for example, many of those which have representatives in the Security Council and whose members' writings have been analysed in Chapter 5 such as the PIR Centre, MGIMO, RISI, RIAC, the Centre of Strategic Estimations and Forecasts, the Centre for Military Strategic Studies of the General Staff, various institutes of the Russian Academy of Sciences, the Russian Academy of Rocket and Artillery Sciences, the Institute of Information Security Problems at the MGU, the Russian Presidential Academy of National Economy and Public Administration, the Skolkovo

[2066] Сухаревская, Алена. Нефтегазовый венчур: как работает Фонд развития интернет-инициатив. РБК, 28 апреля 2016 [Online]. Available: https://www.rbc.ru/magazine/2016/05/570fa16e9a794781cb616fa0 [Accessed: 17th May 2019].

[2067] IRI is connected to the Fond for Developing Internet-Initiatives (FRII) and ROTsIT which is a non-governmental Internet development organization. IRI has faltered after its initiator Viacheslava Volodin left the presidential administration. (Богданов, Юрий. Институт развития интернета укрепит цифровой суверенитет страны. ВЗГЛЯД, 12 марта 2015 [Online]. Available: https://vz.ru/society/2015/3/12/ 734014.html [Accessed: 9th May 2019]; Голицына, Анастасия. Институт развития интернета увольняет сотрудников. У организации начались проблемы с финансированием. Ведомости, 18 января 2017 [Online]. Available: https://www.vedomosti.ru/technology/articles/2017/01/18/673512-institut [Accessed: 17th May 2019].)

[2068] Российский союз промышленников и предпринимателей. Комитет по цифровой экономике [Online]. Available: http://www.rspp.ru/cc/news/60 [Accessed: 17th May 2019].

[2069] Бутрин, Дмитрий. «Конкуренция должна происходить внизу, в экосистеме». Коммерсантъ, №227 от 10.12.2019 [Online]. Available: https://www.kommersant.ru/doc/4187705 [Accessed: 6th January 2020].

[2070] Cf. Chapter 4 and 5; Nocetti 2015; Ristolainen 2017a & 2017b; Tikk & Kerttunen 2018.

[2071] Министерство иностранных дел Российской Федерации. О принятии Генассамблеей ООН российской резолюции по международной информационной безопасности. 7.12.2018 [Online]. Available: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/3437775 [Accessed: 6th May 2019].

[2072] Donaldson & Nadkarni 2019, 138.

[2073] Черненко, Елена. МИД обзаведется новым департаментом. Коммерсантъ №56 от 01.04.2019 [Online]. Available: https://www.kommersant.ru/doc/3930510 [Accessed: 6th January 2020].

[2074] CF. Иванов 2014; Vendil & Oxenstierna 2017.

technology park, and RAEK.[2075] While some of the think tanks might conduct secret research, the forums are open and are meant for exchanging and promoting ideas publicly. These include, for example, the SOC-Forum, the 1T Forum, the Russian Internet Forum, and some foreign policy and security forums like the Valdai Club and the Moscow Conference on International Security.[2076]

The Ministry of Defence is a federal executive organ which commands, controls and manages the Russian Armed Forces and coordinates its actions with other ministries and agencies. It develops and implements defence policy, coordinates with other federal organs on defence issues, and supports the military readiness of the Armed Forces. The MoD manages military procurement through a 'unified information system', cooperates with the OPK and conducts defence-related scientific research. It develops plans for mobilization of the economy including the use of infrastructure, organises the strategic deployment of forces and enables the mobilization of military forces. The MoD supervises the development of the command and control system of the AF, ensures the information security of the AF, organizes federal cooperation on the use of communications networks for the defence of the country, certificates military ICT, and conducts defence intelligence. The MoD also organizes the military-political activity of the AF. The MoD has the power to conduct and order independent construction projects for defence needs. It can conduct foreign policy activities related to the defence and military security of the Russian Federation, including military-technological cooperation. The minister of defence is directly responsible to the president. The MoD drafts, for example, the Defence Plan of RF, the Plan to Prevent and Deter Military Conflicts, the Mobilization Plan, and the Information Confrontation Plan, and the Defence Command and Control (management) Plan.[2077]

The Commander-in-Chief of the Russian Federation Armed Forces is the President. The AF is commanded by the Minister of Defence through the ministry.[2078] The General Staff is subordinated to the Minister of Defence and is responsible for the operational activities of the AF. The GS and the Main Directorate of Communications of the AF are responsible for the organization and maintenance of the telecommunications networks and automated control systems of the Armed Forces and national command and control centres.[2079] The MoD and the Armed Forces manage their own

[2075] RAEK is a commercial lobbying organization with tight relations with the government and the Digital Economy programme and publishes the yearly Economy of RuNet report (Ассоциация электронных коммуникаций (РАЭК) [Online]. Available: https://raec.ru/statute/ [Accessed: 9th May 2019].

[2076] SOC-Форум [Online]. Available: https://soc-forum.ib-bank.ru/ [Accessed: 9th May 2019]; ITForum. XI International it-forum with BRICS and SCO participation [Online]. Available: https://itforum.admhmao.ru/2018/ [Accessed: 9th May 2019]; РИФ. 23-й Российский Интернет Форум [Online]. Available: https://2019.rif.ru/ [Accessed: 9th May 2019; Ministry of Defence of the Russian Federation. VIII Moscow Conference on International Security [Online]. Available: https://eng.mil.ru/ en/mcis/index.htm [Accessed: 9th May 2019].

[2077] Указ Президента РФ от 16.08.2004 N 1082 (ред. от 26.01.2019) "Вопросы Министерства обороны Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_48879/ [Accessed: 9th May 2019].

[2078] Федеральный закон 1996.

[2079] Указ Президента РФ от 23.07.2013 N 631 (ред. от 01.07.2014) "Вопросы Генерального штаба Вооруженных Сил Российской Федерации" (вместе с "Положением о Генеральном штабе Вооруженных Сил Российской Федерации") [Online]. Available: http://www.consultant.ru/document/ cons_doc_LAW_149773/ [Accessed: 9th May 2019]; Mil.ru. Главное управление связи Вооруженных Сил Российской Федерации [Online]. Available: https://structure.mil.ru/structure/ministry_of_defence/details.htm?id=9587@egOrganization [Accessed: 9th May 2019].

networks which are partly disconnected from the public Internet but at least partly rely on the civilian information infrastructure.[2080] They are able to protect their networks through the operations of the Main (Intelligence) Directorate, Information troops, EW troops, science companies, military-scientific institutions, and military SOCs and CERTs.[2081]

The Federal Service for Technical and Export Control Agency (FSTEK) functions under the MoD and is responsible for ensuring the protection of the critical information infrastructure including super-computers, as well as countering foreign technological intelligence activities, ensuring the protection of state secrets, and conducting export control. In practice, the FSTEK regulates the actions of the federal, regional and municipal organs and private actors. It also licenses approved information security actors and provides certificates for officially approved solutions and products—the exception is cryptography which belongs to the mandate of the FSB. The FSTEK has the right to supervise technological counter-intelligence activities and information security systems of public organs except the MoD, SVR, FSB, FSO and the General Directorate of Special Programmes for the President of the Russian Federation (GUSP).[2082] The FSTEK and FSB must approve the security systems and cryptography used in systems transferring secret information across Russia's borders to foreign networks.[2083] The protection of the CII is largely based on the responsibilities of the operators of the CII. They are monitored and regulated by the FSTEK which manages a register of the CII. The FSTEK is responsible for establishing requirements for the protection of the CII but must cooperate with, for example, Minkomsviaz' and the Bank of Russia, in the case of systems related to their authority.[2084] The FSTEK's responsibilities in the area of the CII are based on earlier regulations on the protection of ASUs and critical objects.[2085]

[2080] Cf. Chapter 6.3; Carr 2012; Зыков & Рамм 2016.

[2081] Cf. Chapter 6.3; Независимое военное обозрение 2017; Иванов, Павел. Плакали ваши хакеры. ВПК, № 18 (2017); Туровский Даниил. Российские вооруженные киберсилы Как государство создает военные отряды хакеров. Meduza, 7 ноября 2016 [Online]. Available: https://meduza.io/feature/2016/ 11/07/rossiyskie-vooruzhennye-kibersily [Accessed: 9th May 2019]; Рябов, Кирилл. Мультисервисная транспортная сеть связи для министерства обороны. Военное обозрение, 13 марта 2019 [Online]. Available: https://topwar.ru/155340-multiservisnaja-transportnaja-set-svjazi-dlja-ministerstva-oborony.html [Accessed: 18th April 2019]; Kjellén 2019.

[2082] Указ Президента РФ от 16 августа 2004 г. N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" (с изменениями и дополнениями) [Online]. Available: https://base.garant.ru/ 12136635/ [Accessed: 6th May 2019]; ФСТЭК. Сведения о полномочиях ФСТЭК России; перечень нормативных правовых актов, определяющих эти полномочия. 28 Марта 2016 [Online]. Vailable: https://fstec.ru/obshchaya-informatsiya/polnomochiya [Accessed: 6th May 2019]; Приказ Федеральной службы по техническому и экспортному контролю от 3 апреля 2018 г. N 55 "Об утверждении Положения о системе сертификации средств защиты информации" [Online]. Available: http://ivo. garant.ru/#/document/71942006/paragraph/1:0 [Accessed: 8th May 2019].

[2083] Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_75586/ [Accessed: 6th May 2019].

[2084] Федеральный закон 2017; Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. N 239 "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации" (ред. от 9 август 2019) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_294287/ [Accessed: 6th January 2020].

[2085] Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. N 31 "Об утверждении Требований к обеспечению защиты информации в автоматизированных системах

The military-industrial complex (OPK), understood as the private and state companies and corporations providing equipment and services to the MoD and its armaments programme has a distinct role in providing the 'military Internet' with the connectivity, resources and services it requires. These are mainly military solutions and meant exclusively for the Armed Forces. However, in the context of ICT and cyber security there is much overlap between the military and civilian technologies as dual use is becoming increasingly common. Furthermore, as there are dozens of research institutes operating under the MoD with various commercial connections the lines between the military and OPK become highly blurred.[2086] Many of the think tanks listed above could be rightfully placed into the OPK but at least the 27th TsNII, 16th TsNII, 18th TsNII, 4th TsNII, TsNII EISU, and the Era technology park can be considered inherently part of the OPK.

The Ministry of Interior's role in controlling and developing the national segment of the Internet lays in its power of criminal investigation. Cybercrimes are investigated by Directorate K.[2087] Other ministries like the Ministry of Industry and Trade of the Russian Federation and the Ministry of Economic Development of the Russian Federation affect the national segment mainly through import substitution policies which are meant to promote Russian domestic software and hardware development and production.[2088]

The FSB or the Federal Security Service has an important role in controlling the national segment. Consequently, two of its main functions are counterintelligence and ensuring information security. Firstly, it manages the SORM system for criminal investigation, domestic intelligence, and counter-intelligence purposes and conducts criminal investigations into cybercrimes.[2089] Secondly, it controls the GosSOPKA system through the National Coordination Centre of Computer Incidents (NKTsKI).[2090]

управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды" (с изменениями и дополнениями) [Online]. Available: https://base.garant.ru/70690918/ [Accessed: 6th May 2019].

[2086] Bitzinger, Richard A. and Popescu, Nicu. Defence industries in Russia and China: players and strategies. EU Institute for Security Studies, Report No 38 – December 2017 [Online]. Available: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Report_38_Defence-industries-in-Russia-and-China.pdf [Accessed: 9th May 2019]; Связь. Связь в Вооруженных Силах Российской Федерации 2018. Москва: Информационный мост, 2018.

[2087] Keir 2011; Carr 2012; Министерство Внутренних Дел Российской Федерации. Управление «К» МВД России [Online]. Available: https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii [Accessed: 6th May 2019].

[2088] Шмырова, Валерия. В России хотят запретить госзакупки иностранных СХД. CNews, 8 мая 2019 [Online]. Available: http://www.cnews.ru/news/top/2019-05-08_v_rossii_zapretyat_goszakupki_ inostrannyh_shd?utm_source=yxnews&utm_medium=desktop [Accessed: 9th May 2019].

[2089] Федеральный закон от 03.04.1995 N 40-ФЗ (ред. от 07.03.2018) "О федеральной службе безопасности" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_6300/ [Accessed: 9th May 2019]; Приказ Минкомсвязи России от 12.12.2016 N 645 "Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть I." (Зарегистрировано в Минюсте России 13.01.2017 N 45201) [Online]. Available: https://digital.gov.ru/ru/documents/5413/ [Accessed: 9th May 2019].

[2090] Федеральный закон 2017; Приказ ФСБ России от 24.07.2018 N 366 "О Национальном координационном центре по компьютерным инцидентам" (вместе с "Положением о Национальном координационном центре по компьютерным инцидентам") (Зарегистрировано в Минюсте России 06.09.2018 N 52109) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_306334/ [Accessed: 18th April 2019]; Выписка. "Выписка из Концепции государственной системы обнаружения, предупреждения

Thirdly, the FSB functions as the national authority on certification of cryptographic means and licensing their development.[2091] The FSB encryption certification and investigative powers extend to all government agencies. Moreover, the so-called Anti-Terrorism laws require ‘organizations disseminating information’ to release their encryption keys to the FSB.[2092] The FSB’s main cybercrime investigation unit is the Information Security Centre which was tarnished in an espionage scandal in 2017.[2093] The Communications Security Centre (8th Directorate) operates the NKTsKI and ensures security standards for government communications.[2094] The Centre for Licensing, Certification and Protection of State Secrets manages cryptography licences and certificates.[2095]

The FSO or Federal Protective Service mainly provides and secures the confidential and secret communication of the Presidential Administration and the government or ‘the Russian governmental segment of the Internet.’[2096] The structure of the FSO includes the Special Communications and Information Service (Spetssviaz’) which in practise manages the FSO’s communications responsibilities. The Spetssviaz’ operates the government’s special networks, command and control posts, situation centres, and prepares communications for wartime.[2097] Interestingly, the FSO is also responsible for gathering situation information on the federal level about political, societal and economic issues.[2098]

Multiple CERTs are responsible for incident response in the public networks and in certain segments of private networks and coordinate actions between corporation

и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации” (утв. Президентом РФ 12.12.2014 N К 1274) [Online]. Available: http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf. [Accessed 10 January 2018]; ГосСОПКА. Нормативные документы о безопасности КИИ [Online]. Available: http://gossopka.ru/law/ [Accessed: 6th May 2019].

[2091] Приказ федеральная служба безопасности российской федерации № 41821 23 марта 2016 года [Online]. Available: http://www.fsb.ru/files/PDF/prikaz_182.pdf [Accessed: 6th May 2019].

[2092] Федеральный закон от 06.07.2016 N 374-ФЗ “О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности” (последняя редакция) [Online]. Available: http://www.consultant.ru/document/ cons_doc_LAW_201078/ [Accessed: 9th May 2019].

[2093] Алехина, Маргарита. Хакер из «Шалтая-Болтая» заявил о сотрудничестве с ФСБ. РБК, 9 января 2019 [Online]. Available: https://www.rbc.ru/society/09/01/2019/5c35fab59a7947185fe6da57?from=main [Accessed: 9th May 2019].

[2094] Carr 2012; Жукова, Кристина. ГосСОПКА сдадут под ключ. Коммерсантъ №215 от 20.11.2017 [Online]. Available: https://www.kommersant.ru/doc/3472959?from=four_tech [Accessed: 9th May 2019].

[2095] Центр по лицензированию, сертификации и защите государственной тайны ФСБ России. Перечень средств защиты информации, сертифицированных ФСБ России [Online]. Available: http://clsz.fsb.ru/files/download/svedeniya_po_sertifikatam_22.04.doc [Accessed: 9th May 2019].

[2096] Указ Президента РФ от 07.08.2004 N 1013 (ред. от 27.02.2018) “Вопросы Федеральной службы охраны Российской Федерации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_48778/ [Accessed: 9th May 2019]; Указ Президента Российской Федерации от 22.05.2015 № 260 “О некоторых вопросах информационной безопасности Российской Федерации” [Online]. Available: http://www.consultant.ru/document/Cons_doc_LAW_179963/ [Accessed 11 January 2018]; Susiluoto 2006; Carr 2012.

[2097] Указ Президента Российской Федерации от 14 июля 2003 г. N 774 Вопросы службы специальной связи и информации при Федеральной службе охраны Российской Федерации [Online]. Available: http://www.agentura.ru/dossier/russia/fso/docs/polojeniespecvyaz/ [Accessed: 6th May 2019].

[2098] Звездина, Полина. Охрана для нацпроектов: почему контроль за майским указом отдали ФСО. РБК: 26 октября 2018 [Online]. Available: https://www.rbc.ru/society/26/10/2018/5bd1b4299a7947b26916a555?from=center_5 [Accessed: 6th May 2019].

SOCs.[2099] Moreover, at least some of them are connected to the GosSOPKA network.[2100] Admittedly, when it comes to the cyber security management of confidential government networks, the responsibilities of the FSB, FSO and CERTs are somewhat difficult to distinguish, although their cooperation is increasing.[2101]

The Coordination Centre of National Domain of Internet and Technical Centre Internet are responsible for the administration of the main ccTLD servers and managing .ru, .рф and .su domains. They provide connectivity and technical control on a national level and are the Russian national contact point for the Internet's international multi-stakeholder governance.[2102] Moreover, the Coordination Centre manages a national cybersecurity information platform 'Netoskop' which enables public and private actors to share threat intelligence and, furthermore, to eliminate these threats though the Coordination Centre's ability to remove hostile resources from national domains.[2103]

The role of the ISPs and hardware and software companies is to provide connectivity, resources and services for the national segment of the Internet. They form the core of the segment and provide the infrastructure upon which the federal government and military networks are built. Many of the most critical companies are owned by state corporations.[2104] The companies, be they private or public, do of course affect the national segment in multiple ways, but from the regimes point of view, they appear only as potential resources and tools of control. They form the backbone of digital sovereignty but also an environment that needs to be controlled and delineated from the rest of the cyberspace. However, as Rostelekom owns much of the critical infrastructure of the national segment and many private companies are tightly connected to the regime, they also function as tools of indirect control. This category also includes the commercial and non-commercial, private and state-owned domain name registrars and IXP managers. The final actor affecting the control and development of the national segment is civil society. Although Russia has not developed the same

[2099] Коммерсантъ. Киберугрозы сажают на CERT. В России создают центр реагирования на инциденты в сфере информационной безопасности. Коммерсантъ №160 от 01.09.2016 [Online]. Available: http://www.kommersant.ru/doc/3077603 [Accessed: 9th May 2019]; Коломыченко, Мария. Киберспецслужба: Сбербанк предложил создать штаб борьбы с хакерами. РБК, 1 сентября 2017 [Online]. Available: https://www.rbc.ru/technology_and_media/01/09/2017/59a9799f9a7947375702db15?from=center_7 [Accessed: 9th May 2019].

[2100] Грачёв, Анатолий. Технические аспекты взаимодействия с НКЦКИ. SOC-Форум, 27 ноября 2018 [Online]. Available: https://soc-forum.ib-bank.ru/files/files/SOC%202018/08_Grachev.pdf [Accessed: 9th May 2019]; Григорьев, Дмитрий. Решения от InfoTeCS. Защита от компьютерных атак, 2017 [Online]. Available: http://www.cio-sibir.ru/files/Meet/2017/10/GosSOPKA.pdf [Accessed: 10th May 2019].

[2101] Нефёдова, Мария. Эксперты Group-IB сообщают, что рунет стал чище. Хакер, 5.7.2019 [Online]. Available: https://xakep.ru/2019/07/05/runet-stats/ [Accessed: 7th July 2019].

[2102] Cf. Chapter 6.1.1.

[2103] Координационный центр доменов .RU/.РФ «Национальный координационный центр по компьютерным инцидентам (НКЦКИ)» стал новой компетентной организацией при Координационном центре доменов .RU/.РФ, 6 августа 2019 [Online]. Available: https://cctld.ru/media/news/kc/21309/ [Accessed: 7th August 2019].

[2104] Chapter 3.1; Vendil Pallin 2017; Связь. Связь в Вооруженных Силах Российской Федерации 2017. Москва: Информационный мост, 2017; Связь 2018; Minkomzsiaz'. "Nikolay Nikiforov Presented Branch Plan on Import Substitution of Software," (2015, Apr. 3rd). [Online]. Available: http://minsvyaz.ru/en/events/32967/. [Accessed 12 January 2018].

degree of aggressive voluntary civilian censorship as China, the League of Safe Internet has similar characteristics.[2105]

A few observations are necessary before moving on to laws and policies. First, there are some over-lapping functions that may hinder the control and shaping of the national segment of the Internet. For example, multiple actors are responsible for the monitoring and security of the segment or its distinct parts. However well-defined the policies derived from strategic planning are, the political and institutional system described above combined with multiple actors and the possibility of gathering rents through licences, certificates, government orders etc. may lead to rent-seeking behaviour, corruption, and institutional infighting. Secondly, the whole system of responsibilities described above is an effort to push top-to-bottom control on a network that has developed from the bottom-to-top. This will lead to resistance, friction, and compromise. Thirdly, all the different actors and networks lead to multiple systems which lead to multiple gateways between systems and which quite possibly may lead to multiple vulnerabilities. Russian cyber security actors are aware of this and centralization and dismantling of stove-piped organizations is understood as a necessity. However, this is much easier said than done. Thus, we should not be surprised if the strategic cultural ideas present amongst the epistemic communities and even found in strategic documents and policies do not resonate with the actual performance of the regime. Fourthly, the heavy presence of the security services or more inclusively 'the power ministries' in the managing of the national segment will probably affect the way in which policies are formulated and implemented. This presence is probably somewhat mitigated by the lobbying of Internet industry people whose business model is affected by increased state control. Fifthly, the Russian concept of 'state secret' has a cross-cutting influence on all the actors and their responsibilities. The protection of the secrecy of information is well established in laws and regulations.[2106] Moreover, state secrets have also their own highly secret agency.[2107] And sixthly, it is clear that some people discussed in Chapter 4 and 5 have moved into and out of the institutions developing and implementing policies. Therefore, it is reasonable to expect that there will be some connection between their ideas and the way the Russian elites began to shape cyberspace in the 2000s and 2010s.

6.2.2 International treatises and ideas

This chapter provides an analysis of the way in which the strategic cultural ideas resonate with the international treatises on cyber or information security which Russia has promoted or adopted from 1998 to 2018. I will examine the treatises chronologically to investigate if and how the treatises correlate with changes in the Russian strategic environment.[2108]

[2105] Балашова, Анна, Посыпкина, Александра. Властям предложили штрафовать соцсети и поисковики за запрещенный контент. РБК, 22 октября 2018 [Online]. Available: https://www.rbc.ru/technology_and_media/22/10/2018/5bcda8179a79471e45ad2d1e#ws [Accessed: 9th May 2019]. For China cf. Griffiths 2019.

[2106] It is defined in the Law on State Secrets which designates three levels of secrecy of information – special importance, top secret, and secret. (Закон РФ 1993).

[2107] Кузнецов, Юрий. Сто лет на охране секретов государства. Красная звезда, 2.11.2018 [Online]. Available: http://redstar.ru/sto-let-na-ohrane-sekretov-gosudarstva/ [Accessed: 17th May 2019].

[2108] Previous studies on the subject cf. Popescu, Nicu and Secrieru, Stanislav (Eds.) Hacks, Leaks and Disruptions: Russian Cyber Strategies. Chaillot Papers No. 148, October 2011. Paris: European Union Institute for

The ideas of interstate struggle, digital sovereignty, and information-technological warfare were explicitly present in the Russian proposals on drafting an international norm to ban 'information weapons.' The first proposal was delivered to the United Nations General Assembly in 1998.[2109] Even before this the CIS countries had adopted an appeal "On the Prevention of Information Wars" which was presented to the UN, the OSCE and the Council of Europe in 1997.[2110] In his letter to the Secretary-General of the UN the Russian ambassador to the UN Sergei Lavrov claimed that developments in the information field were being used for purposes incompatible with maintaining international stability and security, as well as the principles of the non-use of force and non-interference in internal affairs. This could lead to the emergence of a fundamentally new area of international confrontation, information wars, which he understood as "actions taken by one country to damage the information resources and systems of another country while at the same time protecting its own infrastructure." A new arms race could develop as information weapons with destructive effects comparable to that of weapons of mass destruction appeared.[2111] Lavrov thus summarized the Russian negotiation position, which has remained more or less unchanged from 1998 to 2018.[2112]

In the context of drafting international cyber security norms, in 2001 Russia argued that information threats included the following: technological attacks against information resources, telecommunications systems and critical structures of the state; the use of information to undermine the state's economic and social systems and psychological manipulation of society for the purposes of destabilising society; illegal penetration of information-telecommunications systems of the state; efforts to dominate the information space by imposing technological standards on less developed countries and restricting their access to advanced technology; the encouragement of the terrorist use of information; the adoption of doctrines aimed at waging information war; the use of information technologies to the detriment of human rights and freedoms; the blurring of state borders and jurisdictions that normally delineate national security; and the manipulation of information flows and spreading of disinformation including the eroding of spiritual values.[2113] Information security was defined for the information space, which included the consciousness of the people, infrastructure and information. Information weapons caused damage to the state interests on technological and psychological level.[2114] The threats and definitions were clearly based on

Security Studies, 2018; Giampiero 2014; von Heinegg, Wolff Heintschel: Legal Implications of Territorial Sovereignty in Cyberspace. In Czosseck, C., Ottis, R. and Ziolkowski, K. (Eds.) 4th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, 2012, 7-20; Nocetti 2015; Eneken 2016; Eneken & Kerttunen 2017; Giles 2012.

[2109] United Nations General Assembly. Resolution adopted by the general assembly. Developments in the field of information and telecommunications in the context of international security. A/RES/53/70 4 January 1999 [Online]. Available: https://undocs.org/A/RES/53/70 [Accessed: 10th May 2019].

[2110] Матяшов, Виктор. Войны в информационном пространстве. Защита и безопасность, № 1 (2009), 17-19.

[2111] Комов 2009, 144.

[2112] Eneken & Kerttunen 2017. Grisby, Alex. Russia and the U.S. Offer Competing Vision of Cyber Norms to the U.N. Defence One, October 29, 2018 [Online]. Available: https://www.defenseone.com/politics/2018/10/russia-us-offer-competing-vision-cyber-norms-un/152382/?oref=d-river [Accessed: 25th February 2019].

[2113] Комов 2009, 189-199.

[2114] Ibid., 181-182.

the idea of territorial state sovereignty in information (cyber) space. The threat 'cavalcade' shows that both information-technological and the psychological aspects were present as distinct threats, although the objective, i.e. the destabilization of a state dominated the understanding. Moreover, information threats were explicitly connected to strategic stability and the interstate struggle in the claim that the 'denial of technology' was used as a tool of domination. Information war was now part of the modern character of war also on the diplomatic level.

In 1999 the CIS adopted the Concept of Information Security of the Members of CIS in the Military Sphere. It recognized a full spectrum of sources of information threats the main one of which was the espionage conducted by 'foreign countries' aimed at achieving unilateral advantages. It also recognized the use of exported hardware and software as a threat and argued for cooperation between the CIS countries in the confines of their national interests. The ultimate goal of the Concept was to form a common information policy, to create "a unified information space [edinnoe informatsionnoe prostranstvo]", and to develop and implement measures to ensure the military information security of the member states."[2115] The strategic cultural ideas were thus present in the CIS concept also already at the beginning of the Putin regime. The presence of the EIP in the context of the CIS shows how the borders of the information space were inherently political.

The effort to build norms in the context of the SCO began in 2006 when the heads of the SCO gave a declaration on the international information security which envisioned information-communication technology as a military-political tool of states on a par with weapons of mass destruction.[2116] Its argument was based on the view that "ICT forms the global information environment, upon which the state of political, economic, defence, socio-cultural and other components of national security and the general system of international security and stability directly depend."[2117] Information had thus become one of the most important political-economic resources, and, consequently, ICT could be used to interfere in the internal affairs of states for terrorist purposes and for military-political ends. The heads of states argued that the development and use of ICT should respect national and cultural traditions and declared their support for a state-centric and UN led process of international information security norm-building.[2118] Based on the declaration, the strategic cultural ideas of Russia and China were quite well synchronized from the beginning. The declaration did not envision an EIP inside the SCO and it was based on technology and military-political threats more than psychological threats. The declaration was probably connected to the ITU/UN led WGIG/WSIS process and was an effort to establish joint SCO views on the issues debated there—thus state sovereignty was a guiding idea.[2119]

[2115] СНГ. Концепция информационной безопасности государств-участников Содружества Независимых Государств в военной сфере, 4 июня 1999 года [Online]. Available: http://www.e-cis.info/page.php?id=21396 [Accessed: 25th February 2019].

[2116] ШОС. Заявление глав государств – членов Шанхайской организации сотрудничество по международной информационной безопасности. Г. Шанхай, 15 июня 2006 года [Online]. Available: http://rus.sectsco.org/ [Available: 2nd April 2019]; Комов 2009, 219-222.

[2117] ШОС 2006.

[2118] Ibid.

[2119] Cf. Chapter 6.1.3.

In 2008 the CIS adopted the Concept of Cooperation of the States Parties of the Commonwealth of Independent States in the Field of Information Security.[2120] It defined information security through threats and was quite state-centric. The threats emanated, for example, from other states trying to destabilize the social-political situation of other countries, from criminals and terrorists, from unsanctioned access to state information, and from states trying to dominate the information space. The concept of space was not defined but the CIS was described as having its own information infrastructure. The objects of threats were, among other things, the interstate cooperation of the CIS states, the information infrastructure of the CIS, the interstate information systems including telecommunications networks and ASUs of military forces, and the services and systems based on those systems. The common tools of the CIS to counter these threats would be legal, organization-technological, and organization-economic.[2121] The Concept was an effort to define many central concepts of information security, but it is clearly a result of compromise and partly vague and partly quite technical. There is a clear tension between proposed technological and technical methods of security and the view that the information threats are partly psychological and highly political. However, there is little in the document that does not resonate with the strategic cultural ideas.

In 2009 the SCO adopted the Agreement on Cooperation in the Field of International Information Security between the Governments of the Member States of the Shanghai Cooperation Organization.[2122] The Agreement did not enter into force until 2012. It was a defining agreement offering a much clearer vision of information security than Russia's previous international treatises. Information threats were categorized into the use of information weapons to wage information war (informatsionnaia voina), which was understood as a confrontation (protivoborstvo) between states in the information space (informatsionnoe prostranstvo), terrorism, crime, the efforts to use a dominant position in the information space to cause damage to others, disseminating harmful information to the political, social, economic, spiritual and cultural systems of other states, and threats to the global information infrastructure. The Agreement defined the protection of information resources and critically important infrastructure as belonging to the state interest. Each party to the agreement had the right to protect its own information resources and structure.[2123] Information resources were defined as the infrastructure and information itself, and critical structures were objects, systems and institutions which if damaged could threaten national security.[2124] This duality resonated with the Russian technological-psychological IW categorization. However, the information-technological and psychological threats, means, and objectives of IW are perhaps more intertwined than in the previous treatises. This resonates with the idea of strategic deterrence which was developing at that

[2120] СНГ. Решение о Концепции сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности и о Комплексном плане мероприятий по реализации Концепции сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности на период с 2008 по 2010 год [Online]. Available: http://www.e-cis.info/page.php?id=20229 [Accessed: 25th February 2019].

[2121] Ibid.

[2122] ШОС. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 16 июня 2009 года. Екатеринбург. [Online]. Available: https://base.garant.ru/2571379/ [29th March 2019].

[2123] Ibid.

[2124] Ibid.

time. The idea of sovereignty over and in information space is present but is not mentioned directly. The threats described in the Agreement are connected to the idea of the interstate struggle and information superiority, although on a strategic level. The SCO Agreement raises the question of how much the Russian elites were affected by domestic ideas and what role Chinese ideas played. The SCO affirmed its commitments to the 2008 Agreement in the 2017 Astana declaration.[2125]

In 2011 and 2015 the members of the SCO and some others submitted their joint proposals for the International Code of Conduct for Information Security for the UN Secretary-General.[2126] They proposed that states would recognize "norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries."[2127] States should not use information and communication technologies to carry out hostile actions, should reaffirm the right of states to protect their information space and should promote multilateral, transparent and democratic governance of the Internet.[2128] To the listed hostile actions, the 2015 version added "interference to internal affairs" and "undermining political, economic and social stability" and emphasised the role of states in the governance of the Internet.[2129] The last point is probably connected to the failed effort of Russia in the WCIT meeting in 2012 Dubai to push through ITU control over IANA/ICANN.[2130] In the proposals the Russian strategic cultural ideas are presented as the building blocks of international norms. Sovereignty was positioned in the information space as new international norms would build borders for it. Interstate struggle and information superiority in the form of strategic balance, i.e. 'equality' were present. Security is the security of states. On this level, the lines between information-technological and psychological warfare are most blurred. The EIP is present as the global and common information space which needs to be regulated—it is however distinct from the idea of how national information spaces should be ordered. Both the 2011 and 2015 proposals should be understood through strategic deterrence as they are meant to prevent threats from materializing and to weaken and restrain powerful opponents.

In 2012 the CIS adopted the Agreement on the Cooperation of the State Members of the Commonwealth of Independent States in the Field of Information Security which

[2125] ШОС. Астанинская декларация глав государств – членов Шанхайской организации сотрудничества 9 июня 2017 года [Online]. Available: http://kremlin.ru/supplement/5206 [Accessed: 10th May 2019].

[2126] For a comparison of the 2011 and 2015 version cf. McKune 2015.

[2127] United Nations General Assembly. Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. A/66/359, 14 September 2011. [Online]. Available: https://undocs.org/A/66/359 [Accessed: 2nd April 2019].

[2128] Ibid.

[2129] United Nations General Assembly. Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed Secretary-General. A/69/723, 13 January 2015 [Online]. Available: https://undocs.org/A/69/723 [Accessed: 2nd April 2019].

[2130] Julian Nocetti argues that the ITU-WCIT 2012 in Dubai was a sign of a new, more contentious phase in Internet governance (Nocetti 2015, 121-125).

updated the 2008 Concept.[2131] It defined practical goals for CIS information security cooperation based on state interests. The object of cooperation was information and 'the interstate information system.' The 2012 Agreement implicitly called for the creation and control of the CIS information space through governance, encryption, cyber security systems, regulation of cross-border traffic, and standardization of technological solutions. As was the case with the 2008 Concept, the strategic cultural ideas are implicitly present. The most interesting point is the drive to shape the CIS EIP into being through cooperation on information security. Still, the CIS agreement demonstrates the tension between the idea of sovereignty and the EIP when they are transferred to a regional context.

In 2013 Russia adopted the Basics of Government Policy in the Area of International Information Security.[2132] Its substance correlated with the 2011 and 2015 International code of conduct for information security initiatives. The document was also in line with the Russian overall foreign policy as it promotes a regional approach in norm-building. The objective of the Russian policy was the achievement and retaining of technological parity with leading world great powers and ensuring the strategic stability. The policy should secure 'the technological sovereignty' of Russia.[2133] The policy represented a clear indication of the move from sovereignty in information space towards full digital sovereignty. It was also explicitly related to interstate struggle and information superiority.

In addition to the SCO, Russia promoted cyber security norms in the CSTO which adopted the Protocol On the Interaction of the State Members of the Collective Security Treaty Organization in Combating Criminal Activities in the Information Sphere in 2014.[2134] The most interesting aspect of the Protocol are the definitions of 'information space'[2135] and 'information sphere'[2136] and the use of the concept of 'the national segment of the Internet' when referring to the part of information space under state jurisdiction. As was noted in Chapter 5 this concept appeared in the context of the CIS and more precisely in Belarussian documents around 2010. The Protocol was a clear move towards territorially defined information sovereignty and an acknowledgement that the Internet should be divided into sovereign segments. Although the Protocol is officially about combatting criminal activities it emphasises the 'destructive effects' against the constitutional order and national security which hardly

[2131] Распоряжение Правительства РФ от 28 мая 2012 г. №856-р. О подписании Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности [Online]. Available: https://digital.gov.ru/ru/documents/3729/ [Accessed: 29th March 2019].

[2132] Основы 2013.

[2133] Ibid.

[2134] ОДКБ. Протокол О взаимодействии государств – членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере, от 23 декабря 2014 года [Online]. Available: http://base.spinform.ru/show_doc.fwx?rgn=77790 [Accessed: 25th February 2019].

[2135] "An area of activity related to the formation, creation, transformation, transfer, use, storage of information that has an impact on the individual and public consciousness, the information infrastructure and the information itself." (ОДКБ 2014). This same definition was used in the Russia–China Information Security Agreement in 2015 (Правительство Российской Федерации 2015a).

[2136] "A set of information, information infrastructure, entities engaged in the collection, formation, dissemination and use of information, as well as a system for regulating the resulting public relations." (ОДКБ 2014).

sound like criminality.[2137] Nevertheless, the crime-aspect silences the influence of some strategic cultural ideas and gives room only to the centrality of sovereignty and the EIP in the form of the national segment of the Internet.

Russia and China signed the Agreement on Cooperation in the Field of International Information Security in 2015.[2138] It expressed the now already established view that information and communications technology could be used for military ends and "to undermine the sovereignty and security of states and interfere in their internal affairs, violate the privacy of citizens, destabilize internal political and socio-economic situation, incite ethnic and religious hatred." The information infrastructure on a state's territory, including the Internet, was under its sovereign rights, and the governance of the Internet should be 'democratised' and 'internationalised'. The Agreement added to the threats expressed in the 2009 SCO Agreement threats to economy and the interference in the internal affairs of states.[2139] The Agreement was clearly based on the idea of information sovereignty and struggle in information space manifested in the notion that some actors had attempted to gain dominance over Russia and China. The wide range of threats resonates with strategic deterrence. The additions to the threat list meant that now information security cut across all spheres of state interests. The 2015 Agreement used the same wording as the 2009 SCO agreement which is further proof that Chinese and Russian ideas have interacted.

The declarations given in the conclusion of the BRICS summits in 2015 and 2017 reflected the views presented in Russia's UN Code of Conduct initiatives and the Basics of Government Policy document. However, their tone was not as confrontational as in the CIS and SCO treaties. Moreover, the aspects of territorial sovereignty and national segments of the Internet were overshadowed by the idea of an open, common, and secure Internet in 2015 and a peaceful, secure, open, cooperative, stable, orderly, accessible and equitable ICT environment in 2017.[2140] The declarations were the result of negotiations between Russia, China, Brazil, India, and South Africa so their substance was based on the interaction between strategic cultural ideas from different nations—as well as cold-blooded realpolitik and compromise.

The Strategy of Collective Security of CSTO for 2025 adopted in 2016 is perhaps the most confrontational of the treatises discussed thus far. It recognized that information and communication technology can be used to pressure states, to interfere in their internal affairs, to inflict destructive socio-political and socio-economic, to and manipulate the public consciousness. It even mentions 'colour revolutions' and 'hy-

[2137] It is possible that Russia wanted to avoid the 'militarization' of the 'information sphere' as it was contrary to its international cyber security norm-building project. Thus, the Protocol concentrated on criminality.

[2138] Распоряжение Правительства Российской Федерации от 30 апреля 2015 г. N 788-р О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности [Online]. Available: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=620700#0463235836450268

[2139] Ibid.

[2140] БРИКС. VII саммит БРИКС Уфимская декларация (Уфа, Российская Федерация, 9 июля 2015 года) [Online]. Available: http://www.brics.utoronto.ca/docs/150709-ufa-declaration-ru.pdf [Accessed: 10th May 2019]; БРИКС. Сямэньская декларация руководителей стран БРИКС (Сямэнь, Китай, 4 сентября 2017 года) [Online]. Available: http://kremlin.ru/events/president/news/55515 [Accessed: 10th May 2019].

brid wars.' To counter these effects, it was seems as necessary to create a secure information space and a system of information security of the CSTO member states.[2141] The Strategy mentions non-state threats, i.e. terrorism, separatism, and criminality but it is definitely state-centric in its approach emphasising the territorial integrity and sovereignty of the member states. All strategic cultural ideas are present in the CSTO Strategy: The idea of struggle now takes new forms; information is used to degrade sovereignty; multifaceted deterrence is needed to counter multifaceted threats; potential adversaries are seen to strive towards superiority through technology; and a system is required to counter threats. However, information threats are described as societal-political and societal-economic and directed against societal consciousness—not so much technological. In June 2019 the Russian MoD proposed that the CSTO should adopt a common information policy and General Kartapalov even compared information-psychological weapons to weapons of mass destruction.[2142]

In 2018 Russia and a group of other countries (including Syria, China, North Korea) submitted their latest initiative for an international code of conduct in the UN. It basically repeated the statements of the 2011 and 2015 proposals. It was more precise in that states should not allow their territory to be used for wrongful acts using information and communications technologies, should not use proxies, and should seek to ensure that non-state actors do not commit such acts from their territory. The role of the private sector and civil society is mentioned once.[2143] Russia claims that its initiative is supported by its 'partners' in BRICS, SCO and CSTO.[2144] It can be argued that little has changed in the Russian approach and that the UN initiative is now almost fully synchronized with the 2015 Russia-China agreement.

The reactivation of Russian cyber diplomacy in 2018 after the failure of UN GGE in 2017 is connected to the National Programme of the Digital Economy. The Programme includes direct tasks for the 'cyber diplomacy team'.[2145] The current Russian worldview was summarized by Sergei Lavrov in the 73th General Assembly of the UN in September 2018 when he claimed that there was a collision under way between the rising centres of power which demanded individual models of political and economic development and the Western status quo powers who were using all means in their possession to slow the inevitable 'progress'.[2146] The Minkomsviaz' argued that the United States and EU countries did not support Russia's latest initiatives because

[2141] ОДКБ. Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года. от 14 октября 2016 года [Online]. Available: http://odkb-csto.org/ documents/detail.php?ELEMENT_ID=8382 [Accessed: 25th February 2019].

[2142] ТАСС. Минобороны РФ предлагает странам ОДКБ сформировать согласованную информационную политику. ТАСС, 20 июня 2019 [Online]. Available: https://tass.ru/armiya-i-opk/6573842 [Accessed: 8th July 2019].

[2143] United Nations General Assembly. Developments in the field of information and telecommunications in the context of international security. A/C.1/73/L.27/, 22 October 2018 [Online]. Available: https://undocs.org/pdf?symbol=en/A/C.1/73/L.27 [Accessed: 2nd April 2019].

[2144] Министерство иностранных дел Российской Федерации. О принятии Генассамблеей ООН российской резолюции по противодействию информационной преступности, 18.12.2018 [Online]. Available: http://www.mid.ru/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/ UsCUTiw2pO53/content/id/3449030 [Accessed: 14th May 2019].

[2145] Распоряжение Правительства РФ 2017.

[2146] Министерство иностранных дел Российской Федерации. Выступление Министра иностранных дел России С.В.Лаврова на 73-й сессии Генеральной Ассамблеи ООН, Нью-Йорк, 28 сентября 2018 года [Online]. Available: http://www.mid.ru/web/guest/general_assembly/-/asset_publisher/lrzZMhfoyRUj/ content/id/3359296 [Accessed: 14th May 2019].

they tried to preserve the digital inequality between the members of the world community.[2147] Moreover, Russia did not support the alternative cyber security proposal as they went against the principles of state sovereignty or implicitly accepted the use of ICT technology in warfare.[2148] When the UN General Assembly in December 2019 voted in support of drafting the Russian cyber-crime treaty, the Russian MFA claimed the treaty would validate the principle of digital sovereignty.[2149]

To summarize. The international treatises on information security resonate strongly with the idea of territorial state sovereignty. The connection has developed over time, but by 2013–2015 it had reached the level of information sovereignty, i.e. state sovereignty defined by information space on a par with other aspects of sovereignty. The interstate struggle is also present and indeed provides the reasoning for the treatises as Russia's great power competitors try to dominate it and its allies through the information space with superior technology to achieve information superiority or dominance in peacetime. Strategic deterrence is present in the regional agreements as military threats and nuclear parity give way to multiple different information-related state and non-state threats which must be prevented and deterred. However, the agreements are more defensive and passive than Russia's own strategic planning documents were. The idea of a unified information space is expanded to include the CIS and CSTO in the documents. This raises the interesting question of where the borders of the Russian national segment of the Internet begin and where they stop. Clearly, the EIP can also be an inclusive concept when politico-militarily or for economic reasons appropriate or culturally feasible. This means that any 'single cause' explanation, like 'the besieged fortress syndrome' cannot fully explain Russian policies toward cyberspace. Information-technological warfare is lost its distinctiveness in the 2010s, which correlates with the appearance of 'Western hybrid and information warfare.' However, there remains a purely technological aspect which is related to the security and functioning of critical information infrastructure, and the destructive effects of information weapons. As the treatises are high-level political documents automated command and control systems do not really feature in them—excluding the mention of CIS information security system, which was probably a more organizational than technological concept. The idea of asymmetric response was not part of international treatises.'

To be analytically accurate, terrorism, separatism and extremism are persistent threats in the documents—especially in the context of the SCO. Moreover, the official texts did not explicitly use the terms digital or information sovereignty. The agreements between the CIS, CSTO and SCO reflect a like-minded and negotiated approach to information security. Thus, Russia is not the sole author of the documents or the sole,

[2147] Министерство иностранных дел Российской Федерации 2018c.

[2148] Комментарий Департамента информации и печати МИД России о российских оценках французской инициативы «Парижский призыв к доверию и безопасности в киберпространстве», 20.11.2018 [Online]. Available: http://www.mid.ru/web/guest/mezdunarodnaa-informacionnaa-bezopasnost /-/asset_publisher/UsCUTiw2pO53/content/id/3413302 [Accessed: 14th May 2019].

[2149] Министерство иностранных дел Российской Федерации. Об итогах голосования в Генассамблее ООН по российскому проекту резолюции по противодействию киберпреступности, 30.12.2019 [Online]. Available: https://www.mid.ru/organs/-/asset_publisher/AfvTBPbEYay2/content/id/3988579 [Accessed: 6th January 2020].

or even original, source of all of the ideas.[2150] Russian ideas most probably interacted with Chinese ideas and ideas from Post-Soviet countries. The international treatises demonstrate that the part of the strategic cultural ideas analysed in this study were already part of the Russian decision-making elite's worldview in 2000–2011. However, Russian policies concerning cyber or information space were largely directed outside of Russia—to change the rules of the international system to balance the perceived disbalance in power between Russia and the United States.[2151] The idea of a Russian national segment of the Internet was already present before 2014 but the elites concentrated mainly on shaping and controlling its external normative borders, not so much its internal elements and functions. After 2014 this project intensified and gained urgency.

6.2.3 The early policies and laws of 2000–2011

This chapter looks at the Russian strategies, policies and laws promulgated and implemented during 2000–2010 to provide a context to the change that occurred after 2010. The basic principles of the government policy concerning information security were established in the Information Security Doctrine of 2000.[2152] Manoilo, Petrenko and Frolov have argued that a long-term programme for coordinating the actions of federal bodies of state power for the development and implementation of state information policy and information warfare was designed in a meeting of the Security Council of the Russian Federation held in July 2000.[2153] As the Doctrine has been analysed previously, and there are few public sources available to trace the policy referred by Manoilo et al., I shall start my analysis on the first public government efforts to shape the Russian cyber and information space.

As was argued above, the Russian regime allowed the Russian Internet to develop largely without state control in the 2000s. In 2002 the Russian government adopted the federal Electronic Russia Programme for 2002–2010. It was meant to ensure the development of the public information infrastructure and services of the government, and to enhance intragovernmental cooperation for the needs of the state authorities throughout the Russian Federation. This included adopting measures aimed at cost-effectiveness, reducing bureaucracy and increasing the transparency of the public administration. The Programme was the government's answer to the digitalization of society and the economy. 'A unified information space' was considered to be an important component in the building of a strong federal state as Russia was characterized by the vastness of its territory and sparseness of the population. In principle, it did not differ from the eGovernment programmes adopted by other governments at

[2150] For example, in 2010 the president of Belarus already gave an edict titled: On the Measures to Improve the Use of the National Segment of the Internet, and in 2019 the county adopted the Concept of Information Security of the Republic of Belarus, which defined such concepts as 'information sovereignty' and 'national segment of the Internet' which are both concepts that Russians have consistently used but never officially defined. (Указ Президента РБ 2010; Постоновление Совета Безопасности Республики Беларусь от 18 марта 2019 № 1 "О Концепции информационной безопасности Республики Беларусь" [Online]. Available: http://president.gov.by/uploads/documents/2019/1post.pdf [Accessed: 2nd April 2019]). Soldatov and Borogan have claimed that Kazakhstan's President Nursultan Nazabayev called for electronic borders and e-sovereignty already at the SCO summit in Astana in June 15, 2011 (Soldatov & Borogan 2013, 29-30).

[2151] For a similar conclusion cf. Giacomi 2014; Nocetti 2015.

[2152] CF. Chapter 4.

[2153] Манойло, Петренко & Фролов 2012, 456.

that time.[2154] However, it envisioned 'a unified, vertically integrated state automated information system of 'Management' (upravlenie)' which would be based on regional databases and the sharing of information between all federal institutions. This system differed from programmes of other governments and resonated strongly with Soviet 'kibernetik' ideas.[2155] The Electronic Russia Programme also included the establishment of regional information-analytical centres and situation centres for 'higher organs of the government'. These new systems would be based on automated information systems harmonized and integrated through federal and municipal levels. In principle, the Programme should have produced a unified federal and municipal government information system based on common computer systems and protected communication channels operated by a single operator.[2156]

According to Ilmari Susiluoto, the Electronic Russia Programme was followed by a push to develop techno parks, centres and cities modelled after the success of the Silicon Valley but based on Soviet 'science cities.' Susiluoto argues that these ideas were connected to the utopian Soviet thinking. They were efforts to control information society without understanding its creativity.[2157] Moreover, they were an effort to fix the decline of the Russian information scientific and industrial civilian and military base through the government support.[2158]

Although this first state-led push to create the information society in Russia in 2002–2008 was dominated by liberal and progressive economic thinking, it also included the first restrictions to Internet freedoms. This was not a surprise as the Information Security Doctrine published in 2000 had practically made information security a national security issue.[2159] In 2003 Russia got a new Federal Law on Communications which strived to regulate the changing information landscape. It included licensing procedures and monopolistic tendencies that tried to give the regime the ability to control the telecoms market.[2160] Ultimately, in 2006 the ISPs were ordered to provide the FSB real-time access to their customer databases.[2161] This development culminated in the Federal Law on Information, Information technology and the Protection of Information, which was adopted in 2006.[2162] Although its first version included only

[2154] Schware, Robert (ed.) E-Development: From Excitement to Effectiveness. Washington D.C.: The World Bank Group, 2004 [Online]. Available: http://documents.worldbank.org/curated/en/261151468325237852/pdf/341470EDevelopment.pdf [Accessed: 13th May 2019].

[2155] The "Management" system is a unified territorially distributed state information system which offers analytics and decision-making support, enables the monitoring of the implementation of federal and municipal programmes and the evaluation of their effectiveness, the monitoring of economic, financial and social situation in the country, and supports strategic planning. (Постановление Правительства Российской Федерации от 25 декабря 2009 г. № 1088 (В редакции от 02.02.2019 № 77) Положение о государственной автоматизированной информационной системе "Управление" [Online]. Available: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102134940 [Accessed: 13th May 2019].)

[2156] Постановление Правительство Российской Федерации от 28 января 2002 г. №65 "ФЦП «Электронная Россия (2002–2010 годы)" [Online]. Available: http://minsvyaz.ru/ru/activity/programs/6/ [Accessed: 4th March 2019].

[2157] Susiluoto 2006.

[2158] Roffey 2013; Locksley 2001; Golts, Alexander M. and Putnam, Tonya L. State Militarism and Its Legacies: Why Military Reform Has Failed in Russia. International Security, Vol. 29, No. 2 (Fall 2004), 121-158.

[2159] Cf. Chapter 4.

[2160] Alexander, Marcus. The Internet and Democratization: The Development of Russian Internet Policy. Demokratizatsiya, The Journal of Post-Soviet Democratization, Vol. 12, No. 4 (2004), 607-627.

[2161] Susiluoto 2006, 393-394.

[2162] Федеральный закон 2006.

basic provisions to bring the Internet into the sphere of legal regulation, it later became 'the law of Internet state control', as will be shown below.

The Russian regime's thinking on critical infrastructure develop during the 2000s with international trends but also with national characteristics. Katri Pynnöniemi and Irina Busygina have argued that Russian views began to change in 2003 after a Security Council meeting.[2163] The planning and preparing for emergency situations developed towards the protection of certain critical objects, and the conceptual basis to protect critical infrastructure was formulated in 2006.[2164] However, at this point the issue was still connected to internal security and emergency situations- The ensuring of resilient and secure functioning of information-telecommunications systems of 'the dangerous objects' was only one of the measures proposed to protect CI. Interestingly, in a similar manner to the Electronic Russia Programme, the concept called for the creation of 'a unified state system for the prevention and elimination of emergency situations.' It also demanded the creation of a national control centre for crisis situations as well as a decision support system, and automated information and forecast-analytical systems for identifying and assessing possible threats. Is also required a certification system for the ICT and software of critical objects.[2165] This system was later named the Unified State System of Emergency Prevention and Response (RSChS).[2166] Sergei Shoigu later managed to construct this system during his post as the Minister of Emergency Situations 1994-2012.[2167]

Although the public and official policies do not mention the subject, the issue of informatization of the society touched also mobilization in the 2000s. Julian Cooper, who has studied the mobilization planning of Russia, claims that the Ministry of Economic Development and Commerce sponsored a federal level integrated system called EMAPU which would have connected 10 000 local government organizations and 25 000 enterprises.[2168] Furthermore, as noted in Chapter 5, the Russian military began to develop concepts for its own unified information space from the early 2000s. Previous studies on the Russian military reform have shown that automated command and control systems and digital communications were at the core of the new armaments programme launched in 2011.[2169] The military-industrial complex had its own strategies and concepts for development.[2170] However, the results would begin to materialize only in the 2010s when there was enough financing and the worst problems of the armament program had been ironed out.[2171]

[2163] Pynnöniemi & Busygina 2013.

[2164] Pynnöniemi 2012; Pynnöniemi & Busygina 2013.

[2165] Президент РФ 28 сентября 2006 г. № Пр-1649 Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз техногенного, природного характера и террористических актов [Online]. Available: https://base.garant.ru/198664/ [Accessed: 13th May 2019].

[2166] Поручение Президента РФ от 15.11.2011 N Пр-3400 Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов на период до 2020 года [Online]. Available: https://www.garant.ru/products/ipo/prime/doc/70041358/ [Available: 13th May 2019].

[2167] Roffey, Roger: Russia's EMERCON: Managing emergencies and political stability, FOI, 2016.

[2168] Cooper 2016, 17.

[2169] Bartles 2011; McDermott 2011; Blank 11; McDermott 2015.

[2170] Растопшин 2004.

[2171] McDermott 2011; McDermott 2015; Renz 2018.

The next push for the informatization and digitalization of the Russian economy and government came with Dmitri Medvedev's presidency. However, the 2008 Strategy for the Development of Information Society in the Russian Federation was adopted already under the reign of Vladimir Putin.[2172] Its main objective was to ensure for Russia 'a worthy place among the leaders of the global information society.' Its tasks included the formation of modern information and telecommunications infrastructure, the development of economy based on the use of ICT, the protection of culture, and strengthening of patriotism, and the thwarting the use of information and telecommunications technologies to threaten Russia's national interests. The ensuring of national security and the enhancement of military defence were a constant theme in the Strategy. The emphasis of national interests was a clear departure from earlier eGovernment initiatives. It demanded the creation of 'a unified information space' inter alia for the needs of the national security and the protection of the information and telecommunications systems of key infrastructure facilities. Despite this 'securitization', the economy, society and government services were the main targets of the Strategy. It promoted public private cooperation, indirect government support instead of state-led projects, and international cooperation.[2173]

The new government adopted in the November of 2008 the Concept of Long-period Social-Economic Development of the Russian Federation until 2020 declared that Russia was yet again becoming an economic great power.[2174] The Concept acknowledged the importance of scientific and technological development and the lag of Russia in this respect, which could increase Russia's vulnerability in the context of growing geopolitical rivalry. Economic development was explicitly connected to combat readiness of the Armed Forces and thus deterrence. Moreover, financial competitiveness was the basis for 'economic sovereignty'. The transformation towards economy of knowledge from energy-based economy was a priority and it included investments to human capital and scientific research. The part of the Concept discussing ICT mentioned the need to develop a unified information space, to stimulate domestic hardware and software production, to create technology parks, and to counter the use of ICT against Russia's national interests. The Concept also called for systems of management to be created to manage different sectors of the Russian economy in the framework of strategic planning.[2175] It was one of the first official references to strategic planning in national policy setting context. Moreover, it echoed the emphasis of sovereignty which Putin had elevated to almost an official ideology.[2176]

[2172] Стратегия. Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 7 февраля 2008 г. № Пр-212) [Online]. Available: https://rg.ru/2008/02/16/informacia-strategia-dok.html [Accessed: 13th May 2019].

[2173] Ibid.

[2174] Распоряжение Правительства РФ от 17.11.2008 N 1662-р "О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года" (вместе с "Концепцией долгосрочного социально-экономического развития Российской Федерации на период до 2020 года"): http://www.consultant.ru/cons/cgi/online.cgi?req=doc&n=82134&base=LAW&from=308069-1847&rnd=0.6960341791725004#0577375847182553 [Accessed: 13th May 2019].

[2175] Распоряжение Правительства РФ 2008a.

[2176] Lo 2015, 31-32; Mankoff 2012, 81-82.

The Strategy and Concept of 2008 were put into practice in the Government Programme on Information Society (2011—2020) adopted in 2010.[2177] The Concept has been significantly updated during 2010-2013 and I will refer here to the original 2010 version. The implementation of the Concept was the responsibility of Minkomsviaz' and a group of other ministries, the FSO, and the FSB. It recognized many future problems and challenges of "ensuring the security of the national segment of the Internet". It had six subprogrammes.[2178] The priority of the programme was to create a unified information space which was a composition of other unified or single systems. The subprogramme of e-state included the creation of state system of electronic identification and the state information-analytical system to support state economic and societal policies, and the development of a protected Russian segment of the Internet for government use. It also called for the integration of government services and the continuing development of the Management System (Upravlenie). The subprogramme of basic infrastructure included, for example, the construction of modern national backbone communication network. The security subprogramme concentrated on preventing terrorism but also included the creation of national software and supercomputer production.[2179] The Concept was meant to enhance Russian information society and economy with limited state intervention. It dispensed almost completely with the national security language of its guiding Strategy and Concept. However, the Concept did retain the drive to integrate, synchronize, and harmonize government networks, and the idea of collecting information on nation-wide basis for the efficient management of the state.

In 2008 the Russian government also adopted the Concept on Forming Electronic Government in the Russian Federation until 2010.[2180] It was drafted by the Ministry of Communications, the Ministry of Economic Development, and the FSO. The Concept noted the technological lag of Russia compared to developed countries and stated that forming a unified information infrastructure between government agencies had failed. The Concept repeated the objectives and tasks of the 2002 Electronic Russia program and thus it was basically an admission of a failed policy. The Concept did not include the national security issues mentioned in the 2008 Strategy.[2181]

During the term of President Medvedev Russia also redefined the roles and tasks of some of its central actors in the information space. Minkomsviaz' and Roskomnadzor got new provisions in 2008 and 2009, and the Federal Law on Security was modified in 2010.[2182] The MoD adopted in 2010 the Regulations on the Information Support Bodies of the Armed Forces of the Russian Federation. The subject of this order were

[2177] Распоряжениие Правительства Российской Федерации от 20 октября 2010 г. N 1815-р Государственная программа Российской Федерации "Информационное общество (2011-2020 годы)" [Online]. Available: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102142714 [Accessed: 11th April 2019].

[2178] The quality of life of the citizens and the conditions for the development of business in the information society; the e-state and government effectiveness; the Russian market of information and telecommunication technologies; the basic infrastructure of the information society; the security in the information society; and the digital content and cultural heritage.

[2179] Ibid.

[2180] Распоряжение Правительства РФ от 6 мая 2008 г. N 632-р Концепция формирования в Российской Федерации электронного правительства до 2010 года [Online]. Available: http://www.garant.ru/products/ipo/prime/doc/93274/ [Accessed: 13th May 2019].

[2181] Распоряжение Правительства РФ 2008b.

[2182] Постановление Правительства РФ 2008; Постановление Правительства РФ 2009a; Федеральный закон 2010.

public relations, not information or cyber security or defence.[2183] It did however point to the fact that the Russian Armed Forces took information warfare increasingly seriously.

Although the 2008 Strategy and Concept did include the element of national interest and a view that Russian was in a geopolitical competition in which it was in danger of being left behind, the early Putin and Medvedev era documents are decidedly technocratic, optimistic, cooperative, and liberal in their character. However, the issue of sovereignty appeared as 'technological independence' or 'technological sovereignty' and so did the claim that information society was connected to hard national security. The issue of technological dependence on the West did not escape the attention of the commentators at that time.[2184] This zero-sum approach was compatible with the idea of interstate struggle, great powerness, and the balance of power. As the threats in the information space are mainly crime and terrorism, deterrence comes up only in the margins. Additionally, the idea of asymmetric response does not really appear as the overall tone is that of catching up with developed countries not finding ways to counter or surpass them. Nevertheless, the idea of information superiority on strategic level guides the need to develop domestic technology. Information-technological warfare was eclipsed by crime and terrorism which were the main threats directed against the information society and the state, but the concept of critical information infrastructure began to form a basis for an understanding of national cyber security. The most important element was the continuing Russian fascination with the idea of a unified, centralized, vertically integrated automated management system on a national level and the related information-analytical systems and situation centres. These systems were explicitly connected to the concept of the national segment of the Internet, although what that segment entailed, remained vague. So, there was already before 2012 a tension between the idea of free and liberal development of the Internet to gain maximum economic benefits and the reflexive need of the elites to control that same Internet and use it to micromanage the society and the economy. As was shown in Chapter 5, similar ideas circulated amongst the Russian military, although, the policies of the MoD and the Armed Forces concentrated first on survival and then from 2008 onwards on military reform.

6.3 The developments of 2012–2019

In 2012 the Russian defence and security elites changed their approach to the Internet. Reasons for this have been examined in Chapter 6.1. This change manifested in a group of laws directed against the political opposition which had used the Internet to mobilize first against the fraudulent Duma election and then against Vladimir Putin's re-election. The Russian regime first reacted to the demonstrations by tightening the regulation on the freedom of assembly and freedom of speech, by staging show trails of the opposition leaders and by mounting a domestic propaganda campaign against

[2183] Приказ Министра обороны РФ от 11 февраля 2010 г. N 70 "Об утверждении Положения об органах информационного обеспечения Вооруженных Сил Российской Федерации" [Online]. Available: http://base.garant.ru/55170392/ [Accessed: 13th May 2019].

[2184] Крикунов, Александр, Королёв, Александр. Информационные войны будущего. О необходимости адекватной защиты отечественной информационной инфраструктуры от кибератак. Военный дипломат, № 1 (2009), 94-103.

the opposition.[2185] The Internet censorship followed after the elite had properly analysed the situation and reoriented itself.[2186]

6.3.1 The laws

The laws aimed at controlling the Internet have mostly been amendments to existing laws such as the Federal Law on Information, Information Technologies and Information Protection, the Law on Mass Media, the Law on Communications or the Criminal Code—the first of which has virtually become a law on Internet censorship.[2187] In 2012 Federal Law № 139-FZ "On Introducing Amendments to the Law on the Protection of Children from Information Harmful to Their Health and Development" was adopted.[2188] The law introduced an Internet blacklist managed by the Roskomnadzor.[2189] The register includes the domain names, IP -addresses, and URLs of banned web sites and services. Providers hosting banned sites need to notify the owner of a site displaying banned information to take down the material or restrict the access to it themselves in 24 hours. Providers include social media companies and any services that offer platforms for user generated material. Failure to restrict access to the banned resources will result in legal prosecution and/or fines. Initially and officially the register was introduced to protect children from harmful material. However, the 'Unified register' has been used to ban services like the Telegram and Zello, and websites of opposition politicians like Alexei Navalnyi.[2190] In 2013 the so-called "Lugovoi Law" gave the authorities the power to block Internet sites and resources disseminating calls for "mass unrest, extremist activities, and participation in mass events held in violation of the established procedure." This law made it administratively much easier, based only on the order of the General Prosecutor's office, to quickly block information about a political event.[2191] Moreover, the authority of Roskomnadzor to independently add sites to the blacklist–blocking has to otherwise be based on law or court order–has increased incrementally and it has begun to 'advise'

[2185] Pomeranz 2019, 156-157.

[2186] FIDH. Table Illustrating Legislative Crackdown on Rights and Freedoms of the Civil Society in Russia since 2012 (2018) [Online]. Available: https://www.fidh.org/en [Accessed: 14th May 2019]; Freedom House 2018; Агора 2016.

[2187] By censorship here is meant: "The suppression or prohibition of any parts of books, films, news, etc. that are considered obscene, politically unacceptable, or a threat to security." (Censorship. Oxford English Dictionary. [Online]. Available: https://en.oxforddictionaries.com/definition/censorship [Accessed: 14th May 2019]. Cf. also Prakash, Pranesh, Rizk, Nagla and Souza, Carlos Affonso (eds.) Global censorship Shifting Modes, Persisting Paradigms. New Haven: Yale Law School 2015 [Online]. Available: https://law.yale.edu/system/files/area/center/isp/documents/a2k_global-censorship_2.pdf [Accessed: 14th May 2019].

[2188] Федеральный закон от 28.07.2012 N 139-ФЗ (последняя редакция) "О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_133282/ [Accessed: 14 May 2019].

[2189] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. Единый реестр [Online]. Available: https://eais.rkn.gov.ru/ [Accessed: 14th May 2019].

[2190] Webb, Isaac. Russian Web Censor Cracks Down Ahead of Next Anti-Corruption Protests. Global Voices, 31 March 2017 [Online]. Available: https://globalvoices.org/2017/03/31/russian-web-censor-cracks-down-ahead-of-next-anti-corruption-protests/ [Accessed: 14th May 2019]; Кантышев, Павел. Роскомнадзор добивается блокировки IP-адресов Amazon. Ведомости, 23 марта 2018 [Online]. Available: https://www.vedomosti.ru/technology/articles/2018/03/23/754777-roskomnadzor-amazon [Accessed: 14th May 2019]; Lenta.ru. Роскомнадзор отказался от попыток веерно заблокировать Telegram. Lenta.ru, 25 апреля 2018 [Online]. Available: https://lenta.ru/news/2018/04/25/telega/ [Accessed: 14th May 2019].

[2191] Федеральный закон от 28 декабря 2013 г. N 398-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" [Online]. Available: https://rg.ru/2013/12/30/extrem-site-dok.html [Accessed: 14th May 2019].

ISPs on how to best restrict access to banned sites such as by using highly intrusive DPI technology.[2192] The somewhat crude procedures and technology behind the blocking efforts have negatively affected the functioning of the Russian segment of the Internet and generated losses for the Internet service and content providers.[2193]

The "Blogger's Law" adopted in April 2014 was a step towards self-censorship as it required bloggers with more than 3,000 visits per day to register as 'organizers of the dissemination of information' (ORI).[2194] ORI became the main regulatory category in the Russian Internet. It was defined as a legal entity or a person who uses computers and/or computer programs for receiving, transmitting, delivering and (or) processing electronic messages of Internet users. The ORIs were required to store information about the reception, transmission, delivery, and (or) processing of voice data, written text, images, sounds or other electronic messages of Internet users and information about these users for six months. They are also required to provide law enforcement and secret services access to it under the threat of banning their sites and receiving fines.[2195]

In July 2016 a federal law was adopted which made Internet news aggregators with over a million users (such as Yandex, Rambler, VKontakt) and disseminating news in Russian, or other languages of the Russia Federation, responsible for the authenticity and legality of the information and links on their sites. These news aggregators were to be registered by Rozkomnadzor to a special register which would monitor the visitor count of the news aggregators.[2196] In 2017 the controlling effort extended to messaging apps and proxy services. Organizers of messaging services were required to identify their users by their cell phone numbers, i.e. abolishing anonymity, and to restrict the use of their services if ordered by the officials. Information about the users

[2192] Зыков, Владимир, Кондратьев, Александр. Роскомнадзор будет оперативно получать решения судов о блокировках Для этого будет создана система электронного взаимодействия. Известия, 2 февраля 2017 [Online]. Available: https://iz.ru/news/662031 [Accessed: 14th May 2019]; Известия. Роскомнадзор обновил рекомендации операторам по фильтрации трафика. Известия, 27 июня 2017 [Online]. Available: https://iz.ru/611620/2017-06-27/roskomnadzor-obnovil-rekomendatcii-operatoram-po-filtratcii-trafika [Accessed: 14th May 2019].

[2193] Брызгалова, Екатерина. Роскомнадзор начал блокировать страницу «МБХ медиа» в «Яндекс.Дзене». Ведомости, 23 февраля 2018 [Online]. Available: https://www.vedomosti.ru/politics/articles/2018/02/22/751870-roskomnadzor-zablokiroval-mbh-yandeksdzene [Accessed: 14th May 2019]; Сухаревская, Алена. Роскомнадзор заблокировал почти триста доменов Google. Ведомости, 11 апреля 2018 [Online]. Available: https://www.vedomosti.ru/technology/articles/2018/04/11/766420-roskomnadzor-zablokiroval-google [Accessed: 14th May 2019].

[2194] The mention about bloggers was later removed cf. Федеральный закон от 29 июля 2017 года № 276-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" [Online]. Available: https://rg.ru/2017/07/30/fz276-site-dok.html [Accessed: 14th May 2019].

[2195] Федеральный закон от 05.05.2014 N 97-ФЗ (ред. от 29.07.2017) "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_162586/ [Accessed: 14th May 2019].

[2196] Федеральный закон от 23.06.2016 N 208-ФЗ "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и Кодекс Российской Федерации об административных правонарушениях" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_200019/ [Accessed: 29th May 2019].

of the services must be stored in Russia.[2197] Moreover, services that provided access to the blacklisted websites from Russia i.e. public proxy and VPN servers, were required to cease their actions if ordered by the Roskomnadzor.[2198] Thus, at least in theory, all public and some private Internet communication were put under legal state control by the end of 2018. This was by no means a waterproof mechanism as the attempt to block the messaging service Telegram has proved.[2199] Moreover, the Russian regime has had only limited success regulating the international Internet companies like Google, Facebook and Twitter—although many of the them do follow the Russian law. The banning of LinkedIn in 2016 proved that the regime was serious.[2200] Google began complying with the blacklisting requirements in 2019 in its transparency report declared that the Russian government accounted for 75 percent of all global requests to delete content in January–July 2018.[2201]

Along with blacklisting sites, monitoring and blocking content, regulating news and social media platforms, and outright banning of whole services, the Russian regime has sought to restrict the foreign ownership of information resources located in Russia. In October 2014 Russia adopted a law that restricted the permissible percentage of foreign ownership of any print media, registered online media, television, or radio broadcasters to 20 percent.[2202] In December 2015 a follow-up law ordered media companies to declare any foreign financing they received once every quarter.[2203] These were amendments to the Law on Mass Media whereas the ownership of major telecommunications, television, radio and newspaper companies is regulated by the Law on Foreign Investments in Strategic Assets.[2204] Admittedly, it would have been somewhat difficult to designate Internet sites as strategic assets. However, only Russian companies or citizens could own Internet news aggregators (ORI).[2205] The major Russian telecommunications companies which provide the backbone for the Russian Internet are 'strategic assets.' So are the state-owned television companies the websites of which are amongst the most popular in the RuNet.[2206] Moreover, as many major Russian companies are either directly stated owned or owned by the oligarchs, the

[2197] Федеральный закон от 29.07.2017 N 241-ФЗ "О внесении изменений в статьи 10.1 и 15.4 Федерального закона "Об информации, информационных технологиях и о защите информации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_221183/ [Accessed: 14th May 2019].

[2198] Федеральный закон 2017c.

[2199] Роскомсвобода. Telegram: год под «блокировкой». Роскомсвобода, 16.4.2019 [Online]. Available: https://roskomsvoboda.org/46556/ [Accessed: 14th May 2019]. For the case of Telegram cf. Griffiths 2019.

[2200] Soldatov & Borogan 2015; Rambler News Service. Итоги года: рунет 2016 [Online]. Available: https://rns.online/articles/Itogi-goda-runet-2017-01-02/ [Accessed: 14th May 2019]; Freedom House 2018.

[2201] Moscow Times. Google Began Censoring Search Results in Russia, Reports Say. Moscow Times, February 7, 2019 [Online]. Available: https://www.themoscowtimes.com/2019/02/07/google-began-censoring-search-results-russia-reports-say-a64423 [Accessed: 29th May 2019].

[2202] Федеральный закон от 14.10.2014 N 305-ФЗ (последняя редакция) "О внесении изменений в Закон Российской Федерации "О средствах массовой информации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_169740/ [Accessed: 14th May 2019].

[2203] Федеральный закон от 30.12.2015 N 464-ФЗ "О внесении изменений в Закон Российской Федерации "О средствах массовой информации" и Кодекс Российской Федерации об административных правонарушениях" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_191539/ [Accessed: 14th May 2019].

[2204] Федеральный закон от 29 апреля 2008 г. N 57-ФЗ "О порядке осуществления иностранных инвестиций в хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства" [Online]. Available: http://ivo.garant.ru/#/document/ 12160212/paragraph/3780:0 [Accessed: 14th May 2019].

[2205] Федеральный закон 2016a.

[2206] Федеральный закон 2008.

state influence on the national segment is quite solid even without tight legal regulation of the ownership of the Internet services. This has not stopped the introduction of a draft law on restricting the foreign ownership of 'Internet resources.'[2207]

Data localization is another issue that the regime has pursued through law-making. In July 2014 the Law on Personal Data was amended so that the personal data of Russian citizens had to be stored inside Russian borders. Subsequently, Roskomnadzor was mandated to monitor that this law was followed by the foreign and Russian ISPs.[2208] The law entered into force in September 2015 but Roskomnadzor' was still pushing international Internet companies like Facebook and Twitter to comply with at in the end of 2019.[2209] Data localization has been driven by both economic and security interests. By insisting that international companies store their data on Russian citizens in Russia, the government creates demand for the ICT sector. It also makes Russian laws applicable to that data and gives the law enforcement and security services access to it. Moreover, personal data would be, from the Russian state's point-of-view, better protected than if it was stored in 'the cloud' i.e. under some other state's jurisdiction.

The so-called Iarovaia Laws or Anti-Terrorism laws which were signed by Putin in July 2016 and entered into force in July 2018 take the data localization to the extreme in the form of massive data retention.[2210] Originally, the laws demanded that the telecommunications companies and the ISPs retained all text messages, voice, data, and images for six months and metadata about the time, location, and sender and recipients of messages for three years. All this data had to be stored in Russia. Moreover, the companies were ordered to give the law enforcement and secret services access to that data including the means to decrypt it. Later, the demands have been slightly modified.[2211] The Russian ISPs have tried to get the requirements of the laws eased and complained that they will be either impossible or exceedingly costly (17 trillion roubles) to implement—as the ISPs themselves are required to provide the equipment for the data storage.[2212] Furthermore, there were no certified domestic equipment or government guidelines available when the law entered into force. The use of foreign equipment was, in principle, banned as it was seen as a security risk, or was considered

[2207] Seddon 2019.

[2208] Федеральный закон от 21 июля 2014 г. N 242-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях" [Online]. Available: http://ivo.garant.ru/#/ document/70700506/paragraph/1:0 [Accessed: 14th May 2019].

[2209] ТАСС. Жаров: Twitter и Facebook должны локализовать данные пользователей РФ к декабрю-январю. ТАСС сентября [Online]. https://tass.ru/obschestvo/6921980 [Accessed: 6th January 2020].

[2210] Федеральный закон 2016b; Федеральный закон от 06.07.2016 N 375-ФЗ (последняя редакция) "О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности" [Online]. Available: http://www.consultant.ru/document/ cons_doc_LAW_201087/ [Accessed: 14th May 2019].

[2211] Трунина, Анна. Интернет-сервисы в России обязали хранить трафик пользователей полгода. РБК, 5 февраля 2019 [Online]. Available: https://www.rbc.ru/technology_and_media/28/06/2018/5b34f94f9a79476cbd07e0e8?from=main [Accessed: 14th May 2019].

[2212] Тишина, Юлия. «Закон Яровой» вписали в инфляцию. Объемы хранения данных и затраты операторов могут вырасти. Коммерсантъ, №61 от 10.04.2017 [Online]. Available: https://www. kommersant.ru/doc/3267272 [Accessed: 14th May 2019]; Тишина, Юлия. «Закон Яровой» сводят с реальностью Власти смягчают его условия и сроки введения. Коммерсантъ, №10 от 22.01.2018 [Online]. Available: https://www.kommersant.ru/doc/3526894 [Accessed: 14th May 2019].

a competitor to the Russian domestic ICT industry.[2213] In addition to being a domestic security measure, the 'Iarovaia laws' have become a tool for building digital sovereignty. Data does not just flow through Russia but, in principle, resides there on Russian servers under state jurisdiction.

Although the laws discussed above are important tools of political control, their relevance comes from some other laws enacted between 2012–2018, and from the Roskomnadzor's, FSB's and other officials' use of those laws. These laws designate what kind of information and actions in the information space can be regulated and by whom, and they all leave enough room for discretion in the implementation so that they can be used against any politically undesirable action on the Internet.[2214] Although, the censorship laws have mainly empowered Roskomnadzor, the powers of the FSB were increased in December 2013 as its mandate on criminal intelligence and surveillance operations was extended to the 'information security' of the Russian Federation.[2215] The Agora organization has claimed that the failure to deploy effective Internet censorship in 2016–2017 has led to the side-lining of the Roskomnadzor as the FSB uses its increased powers and new laws to pursue 'illegal' web resources and activities through criminal investigation instead of censorship.[2216]

One additional legislation effort that has not yet succeeded to gather enough support is mandatory state certified encryption. From 2016 the FSB has published administrative orders (prikaz) which demand that the Internet companies relinquish their crypto keys to the FSB.[2217] This policy escalated to the total ban of Telegram in Russia in April 2018 when the company refused to hand over its keys and user data.[2218] Moreover, as the use of the HTTPS protocol increased in the Russian segment, the FSB and Roskomnadzor pushed for a mandatory national SSL certificate in 2016 which would give them the ability to conduct MITM attacks on all encrypted traffic in the national segment using the national certificate.[2219] This would have been possible, for

[2213] Lenta.ru. «Закон Яровой» оказался неисполним. Lenta.ru, 3 июля 2018 [Online]. Available: https://lenta.ru/news/2018/07/03/illegal/ [Accessed: 14th May 2019]; Баленко, Евгения, Посыпкина, Александра. Не дописали: почему интернет-компании не могут исполнять «закон Яровой» РБК, 13 июля 2018 [Online]. Available: https://www.rbc.ru/technology_and_media/31/07/2018/5b5f22609-a7947e1f4470779?from=main [Accessed: 14th May 2019]; Роскомсвобода. Минпромторг хочет запретить реализацию «пакета Яровой» на иностранном оборудовании. Роскомсвобода, 7.5.2019 [Online]. Available: https://roskomsvoboda.org/46996/ [Accessed: 14th May 2019].

[2214] FIDH 2018; Agora 2018; HWR 2018.

[2215] Федеральный закон от 21 декабря 2013 г. N 369-ФЗ "О внесении изменений в Федеральный закон "Об оперативно-розыскной деятельности" и статью 13 Федерального закона "О федеральной службе безопасности" [Online]. Available: https://rg.ru/2013/12/25/deatelnost-dok.html [Accessed: 14th May 2019].

[2216] Корня, Анастасия. Главным регулятором рунета становится ФСБ. Свободы в российском интернете все меньше, считают правозащитники. Ведомости, 05 февраля 2018 [Online]. Available: https://www.vedomosti.ru/politics/articles/2018/02/05/749913-regulyatorom-runeta-fsb [Accessed: 14th May 2019].

[2217] Кантышев, Павел. ФСБ хочет получать ключи от электронной переписки за 10 дней. Спецслужба уточнила требования к интернет-компаниям, но выполнить их будет сложно.Ведомости, 07 декабря 2017 [Online]. Available: https://www.vedomosti.ru/technology/articles/2017/12/07/744550-fsb [Accessed: 15th May 2019].

[2218] Рожков, Роман, Новый, Владислав. Telegram не сдал ключи. Роскомнадзор будет добиваться ограничения доступа к мессенджеру через суд. Коммерсантъ №58 от 05.04.2018 [Online]. Available: https://www.kommersant.ru/doc/3593600 [Accessed: 15th May 2019].

[2219] Коломыченко, Мария. Шифр и меч. ФСБ собирается взять интернет-трафик на контроль. Коммерсантъ" №174 от 21.09.2016 [Online]. Available: https://www.kommersant.ru/doc/3094848 [Accessed: 9th May 2019].

example, through the use of Russian web browsers and by establishing national certification authorities. The domestic Sputnik browser and state websites began the test trial of Russian SSL certification in 2017.[2220] It seems that this policy is incorporated into the new 'Law on Sovereign Internet' although the cryptography part will only come into an effect in 2021.[2221] The Security Council has also authorized the FSB to created national encryption for mobile networks called "Konus" which includes SIM cards with Russian crypto keys, hardware security modules on the network side, and authentication of users through national register connecting SIM cards to natural or judicial persons.[2222] Moreover, in December 2019 Putin signed a law that obliged the electronic devices sold in Russia to have pre-installed Russian applications.[2223]

If the development of censorship laws is compared to the changes in Russia's strategic environment, it is obvious that the efforts to control the substance of the national segment of the Internet were based in the domestic and international events of 2011–2012. The tone of those efforts changed slightly in 2014 and became more resolute as the perceived information war with the West intensified and the Ukrainian revolution was interpreted as a Western regime change operation. The direct control of the Internet through regulation became increasingly pronounced. It was important to restrict the ability of the opposition to collective action, but it became ever more important to push the outside influence in the Russian information space to a minimum. Nevertheless, it is important to keep in mind that the Russia regime did not initially pursue the kind of total censorship that, for example, China was using by the 2010s. Developments were incremental, opposed by civil society and the private sector, and a system like China's "Great Firewall" was probably technologically impossible to achieve in the timeframe of 2012-2019.[2224] Nevertheless, the laws adopted in 2011-2019 make concrete the strategic cultural ideas as information sovereignty is given substance, and the EIP borders, strategic deterrence and interstate information struggle is provided means, asymmetric response and information superiority enhanced by denying the opponent's the freedom of action, and the legal basis for automated systems of information-technological security and defence are created.

[2220] Зыков, Владимир. Российское шифрование протестируют на сайте госуслуг. Начато тестовое внедрение российских систем защиты интернет-трафика. Известия, 31 августа 2017 [Online]. Available: https://iz.ru/636884/sertifikat-dlia-gosuslug-i-sputnika [Accessed: 15th May 2019].

[2221] Коломыченко, Мария. Депутаты предложили защитить Рунет с помощью отечественного шифрования. РБК, 2 апреля 2019 [Online]. Available: https://www.rbc.ru/technology_and_media/02/04/2019/5ca2138a9a79477cb5e399e7 [Accessed: 9th May 2019].

[2222] Коломыченко, Мария, Посыпкина, Александра. Российские сим-карты запустят на чипах Samsung Отечественное шифрование нужно ФСБ для борьбы с иностранными разведками. РБК, 23 мая 2019 [Online]. Available: https://www.rbc.ru/technology_and_media/23/05/2019/5ce53a039a79471bde8de739?from=center [Accessed: 26th May 2019].

[2223] Кречетова, Ангелина, Харатьян, Петр. Путин подписал закон о предустановке российского софта на гаджеты. Ведомости 02 декабря 2019 [Online]. Available: https://www.vedomosti.ru/technology/ articles/2019/12/02/817628-putin-podpisal-zakon [Accessed: 6th January 2020].

[2224] Based on human rights organizations' and Internet activists' reporting Russian censorship is working and it is enforced by legal persecution although there are enough technological loopholes that the current methods can be circumvented if there is will and moderate technical knowhow. (Агора 2018; Dobrokhotov, Roman. Putin vs the Russian Internet - 0:1. Al Jazeera, 25 Apr 2018 [Online]. Available: https://www.aljazeera. com/indepth/opinion/putin-russian-internet-01-180424170551334.html [Accessed: 17th May 2019]; Ermoshina, Ksenia and Musiani, Francesca. Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era. Media and Communications, Vol. 5, No. 1 (2017), 42-53.)

The critical information infrastructure and the regulations and systems created to protect it constitute another element of normative control. The Russian concept of CII grew out of the laws and regulations on emergency situations and the protection of critical objects of the energy and transportation sector in the period of 2003-2011.[2225] In 2012 the Fundamentals of the State Policy in the Field of Ensuring the Safety of the Population of the Russian Federation and the Protection of Critical and Potentially Dangerous Objects from Natural Threats, Man-made and Terrorist Acts for the Period up to 2020, drafted by the Security Council, for the first time defined the CII as "a set of automated control systems and interaction-enabling information and telecommunications networks of the critically important objects that are designed to meet the challenges of public administration, defence, security and law and order, the disruption (or termination) of which may cause serious consequences."[2226] The document also introduced the concept of the future national cyber security system GosSOPKA (Gosudartsvennia sistema obnaruzheniia, preduprezdeniia i likvidatsii posledsvii komp'iuternykh atak) (cf. Chapter 6.4.1). Furthermore, the document practically introduced the official Russian language of information-technological security concerning the CII. It did not, however, include the term cyber.

According to the Fundamentals, the reasons for protecting the CII were the blurred and vulnerable boundaries between 'the national segments of telecommunications networks.' The main task of the government was to develop a system of government management and control over the CII, to ensure the resilience of the national segment of the global information network, to create a system of protection of the CII, to prevent the flow of information critical for the CII through foreign countries, and to promote domestic ICT industry and import substitution. After a preparatory period in 2012–2016, the policy would be implemented in 2017–2020.[2227] In the absence of a national cyber security strategy, the Fundamentals provide a substitute. It resonates quite significantly with the idea of digital sovereignty and the unified information space. It also incorporates the concept of ASUs to the CII and creates an interesting dichotomy between them. Most importantly, it defines the framework and language for the defensive side of strategic level information-technological security and defence. The protection of the CII is a task of national level cyber defence and the authority concerning it is given to the FSB.

The project to protect the CII was largely frozen between 2014–2017 as Minkomsviaz', the FSTEK, and the FSB fought over the power to control the CII through various draft laws. In 2017 the Law on Critical Information Infrastructure was finally adopted and it affirmed the leading role of the FSB.[2228] It defined the CII as "information systems, information and telecommunications networks, automated control systems of critical information infrastructure subjects [state administration,

[2225] Комаров, Алексей. Нормативные документы по безопасности АСУ ТП, АСУ ПиТП, КСИИ, КВО, КИИ [Online]. Available: https://www.securitylab.ru/blog/personal/zlonov/144489.php [Accessed: 15th May 2019]; Pynnöniemi 2012; Pynnöniemi & Busygina 2013.

[2226] Основные направления. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом РФ 03.02.2012 N 803) [Online]. Available: http://www.scrf.gov.ru/security/information/document113/ [Accessed: 18th April 2019].

[2227] Ibid.

[2228] Ristolainen 2017a & 2017b.

persons or firms].”[2229] The critical aspect was linked to the infrastructure related to the health care, science, transport, communications, energy, banking and other areas of the financial market, the fuel and energy complex, the field of atomic energy, defence, rocket and space, mining, metallurgical and chemical industries. The security of CII meant its resilient functioning under computer attack.[2230] The law on the CII is decidedly state-centric, materialistic, and technology-oriented in its approach. It makes a distinction between electronic communication networks and the CII/ASUs. The former was regulated by the Law on Communication and belonged to the authority of Minkomsviaz'. However, as the GosSOPKA system was envisioned to cover both, and the authority to define and regulate what exactly belonged to the CII was given to the FSTEK, tensions between institutions were inevitable. The ‘significant objects’ of CII were to be categorized by the operators of CII objects themselves and then submitted to the FSTEK for approval. The categories were based on social, political, economic, ecological, and defence and security significance, and the degree of criticality was based on three levels of damaging effects from minor to catastrophic. The criteria for the categorization of the ‘significant objects’ of CII are provided in a government decree published in 2018 and they are based on the indicators of human casualties, economic losses, territorial magnitude, and the hierarchy of state power.[2231] The FSTEK approves the categorizations and designation, and places the CII in a special register. However, the operators are themselves responsible for the protection of CII objects, and must react to incidents in a way defined by the FSTEK/FSB. They must also share information with them and must ensure the access of the FSB to the objects of CII under their control.[2232] The monitoring and security systems of these objects could be connected, if operators so wished, to the GosSOPKA (cf. Chapter 6.4.1).

Based on the above it can be argued that, the Russian state cyber security understanding focuses around the concept of CII. To protect its ‘significant objects’ a vertical, hierarchical, and centralized system is being built which has the possibility to connect all strategic sectors of the nation to a system of cyber security operated by the FSB. The CII is the infrastructural part of the unified information space and thus digital sovereignty and its defence resonates quite strongly with strategic deterrence and with retaining the information superiority. The laws and directives concerning the CII and GosSOPKA state quite clearly that the control of the infrastructure is a source of sovereignty and material and technological power, and that the CII must be protected primarily from foreign actors and influence. Moreover, the CII is central to nation level information-technological warfare combining the vulnerabilities and strengths of ASUs for a new era. GosSOPKA with its multilevel centres and systems is a clear manifestation of the information security system of systems that Russian information warfare theorists were promoting from the 2000s. Thus, it combines the idea of the EIP and ASUs.

[2229] Федеральный закон 2017a.

[2230] Ibid.

[2231] Постановление Правительства РФ (2018a) от 8 февраля 2018 г. № 127 Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений (с изменениями от 13 апреля 2019 г.) [Online]. Available: https://fstec.ru/component/attachments/download/1917 [Accessed: 15th May 2019].

[2232] Ibid.

6.3.2 The strategies

Parallel and concurrently with the censorship policies, law enforcement, and protection of critical infrastructure, the Russian regime has implemented its information society strategy and doctrine. The Russian government led again by Dmitri Medvedev in November 2013 published the Development Strategy of the Information Technology Industry in the Russian Federation for 2014–2020 and for the Future up to 2025.[2233] It was based on the 2008–2009 Strategy and Concept. It would contribute to ensuring the information security and high quality of Russia's defence through new technologies and by neutralizing global information threats. The Strategy recognized the problems of Russian ICT sector but was quite optimistic about the global prospects of Russian companies. It stated the main civilian and military technologies that must be pursued were to be AI, quantum technologies, and robotics. Information security required the production of domestic technologies. The objective was to ensure the sovereignty of the information technology sector.[2234] Although the Strategy incorporated the ideas of sovereignty and great power struggle, it was decidedly business-oriented and information security was almost an afterthought. However, information technology was now accepted as a defining element of state and military power.

The new Government Programme of Information Society (2011–2020) was adopted in 2013.[2235] It was based on previous strategic documents and emphasised economic and technological competition. It consisted of four 'directions' (napravlenie) of information and telecommunications infrastructure and services, information environment, security in information society, and information government. The objective of the first was to modernize the Russian ICT infrastructure. The second included both domestic and international strategic communication and public affairs projects like support for the Russia Today TV-channel. The third direction was based on creating resilient information infrastructure, on counterterrorism and extremism efforts, and on controlling and monitoring of communications. The fourth direction was about e-government and the removal of domestic 'digital inequality'. Overall, the 2013 Programme did not diverge very much from the direction set by the earlier governments. It still included the Management System and the protected government segment, the information-analytical system for special purposes, and the unified information space in the sphere of technological and information-communication management of the government, and multiple unified and single subsystems. The term unified information space, as a main principle, was however dropped.[2236]

The Programme was decidedly revised in March 2017 and has been revised multiple times after that. It was now based on the 2016 Information Security Doctrine. Under

[2233] Распоряжение Правительства РФ от 01.11.2013 N 2036-р (ред. от 18.10.2018) "Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года" [Online]. Available: https://digital.gov.ru/common/upload/ Strategiya_razvitiya_otrasli_IT_2014-2020_2025.pdf [Accessed: 15th May 2019].

[2234] Ibid.

[2235] The comparisons of different versions was done using the Consultant.ru service. For the latest version cf. Постановление Правительства РФ от 15.04.2014 N 313 (ред. от 29.03.2019) "Об утверждении государственной программы Российской Федерации "Информационное общество" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_162184/ [Accessed: 15th May 2019].

[2236] Ibid.

priorities and targets, for example, it mentions, strategic deterrence and the prevention of military conflicts that may arise as a result of the use of information technology; countering the use of information technology to promote extremism, xenophobia and nationalism; and eliminating the dependence of the domestic industry on foreign information technologies. The third 'direction' was now about "the prevention of threats in the information society" and was based decidedly on blacklisting and content monitoring but also on data privacy protection and counter-terrorism. It lacked any mention of fighting cybercrime, but as responses to nation level cyber security threats it promoted the creation of a national routing information register and 'the cybersecurity of the microprocessors of transportation.' The fourth direction was still about e-government but emphasised the information infrastructure and services the government required, not so much the services it was supposed to offer.[2237] National security issues clearly gained importance, but it would be exaggeration to claim that the Programme was militarized, securitized, or had a 'mobilizing' character. It combined many older projects but placed the emphasis on security and domestic production of hardware and software. One important detail is that between 2017-2019 versions of the program the national segment of the Internet replaced the EIP as a guiding concept.[2238]

The change in the tone of the Programme was related to the domestic political debate on the information sovereignty and the suspected foreign plans to 'disconnect the Russian Internet', a threat promoted perhaps most vocally by the Minkomsviaz'. The idea of information or digital sovereignty was embraced by some Russia politicians already in 2012. The Federal Council drafted in 2012–2013 a Concept of Cyber Security of the Russian Federation which was never approved. The Concept introduced the concepts of cyberspace[2239], cyber security[2240] and cyber war, but tried as well to include the information-psychological aspects of previous doctrines and strategies.[2241] The advocate of the failed Russian cyber security strategy in the Federal Council, Ruslan Gattarov, stated in 2012 that the goal of the document was to shape the county's 'digital sovereignty'.[2242] Ruslan Gattarov argued that "an infrastructure must be created so that the system [infrastructure of security] does not depend on a single cable, and in the case of a state of emergency it could redistribute the load for the smooth operation of the Russian Internet […] That is, the strategy should guarantee

[2237] Ibid.

[2238] The comparison of different versions was done with Consultant.ru service.

[2239] "Cyberspace is a sphere of activity in the information space, formed by a set of communication channels of the Internet and other telecommunication networks, technological infrastructure ensuring their functioning, and any forms of human activity carried out through their use (person, organization, state)." (Концепция. Концепция Стратегии Кибербезопасности Российской Федераци [Проект], 2013 [Online]. Available: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf [Accessed: 27th February 2019].)

[2240] "a set of conditions under which all components of cyberspace are protected from the maximum possible number of threats and impacts with undesirable consequences." (Ibid.)

[2241] Ibid.

[2242] Совет Федерации Федерального Собрания Российской Федерации. Проект стратегии кибербезопасности России направлен на формирование цифрового суверенитета страны, 27 февраля 2013 [Online]. Available: http://council.gov.ru/events/news/14575/ [Accessed: 27th February 2019]; Иванов, Максим. Совет федерации занялся цифровым суверенитетом: Стратегии кибербезопасности наметили основные направления. Коммерсантъ № 209 от 06.11.2012 [Online]. Available: https://www.kommersant.ru/doc/2060832 [Accessed: 4th December 2018]; Рябухина, П. П., Бондуровского, В. В., Перекопского, Г. И. (Под ред.) Законодательство государств - членов ОДКБ в сфере обеспечения информационной безопасности: опыт, проблемы и перспективы гармонизации. Материалы международной научно-практической конференции. СПб.: Секретариат МПА СНГ.

"digital sovereignty"."[2243] Dennis Davydov the Director of the League for a Secure Internet claimed in response to Gattarov that "Digital sovereignty is part of our state sovereignty, part of absolute and complete autonomy in determining policies and setting any rules. Globally, only three powers have the digital sovereignty: The United States, China and, to a lesser extent, the Russian Federation. Here, from the point of view of digital sovereignty one can speak about the presence of one's own search engines, one's own social networks, browsers and operating systems."[2244] Russia's Minister of Telecommunications Nikolai Nikiforov (2010–2018) was also a supporter of the idea of 'information sovereignty'. For him, sovereignty meant domestic hardware and software production i.e. independence from foreign technological solutions.[2245] Consequently, the concept of sovereignty was associated with ICT and the Internet in the names of government workgroups and projects. For example, in 2016 a working group titled 'Internet + sovereignty' was established in the presidential administration to draft a road map for "ensuring sovereignty in the field of information technology and telecommunications."[2246]

The war in Ukraine and the Western reactions to it brought about a real policy change instead of just philosophical debates.[2247] In July 2014 the Minkomsviaz', the FSB, the FSO, the Ministry of Defence and Rostelekom (including the Coordination Centre of National Domain of Internet and the Technical Centre) conducted an exercise to assess the security and stability of the national segment, the degree of its connection to the global infrastructure, its potential vulnerabilities, and the level of readiness for joint work of industry organizations, telecom operators and situation centres of the federal executive bodies.[2248] According to Oleg Demidov, the scenario of the exercise was based on the ENISA Threat Landscape of Internet Infrastructure report published in 2008 and it involved threats against the DNS, BGP and IP routing, DDoS attacks, and the disconnection of traffic to and from Russia by foreign actors. Demidov claims that the exercise proved that the segment was resilient but the cooperation between different actors had serious problems.[2249] However, the Security Council adopted a statement that argued that the exercise had shown that the national segment was vulnerable. Minkomsviaz' was probably given a task to draft a proposal on how to ensure the resilience of the national segment, and yearly cyber exercises including the Minkomsviaz', the FSB and the MoD were announced.[2250]

[2243] Иванов 2012.

[2244] Хизриев, Арсен, Балтачева, Марина. «Используют тактику «выжженной земли». ВЗГЛЯД, 27 сентября 2013 [Online]. Available: https://vz.ru/politics/2013/9/27/652418.html [Accessed: 27th February].

[2245] Латухина, Кира. Спецфонд безопасности. Российская газета 25.09.2014 [Online]. Available: https://rg.ru/2014/09/24/putin-site.html [Accessed: 28th February 2019].

[2246] Анненков, Андрей. «Интернет+суверенитет» рабочей группы по Интернету рассмотрела проект дорожной карты. D-Russia.ru 29 сентября 2016 [Online]. Available: http://d-russia.ru/podgruppa-internetsuverenitet-rabochej-gruppy-po-internetu-rassmotrela-proekt-dorozhnoj-karty.html [Accessed: 28th February 2019].

[2247] Резчиков, Андрей. Избежать отключения от интернета России поможет Китай. ВЗГЛЯД, 29 декабря 2016 [Online]. Available: https://vz.ru/society/2016/12/29/744236.html [Accessed: 16th May 2019].

[2248] Минкомсвязь. Минкомсвязь, ФСБ и Минобороны провели учения по защите российского сегмента интернета. 28 июля 2014 года [Online]. Available: https://digital.gov.ru/ru/events/31441/ [Accessed: 16th May 2019].

[2249] Демидов & Махукова 2016.

[2250] Совет Безопасности Российской Федерации 2014; Голицына, Анастасия. Совет безопасности обсудит отключение России от глобального интернета. Ведомости, 19 сентября 2014 [Online]. Available: https://www.vedomosti.ru/politics/articles/2014/09/19/suverennyj-internet [Accessed: 16th May 2019]; Кантышев, Павел, Болецкая, Ксения, Никольский, Алексей. Россия не будет отключена от интернета.

Ex-minister of Communications Igor Chshegolev and the then advisor of the president on information technology claimed in October 2014 that the Security Council considered the functioning of the Internet to be a national security issue and that Russia was being isolated from the outside. The critical services of the national segment resided outside Russia and it did not control them. Russian ccTLDs could be removed from DNS root-files or its AS and IP -address spaces from RIPE registries and/or from the routing policies of neighbouring networks. Moreover the leading Internet companies were American and their data was in the disposal of American intelligence services.[2251] Later, in May 2015 Chshegolev claimed that the national security of states would be secured if they had the sovereign right to control their national segments, domestic laws to regulate global Internet companies were formulated, and the governance of the Internet was established on equal grounds.[2252] These views were shared by the President's advisor on the Internet German Klimenko who in December 2016 claimed that Russia had to be ready for it to be disconnected from the Internet from the outside and this required laws to regulate the national segment of the Internet.[2253] Klimenko also argued in a meeting of the General Staff in 2017 that the only way to secure the Russian Internet was to copy the information security system of China. This policy is nowadays called 'kitaizatsiia' or Sinicization.[2254] It is thus safe to argue that the views later manifested in the government programs and laws were quite widely shared by the security and defence elite of Russia by 2015-2016.

Minkomsviaz' drafted a proposal for securing the resilience and security of the national segment which was 'leaked' in March 2015. It included measures such as taking state control of the MSK-IX, the Coordination Centre of National Domain of Internet and the Technical Centre, implementing a ban on using cross-border connections by commercial companies, and the duplication of ccTLD DNS architecture and national AS/IP -registries managed by the RIPE/ICANN.[2255] Minister Nikiforov planned to bring his ideas on information sovereignty to the government and Putin in April 2015, but for reasons unknown he did not publicly present his report and the

Ведомости, 02 октября 2014 [Online]. Available: https://www.vedomosti.ru/technology/articles/2014/10/02/na-strazhe-interneta [Accessed: 16th May 2019]; ТАСС. Глава Минкомсвязи пообещал проводить ежегодные учения по обеспечению устойчивости рунета. ТАСС, 19 ноября 2014 [Online]. Available: https://digital.gov.ru/ru/events/32136/ [Accessed: 16th May 2019].

[2251] Анненков, Андрей. Игорь Щёголев: «Учения подтвердили недостаточную устойчивость Рунета при недружественных «целенаправленных действиях». D-Russia.ru, 17.10.2014 [Online]. Available: http://d-russia.ru/ucheniya-podtverdili-nedostatochnuyu-ustojchivost-runeta-pri-nedruzhestvennyx-celenapravlennyx-dejstviyax.html [Accessed: 29th May 2019].

[2252] Анненков, Андрей. Игорь Щёголев: безопасность Интернета и безопасность граждан должны обеспечиваться суверенитетом государств в киберпространстве. D-Russia.ru, 12.5.2015 [Online]. Available: http://d-russia.ru/igor-shhyogolev-bezopasnost-interneta-i-bezopasnost-grazhdan-dolzhny-obespechivatsya-suverenitetom-gosudarstv-v-kiberprostranstve.html [Accessed: 16th May 2019].

[2253] Ведомости. Клименко предупредил россиян о возможном отключении от мирового интернета. Ведомости, 29 декабря 2016 [Online]. Available: https://www.vedomosti.ru/politics/news/2016/12/29/671725-klimenko [Accessed: 16th May 2019].

[2254] Интерфакс. Советник президента Клименко предложил ограничить в России интернет. Интерфакс, 26 января 2017 [Online]. Available: https://meduza.io/news/2017/01/26/sovetnik-putina-nazval-kitayskiy-variant-edinstvennym-sposobom-obespechit-informatsionnuyu-bezopasnost-rf [Accessed: 17th May 2019]; Роскомсвобода. «Китаизация» Рунета входит в активную фазу и начнётся с точек обмена трафиком. Роскомсвобода, 18.8.2017 [Online]. Available: https://roskomsvoboda.org/31224/ [Accessed: 17th May 2019].

[2255] Голицына & Серьгина 2015.

discussion on sovereignty was put aside.[2256] However as will become clear below, the ideas in the Minkomsviaz' report were included in the National Programme of the Digital Economy adopted in 2017. Minkomsviaz' tried to push its views into law during 2015-–2018 but it ultimately failed as first the new Information Security Doctrine was adopted in December 2016 and then the FSB managed to get its own law on critical information infrastructure accepted in July 2017.[2257] However, Minkomsviaz' gained control of the Digital Economy Programme which incorporated almost everything Nikiferov had promoted. Moreover, Rostelekom took control of the critical services listed by the Minkomsviaz' between 2017–2018.[2258]

Consequently, in 2018 Nikiforov begun to use the term 'digital' instead of 'information' sovereignty.[2259] The term 'digital sovereignty' was also used by Natal'ia Kasperskaia who stated in 2017 that "Digital state sovereignty is the right and the ability of a country to independently determine what is happening in its information space […] The components of digital sovereignty are its own hardware platform, its own software platform, its own enterprise and state management systems, its own Internet infrastructure, its own online payment system and electronic commerce system with the remote identity verification subsystem, its own media structure of the Internet, and its own information management system."[2260] She also stated that only the Unites States is currently digitally sovereign. For Kasperskaia digital sovereignty obviously included both the psychological or, more precisely, content aspect of information and the technological or infrastructural aspect.[2261] For her, digital sovereignty was a system of systems run over common platform.

The above examined discussions were reflected in the new Strategy of the Development of Information Society for 2017—2030 which was signed by the President in May 2017.[2262] It was an official strategic planning document and incorporated fully the guidance of 2015 NSS and 2016 Information Security Doctrine. It offered many definitions of central concepts and defined, for example, information space (informatsionnoe prostranstvo) as "a set of information resources created by subjects of the information sphere, means of interaction of such subjects, their information systems and the necessary information infrastructure." The basic premise was that new

[2256] Голицынаб Анастасия. Правительство не планирует рассматривать вопрос о суверенитете рунета. Ведомости, 31 марта 2015 [Online]. Available: https://www.vedomosti.ru/technology/articles/2015/03/31/pravitelstvo-ne-planiruet-rassmatrivat-vopros-o-suverenitete-runeta [Accessed: 16th May 2019].

[2257] Ristolainen 2017a & 2017b; Голицына, Анастасия, Серьгина, Елизавета, Козлов, Петр. Государство хочет контролировать маршруты интернет-трафика в стране. Ведомости, 11 февраля 2016 [Online]. Available: https://www.vedomosti.ru/politics/articles/2016/02/11/628508-gosudarstvo-hochet-kontrolirovat-rossiiskii-zarubezhnii-internet-trafik-strane [Accessed: 16th May 2019]; Балашова, Анна, Коломыченко, Мария. Власти предложили новые ограничения для владельцев точек обмена трафиком. РБК, 16 август 2019 [Online]. Available: https://www.rbc.ru/technology_and_media/16/08/2017/ 59942b429a794794dd46800c [Accessed: 16th May 2019].

[2258] Cf. Chapter 6.1.

[2259] АиФ 2018.

[2260] Бирюлин, Роман. Стремление к цифровому суверенитету. Кразная звезда, № 136 6 декабря 2017.

[2261] Kasperskaia is the leader of the work group on information security in ANO Digital Economy. She is also the President of the InfoWatch group of companies, co-founder of Kaspersky Lab, a member of the Grant Committee of the Skolkovo Foundation, Chairman of the Board of the Association of Software Developers "Otechestvenniy Soft", member of the Expert Council on Russian Software at the Ministry of Communications and Mass Media. (Цифровая экономика. Информационная безопасность [Online]. Available: https://data-economy.ru/security#rec34030444 [Accessed: 28th February 2019].)

[2262] Указ Президента РФ 2017a.

and future technologies[2263] would create a national digital economy which would provide a source of wealth but also protect the country from vulnerabilities and outside attacks. The way in which information technologies had developed, especially the Internet, gave states with developed technologies the possibility to influence the populations of other countries to advance their own interests. The Strategy stated that "to effectively manage the communication networks of the Russian Federation, to ensure their integrity [tselostnost'], unity [edinstvo], resilient [ustoichivyi] operation and security [bezopasnost'], it is necessary to: a) create a centralized system for monitoring and managing the unified telecommunications network of the Russian Federation; b) to create systems enabling stable, safe and independent functioning of the Russian segment of the Internet; c) ensure the reliability and availability of communication services in Russia, including in rural areas and inaccessible localities; d) create state bodies and organizations for expanding the use of domestic telecommunications equipment and software in communication networks; e) maintain the infrastructure of traditional communication services (postal services, telecommunications)."[2264] To these requirements were added the uniformity of state regulation, e-government services, the use of Russian crypto algorithms, ensuring information technological independence, the deployment of the GosSOPKA, and ensuring data localization and privacy.[2265] The concepts of technological independence and competitiveness were derived from the Strategy of Scientific-Technological Development of the Russian Federation which was adopted in 2016.[2266] The Strategy reflects the increasing importance of sovereignty and information struggle which were observed already above in the way the Programme of Information Society developed between 2013—2017 and the Russian internal information and cyber security debate proceeded between 2013—2016.

The Strategy used the concept of 'the national segment of the Internet' to emphasis the sovereign right of the state to control its information space. The national segment implicitly consists of the national information infrastructure (software and services, information systems, data centres and networks), mainly but not altogether understood as a part of the Internet. Interacting upon and with it are political, military, economic, and information (cultural) spheres of life which are under the state jurisdiction. The concept of 'information space' was used to denote a Russian value, language and culture-based space while critical infrastructure was the material and technological base of the national segment. Thus, the Strategy incorporated both information-technological and psychological aspects of information. According to the Strategy, Russian interests included, amongst increased competitiveness, strengthening of economy and the protection of private and business interests, 'technological independence', and the securing of Russian public and private information. Import restrictions would protect its developing industry.[2267] The Strategy resonates with the idea of struggle and information superiority through the strategic technological-scientific advantage it pursues. The emphasis of future breakthrough technologies and the

[2263] Nano- and biotechnologies, optical technologies, data analytics and storage (big data, IoT, and cloud-based services), artificial intelligence, and alternative energy sources.

[2264] Указ Президента РФ 2017a.

[2265] Ibid.

[2266] Указ Президента РФ от 01.12.2016 N 642 "О Стратегии научно-технологического развития Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_ 207967/ [Accessed: 16th May 2019].

[2267] Ibid.

simultaneous protection of own industry and society is compatible with an asymmetric response. The whole Strategy is a means to produce measures for strategic deterrence and to create substance for digital sovereignty.

6.3.3 The policies

The main implementation policy document related to the national segment of the Internet is the government programme and later national programme of Digital Economy. It is based on the Strategy of the Development of Information Society and, to a lesser extent, the Information Security Doctrine.[2268] It is thus part of the strategic planning process of the state and has both socio-economic and (military) security aspects.[2269]

The Programme of Digital Economy sets its objectives and tasks in the context of five directions (napravlenie): normative regulation, cadres and education, research and technical reserves, information infrastructure, and information security. The last two are of interest when examining how Russia is shaping cyberspace and trying to control the national segment of the Internet. Information infrastructure and security related objectives and tasks are based on external and internal challenges and threats, and the main objective is: "ensuring the unity [edinstvo], resilience [ustoichivost'] and security [bezopasnost'] of information-telecommunications infrastructure of the Russian Federation on all levels of information space."[2270] The Programme combines security with economy by emphasising the use of domestic software, hardware, and cryptographic solutions. Most interestingly, the Programme presents a 'road-map' which states that in 2020 Russia will ensure its 'digital sovereignty' and in 2024 all the objectives of the Programme will be achieved. In relation to this, according to the Programme, in 2024 only 10% of internal traffic of the 'Russian segment of Internet' will be routed through foreign servers.[2271]

Between December 2017 and February 2018 'the Government Commission on the Use of Information technology to Improve the Quality of Life and Business Conditions' approved action plans for the five 'directions' of Programme of the Digital economy.[2272] According to the action plans the total budget of 'the Digital Economy' would be 522 billion roubles.[2273] However, the Programme was updated to a status of a national programme in May 2018 and its budget was raised first to 3,5 trillion roubles

[2268] Распоряжение Правительства РФ 2017.
[2269] Распоряжение Правительства РФ 2017; Указ Президента РФ 2016b; Федеральный закон от 2014a. Another important document is the Strategy of Scientific-Technological Development of the Russian Federation (Указ Президента РФ 2016a). The following examination of the Digital Economy Programme is taken from a previously published research paper and updated (Kukkola, Juha. New guidance for preparing Russian 'digital sovereignty' released, Finnish Defence Research Agency, Research Bulletin 01 – 2018).
[2270] Распоряжение Правительства РФ 2017.
[2271] Ibid.
[2272] Правительство Российской Федерации. О «дорожных картах» по направлениям программы «Цифровая экономика Российской Федерации». 9 января 2018 [Online]. Available: http://government.ru/orders/selection/401/30895/ [Accessed: 16th May 2019]; Правительство Российской Федерации. Утверждён план мероприятий по направлению «Кадры и образование» программы «Цифровая экономика Российской Федерации» 21 февраля 2018 [Online]. Available: http://government.ru/news/31428/ [Accessed: 22 March 2018].
[2273] Тишина, Юлия, Жукова, Кристина. Оцифрованные миллиарды. Правительство утвердило проекты «Цифровой экономики». Коммерсантъ №2 от 10.01.2018 [Online]. Available: https://www.kommersant.ru/doc/3515334 [Accessed: 22 May 2018].

and then by December 2019 lowered to 1,7—1,8 trillion roubles of which 1 trillion would be designated from the federal budget for 2019—2024 and the rest would come from the private sector.[2274] For comparison the whole budget of the national programmes initiated by Putin's 2018 May Edicts is 25,7 trillion roubles.[2275] In comparison the budget of arms procurement programme GPV 2018— is approximately 19 trillion roubles.[2276] The responsibility for implementing 'directions' of 'information infrastructure' and 'information security' was given to Minkomsviaz', and a non-commercial organisation 'Digital Economy' was created to coordinate the public and private activities and to monitor the realization of the state programme.[2277]

Practically all state power ministries and security agencies are listed as responsible actors for 'the direction of information infrastructure.'[2278] The same applies to major IT-companies which are listed as participating contractors. The main objectives of 'the direction' are: Adequate national communication network; domestic infrastructure for data storage and processing which provides affordable, sustainable, safe, and cost-effective services; and adequate digital platforms for the needs of citizens, business and the government. In practice, the first objective includes, for example, creating normative base for the use of information technology, high-speed Internet (100Mb/s) to almost every household and government institution by 2024, speech and data connection to all priority objects of transport infrastructure, the implementation of 5G technology by the economic sector, developing state-wide narrow-band IoT network (LPWAN), and state-wide (including the Arctic EEZ) satellite services. The second objective includes, for example, the establishment of federal datacentres (eight by 2024)[2279] and unified cloud services for the government. The third objective includes, for example, e-government services and their management systems, space based remote sensing system and geodetic control network, and services based on these systems. 'The direction of information infrastructure' is the most expensive one and amounts to circa 436 billion roubles (7,6$ mrd). The FSB, FSO and FSTEC have a definite role in planning these projects but implementation is left to state corporations and private sector.

Russia is planning, as a part of Sfera which is a more comprehensive satellite programme including navigation and communication services, to either participate or clone the OneWeb, SpaceX and Telsat LEO satellite mega-constellations projects to provide Internet regionally and globally to 'friendly' countries. This project has faced

[2274] Шмырова, Валерия. «Цифровая экономика» исполняет бюджет хуже всех нацпрограмм, потому что обо всем советуется с бизнесом. CNews, 11.11.2019 [Online]. Available: https://cnews.ru/news/top/2019-11-08_tsifrovaya_ekonomika_ispolnyaet [Accessed: 6th January 2020].

[2275] Баленко, Евгения, Кузнецова, Евгения. Исполнение законопроекта о суверенном Рунете подорожало до ₽30 млрд. РБК, 26 мая 2019 [Online]. Available: https://www.rbc.ru/technology_and _media/26/03/2019/5c98f1bd9a79476ea86fc631?from=center [Accessed: 16th May 2019].

[2276] Connolly & Boulégue 2018.

[2277] Постановление Правительства РФ 2019a.

[2278] Правительственная комиссия. План мероприятий по направлению "Информационная инфраструктура" программы "Цифровая экономика Российской Федерации" (утв. Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 18.12.2017 N 2)) [Online]. Available: http://static.government.ru/media/files/DAMotdOImu8U89bhM7lZ8Fs23msHtcim.pdf [Accessed: 16th May 2019].

[2279] Situated in the Central Federal Okrug, North-Western Federal Okrug, Uralskii Federal Okrug, Siberian Federal Okrug , Privolzhzkii Federal Okrug , and the Far-Eastern Federal Okrug , and probably two more to ensure resiliency of the system.

opposition from parts of the government and domestic companies.[2280] Most importantly, the FSB has opposed the project demanding that it must have access to all data traffic going through the Russian national segment of the Internet, and the MoD, which controls the frequency allocation in Russia, has been unwilling to provide up- and downstream frequency bands for the satellites.[2281] The plans to deploy 5G IoT and SmartCity and SmartGrid networks in the biggest Russian cities has also faced resistance from the FSO and the MoD.[2282] The most important challenge to all these projects has been the lack of financing and technology which has led Russia to partner with China.[2283] However, the demands that the Digital Economy projects should be based on Russian hardware and software might make this cooperation challenging.[2284] The other member of the EEU have already complained about Russian protectionist ICT policies.[2285]

'The direction of information security' does not include the Ministry of Defence in its list of responsible actors, although, it is consulted in some of the projects. All the other security ministries and agencies are present. The main objectives of information security are: ensuring the integrity (tselostnost'), resilience (ustoichivost') and security (bezopasnost') of information-telecommunications infrastructure of the Russian Federation on all levels of information space; ensuring organizational and legal protection of individual, business and state interests in the framework of the digital economy; and the creation of conditions for Russia's leading position in the export of information security services and technologies, as well as the integration of national interests in the international documents on information security issues.[2286]

[2280] Джорджевич, Александра. Сферический триллион в «Эфире»ю Как «Роскосмос» конкурирует с Илоном Маском за глобальный спутниковый интернет. Новая газета, № 140 от 13 декабря 2019 [Online]. Available: https://novayagazeta.ru/articles/2019/12/12/83136-sfericheskiy-trillion-v-efire [Accessed: 7th January 2020].

[2281] Балашова, Анна, Сидоркова, Инна, Коломыченко, Мария. Правительству предложат создать глобальную спутниковую сеть за ₽299 млрд. РБК, 22 ноября 2017 [Online]. Available: https://www.rbc.ru/technology_and_media/22/11/2017/5a159bdb9a79476a55456d2b?from=center_4 [Accessed: 15th April 2019]; Сафронов, Иван. «Группировка будет развернута в любом случае: с нашим участием или без него». Коммерсантъ №33 от 25.02.2019 [Online]. Available: https://www.kommersant.ru/doc/3894154?from=author_tech [Accessed: 15th April 2019].

[2282] Репин, Андрей. «Новинки Smart City» будет достраивать АО «СЗ НО «Дирекция по строительству». Коммерсант, 12 декабря 2018 [Online]. Available: https://www.kommersant.ru/doc/3827866 [Accessed: 15th April 2019]; Чурапченко, Евгения, Семашко, Наталья. Энергетика цифры. Коммерсантъ, 2 октября 2018 [Online]. Available: https://www.kommersant.ru/doc/3758627?query=smart%20grid [Accessed: 15th April 2019]; Кодачигов, Валерий. Минобороны отказалось передавать операторам частоты для 5G. Без этого появление в России связи пятого поколения невозможно. Ведомости, 28 марта 2019 [Online]. Available: https://meduza.io/news/2019/03/29/minoborony-otkazalos-peredavat-operatoram-svyazi-chastoty-dlya-5g [Accessed: 15th April 2019]; Балашова, Анна, Сидоркова, Инна. Роскомнадзор выступил против выдачи частот для глобальной сети OneWeb. РВК, 14 апреля 2018 [Online]. Available: https://www.rbc.ru/technology_and_media/14/04/2018/5ad0ac9d9a794746645fa041?from=main [Accessed: 15th April 2019].

[2283] Балашова, Анна, Кирьянов, Роман. Акимов объявил о создании российско-китайского конкурента OneWeb. РБК, 17.9.2019 [Online]. Available: https://www.rbc.ru/technology_and_media/17/09/2019/5d80eea69a794755e1c48c87 [Accessed: 7th January 2020]; Bendett & Kania 2019.

[2284] Балашова, Анна, Баленко, Евгения. Операторов 5G переведут на российские серверы. РБК, 2.9.2019 [Online]. Available: https://www.rbc.ru/technology_and_media/02/10/2019/5d9363d59a7947b1a00cd012 [Accessed: 7th January 2020].

[2285] Кинякина, Екатерина, Жукова, Кристина. Соседи России раскритиковали закон о предустановке российского софта. Ведомости, 22 декабря 2019 [Online]. Available: https://www.vedomosti.ru/ technology/articles/2019/12/22/819374-raskritikovali-zakon-po [Accessed: 7th January 2020].

[2286] Правительственная комиссия. План мероприятий по направлению "Информационная безопасность" программы "Цифровая экономика Российской Федерации" (утв. Правительственной комиссией

The first objective is defined by its indicators to mean reducing the percentage of domestic traffic routing through foreign servers to 10% by 2024, the almost total replacement of foreign produced hardware and software by domestic versions in federal and local administrative organizations, state corporations and corporations connected to state, and the comprehensive implementation of Russian standards of information security by those same actors by 2024. In practice, the resilience and security (ustoichivost' and bezopasnost') of 'the unified telecommunications network of RF is guaranteed by establishing a 'centralized system of monitoring and managing the public communication networks'. This is an organizational and technological project, which is managed by a designated operator, and includes the Ministry of Defence. It functions in cooperation with NKTsKI. The system should be up and running by 2020. Stability and security also include the creation of standards for domestic cloud, fog, and quantum technology, and for systems of augmented reality and artificial intelligence.[2287] As part of the security 'direction' the Russian government is ordering the federal organs to buy Russian office software etc.[2288]

The manageability and reliability (upravliaemost' and nadezhnost') aspect of the first objective concentrates on the 'Russian segment of Internet' and circuiting (zamykanie) its network traffic exclusively inside the territory of the Russian federation. The objective is achieved by establishing a register of routing-address information (Internet Number Registry), a monitoring system of routing information (Internet Routing Registry), nationally controlled DNS root-servers, a national certificate authority centre, through blocking of unlawful content, and cooperation with NKTsKI. These 'subsystems' should be managed by a designed operator. Furthermore, the 'technological independence' and security of data processing infrastructure and systems should be guaranteed.[2289]

The second objective of 'the direction of information security' emphasises the authentication and identification of the subjects of the national segment. Moreover, information security is not only a technological issue but also a normative one and cloud service providers' use of data should be regulated, security standards for big data management should be enforced, criminal code should be updated, and users of communication networks should be identified. The 'Digital economy's' security concept also reflects the Russian understanding of information threats by including the prevention of the appearance of 'unlawful information' (protivopravnaia informatsiia). In practice, information security is based on information sharing and networked systems. One of the systems, probably GosSOPKA, should provide indicators of harmful activity to Central and Regional Coordination Centres of Computer Incidents (NKTsKI and RKTsKI). The substance of another system called 'the centralized system of monitoring and managing the public communication networks' was unclear until 2019 when 'the Law on Sovereign Internet' was approved and a similarly

по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 18.12.2017 N 2)) [Online]. Available: http://static.government.ru/media/files/AEO92iUpNPX7Aaonq34q6BxpAHCY2umQ.pdf [Accessed: 16th May 2019].

[2287] Ibid.

[2288] Жукова, Кристина. Росгвардия купила российский офисный софт на 60 млн рублей. Ведомости, 30 октября 2019 [Online]. Available: https://www.vedomosti.ru/technology/articles/2019/10/30/815092-rosgvardiya [Accessed: 7th January 2020].

[2289] Правительственная комиссия 2017b.

named national system of traffic filtering operated by the Minkomsviaz' was established.[2290] There is also a plan to enforce domestic anti-virus software on all personal computers in Russia—this software would probably send data on the hosts to centrally controlled system.[2291]

The third objective of information security has a definite foreign policy character, although exporting Russian IT-solutions is at the forefront. The term 'cyberphysical' (kiberfizicheskii) system is introduced and it is connected to IoT (Internet of Things) and to critical information infrastructure. The term's definition is left open, but it is preliminary put into a legal-normative framework where unauthorized interference of 'cyberphysical' systems should be prohibited. This new term has a clear connection to the previous Russian endeavours in the United Nations to ban the hostile use of ICT. The foreign policy element is emphasized by stating that the international information security standards should be developed in accordance with Russian interests, cooperation within the Eurasian Economic Union should be advanced[2292], and the Russian norm proposal on international information security should be approved by the UN by 2020.[2293] Thus, the Digital Economy Programme has also incorporated the Russian cyber diplomacy initiative.

A document stating the specific targets and indicators of the Digital Economy was released in December 2018.[2294] It redefined 'the directions' for projects for the normative regulation of the digital environment, information infrastructure, cadres for the digital economy, information security, digital technology, and digital governmental services. There were some changes and adjustments. For example, the government and presidential administration should acquire a network of distributed situation centres, and the communication satellite network Ekspress-RV and the secure government segment RSNet should be operational by 2024. Rostelekom and Rosenergoatom should build a distributed network of catastrophe resilient datacentres by 2021. The project concerning cadres included the education of over a hundred thousand specialists and the creation of tens of 'digital universities' to teach mathematics, informatics, and technology. GosSOPKA should be operational and the CII categorized by 2021. Moreover, a national fibre optic network should be secured by quantum cryptography by 2021.[2295] The digital economy and technology parts of the programme now concentrated on identifying a group of leading Russian research institutions and companies and providing state support for them to pursue the so-called cross-cutting (skvoznyi) technologies.[2296] Consequently, in February 2019 Vladimir

[2290] Федеральный закон 2019.

[2291] Правительственная комиссия 2017b.

[2292] In this context common normative regulation and standards, joint exercises, and 'a zone of digital trust' are mentioned.

[2293] Правительственная комиссия 2017b.

[2294] Президиум Совета при Президенте Российской Федерации 2018.

[2295] It is unclear if this means the deployment of post-quantum cryptography (PQC) or quantum key distribution (QKD).

[2296] These were big data, neurotechnology and artificial intelligence, distributed registry systems, quantum technologies, new manufacturing technologies, industrial internet, components of robotics and sensorics, wireless technology, virtual and augmented reality technology.

Putin ordered the government to come up with a national strategy on artificial intelligence which it did in October 2019.[2297] For Putin the development of AI technology is the key to 'technological dominance and technological sovereignty', but Russia's ability to create an ecosystems that supports the adoption and adaptation of AI technologies is suspect.[2298] Furthermore, the Security Council has taken part in the policy formulation related to the Digital Economy which demonstrates that digital economy and sovereignty really are a national security issue.[2299]

The 'Digital Economy' is being implemented initially through laws. The so-called 'Law on the Sovereign Internet', was adopted in April 2019 and entered into force in December 2019.[2300] The law draft claimed it ensured the autonomous functioning of the Russian segment of Internet against the threat of disconnection from the outside, i.e. the threat which the new 'active-defence' based Cyber Strategy of the United States presented. Basically, the law requires ISPs to install DPI -equipment controlled by the Roskomnadzor into their networks. This equipment will be used to filter traffic based on the 'Unified register' or blacklist of banned sites and to cut the Russian segment of Internet from the global Internet if Russian critical information infrastructure is faced with a critical threat. These measures will ensure the resilience (ustoichivost'), security (bezopasnost'), and integrity (tselostnost') of that part of the Internet that functions on the territory of the Russian Federation.[2301]

The law mandates the duplication of critical services, i.e. the national system of domain names, envisioned by the Minkomsviaz' already in 2015. It prohibits the use of foreign databases or equipment by state organs or corporations. Moreover, it dictates that state organs and corporations must ensure the possibility of using state sanctioned encryption.[2302] The Committee of Information Politics of Duma tried to get mandatory national SSL certification into the law but did not succeed.[2303] The law is already being implemented as the government has approved the funding of the Centre

[2297] Рябова, Вика. Владимир Путин поручил правительству обеспечить разработку национальной стратегии в области ИИ. D-Russia.ru, 27.2.2019 [Online]. Available: http://d-russia.ru/vladimir-putin-poruchil-pravitelstvu-obespechit-razrabotku-natsionalnoj-strategii-v-oblasti-ii.html [Accessed: 16th May 2019];
Указ Президента РФ от 10.10.2019 N 490 "О развитии искусственного интеллекта в Российской Федерации" (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года") [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_335184/ [Accessed: 7th January 2020].

[2298] Путин, Владимир. Совещание по вопросам развития технологий в области искусственного интеллекта. Kremlin.ru, 30 мая 2019 года [Online]. Available: http://www.kremlin.ru/events/ president/news/60630 [Accessed: 9th July 2019]; Dear, Keith. Will Russia Rule the World Through AI?, The RUSI Journal, Vol. 164, No. 5-6 (2019), 36-60; Bendett, Samuel. Handicaps: weak private sector, Soviet-style bureaucracy. Helps: Great STEM education — and history. Defense One, 25 November 2019 [Online]. Available: https://www.defenseone.com/ideas/2019/11/russias-ai-quest-state-driven-even-more-chinas-can-it-work/161519/?oref=d-topstory [Accessed: 7th January 2020].

[2299] Совет Безопасности РФ 2017.

[2300] Мартынов, Кирилл. Откуда втекает интернет Парламентарии Клишас и Луговой предлагают россиянам самоизолироваться от глобальной сети. Новая газета, 15 декабря 2018 [Online]. Available: https://www.novayagazeta.ru/articles/2018/12/15/78947-otkuda-vtekaet-internet [Accessed: 28th February 2019].

[2301] Федеральный закон 2019.

[2302] Ibid.

[2303] Коломыченко 2019.

of Monitoring and Managing of the Public Communication Networks (Tsentr monitoringa i upravleniia setiu sviazi obshchogo polzovaniia) (TsMUSSOP).[2304] This Centre is planned to be operational in January 2020 and its task is to ensure the security of the Russian segment of the Internet.[2305] In the autumn of 2019 Russia began testing and exercising the disconnecting of the national segment from the global Internet, although, at that time these test had an experimental and technical nature.[2306] Additionally, a set of national cyber security exercises have been planned for 2020.[2307] These annual exercises are required by a government degree.[2308] Additionally, Minkomsviaz' awarded Rostelekom a contract to construct a 'cyber-poligon', or an exercise platform, for nation level cyber exercises and training of specialists.[2309]

Minkomsviaz' presented a draft law in May 2019 "On the approval of the procedure for centralized management of a public telecommunications network." It is meant to regulate how the threats permitting the activation of the 'centralized management' will be defined and when individual ISPs (actors operating lines of communication or autonomous systems crossing state borders) are required to act. The mandate to define the relevance of threats is given to Minkomsviaz' and the FSB, the probability of threats to Rozkomnadzor, and the operation of the system when the threat is deemed high to the Radio Frequency Service which belongs to Rozkomnadzor. Perhaps the most important part of the legal draft are the three definitions of threats to integrity, resilience and security to public networks which basically defines the official Russian view on cyber security. Integrity is about the ability of communication networks to interoperate and connect clients to resources, resilience is the ability of networks to operate under internal and external disturbances and to return to their initial state, and security is the ability to deny unauthorized access and intentional disruption of communication networks.[2310] In addition to Minkomsviaz's draft, multiple other ad-

[2304] Постановление Правительства Российской Федерации от 30.04.2019 № 528 "Об утверждении Правил предоставления из федерального бюджета субсидии на создание и функционирование Центра мониторинга и управления сетью связи общего пользования, а также создание, эксплуатацию и развитие информационной системы мониторинга и управления сетью связи общего пользования" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_324051/ [Accessed: 17th May 2019].

[2305] Панов, Павел, Галанина, Ангелина. Написано связью: правительство начнет контролировать интернет. За трафиком будет следить специальная государственная структура. Известия, 22 февраля 2019 [Online]. Available: https://iz.ru/848412/pavel-panov-angelina-galanina/napisano-sviaziu-pravitelstvo-nachnet-kontrolirovat-internet [Accessed: 17th May 2019].

[2306] Роскомсвобода. Чему научили учения по Суверенному Рунету? Роскомсвобода, 24.12.2019 [Online]. Available: https://roskomsvoboda.org/53902/ [Accessed: 7th January 2020]; Стадник, Илона. Ошибка сети: что показал учебный запуск «суверенного Рунета». РБК, 26.12.2019 [Online]. Available: https://www.rbc.ru/opinions/technology_and_media/26/12/2019/5e046d649a794756d9e55596 [Accessed: 7th January 2020].

[2307]

[2308] Приказ Министерства цифрового развития, связи и массовых коммуникаций оссийской Российской Федерации от 12.12.2019 № 839 "Об утверждении графика проведения плановых учений" [Online]. Available: https://digital.gov.ru/ru/documents/7002/https://digital.gov.ru/ru/documents/7002/ [Accessed: 7th January 2020].

[2309] Роскомсвобода. Ростелеком создаст киберполигон, 06.12.2019 [Online]. Available: https://roskomsvoboda.org/53137/ [Accessed: 10th January 2020].

[2310] Минкомсвязь. Об утверждении Порядка централизованного управления сетью связи общего пользования [Проект] 23 мая 2019 г. [Online]. Available: https://regulation.gov.ru/projects#npa=91558 [Accessed: 15th May 2019].

ministrative orders are being drafted which aim to create multiple registers and regulations.[2311] Many of these orders will not be subjected to a public discussion or parliamentary overview.

The developments of 2012–2019 can be summarized as follows. The laws adopted in 2013–2016 were primarily a reaction to the events of 2011–2012 but by 2016 the need for direct control over the national Internet and information in it and its protection from outside influence became pronounced. By 2017 the concept of the CII had matured to provide the basis for the Russian understanding of national cyber security. After the of Digital Economy Programme was approved, laws were used to define what was meant by the national segment of the Internet. On the strategy level a definite change occurred between 2015-2017 following the reorientation of 2014 with the release of the new Information Security Doctrine in 2016 and Strategy of the Development of Information Society in 2017.[2312] This changed much of the language and made national security a priority issue in building information society and economy. The Doctrine and Strategy were reactions to the events of 2014, not 2011, but combined many of the parallel developments: the Internet as a source of political challenge to the regime, the influences from the Chinese state control over the Internet, the militarization of cyberspace, the growing importance of the CII, the fear of new threats towards the vulnerabilities of the Russian Internet, and the new overall geopolitical situation. Elite reactions to these developments were guided by the strategic cultural ideas. Digital or information sovereignty is a central concept guiding the 2015–2017 documents. The information space as a sphere of politico-military action is connected to strategic deterrence and the great power balance. An asymmetric response due to new technologies and by denying opponents the ability to exploit Russian vulnerabilities. Information superiority on the strategic level is ensured through scientific-technological and educational potential and on operational level by multiple systems of information collection, analysis and response. The EIP will become the national segment of the Internet and will be populated by ASUs in the form of systems and systems-of-systems. The CII provides the framework for national information-technological security, i.e. cyber security.

The National Programme of the Digital Economy synthesised these developments and ideas into a single whole although the regulation of the CII and cyber diplomacy efforts remained largely independent vectors. A strategy for controlling the national information space was thus planned and implemented, and continuously updated as the change of policy level documents have demonstrated. This strategy has been used to shape the national cyberspace to increase state control over a bottom-to-top developed network. However, it is important to note that the making of strategy is not unidirectional process and the National Programme of the Digital Economy has already faced serious doubts concerning the ability of the Russian economy to reach

[2311] Роскомсвобода. «Суверенный Рунет» продолжает обрастать подзаконными актами, 29.05.2019 [Online]. Available: https://roskomsvoboda.org/47342/ [Accessed: 30th May 2019]; Эшер II. Проекты нормативных правовых актов по устойчивому Рунету [Online]. Available: https://usher2.club/ helpers/stable-runet-npa-list [Accessed: 7th January 2020].

[2312] This view is supported by Leonid Levin, the Chair of the Information Policy, Technology and Communications of the Duma (Левин, Леонид. О законодательных мерах по обеспечению информационной безопасности Российской Федерации. Федеральный справочник 2015 [Online]. Available: http://federal-book.ru/files/BEZOPASNOST/soderghanie/NB_2/NB2-2015-LevinLL.pdf [Accessed: 17th May 2019].)

the objectives set to it.[2313] Moreover, in 2018 the direction of security reportedly received only 5% of the planned financing.[2314] However, as the last minute implementation of the last May Edicts in January 2018 demonstrated, financing is only a question of political will.[2315]

6.4 The systems

This chapter examines what kind of civilian and military information systems and networks the Russian regime has built and is building or directing the private sector to build. It introduces the systems which, in principle, form the Russian segment of Internet and which will be used in Chapter 7 to construct the model of system of systems of information security and defence.[2316]

6.4.1 Civilian systems

The strategies, doctrines and policies drafted and adopted by the Russian regime have produced multiple information systems, although the first 2002 eGovernment policy had a halting start and produced few results. As part of Medvedev's liberalization and informatization agenda, the Russian government established its public portal for electronic services in 2009 which began to support services requiring authentication in 2010. These developed in 2011–2013 into the Single System of Identification and Authentication (ESIA) and the Single Portal of State and Municipal Services (EPGU).[2317] 70.5 million people had registered to ESIA in 2017 and 46.6 million had used electronic public services in 2017. The number was up from 20.3 million in 2015 and 31.7 million in 2016. Since 2012 the number of citizens using the EPGU had increased twenty-fold.[2318] Thus, Russian e-governance did not start to develop, despite official declarations, until during Putin's third term.

In 2015 President Putin ordered federal government institutions to connect their information resources to 'the Russia government segment of the Russian information-telecommunications network Internet' (known as the GIS Internet). The task to establish this segment was given to the FSO.[2319] In 2016 the FSO gave an administrative order to develop a governmental segment named RSNet. The idea of RSNet was to

[2313] Российский союз промышленников и предпринимателей. На заседании Комитета РСПП по цифровой экономике обсудили меры господдержки импортозамещения программного обеспечения. 23 апреля 2019 [Online]. Available: http://www.rspp.ru/cc/news/60/16247 [Accessed: 17th May 2019].

[2314] Бодрик, Александр. Кибербезопасность в России: итоги 2018 года и стратегии для 2019-го. IT-Week, 4.2.2019 [Online]. Available: https://www.itweek.ru/security/article/detail.php?ID=205189 [Accessed: 17th May 2019].

[2315] OSCE. Russian Federation Presidential Election 18 March 2018. ODIHR Election Observation Mission Final Report [Online]. Available: https://www.osce.org/odihr/elections/383577?download=true [Accessed: 17th May 2019].

[2316] This chapter is partly based on Kukkola, Juha. Civilian and Military Information Infrastructure and the Control of the Russian Segment of the Internet. Presented in the International Conference on Military Communications and Information Systems (ICMCIS) Warsaw, Poland, May 22.-23., 2018.

[2317] РАЭК. Интернет в России 2014: Состояние, тенденции и перспективы развития. Москва, 2015 [Online]. Available: http://www.fapmc.ru/rospechat/newsandevents/newsagency/2015/08/item1/main/custom/00/0/file.pdf [Accessed: 10th April 2019].

[2318] РАЭК 2018.

[2319] Указ Президента РФ 2015.

connect state information systems to the Internet and to offer public services to citizens through a web-portal. RSNet is operated by the Spetssviazi of the FSO. It is connected to Internet through a gateway and has its own IP-address space and domain zone (gov.ru).[2320] Basically then, RSNet is a Russian government secure Intranet with an Internet gateway. However, at the same time, Minkomsviaz' together with Rostelekom have been developing a Unified Data Network (ESPD) for government agencies which is also a data network.[2321] Its technical monitoring and administration is the responsibility of the Federal Situation Centre of the Electronic Government.[2322] It would seem that RSNet and ESPD are supposed to be part of the same government backbone network with data-centres and multiple layers.[2323] ESPD and RSNet support the System of Interdepartmental Electronic Interaction (SMEV) which is basically a service platform based on a network of seven data centres hosting the services and data for the federal government, agencies and subjects.[2324]

As was noted in Chapter 6.2.3, the Russian government began to develop the Upravlenie system in 2002 which was at first an information sharing platform.[2325] However, Upravlenie was redefined in 2015 as the digital platform for strategic planning together with multiple other information systems like the Unified Intradepartmental Information-Statistical System, the Electronic Budget, and the information-analytical system for monitoring the national security of the Russian Federation. Upravlenie would be based on sharing data between authorities and it would provide a digital,

[2320] Приказ ФСО России от 07.09.2016 N 443 "Об утверждении Положения о российском государственном сегменте информационно-телекоммуникационной сети "Интернет" (Зарегистрировано в Минюсте России 14.10.2016 N 44039) [Online]. Available: http://www.gov.ru/ rsnet/pr_fso_443_07092016.pdf [Accessed: 15th April 2019]; Правительство Российской Федерации. Временные правила администрирования домена gov.ru 2018. [Online]. Available: http://www.gov.ru/ main/rsnet/page541.html. [Accessed 11 January 2018]; Правительство Российской Федерации. Информация администрации сети RSNet [Online]. Available: http://www.gov.ru/main/page5.html [Accessed: 15th April 2019]; Указ Президента РФ 2015.

[2321] Минкомсвязь. Единую сеть передачи данных в 2016 году будут использовать 14 госорганов, 20 января 2016 [Online]. Available: https://digital.gov.ru/ru/events/34535/ [Accessed: 15th April 2019].

[2322] Приказ Министерства связи и массовых коммуникаций Российской Федерации от 16.08.2017 г. № 422 "О порядке функционирования и подключения к федеральной государственной информационной системе "Федеральный ситуационный центр электронного правительства" и признании утратившим силу приказа Министерства связи и массовых коммуникаций Российской Федерации от 1 июля 2014 г. № 184" [Online]. Available: https://rg.ru/2017/10/04/minsvyaz-prikaz422-site-dok.html [Accessed: 15th April 2019].

[2323] Минкомсвязь. Единая информационнотелекоммуникационная инфраструктура органов власти [Online]. Available: https://digital.gov.ru/uploaded/presentations/prezentvopros-2tebenkovedinaya-informtelekinfr.pdf [Accessed: 15th April 2019].

[2324] Udomlia, Ekaterinburg, Novosibirsk, St. Petersburg, Nizhnii Novgorod, Khabarovsk and Rostov-na-Donu. These are the data centres envisioned by the Digital Economy program (Минкомсвязь. Система межведомственного электронного взаимодействия (СМЭВ) [Online]. Available: https://digital.gov.ru/ ru/activity/directions/49/ [Accessed: 15th April 2019]; Ростелеком. Облачные сервисы в Цифровой трансформации, 20.2.2017 [Online]. Available: http://www.rtk-dc.ru/upload/iblock/66b/66b7243122a76c89f8f1be681-cc5f0fb.pdf [Accessed: 15th April 2019]; Tadviser. Система межведомственного электронного взаимодействия (СМЭВ) [Online] . Available: http://www.tadviser.ru/a/71478 [Accessed: 15th April 2019].)

[2325] Постановление Правительства Российской Федерации от 27 ноября 2015 г. N 1278 О федеральной информационной системе стратегического планирования и внесении изменений в Положение о государственной автоматизированной информационной системе "Управление" [Online]. Available: http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102134940&backlink=1&&nd=102383211 [Accessed: 13th May 2019]; Постановление Правительства РФ от 2009b.

cross departmental platform for cooperation.[2326] Consequently, it would make regional and local administration more transparent and controllable to the federal centre of power.

'Upravlenie' operates over the SMEV and consists of an open Internet portal, a semi-closed portion based on the RSNet, and secure (Kontur) parts, an information-analytical subsystem for monitoring, analysing and manipulating information, a subsystem for data management (registers, directories and classifiers) and the central information subsystem 'Federatsiia' which includes databases and modules for collecting and storing data.[2327] The secure Kontur part is reserved for the presidential administration and the government and is not directly connected to the Internet. However, it enables the regime to access all data entered into the 'Upravlenie'. A subsystem of 'Federatsiia' is used to securely input situation data from federal and regional organs into shared databases.[2328] Upravlenie is based on a network of territorially distributed data centres.[2329] Its current operational status, besides official declarations, is unknown. The Digital Economy Programme has added the National System of Information Management (NSUD) to the above described system of systems. It should integrate different government databases and provide interfaces to them by 2024.[2330] In 2019 it was announced that a secure intranet ETsP OGV would be created for the Presidential Administration, the Security Council, the Government and the Federal Assembly in the context of Digital Economy.[2331] Moreover, in December 2019 the government degreed that a 'national information management system' would be created which would, in effect, be a national, unified and single statistical service.[2332]

It is quite possible that Upravlenie is envisioned as the basis for the system of situation centres highlighted by Julian Cooper. In 2012 Cooper claimed that 100 of these centres from the presidential down to the regional level were in existence, their function being the monitoring of the socio-economic and national security situation of the country for the interests of strategic planning.[2333] In 2013 a system of distributed situation centres was set up which was supposed to improve the current system with integrated and coordinated information systems (SRSTs) and services.[2334] The responsibility of this system was given to the FSO and its most important centres currently

[2326] Постановление Правительства РФ 2009b.

[2327] ГАС Управление. Государственная автоматизированная информационная система "Управление" Прикладное программное обеспечение государственной автоматизированной информационной системы «Управление» Регламент подключения и интеграции с ГАС «Управление» [Online]. Available: http://gasu.gov.ru/rest/documents/file/download?fileId=9681 [Accessed: 26th March 2019].

[2328] ГАС Управление. Государственная автоматизированная информационная система "Управление" [Online]. Available: http://gasu.gov.ru/about [Accessed: 26th March 2019].

[2329] ГАС Управление. Прикладное программное обеспечениегосударственной автоматизированной информационной системы «Управление» [Online]. Available: http://gasu.gov.ru/preview?fileId=9681 [Accessed: 15th April 2019].

[2330] Краснушкина, Надежда. Госданным прописали архитектуру. Единая информсреда объединит сотни ГИС. Коммерсантъ" №221 от 30.11.2018 [Online]. Available: https://www.kommersant.ru/doc/3814604 [Accessed: 17th May 2019].

[2331] Королев, Игорь. ФСО и ФСБ получат 1,8 миллиарда на цифровую поддержку Путина и Медведева. Cnews, 21.10.2019 [Online]. Available: https://www.cnews.ru/news/top/2019-10-18_fso_i_fsb_poluchat_18_milliarda [Accessed: 7th January 2020].

[2332] Распоряжение Правительства РФ от 17 декабря 2019 года №3074-р "Концепция создания цифровой аналитической платформы предоставления статистических данных" [Online]. Available: http://static.government.ru/media/files/4YejV8mvcCSeGWTg2kXprmthtNbWyfrU.pdf [Accessed: 7th January 2020].

[2333] Cooper 2012, 6-7.

[2334] Cooper 2018a.

include the Presidential Administration's and Security Council's centres and the National Defence Management Centre. In 2018 Cooper argued that the SRSTs were an "echo of past Soviet aspirations."[2335]

Federal systems are supplemented by sectoral systems. One of these is the State Information System of Fuel and Energy Complex which, according to the law, should automate the collection and distribution of information on the status of the state owned fuel and energy industry and provide forecasts on its development.[2336] The system's development began in 2011 and was still incomplete in the spring of 2019. It could, at least in theory, enable Soviet like micromanagement of the energy sector.[2337] Another system was developed as a response to the fears of Russia being disconnected from the global financial system. In 2014 Russia deployed its own national version of the SWIFT financial messaging service—the Financial Reporting System (SPFS). In 2018 it had 396 Russian customers whereas SWIFT had 398.[2338] SPFS acquired its first foreign customer bank in late 2018 from Belarus and in 2019 Russia negotiated with China, India, Iran and Turkey about the joint use of the system.[2339] The grandiose plans of the Russian e-government are, however, faced by the multiple challenges posed by Russia's vast territory, legacy systems, bureaucratic stove piping, and corruption. Starting from 2009–2010 the governmental systems have largely been built and probably operated by the stated owned Rostelekom. It has acquired smaller private companies as their services and products have become critical for the government networks.[2340]

The government also supports the domestic production of software to create a truly Russian information ecosystem. In 2015, the Register of Russian Software was established to control computer programs and services, which could be used by the federal and regional administration and be promoted as domestically produced products. The Register was part of an import substitution programme but also an intentional effort to create competitors to Western (and perhaps Chinese) products.[2341] Officially, the Register included by 2019 over 5,000 programs and supplied 65% of government

[2335] In principle, the situation centres might connect all the power ministries and their regional and vertical organizations. The system is supported by multiple information-analytical systems which monitor developments, conduct multifactor analyses of situations, model, forecast and plan, build scenarios, and offer support for effective and timely management. Cooper claimed that this kind of 'automated' system of monitoring and analysis could lead to economic. (Cooper 2018a).

[2336] Федеральный закон от 03.12.2011 N 382-ФЗ (ред. от 5 июля 2018) "О государственной информационной системе топливно-энергетического комплекса" [Online]. Available: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102152618 [Accessed: 17th April 2019].

[2337] Tadviser. Государственная информационная система топливно-энергетического комплекса [Online]. Available: http://www.tadviser.ru/a/248699 [Accessed: 17th April 2019].

[2338] Михеева, Анна. ЦБ снизит тарифы в своем аналоге системы SWIFT. РБК, 13 февраля 2018 [Online]. Available: https://www.rbc.ru/finances/13/02/2018/5a82f3019a79472864bb5ada?from=main [Accessed: 17th April 2019]; Чернышова, Евгения, Михеева, Анна. В российском аналоге SWIFT появился первый зарубежный участник. РБК, 22 ноября 2018 [Online]. Available: https://www.rbc.ru/finances/22/11/2018/5bf6bbd09a79476d3e8100d5?from=main [Accessed: 17th April 2019].

[2339] Reuters. Russia backs global use of its alternative SWIFT system. Reuters, March 19, 2019 [Online]. Available: https://uk.reuters.com/article/russia-banks-swift/russia-backs-global-use-of-its-alternative-swift-system-idUKL8N2163BU [Accessed: 17th April 2019].

[2340] РАЭК 2015; Ростелеком. Роль ПАО «Ростелеком» в цифровой экономике. Май, 2017 [Online]. Available: https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2017/06_Saint_ Petersburg/Presentations/ITU%20Workshop%2019.06%20-%20Alexei%20Borodin%202.pdf [Accessed: 17th May 2019].

[2341] Воейков 2018.

orders.[2342] In 2018 Rostelekom announced that it would develop a smartphone OS Sailfish for the Chinese Inoi R7 phone for secure use for public officials.[2343] Moreover, Astra Linux has been developed and approved in 2019 as a secure operating system for the federal government and other public officials.[2344]

National information security is provided by SORM (Sistema tekhnicheskikh sredstv dlia obeshpecheniia funktsii Operativno-Rozysknykh Meropriiatii), GosSOPKA and the still incomplete system centralized management of the public telecommunications network. SORM consists of multiple systems. SORM-1 was deployed during the Soviet era and captures landline and mobile phone communications. SORM-2 was deployed in 1998 and intercepts TCP/IP traffic. SORM-3 was deployed officially by Minkomsviaz' in 2015 and "collects information from all forms of communication, providing long-term storage of all information and data on subscribers, including actual recordings and locations."[2345] The FSB uses the system for targeted monitoring and intercepting data traffic in the national segment of the Internet. According to Andrei Soldatov and Irina Borogan, SORM is based on control centres that are connected directly to ISP's and telecom operators' computer servers. Control centres issue commands to intercept certain traffic, which the operators implement automatically. "This system is replicated across the country. In every Russian town, there are protected underground cables, which connect the local FSB bureau to all Internet Service Providers (ISPs) and telecoms operators in the region."[2346] SORM-3 has DPI functionality and can track traffic in all generation mobile networks.[2347] FSB requires a court order to eavesdrop on traffic but does not have to present the order to the ISPs.[2348] Soldatov and Borogan claim that Belarus, Ukraine, and Kyrgyzstan have similar systems.[2349] According to the law, the ISPs are responsible for paying for the SORM equipment and for installing it, and the two biggest manufacturers of the SORM equipment earn 5-6 billion roubles per year (the total business is around 10 billion roubles).[2350] According to some sources, Tsidatel', a company owned by the holding corporation USM of oligarch Alisher Usmanov, owns MFI SOFT, Signatek and Tekhapros Spetssistemy which together are the main producers of the SORM equipment—other companies being Norsi-trans and Orion.[2351] The SORM system has been deployed to gather data on mass events like demonstrations with blanket

[2342] РБК 2019.

[2343] Жукова, Новый & Скоробогатько 2018.

[2344] Tucker, Patrick. Russia's Would-Be Windows Replacement Gets a Security Upgrade. Defense One, May 28th, 2019 [Online]. Available: https://www.defenseone.com/technology/2019/05/russias-microsoft-knock-off-gets-security-upgrade/157310/?oref=d-skybox [Accessed: 9th July 2019].

[2345] Приказ министерства связи и массовых коммуникаций Российской Федерации от 16 апреля 2014 г. N 83 Об утверждении правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. часть iii. [Online]. Available: https://rulaws.ru/acts/Prikaz-Minkomsvyazi-Rossii-ot-16.04.2014-N-83/ [Accessed: 14th May 2019]; Susiluoto 2006, 303.

[2346] Soldatov & Borogan 2012, 25.

[2347] Приказ министерства связи и массовых коммуникаций Российской Федерации 2014.

[2348] Ibid.

[2349] Soldatov & Borogan2012, 30.

[2350] Ermoshina & Musiani 2017.

[2351] Кантышев, Павел. Партнер Усманова по киберспорту поучаствует в законе Яровой. Ведомости, 31 января 2018 [Online]. Available: https://www.vedomosti.ru/technology/articles/2018/01/31/749576-partner-usmanova [Accessed: 17th April 2019]; Ястребова, Светлана. Партнер Усманова может контролировать еще одну компанию для исполнения закона Яровой. Ведомости, 13 июля 2018 [Online]. Available: https://www.vedomosti.ru/technology/articles/2018/07/13/775384-sorm-yarovoi [Accessed: 17th April 2019].

authorization.[2352] It is somewhat unclear how SORM is connected to the data retention and localization requirements of the so-called 'Iarovaia laws', nevertheless, the FSB needs an interface to the data maintained by the ISPs.[2353] The system is developing and in 2019 Minkomsviaz' proposed to expand SORM to IoT devices and their databases and data flows.[2354] Despite the slightly mythical reputation of SORM, its implementation has been sometimes haphazard and ineffectual mainly because the telecoms companies have tried to cut costs or otherwise circumvent the regulations.[2355] The FGUP TsNIIS is responsible for analysing, monitoring and, developing the SORM system.[2356]

The GosSOPKA system has been officially described as "a unified state system for detecting and preventing computer attacks on critical information infrastructure and assessing the level of objective and real-time security of its elements which include a centralized, hierarchical, geographically distributed structure that includes the forces and means of detecting and preventing computer attacks, as well as organs of control at various levels, whose powers include the ensuring of the security of the automated control systems of the elements of the critical information infrastructure."[2357] The order for the creation of GosSOPKA and its delegation to the FSB was given by President Putin in 2013.[2358] The structure of GosSOPKA was defined in 2014[2359] and its final conceptual form was specified in the Law on Critical Information Infrastructure adopted in 2017.[2360]

GosSOPKA is basically a nation-level System of Incident and Event Management (SIEM) combined with protection systems, threat intelligence databases, and information sharing platforms designed to protect information systems, information-telecommunications systems, and ASUs designated as objects of CII by law and based on the evaluation of their importance.[2361] Although the FSB was given the authority over the GosSOPKA, the FSTEK was later given the responsibility to manage the regulation and licensing related to the CII. The roles of the FSB and FSTEK have

[2352] Freedom House. Freedom on the Net 2014 - Russia [Online]. Available: https://freedomhouse.org/sites/default/files/resources/Russia.pdf [Accessed: 17th April 2019].

[2353] Роскомсвобода. Итоги госрегулирования Рунета в 2018 году. Роскомсвобода, 28.12.2018 [Online]. Available: https://roskomsvoboda.org/44118/ [Accessed: 17th April 2019].

[2354] Роскомсвобода. Интернет вещей подключат к СОРМ. Роскомсвобода, 27.03.2019 [Online]. Available: https://roskomsvoboda.org/46080/ [Accessed: 17th April 2019].

[2355] Коломыченко, Мария, Линделл, Дада. Вне прослушки: почему Роскомнадзор и ФСБ судятся с операторами связи. РБК, 09 ноября 2017 [Online]. Available: http://www.rbc.ru/technology_and_ media/09/11/2017/5a03187e9a7947d88f988f53?from=center_1 [Accessed: 17th April 2019].

[2356] Центральный научно-исследовательский институт связи 2019.

[2357] Ibid.

[2358] Указ Президента РФ от 15 января 2013 г. № 31с "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации" [Online]. Available: http://www.garant.ru/products/ipo/prime/doc/70199068/ [Accessed: 15th May 2019].

[2359] Выписка 2014.

[2360] Федеральный закон 2017a.

[2361] Ibid. Кобцев, Роман. Подключение к ГосСОПКА. Оргвопросы. 22 марта 2018 [Online]. Available: https://infotecs.ru/webinars/archive/?show=11428 [Accessed: 18th April 2019]; Васильев, Алексей. Подключение к ГосСОПКА. Техвопросы. 3 апреля 2018 [Online]. Available: https://infotecs.ru/webinars/archive/?show=11430 [Accessed: 18th April 2019]; Дрюков, Владимир. ГосСОПКА: то, о чем обычно молчат. Задачи операционной безопасности объектов КИИ в рамках функционирования центров ГосСОПКА: то, что забывают сказать. ВПК, 05 декабря 2017 [Online]. Available: https://vpk-news.ru/ articles/40284 [Accessed: 15th May 2019].

become somewhat blurred, and thus, there has been some confusion on how CII and GosSOPKA relate to each other and who has the overall authority over them.[2362]

GosSOPKA consists of main, regional, and territorial centres that are managed by the FSB and are connected to government department centres and corporate centres of state corporations, operators of communications networks, and private companies licensing GosSOPKA equipment. Licensing is based on the responsibility to protect certified objects of CII as the Law on Critical Information Infrastructure dictates.[2363] The operators etc. are required to connect their networks to the main, regional and/or territorial centres of GosSOPKA, thus enabling the monitoring of their networks by the FSB (limited due to the available incident data). Failure to protect the CII will lead to legal consequences (up to six years in prison). GosSOPKA enables a centralized, nation-level response to cyber threats and facilitates technical information sharing with corporations, the state administration, the FSB, and the CERTs.[2364] The main centre of the system is the FSB's NKTsKI.[2365] The Solar Security and Positive technology companies will develop the departmental and state-corporation corporate centres of GosSOPKA but other private firms offer technological solutions to private actors for connecting their networks to the GosSOPKA.[2366] In March 2018 Rostelekom bought Solar Security.[2367] An equivalent to GosSOPKA might be the American Einstein E^{3}A, although the Russian system, due to its connection to the federal law, incorporates both the public and private sector and includes all strategic sectors of the economy, and is mandatory in its approach.[2368] Thus the borders between the public and private sectors are hazy and indirect state ownership and control of the whole system is much wider than it would seem at the first glance.

The system for the centralized management of the public telecommunications network is still under development. It will be controlled from the Centre of Monitoring and Managing of the Public Communication Networks (TsMUSSOP) by the Radio Frequency Service. ISPs are required to install certain equipment into their networks which can monitor and filter traffic and if needed completely block it. This would, in

[2362] Федеральный закон 2017a; Приказ Федеральной службы по техническому и экспортному контролю 2017; Указ Президента РФ от 22 декабря 2017 г. № 620 "О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации" [Online]. Available: https://www.garant.ru/products/ ipo/prime/doc/ 71740924/ [Accessed: 18th April 2019]; ГосСОПКА. В 2019 году планируется уточнение нормативной базы в области кии, в том числе. 16.01.2019 [Online]. Available: http://gossopka.ru/ 2019/01/16 /в-2019-году-планируется-уточнение-нормат/ [Accessed: 18th April 2019].

[2363] Постановление Правительства Российской Федерации 2018a.

[2364] Григорьев 2017; Кобцев 2018; Васильев 2018; Positive Technologies. Построение центра ГосСОПКА — краткое описание решения [Online]. Available: https://www.ptsecurity.com/upload/corporate/ru-ru/solutions/center-gossopka/PT-GosSOPKA-PB-rus.pdf [Accessed: 18th April 2019]; Торбенко, Елена. Практика категорирования объектов КИИ. SOC форум 27 ноября 2019 [Online]. Available: https://soc-forum.ib-bank.ru/files/files/SOC%202018/05_Torbenko.pdf [Accessed: 18th April 2019]; Грачёв 2019.

[2365] Приказ ФСБ 2018; Agentura.ru. 2018.

[2366] One of these is the firm Infotecs whose solution is composed of ViPNet family of products (Жукова 2017.)

[2367] Ведомости. "Ростелеком" купил компанию в сфере кибербезопасности за 1,5 млрд рублей. Ведомости, 22 мая 2018 [Online]. Available: https://www.vedomosti.ru/business/news/2018/05/22/ 770293-rostelekom [Accessed: 18th April 2019].

[2368] The United States Department of Homeland Defence. Privacy Impact Assessment for EINSTEIN 3 - Accelerated (E3A) April 19, 2013 DHS/PIA/NPPD-027 [Online]. Available: https://www.dhs.gov/sites/ default/files/publications/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed-%20508%20compliant.pdf [Accessed: 18th April 2019].

theory, disconnect the Russian segment of Internet from the global Internet. In addition to protecting the segment from outside attacks it will be used to centrally implement and enforce the blacklist maintained by the Roskomnadzor.[2369]

Foreign and international LEO massive satellite constellations threaten all the controlling systems the Russian regime has been developing. In 2019 it seemed that the Russian regime was prepared to sponsor its own constellation. From the perspective of digital sovereignty, the location of satellite ground stations is more important than the orbits of the satellites and this will be a challenging issue to resolve in the future. Perhaps an even more pressing issue is that the constellations of LEO satellites may be used for military purposes.[2370] In addition to satellites, SORM, GosSOPKA, TsMUSSOP and other similar systems will have problems with technologies like 5G, LPWANs, an IoT where systems connect and communicate autonomously—which just shows that the ability to control and shape cyberspace is always tempered by technology.

The systems described in this chapter demonstrate that the strategic cultural ideas of unified information space, information-technological warfare, and automated command and control systems resonate with the concrete ways in which the Russian elites strive to shape cyberspace and control the national segment. Kibernetik ideas provide reason to construct centralized, vertically controlled, and horizontally integrated system of systems. Information is collected and forwarded to the centre and decisions are transmitted down to the subsystems. As such there is nothing particularly 'Russian' in the technological systems themselves—it is the scope and the state-centric political, social and economic agenda which defines these systems and gives them purpose.

6.4.2 The Military

The concrete policies, procurement, and construction concerning military information networks and systems are largely secret. However, some information can be gained from public sources. The only official public conceptual document on cyber and information warfare produced by the military is titled: Conceptual Views on the Activities of the Ministry of Defence of the Russian Federation in the Information Space and was released in late 2011.[2371] Arguably, the document may not genuinely

[2369] Минкомсвязь. Об утверждении Порядка централизованного управления сетью связи общего пользования [Проект] 23 мая 2019 г. [Online]. Available: https://regulation.gov.ru/projects#npa=91558 [Accessed: 15th May 2019]; Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31.07.2019 № 225 "Об утверждении Положения о Центре мониторинга и управления сетью связи общего пользования" [Online]. Available: http://publication.pravo.gov.ru/Document/View/0001201911250011 [Accessed: 7th January 2020].

[2370] del Portillo, Inigo, Barrios, Cameron, Bruce, Crawley, Edward. Ground segment architectures for large LEO constellations with feeder links in EHF-bands. 2018 IEEE Aerospace Conference [Online]. Available: https://www.researchgate.net/publication/326072504_Ground_segment_architectures_for_large_LEO_constellations_with_feeder_links_in_EHF-bands [Accessed: 17th May 2019]; Erwin, Sandra. Air Force laying groundwork for future military use of commercial megaconstellations. SpaceNews, February 28, 2019 [Online]. Available: https://spacenews.com/air-force-laying-groundwork-for-future-military-use-of-commercial-megaconstellations/ [Accessed: 17th May 2019]; Роскомсвобода. Спутниковый трафик под надзором ФСБ. Роскомсвобода, 26.2.2019 [Online]. Available: https://roskomsvoboda.org/45251/ [Accessed: 17th May 2019].

[2371] Министерство обороны Российской Федерации 2011.

reflect the views of the MoD or the Armed Forces as it is related to Russia's international efforts to ban or restrict the use of information weapons.[2372] The document adopts the language and terms of information space (prostranstvo), information weapons (oruzhie) and information war (voina). It associates the military aspects of information issues to the use of information weapons and defines information war as: "A confrontation between two or more states in the information space in order to damage information systems, processes and resources, critical and other structures, undermine the political, economic and social systems, to massively psychologically affect the population to destabilize the society and the state, as well as forcing the state to decisions in the interests of the opposing side"[2373] The document defines the activities of the Armed Forces in the information space to consist of intelligence, maskirovka (deception), electronic warfare, communications, covert and automated command and control, as well as the protection of Russia's own information systems from electronic, computer and other attacks.[2374] The activities of the Armed Forces are part deterrence and prevention of conflicts as well as the resolution of conflicts. These tasks have an active information-psychological aspect on the part of the Armed forces.[2375] Despite its 'diplomatic' approach, the Conceptual View succeeds to resonate with all the strategic cultural ideas, with the exclusion of asymmetric response.

The Conceptual Views document is in line with the current strategic planning documents.[2376] Perhaps the most important aspect of all of these documents is that they recognize a distinct sphere of military information warfare, i.e. the military-political use of ICT—although with fuzzy borders because of the increased emphasis on intragovernmental cooperation, the whole-of-government approach, and mobilization issues. The distinct EIP of the military mentioned by multiple sources forms conceptual borders for the military's authority and responsibilities—it is a special network or a collection of them recognized by Russian law. Nevertheless, as was argued in Chapter 6.2.1 the mandate of the FSB and the FSTEK also reach into military networks. The MoD has influence outside its own information infrastructure. It has, for example, blocked the opening of some frequency bands to 5G networks.[2377] It has also strived to regulate the use of mobile phones and social media of the conscripts and the military staff to maintain operational security.[2378]

The drive to create an NCW capable force which was noted in Chapter 5 has affected the organization of the Armed Forces and EW troops were established in 2009.[2379]

[2372] Cf. Eneken 2016; Eneken & Kerttunen 2017.

[2373] Ibid., 5. This definition corresponds to the one Russia has been promoting in the UN and is the same as the one offered in the SCO Agreement on Information Security (Костюхин А.А. и др. Словарь терминов и определений в области информационной безопасности. Москва: ГШ ВС РФ, 2008, 255 ft. 117; ШОС 2009)

[2374] Ibid., 8.

[2375] Ibid., 10-13.

[2376] Cf. Chapter 5.

[2377] Кодачигов 2019.

[2378] ТАСС. Госдума запретила военным пользоваться смартфонами на службе. ТАСС, 19 февраля 2019 [Online]. Available: https://tass.ru/obschestvo/6132986?... [Accessed: 18th May 2019].

[2379] Известия. В российской армии будут созданы войска РЭБ, 17 апреля 2009 [Online]. Available: https://iz.ru/news/449161 [Accessed: 9th March 2019].

The drive towards jointness, integration, and synergy led to the creation of the Aerospace Defence Forces in 2011[2380] and then the Aerospace Forces in 2015.[2381] Furthermore, as Professor and Retired Lieutenant General V. V. Barbinenko argued in 2015, these new organizations also required networks, ASUs, and technological support to operate in accordance with the principles of the NCW.[2382] Thus, already by 2011 the Russian Ground forces allegedly had two ASUVs in experimental use: ESU TZ on a tactical level and Akatsiia-M on an operative-strategic level. Airborne troops developed Andromeda-D. Furthermore, there were branch-based systems like the air defence force's Poliana-D4 and Barnaul-T. Many of these systems, however, were not compatible with each other.[2383] The progress in the development of ASUs has been slower than was hoped for but they remain a high priority for the Armed Forces.[2384] According to General Gerasimov, the long-waited ESU TZ was being distributed to the forces in 2018.[2385] Moreover, in 2019 a new army (operational) level ASUV based on Akatsiia was allegedly deployed which doubled the speed of 'the cycle of command' and integrated all branches and command levels in accordance with the principles of the NCW.[2386]

On a more strategic level 'the military Internet', i.e. 'closed data segment' (Zakrytii segment peredachi dannykh) was declared operational in 2016.[2387] Its infrastructure is partly leased from Rostelekom and partly based on the infrastructure of the MoD. Military units have their own servers and routers which encrypt information and transmit it using packet-based protocols. The network is air-gapped from the Internet and hosts are special workstations certified and controlled by the MoD. The use of flash drives is restricted. The 'military Internet' has its own second and third level DNS domains (domain.mil.zs).[2388] It is possible that the operating system, at least on

[2380] РИА Новости. Войска Воздушно-космической обороны заступают на боевое дежурство в РФ, 1 декабря 2011 [Online]. Available: https://ria.ru/20111201/503030677.html [Accessed: 9th March 2019].

[2381] Интерфакс. Воздушно-космические силы РФ приступили к службе, 3 августа 2015 [Online]. Available: https://www.interfax.ru/russia/457604 [Accessed: 9th March 2019].

[2382] Барвиненко, Владимир. Война на опережение — часть I. Как противостоять сетецентрическим действиям противника. ВПК, № 24 (590) за 1 июля 2015 года; Барвиненко, Владимир. Война на опережение — часть II Как противостоять сетецентрическим действиям противника. ВПК, № 25 (591) за 8 июля 2015 года.

[2383] Богданов, Константин. Всю систему менять надо. ВПК, № 16 (382) за 27 апреля 2011 года.

[2384] Костюкевич, Н.Е. Предложения по изменению подходов к созданию (модернизации) систем и комплексов средств автоматизации управления военного назначения. Вестник академии военных наук, № 1 (54) 2016; Фаличев, Олег. Закодированы на отставаниею Проблемы отечественной микроэлектроники приходится решать с помощью «Шилки»ю ВПК, № 41 (754) за 23 октября 2018 года; Гареев 2015b; Рамм, Алексей, Козаченко, Алексей, Степовой, Богдан Код в сапогах: военные разработали боевой антивирус. Известия, 31 октября 2019 [Online]. Available: https://iz.ru/937787/aleksei-ramm-aleksei-kozachenko-bogdan-stepovoi/kod-v-sapogakh-voennye-razrabotali-boevoi-antivirus [Accessed: 7th January 2020].

[2385] Герасимов, В.В. Влияние современного характера вооруженной борьбы на направленность строительства и развития Вооруженных сил Российской Федерации. Приоритетные задачи военной науки в обеспечении обороны страны. Вестник академии военных наук, № 2 (63) 2018, 16-22.

[2386] Рамм, Алексей, Козаченко, Алексей. Командир на автопилоте: управлять армиями поможет компьютер. В Санкт-Петербурге открывается «Штаб звездных войн». Известия, 5 июня 2019 [Online]. Available: https://iz.ru/884970/aleksei-ramm-aleksei-kozachenko/komandir-na-avtopilote-upravliat-armiiami-pomozhet-kompiuter [Accessed: 9th July 2019].

[2387] Зыков, & Рамм 2016a.

[2388] Ibid.

a tactical level, is Astra Linux and some of the hardware is based on Russian components manufactured by Voentelekom.[2389] The main provider of communications and control systems to the Armed Forces is the United Instrument Manufacturing Corporation (under state corporation Rostek) which includes, for example, the TSNII EISU.[2390]

The infrastructure of 'the military Internet' most probably refers to the 'Integrated Automated Digital Communication System' or OATsSS which was discussed in Chapter 5. It is characterized as an integrated system of communications for military purposes. According to sources, it ensures the resilience, continuity, operationality and secrecy of the operations of joint forces. It provides the Armed forces and the MoD with information-telecommunications services on a global scale under any adverse conditions. Additionally, it ensures the security, reliability and integrity of the information circulating in the system during its transmitting, storage and processing.[2391] In 2014 the system was characterised by Colonel General Khalil Arslanov, the Chief of the Main Directorate of Communications of the GS, to be composed of digital satellite, radio, radio-relay, tropospheric and optical communications systems. It was based on standardized and secure solutions. The role of domestic components was highlighted.[2392] Arslanov repeated his characterization word-to-word in 2018.[2393] Civilian academicians Likhachev, A. Abramovich and A. Prisiazhniuk wrote a paper in 2016 proposing a conceptual solution for the automated control system (ASU) of OATsSS.[2394] It would control OATsSS' technical parameters, manage its stability and security and offer information-analytical services during different phases of conflict. The authors argued that the system should be based on the principles of centralization and specialization of management, unification, constant monitoring and direct control. The ASU OATsSS would be a system of systems, and different systems could be further divided into subsystems, some of which could be regionally distributed, for example, on the basis of military districts.[2395] In 2018 the OATsSS was characterized by its developers as a communications system that would unite all functions, echelons, i.e. domains (air, sea, land, space), and commands of the Armed Forces under a unified information-telecommunications space. It would have a unitary management and its structure would be flexible.[2396] According to the representatives of Voentelekom, the fixed component of the OATsSS was envisioned as quite similar to other modern WANs where the data traffic of the Armed Forces was virtually routed over leased

[2389] Зыков & Рамм 2016b; ЗВЕЗДА. Военный Интернет: как работают закрытые технологии министерства обороны. ЗВЕЗДА, 9 априль 2017 [Online]. Available: https://tvzvezda.ru/news/vstrane_ i_mire/content/201704091018-4ygi.htm [Accessed: 18th April 2019]; Tucker 2019.

[2390] Рамм 2014.

[2391] Мейчик, Евгений Робертович. Перспективы развития системы связи и автоматизированных систем управления вооруженных сил. Российской Федерациию Федеральный справочник. Оборонно-промышленный комплекс России, Том № 3, 2009, 379-384 [Online]. Available: http://federalbook.ru/files/OPK/Soderjanie/OPK-6/III/meychik.pdf [Accessed: 6th March 2019].

[2392] Арсланов2014.

[2393] Арсланов, Халил. На острие технического прогресса. Красная звезда, 19 октября 2018 [Online]. Available: http://redstar.ru/na-ostrie-tehnicheskogo-progressa/ [Accessed: 6th March 2019].

[2394] Лихачев, А. М., Абрамович, А. В., Присяжнюк, А. С. Концептуальные основы создания и развития автоматизированной системы управления ОАЦСС ВС РФ. Информация и космос, №2 (2016), 6-21.

[2395] Ibid.

[2396] Элькин, Г. И., Казанский, А. Г. Перспективы развития системы связи Вооружённых Сил Российской Федерации. Итоги деятельности Совета главных конструкторов системы связи ВС РФ. Связь в Вооруженных Силах Российской Федерации 2018. Москва: Информационный мост 2018, 28-29.

information-telecommunications infrastructure to nodes controlled by the Armed Forces.[2397]

When fully developed, the OATsSS should provide automated command and control of communications for the Russian Armed forces in space, air, ground, and sea environments. It interconnects all military command posts from the battalion level up to the NDMC and is based on standardized digital technology. Its core is a fixed encrypted packet-routing based backbone network probably partially built upon the leased transport networks of state and private ISPs. The core networks are connected to military field networks and other special communication networks. Military districts are very likely the administrative organizations of this network.[2398] The network is probably protected by a system developed specifically for the MoD.[2399] Some of the main developers based on articles written about the OATsSS are the 16th TSNII, Voentelekom and NII Rubin. OATsSS should provide centralized command and control of forces from the MoD through the military districts down to the formation level, and the decentralized control of networks if needed. It is part of the effort of the Russian armed forces to homogenize the communications and command and control systems of armed forces.

In addition to leased capacity, the communications infrastructure of the Armed Forces is based on optic fibre, satellite, and microwave relay networks operated by the MoD. By 2017 the T8 corporation claims to have laid 67,000 km of fibre optic cable, of which 15,000 km is based on the 100 Gbit/s DWDM system "Volga", although it is unclear how much of this is dedicated to the Armed Forces.[2400] The Armed Forces plan to lay 24,000 km of optic cable as part of GPV 2018-2024.[2401] The MoD is also constructing its own network of data centres called the Territorial Disaster-Resistant Data Centres (TrKTsOD) which should offer secure cloud services for the Armed Forces. The services of 'the military Internet' will be transferred to the TrKTsOD when it becomes operational in 2020.[2402] It seems that the above mentioned physical and logical solutions are to be combined in a multiservice transport network (MTSS) which will be operational in 2021. The MoD claims that the system will be detached from the Internet traffic exchange points and will have dedicated

[2397] Сухотеплый, А. П., Жилков, Е. А. Цифровая экономика. Цель номер один — технологический и цифровой суверенитет. Связь в Вооруженных Силах Российской Федерации 2018. Москва: Информационный мост 2018, 112-114. Also, Харченко, Сазыкин & Лысенков 2017.

[2398] Мейчик 2009; Арсланов 2014; Лихачев, Абрамович & Присяжнюк 2016; Элькин & Казанский 2018; Сухотеплый & Жилков 2018; Харченко, Сазыкин & Лысенков 2018; Арсланов, Халил, Лихачев, Александр. Актуальные научно-практические проблемы развития ОАЦСС ВС РФ. Связь в Вооруженных Силах Российской Федерации 2015. Москва: Информационный мост 2015, 29-36.

[2399] ТАСС. Система защиты Минобороны РФ от кибератак завершила тестовые испытания и будет расширена. ТАСС, 24 октября 2016 [Online]. Available: https://tass.ru/armiya-i-opk/3728399 [Accessed: 18th April 2019].

[2400] Слепцов, Михаил. DWDM-системы связи для Вооружённых сил РФ. Связь в Вооруженных Силах Российской Федерации 2017. Москва: Информационный мост 2017, 124.

[2401] Независимое военное обозрение. Тыл становится передним краем Минобороны. В структуре несекретной части расходов социальная часть потеснила военную. Независимое военное обозрение, № 16 (947) 2017.

[2402] Масленников, Олег. Территориальнораспределенный катастрофо-устойчивый центр обработки данных Вооружённых Сил Российской Федерации. Связь в Вооруженных Силах Российской Федерации – 2018. Москва: Информационный мост 2018, 30-31; Круглов, Рамм & Степовой 2018; Бец, Киселенко, Орлов 2017.

physical lines of communication—including a new Arctic cable—which will be divided into zonal communication channels.[2403] Based on the articles published in scientific and professional journals, the backbone and access networks of the Russian OATsSS or MTSS are based on NGN IP/MPLS technology.[2404] Moreover, by using field communications the core network can be expanded to other regions of the globe to support Russian expeditionary operations.[2405] This claim rests on signal units with satellite communication capabilities and a network of high-bandwidth communication satellites.

Communication satellites are necessary for military communications because the Russian geography restricts the operability of nationwide fibre connections. The Russian military operates its own satellite fleet which consists of at least thirty 'store-and-dumb' communication satellites and approximately twenty-seven GLONASS -navigation satellites. The Armed Forces probably also use commercial SATCOM satellites.[2406] There are also a couple of nuclear strike early warning satellites.[2407] The Russian military also uses terrestrial radio relay links on HF/UHF/SHF frequencies which provide varied data transmission capacity.[2408] Because of the multiplicity of systems and the continued use of legacy systems, the Armed Force's communications may not be as efficient as Russian commercial systems, but there is, however, a clear interest in maintaining a distinct, redundant, and resilient military data network.

The OATsSS/MTSS enables the functioning of the National Defence Management Centre.[2409] The Centre analyses the situation in strategic directions and problematic regions and offers short-term prognoses; it coordinates the activities of federal organs on the operational level in matters of national defence; and it enables the day-to-day management of the Armed Forces and their operational command and control including the strategic nuclear forces.[2410] To enable these functions, subordinate centres

[2403] Рамм, Алексей, Козаченко, Алексей, Степовой, Богдан. Военный, красивый, суверенный: армия РФ создает закрытый интернет. Вся важная информация будет храниться только на серверах Минобороны. Известия, 12 марта 2019 [Online]. Available: https://iz.ru/854961/aleksei-ramm-aleksei-kozachenko-bogdan-stepovoi/voennyi-krasivyi-suverennyi-armiia-rf-sozdaet-zakrytyi-internet [Accessed: 18th April 2019]; Рябов 2019.

[2404] Легков 2013; Будко, Чихачев, Баринов & Винограденко 2013; Легков К.Е. Организация и модели функционирования современных инфокоммуникационных сетей специального назначения. T-Comm Vol.9. #8-2015, 14-19.

[2405] Валагин, Антон. Россия испытала в Сирии высокоскоростной военный интернет. RG.RU, 7 апреля 2016 [Online]. Available: https://rg.ru/2016/04/07/rossiia-ispytala-v-sirii-vysoskorostnoj-voennyj-internet.html [Accessed: 3rd May 2019].

[2406] Union of Concerned Scientists, "UCS Satellite Database," 2017. [Online]. Available: http://www.ucsusa.org/nuclear-weapons/spaceweapons/satellite-database#.Wg0WlUpl9PY. [Accessed 16 November 2017]; Владыкин, Олег. Интернет доступен на российских кораблях. Система действует на девяти судах. Независимое военное обозрение № 23 (954) 2017.

[2407] Мясников Виктор. Единая космическая система предупредит о ядерном нападении. Независимое военное обозрение, № 37 (826) 2014 [Online]. Available: http://nvo.ng.ru/nvo/2014-10-17/1_shojgu.html [Accessed: 18th April 2019].

[2408] Малюков, Вадим. Современным войскам — современную связь. Связь в Вооруженных Силах Российской Федерации 2013. Москва: Информационный мост 2013, 14-16.

[2409] Арсланов & Лихачев 2015; Гаврилов, Юрий. Глава Генштаба объяснил, как будет работать Центр управления обороной. Российская газета, 1.11.2014 [Online]. Available: https://rg.ru/2014/11/01/center-site.html [Accessed: 18th April 2019].

[2410] Monaghan 2017, 71; Владыкин, Олег. Путин: Российская армия должна быть оснащена лучше зарубежных. Независимая газета, 20 декабря 2014 [Online]. Available: http://www.ng.ru/armies/2014-12-20/100_collegium.html [Accessed: 6th March 2019].

of command, control and management were being created on strategic, the operational and tactical level and in services and branches in the timeframe of 2015–2018.[2411] The Centre is supported by an ASU of national defence, the functions of which would be duplicated in the regional level data centres. The Centre is also connected to the military-industrial complex and monitors the fulfilment of weapons procurement.[2412] It physically brings together all Russian security agencies and ministries and collects information from various secret and public sources to create a common national situation picture.[2413] In 2019 Defence Minister Sergei Shoigu stated that Centres for the Coordination of Security Agencies in Crisis Situations would be established in all federal regions and these would connect local (municipal) administration to the MoD and the Armed Forces.[2414]

It is probable that the 'military Internet' and most of the networks used by the NDMC are physically and/or logically distinct from the communication networks used by the strategic nuclear forces for obvious security reasons.[2415] Additionally, there are other branch and service specific networks that require special gateways for connecting to 'unified information space'.[2416] There is also a 'unified cosmic system' (Edinaia Kosmicheskaia Sistema), which refers to the ballistic missile early warning system which is a network of satellites, long-range radars, and command and control centres.[2417] Additionally, the CIS has a partly completed project to create a common air defence network.[2418] Moreover, the CSTO has adopted a resolution to enhance common information (technological and psychological) security.[2419] Because there is a theoretical threat of penetration of Russian military networks through these allied systems, the connections are highly probably implemented through controlled gateways—or they are possibly even air-gapped. On the cross-sectoral side, Voentelekom has been constructing a separated closed network for the needs of the OPK called 'System of Protected Communications' (SZS). This should combine the OPK with ministries, agencies, and armed forces during peacetime and in crises situations and can be accessed

[2411] Тихонов, Александр. К единому информационному пространству. Красная звезда № 173 (2015); Хомутов 2015, 17-22.

[2412] Владыкин 2014.

[2413] Тихонов, Александр. К единому информационному пространству. Красная звезда № 173 (2015).

[2414] Сидоркова, Инна, Дергачев, Владимир, Антонова, Елизавета. В регионах появятся центры на случай военного положения. РБК, 09 апруля 2019 [Online]. Available: https://www.rbc.ru/politics/09/04/2019/5caca4919a79475d5519d425?from=center [Accessed: 18th April 2019].

[2415] The National Defence Management Centre combines and centralizes the governmental and military command under the General Staff already during peace time to provide unified strategic leadership for national defence, strategic nuclear weapons, and joint strategic military formations (OSK/military districts) based on resilient and effective command and control communications and also allows the independent action of military formations. The system was based on the lessons learned during the Great Patriotic War and on the analysis of the U.S. 'instant global strike' doctrine. (Герасимов 2015). These command and control networks of early-warning and ballistic missile defence and strategic nuclear weapons are in principle vulnerable to cyber-attacks. On nuclear forces command and control networks cf. Cimbala 2015; Acton, James M. Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War. International Security, Vol. 43, No. 1 (Summer 2018), 56-99.

[2416] Ланчев, Василий. АСУ ВКО: модель для сборки. Учебные командные пункты должны лечь в основу подготовки специалистов ВКО. ВПК, № 39 (605) 14 –20 октября 2015 года.

[2417] Мясников 2014; Соколов, Анатолий. Новый космический щит России. Русская Планета, 18 ноября 2015 [Online]. Available: http://rusplt.ru/society/novyiy-kosmicheskiy-schit-rossii-19771.html [Accessed: 5th March 2019].

[2418] Plopsky, G. Russia's Big Plans for Air Defense in Eurasia: Big plans, indeed, but will they materialize? The Diplomat (2017, Apr, 7). [Online]. Available: https://thediplomat.com/2017/04/russias-big-plans-for-air-defensein-eurasia/. [Accessed 11 January 2018].

[2419] Рябухина, Бондуровского, & Перекопского 2014.

only by using special equipment.[2420] This kind of arrangement should, in principle, ensure the horizontal and vertical integration of all elements of the mobilization system that some military scientists have called for.[2421] Currently, the Russian Armed Forces operates an ASU of Mobilization Deployment the component systems of which have reached operational status gradually during 2008–2017.[2422] Compared to the United States armed forces' concept[2423] of the 'military Internet' the clear difference with the Russian version is that the Russian approach is more rooted in the idea of total and territorial defence in which all state security organizations are connected by the same command, control and communications systems.

The Russian military cyber actors have been and still are an 'open secret'. It is quite difficult to find information about them in open sources but based on the strategic cultural ideas analysed in Chapter 5, it is inconceivable (reasonable) that the Russian military would not have a dedicated cyber force for espionage, sabotage, and subversion and deterrence. In 2014 an anonymous source stated that the MoD had created information operation forces to defend its own networks from cyber-attacks.[2424] In 2017 Defence Minister Shoigu declared that information troops had been created, although their tasks were characterised more as strategic communications than cyber warfare.[2425] Moreover, there are at least five science companies, the 4th, 7th, 6th, 9th, 11th out of sixteen established between 2013–2018 which conduct research and train cyber security specialists for the Armed Forces.[2426] Then there are the proper scientific-technological institutions under the MoD like 16th, 18th and 27th TsNII.[2427] It is also quite possible that EW Troops have an operational-tactical role in cyber warfare.[2428] Information warfare forces have taken part in operational-strategic exercises since 2016.[2429]

[2420] Зыков & Рамм 2016; Воентелеком. Глава "Воентелекома": технология блокчейн может появиться в армии России. Воентелеком, 22.08.2017 [Online]. Available: https://voentelecom.ru/news/novosti-kompanii/glava-voentelekoma-tekhnologiya-blokcheyn-mozhet-poyavitsya-v-armii-rossii/ [Accessed: 18th April 2019].

[2421] Легков, К.Е. Основные теоретические и прикладные проблемы технической основы системы управления специального назначения и основные направления создания инфокоммуникационной системы специального назначения. T-Comm #6 2013, 42-46; Будко П.А., Чихачев А.В., Баринов М.А., Винограденко А.М. Принципы организации и планирования сильносвязной телекоммуникационной среды сил специального назначения. T-Comm #6 2013, 8-12.

[2422] Ермаков, А. А., Ткачук, А. В., Мишенев, А. М. Опыт создания единой автоматизированной системы управления мобилизационным развертыванием Вооруженных Сил Российской Федерации. Военная мысль № 7 2019, 77-80.

[2423] Joint Staff J6. The Global Information Grid (GIG) 2.0 Concept of Operations Version 1.1, 11 March 2009 [Online]. Available: https://info.publicintelligence.net/DoD-GIG2-CONOPS.pdf [Accessed: 7th January 2020].

[2424] ТАСС. Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций. ТАСС, 12 мая 2014 [Online]. Available: https:/tass.ru/politika/1179830 [Accessed: 18th May 2019].

[2425] Независимое военное обозрение 2017.

[2426] Thomas 2015; ТАСС. Минобороны РФ: научные роты пополнили 300 призывников по итогам осенней кампании 2018 года. ТАСС, 12 декабря 2018 [Online]. Available: https://tass.ru/armiya-i-opk/5902450 [Accessed: 18th May 2019]; Boltenkov, Dmitry. Russian MoD's "Science Companies". Moscow Defense Brief, No. 6 (2017), 10-12.

[2427] Cf. Chapter 5 footnotes of descriptions.

[2428] McDermott2017; Kjellén 2019.

[2429] In 2016 General Gerasimov stated that IW had been part of the Kavkaz-2016 strategic command and staff exercise. It had been conducted by an Information Warfare Group and its tasks had been akin to fire missions. The group consisted of the elements of the Operational Directorate of the GS and its subunits, i.e. centres of information warfare that had been created under military districts, and of the forces of information operations, forces and means of EW, and units of the State Secrets Protection Service ТАСС. Военные РФ впервые отработали информационное противоборство на учениях "Кавказ". ТАСС, 14 сентября 2016 [Online]. Available: https://tass.ru/armiya-i-opk/3619816 [Accessed: 12 June 2019].

Based on Western reports, the Main Directorate of the General Staff or GRU is mostly responsible for active military-strategic level espionage, sabotage, and subversion operations during peacetime—although it is not the only active Russian offensive cyber actor.[2430] The Russian cyber security company Zekurion Analytics claimed in 2017 that Russia had the world's fifth largest cyber force with 1,000 operators and a budget of 300$ million.[2431]

Despite of the declarations about the operability of OATsSS and MTSS, it is safe to argue that the Russian military networks remain fragmented in 2019, perhaps excluding some dedicated vertical lines of command. However, the desired end-state is horizontal and vertical integration across the AF according to the principles of NCW.[2432] The development of military networks and command and control systems remains a priority in the context of GPV 2018–2027.[2433] The idea of information superiority achieved through the unified information space, information-technological means, and ASUs resonates strongly with the Russian military approach to cyber and information warfare. The military EIP is a prerequisite for national defence and security and, thus, to sovereignty. Nevertheless, the military also sees the information-psychological aspect of warfare as at least as important as the technological aspects and fully supports the patriotism and militarism promoted by the regime and is itself an active participant in shaping the wider information space of Russia.[2434] For the military, the technological and psychological aspects of information warfare are part both part of strategic deterrence. An asymmetric response is present in the ever-continuing information weapon–counter-weapon struggle. The problem is how to keep this process in the framework of a cost-effective and innovative (cunning) track, and not to fall into the trap of C4ISR procurement bureaucracy.

6.5 The system of systems of information security and defence

In this chapter I will draw on the previous Chapters and present a model of the Russian national segment of the Internet as a system of systems of information security and defence in a continuum of interstate relations and in the context of military threats to understand how a closed national network could function. It was argued in Chapter

[2430] The U.S. Department of Homeland Security. Enhanced Analysis of GRIZZLY STEPPE Activity. Reference Number: AR-17-20045 February 10, 2017 [Online]. Available: https://assets.documentcloud.org/ documents/3469157/Document-12-National-Cybersecurity-and.pdf [Accessed: 18th May 2019]; National Cyber Security Centre. Reckless campaign of cyber-attacks by Russian military intelligence service exposed. October 3rd, 2018 [Online]. Available: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed [18th May 2019].

[2431] Коломыченко, Мария. В интернет ввели кибервойска. Аналитики оценили количество хакеров на госслужбе. Коммерсантъ, №2 от 10.01.2017 [Online]. Available: https://www.kommersant.ru/doc/ 3187320?utm_source=kommersant&utm_medium=tech&utm_campaign=four [Accessed: 18th May 2019].

[2432] McDermott, Roger. Russia's Network-Centric Warfare Capability: Tried and Tested in Syria. Eurasia Daily Monitor Volume: 15 Issue: 154 [Online]. Available: https://jamestown.org/program/russias-network-centric-warfare-capability-tried-and-tested-in-syria/ [Accessed: 18 April 2019].

[2433] Connolly & Boulégue 2018; Герасимов, В. В. О ходе выполнения указов Президента Российской Федерации от 7 мая 2012 года N603, 604 и развития Вооруженных Сил Российской Федерации. Военная мысль, № 12 (2017), 7-21.

[2434] Golts 2018; Сафронов, Иван, Джорджевич, Александра. На главном политическом направлении. Генерал Андрей Картаполов возглавит новый главк Минобороны. Коммерсантъ №134 от 31.07.2018 [Online]. Available: https://www.kommersant.ru/doc/3701013 [Accessed: 18th May 2019]; ТАСС. Юнармия России: для чего возродилось всероссийское военно-патриотическое движение. ТАСС, 22 февраля 2018 [Online]. Available: 18th May 2019].

3.5 that the military strategic reasoning behind the shaping and controlling of the Russian national segment of the Internet is that it can provide a decisive advantage. A closed national network, that is a disconnected but internally functioning national segment, might even provide an asymmetrical advantage in relation to nations leaving their networks open. In this Chapter I propose one approach to understanding how the Russian national network could function in practice as a closed national network. The approach is based on an abductive interpretation of Russian strategic cultural ideas examined in Chapter 4 and 5 and the theories on cyberspace and the closed national segment presented in Chapters 3.[2435]

It was previously argued that cyberspace can be understood as a digital territory consisting of functional, normative, and political elements which can be shaped by technology, governance, norms, and politics. Digital territory can be mapped on a case-by-case basis. In this case I choose to map the Russian national segment as a system of systems. This approach resonates with the ideas proposed by Russian information warfare scholars who envision the unified information space as a system or a system of systems, information warfare as a struggle between systems, and the control of that struggle as the function of a national system of information command, control and management.[2436] This system of systems is composed of subsystems which are not exclusively technological. They should be understood more as political, governance, normative, organizational, economic, technological, and security and military entities. These subsystems have been created based on the influence of the strategic cultural ideas implemented through strategies and government policies to create a national segment of the Internet.

The most influential idea is the idea of a national, unified information space controlled through a system of systems of command, control and management. This EIP is based on vertical control and horizontal integration, centralization, the delimitation of borders and technological and scientific self-sufficiency. The result is a delineated, technologically independent, and functionally self-sufficient national segment. Moreover, the idea of information struggle necessitates the ability to control one's own information space or system while simultaneously influencing the opponent's space or system. As information has become a part of strategic deterrence there is also a military strategic logic to denying an adversary's freedom of action, to deny its objectives through resilient networks, and to threaten it with retaliation from behind "unbreakable" walls. The system's theoretical rationality to create such a construct is that to protect one's own system and to deny the information superiority of an opponent one can move away from the threat, remove the source of threat, control information channels including setting barriers, control information itself, and engage in self-modification. Because the first two are not possible to achieve in the short or medium term, the last three provide strategic solutions.

[2435] Most specifically Kukkola, Nikkarila & Ristolainen 2017; Kukkola 2017a & 2018b. The model of system of systems was first proposed in Kukkola 2018c.

[2436] These scholars include, for example, E. A. Derbin, S. A. Komov, E. G. Shalamberidze, D. Chereskin, G. Smolian, V. Tsygichko, I. Sheremet, A. Ia Cherysh, V. V. Popov, A. A. Sidak, V. V. Tsyganov, Iu. G. Bochkareva, V. K. Novikov, S. I. Makarenko, Kh. I. Saifetdinov, V. Kruglov, V. V. Tsyganov, S. N. Bukharin, A. V. Manoilo, S. P. Rastorguev, and Igor Panarin.

The national segment of the Internet could be examined though many different approaches. It could be considered as a part of larger cyberspace and thus its effects on this space could be analysed. The subject of analysis could be the alleged asymmetry created by a closed national network. The segment could be approached as an economic or a cultural system and the analysis could concentrate on the building of technological independence or cultural identity. Moreover, it could be approached as the basis of information and digital sovereignty and thus political processes would be at the heart of the analysis. I choose to approach the Russian national segment through a military strategic framework which consists of multiple elements. Firstly, it includes the continuum of interstate relations as understood by the Russians. Secondly, different national and military security threats and the Russian understanding of them are included. Thirdly, a systems thinking approach to information security in applied. Fourthly, the integrity, resilience and security of national segment, including the CII, understood as the core of Russian national cyber security thinking, are incorporated into the framework. Sixthly, the different Russian information and cyber security actors and their responsibilities, are used to examine how the segment could be operated as a closed national segment.

The continuum of interstate relations is based on the analysis presented in Chapter 5.2 and it includes the phases of peacetime, intensified competition, conflict including the initial phase of war, and war. The different national security threats are based on official and unofficial Russian military threats and the basic premises of national security thinking and were analysed in Chapter 5.2 and 5.3. The threats include, on a scale from least to most destructive, espionage and terrorism, local conflicts and internal disturbances, full-scale colour revolutions and regional wars, and great power wars including conventional, high-tech, non-contact warfare and total nuclear war. These do not correspond to official Russian threat scenarios but are interpretations of Russian strategic thinking in the context of cyber and information warfare. The basic premises of the Russian understanding of national and military security threats are interpreted through the concepts of strategic planning, territorial defence, and the whole-of-state management as analysed in Chapter 5.1-5.3. Thus, an approach, which includes centralized management and control, territorial approach to cyber security and defence, and all state organs as active participants in information and cyber security, is adopted. The interpretation of the national segment as system of systems is argued in Chapter 3.5. The elements and functions of different subsystems, and explicitly the functioning the whole system of systems, is based on the material presented in Chapters 5 (ideas) and 6 (systems). The Russian understanding of national cyber security and defence is based on the integrity, resilience and security of the national segment, including its CII. The information-technological element forms the basis of broader information security as has been discussed in Chapter 6.1.3. Lastly, the analysis of the Russian security actors and their responsibilities presented in Chapter 6.2.1 provides means to examine who is responsible for the functioning, and command and control of the national segment.

The above defined military strategic framework sets the prerequisites for constructing a model of the Russian national segment as a national system of systems of information security and defence. It is, thus, a system of systems of information, not cyber, security and defence because it is directed against both technological and psychological threats and its systems have legal, economic, intelligence, law enforcement, and military functions, which function through peacetime to wartime. It is arguably an interpretation and an ideal type, and no claims are made that the model fully corresponds to the thinking of the Russian defence and security elites, but it nevertheless fits the aspirations of many Russian scholars and officers and is reasonable from the point of view of strategic cultural ideas. Consequently, my analysis proceeds as follows. First, I will analyse the different subsystems of the national segment. Secondly, this system of systems is put into a context of a continuum of conflict and different military threats. And thirdly a synthesis of the functioning of the Russian national segment as a closed national network is presented.

The subsystems of this system of systems can be grouped in many ways. One way would be to delineate the systems through their military functions: intelligence, offensive, defence, command and control, support etc. However, this would emphasize warfare and would not correspond to the Russian ideas concerning the information struggle. Here, the subsystems are grouped based on their distinct purpose, components, functions, principles, and objectives into seven subsystems. Previous chapters provide descriptions of the individual components mentioned below. It is assumed that the principle relations between the subsystems go through the seventh, monitoring and controlling, subsystem. Thus, the analysis on the interdependencies and interaction between the subsystems is left out of this examination. However, they are an important subject for further research.

The first subsystem is an economic and scientific mechanism based on import substitution, autarkic economic policies, and investment in education and science. It aims to replace foreign information technology, i.e. both hardware and software in the Russian public and private spheres with domestic products and to modernize the Russian information infrastructure with state-led projects. The subsystem is also used to finance scientific-technological research to discover future, disruptive technologies. Subsystem's primary function is to create domestic digital economy and thus to improve the Russian economy and the stability of society, and to shape national cyberspace towards a direction beneficial to the regime. It creates potential cyber power and the basis for sovereignty. Its secondary function is to find asymmetric responses in the information-technological sphere if the balance-of-power cannot be achieved symmetrically. Thirdly, together with the subsystem of national encryption, in principle, it offers national security through obscurity. It limits the threat of supply-chain attacks and provides tools for the security services to install their own backdoors or to create secret vulnerabilities in domestic products and services. If successful, it offers a means to project Russian power by exporting Russian ICT solutions and thus creating dependencies.

The second subsystem is state authentication and encryption. It is based on the mandatory national encryption systems and authentication certificates which make all data traffic in the national segment transparent to the security services—excluding, perhaps, transiting encrypted foreign data. Web traffic of users residing in Russia, data transmitted through backbone networks, and data residing in storage is encrypted and decrypted with keys which are under state control. The subsystem achieves security through secrecy and inversely through transparency as the security services have access to the crypto keys and certificates. It is an important part of the idea of digital sovereignty as a state can only be sovereign if it can exercise its powers in relation to information. The function of the subsystem is to enable unhindered counterintelligence, law enforcement, political control, and to strengthen national security.

The third subsystem is composed of administrative and technical measures to remove from and restrict access to unwanted content on the Internet through blacklisting, including banning foreign Internet services. Additionally, ISPs are made legally responsible for the content of their services and the right to disseminate information is restricted. This subsystem includes the efforts to remove anonymity from the Russian Internet by restricting the use of VPNs, by introducing digital identification and registries of mobile users. It also includes denigrating foreign information sources as 'foreign agents.' The subsystem includes self-censorship and 'citizen vigilance groups' who monitor the national segment for 'unlawful' content. This subsystem provides tools for the information struggle in the national segment. The function of this system is primarily political control based on removing content and restricting access, and secondarily law enforcement.

The fourth subsystem consists of the targeted surveillance system SORM[2437] and the massive Internet data traffic localization and retention conducted by the ISPs as ordered by the state. This enables traffic and content-based analyses of security threats and appropriate actions inside and outside cyberspace by the security services. The subsystem makes the digital information in transit and in store in the national segment available to the security services and enables advanced methods of big data analysis and forecasting. It is based on massive, distributed data centres and networked monitoring systems. The information struggle and strategic deterrence requires intelligence on possible threats. The functions of this system are counterintelligence, law enforcement, and political control as access to data can be used for political purposes.

The fifth subsystem is the critical information infrastructure and its regulation. This designates and categorises the national information infrastructure that needs to be controlled by the state either through state-owned companies or through the mandatory responsibilities of private companies supervised by the security services. It is also based on the national duplication of the critical Internet services, most importantly DNS, which are supposed to ensure the integrity, resilience, and security of the national segment. Consequently, it enables the functioning of the national segment in the case it is disconnected from the global Internet, and it ensures the segment's resilience against information-technological threats. In the future, the CII might even include 'information resources' that is websites and content providers. The CII is an example of a Russian version of public-private partnership were the state makes the private sector pay for its own protection. The CII creates a distinct subsegment of the national segment where state interests are paramount and transfers the control of some parts of the bottom-to-top evolved Russian Internet to the state, thus creating borders for digital sovereignty. Information superiority in any conflict is only possible to achieve if the state controls its own information space—in this case its technological, i.e. cyber side. The subsystem's function is mainly related to national cyber secu-

[2437] SORM could be placed in the seventh subsystem as it is a monitoring system. However, SORM is primarily a targeted eavesdropping system with specific function of law enforcement and, thus, belongs to the system that is used to get access to the substance of information.

rity as it legitimizes, empowers, and organizes the state control over the Internet, enables its shaping along territorial state borders, orders the social relationships, and provides a common understanding of security.

The sixth subsystems consist of the various Russian cyber diplomacy efforts and the organizations promoting them. Its purpose is to advance the Kremlin's agenda which is based on making state sovereignty the guiding principle of Internet governance, the use of information weapons proscribed, and promoting Russia's status as an international norm-setter. The cyber diplomacy efforts are coordinated on a national level, have a consistent message and resources to support them. They are advanced on both the international (UN) and regional level (EEU, SCO, CSTO, BRICS). This subsystem's function is to shape cyberspace through politics and norms to create internationally recognized territorial borders for the national segment and to prevent information and cyber threats from materializing.

The seventh subsystem consists of feedback, monitoring, control, and management systems. It includes GosSOPKA[2438], TsMUSSOP, the Upravlenie (and other state information systems), the network of CERTs functioning in different public and special networks, and civilian and the military networks of situation centres. This is the subsystem provides, in principle, the vertical control and horizontal integration of the national segment. It is admittedly a system of systems but here for simplicity's sake it is considered as one subsystem. It provides information on the national segment, and the whole society, a threat analysis of all information threats, not just cyber, and enables the control of information flows in the segment and its borders. From a cybernetic point of view, it is used to maintain the homeostasis of the whole system. This subsystem is the materialization of the ideas of the unified information space, information superiority, and automated management systems on a national level. However, the interconnectivity of its many elements may only be theoretical as organizational stove-piping and technical incompatibilities are likely. Its functions are related to the national security in information space through preparation, defence, and the control of the battlespace.

The system of systems of information security and defence consisting of seven subsystems has different uses and modes in different phases of interstate struggle and in the context of different threats. All subsystems are active in every phase, but their importance differs. The first and fifth subsystems provide the basis for the state's ability to function in cyberspace and thus its ability to shape cyberspace as a battlefield in all phases. They are the source of potential cyber power. During the first phase of peacetime or peaceful competition, states primarily use non-violent and non-military means of struggle. The second, third and fourth subsystems provide intelligence and make espionage and exploitation more difficult and as such increase the costs for would-be aggressors. They enable the resilience against information-psychological influence operations which might be used to foster colour revolutions or separatist and terrorist actions. The sixth system proactively prevents threats from materializing. The seventh system is used to resolve everyday cyber security issues and the integrity

[2438] GosSOPKA could be placed in the fifth subsystem as it is related to the protection of CII. However, as it is part of a larger network of national cyber security systems and a tool of monitoring and controlling (responding to threats), I choose to place it in the seventh system.

of networks. At this point the national segment can be considered ‘monitored’. The whole system of systems forms part of the strategic deterrence in peacetime as it signals deterrence by denial and possibly punishment. Russia can disconnect itself from the global network, protect its strategic systems, and strike back with any means necessary—at least in theory.

During a phase of intensified competition, a clear and present military danger will have emerged, and operations directed against the elements of the national segment of the Internet have increased. The means used in the interstate struggle are still covert, indirect, and non-military. The situation might call for ‘a state of emergency’ or at least increased intervention of the state to enable the functioning of the Internet. The nature of the threat affects the way in which the state control is deployed. Internal disturbances and terrorism, local conflict with a smaller state, or imminent attack from another great power require different solutions. The second, third and fourth subsystems are probably fully activated to provide maximum intelligence and control over the substance of the information circulating in the national segment. Moreover, the fifth subsystem is enforced and the seventh is used in a centrally coordinated and controlled manner. Its elements are used to monitor, counter and attribute aggressive operations. Defence-in-depth is used on a national scale and traffic might be restricted although not yet fully disconnected. This increases the resilience of the national segment but additionally allows Russia to, in the best case, attribute the attackers. This enables the sixth system to name-and-shame attackers. It is also used to incur diplomatic pressure on the adversary. The ability to monitor rising threats against critical infrastructure and to counter exploitation operations—intended to enable future attack—gives the state a definite advantage when individual private sector actors are not left alone to fend off attacks. This also provides better situation awareness and thus helps the state to prepare for potential future cyberattacks. At this point the national network is ‘controlled’ and has been prepared to withstand a wider and more aggressive attack, and both technological and psychological effects are kept in check.

During a phase of conflict, the military danger has become a real threat and the interstate struggle has acquired an overt, direct and military form and the aggressor has been very likely identified. In the case of a colour revolution or local military uprising, a foreign state or alliance aggressor is most likely indicated with or without any basis on facts. The phase includes the initial phase of war which will be decisive as it probably includes a massive, high-tech, aerospace attack. If the aggressor is a state, it has probably shifted from espionage and exploitation to direct attacks against the CII and the Armed Forces, and the psychological element in the attacks might have lessened in relation to the technological element. A non-state actor might use sabotage attacks against the government, the Armed Forces and other security services, or the civilian infrastructure with terrorist intent. However, a non-state actor would be likely to try to get external and internal support for its cause through information-psychological means. At this point all subsystems are functioning at full strength. They produce information, forecasting, support planning, and enable the control and management of the mobilized society, economy and military. Cyber diplomacy becomes part of the overall diplomatic effort to contain and, in the case of a colour revolution, to isolate the conflict. If the system fails to provide adequate protection or if the aggressor tries to undermine the basis of the Russian information society by bringing down or disconnecting the whole national segment of the Internet from the outside, subsystem seven is deployed to disconnect the segment in a controlled manner. This significantly reduces the possible attack vectors and outside psychological information operations are greatly restricted—at least temporarily. Additionally, the traffic inside the segment is heavily controlled and monitored which increases the protection against insider attacks. Thus, the ability of an internal non-state actor to coordinate its actions or reach foreign audiences is hampered. However, the disconnection is an escalatory measure and a signal that softer means of deterrence have failed. The state now has full control of the national segment of the Internet and the private sector is mobilized to sustain critical services needed for the functioning of the government, the military, and the basic services for the citizens. Adaptation and recovery are provided by the interaction of all subsystems. At this point the national network is 'closed'.

During the fourth phase of interstate struggle, i.e. war, the Russian state has been mobilized for total war. A great power aggressor is using all means available to disrupt, degrade, and destroy the Russian CII using both non-kinetic and kinetic direct means. Non-state actors at this point are considered part of the forces of the state aggressor whatever their motives might be. Some of the subsystems will probably lose their functionality because of the damage inflicted by the aggressor. The first and fifth subsystems enable the Russian state to withstand this phase of confrontation—as the Internet, in fact, was originally supposed to do.[2439] Satellites, fibreoptic cables, radio frequency-based technologies, physically distinct special networks of the government and the military, and dispersed server farms enable the national segment of the Internet to fragment but still function in a coherent, territorially based manner. The military is provided with connectivity in separate theatres or directions of war and nuclear weapons can be launched in a controlled manner. Although integrity on a national level is lost, separated parts of the national segment are still resilient and secure to a certain extent thanks to the modular nature of the subsystems. It is quite possible that these fragments will be divided along the borders of military districts or federal regions. At this point the national network is 'fragmented' but still resilient in its parts. After a conflict or war is over, the parts of the segment that have survived can be used to start rebuilding the communications and the nation. A summary of the subsystems and phases of interstate relations is presented in Figure 3.

[2439] Kaplan 2016.

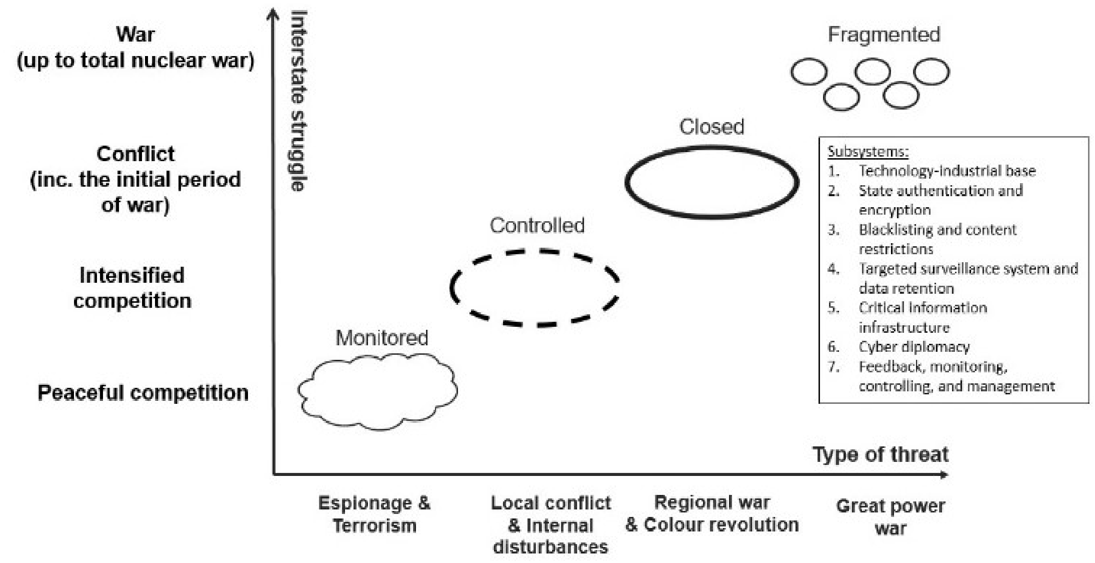
War
(up to total nuclear war)
Conflict
(inc. the initial period of war)
Intensified competition
Peaceful competition
Interstate struggle
Fragmented
Closed
Controlled
Monitored
Subsystems:
1. Technology-industrial base
2. State authentication and encryption
3. Blacklisting and content restrictions
4. Targeted surveillance system and data retention
5. Critical information infrastructure
6. Cyber diplomacy
7. Feedback, monitoring, controlling, and management
Type of threat
Espionage & Terrorism
Local conflict & Internal disturbances
Regional war & Colour revolution
Great power war

Figure 3. The national system of systems of information security and defence in the context of interstate relations.

The system of systems perspective combined with the concepts of territorial defence and whole-of-state approach helps to understand which state institutions are responsible for the control of the national segment of the Internet and offers insights into how the state authority in the Russian segment is organized. The military strategic aspect of this issue is the spatial and temporal border between the security services and the military. Arguably, during peacetime the FSB is the main national cyber security actor, supported in the government networks by the FSO. The MVD has a limited role in fighting cybercrime. However, the Roskomnadzor operates important elements of the seventh subsystem and the FSTEK regulates the CII. There is also some 'manual control' from the Kremlin. During intensified competition and the early phases of conflict and especially in the colour revolution scenario the Security Council manages cooperation between all power ministries. This cooperation requires peacetime strategic planning, exercises, and most importantly information sharing between multiple special networks and their operators. It also requires well-planned, geographically distributed, and redundant networks and services. The Radio Frequency Service under Roskomnadzor becomes an essential actor, as it controls the flow of traffic in the segment, although the threat analysis is still based on the assessment of the security services. War is the domain of the military and its supreme (political) command. Because a great power war is still a threat guiding the Russian strategic planning, the military strives to create separate networks, protects them and uses its capabilities primarily to support military efforts. The military is also given authority over civilian networks in a state emergency or war. However, regional and larger wars are a whole-of-state and nation effort, and thus the military might not be able to operate as independently as it wants. It is unlikely that it has the competence and resources to operate national networks without comprehensive cooperation with the ISPs.

Arguably then, the national segment as a system of systems provides information-technological and information-psychological integrity, resilience and security for the Russian national segment of the Internet. In principle, it is quite flexible and enables the mobilization of the resources of the whole state to protect the Russian national interests in cyberspace. The concepts of whole-of-state security, territorial defence, and mobilization give it some of its distinct Russian characteristics. There are some issues though. The governance of the national segment is still fragmented between different government organs, which will lead to friction. Satellite communications and the future 5G networks with billions of IoT devices make controlling and closing a highly connected and geographically vast national segment a challenge. Quantum technologies, blockchain and AI might provide support, but also produce new vulnerabilities. The civilian government's mandate to filter and disconnect Internet traffic might damage the operability of military command and control networks domestically and particularly the communications of forces operating abroad, depending on the technical solution adopted. Moreover, in the Russian political system the authority given to the state institutions to decide what systems must be used to protect the networks and by whom may lead to corruption and rent-seeking behaviour. If the private sector is forced to protect the CII, the result might not be optimal. Allied nations who rely on Russian datacentres would lose their services in the event of disconnection—to say nothing about economic damage to international corporations—so filtering traffic would be a highly political act. In fact, the Russian protectionist ICT policies are already affecting its allies. The disconnection of the national segment could even be considered preparation for a surprise attack and thus cause a preventive counterattack. Lastly, the whole national segment with different networks and elements could be considered a highly complex and tightly coupled system with an accident is waiting to happen—an accident that could disconnect Russia from the Internet unintentionally and without warning.[2440] Moreover, the multiplicity of systems and networks will lead to multiple gateways and interfaces that might provide vulnerable points of attack.

What does the case of the Russian national segment of the Internet tell us about closed national segments when approached as a system of systems of information security and defence? The most important argument is that closed national networks are much more than just the ability to 'shutdown the Internet.' A true closed national network should be able to function independently and self-sufficiently. Still, it is not a 'unified network' but a collection of relatively separated networks, services, resources, organizations, and policies. Thus, it is beneficial to approach it as a system of systems with internal processes which may sometimes be contradictory. Most surely, the network will be centrally and vertically controlled to enable the cooperation and integration of the multiple systems operated by different actors. This seeming simplicity might, however, result in a complex system as the data flows required for controlling a whole nation intertwine.

Closed national networks would probably tend towards homogenised hardware and software solutions as they are required by the implicit economic policies driving the construction of the closed networks and the needs of centralized control. Thus, some effort will be made to develop proprietary or domestic protocols and encryption, which will make the network and the information in it opaque. These domestic solu-

[2440] On these kind of system cf. Perrow. Charles Normal Accidents: Living with High Risk Technologies. Princeton, NJ: Princeton University Press 1999.

tions will be offered (or forced) on allies as an alternative to the international commercial and open-source solutions and will, in all likelihood, be forced upon own the administration and major sectors of industry. The infrastructure will be based on domestic datacentres and backup centres and a national backbone network. Its critical parts will be operated by state companies. They, and private companies allowed to operate such resources, will be monitored, controlled, and tightly regulated by the government and the security services. Technologies such as the SDN and the DPI and protocols such as the BGP offer the easiest way to regulate the data traffic in those networks. The closing of a national network would not be an all or nothing affair. It could be based on data traffic type, source, destination, amount, time, and geography. Some parts of the network could be disconnected while others remained open to the global network. This manipulation requires the duplication of the basic infrastructure services of the Internet, so national DNS, time, location, and routing services are required. It is probable, that the military would have its own logically and physically separated networks. The complexity of the national or civilian system is too unpredictable to give the military the reliability needed for its operations. Moreover, connections to strategic allies and forces operating abroad would have to remain open despite the closing of networks. A closed national network would benefit from the use of defensive machine or artificial intelligence. Its complexity and security requirements go beyond human capabilities and AI could be used for testing and analysing the system, forecasting, and for decision-making, in addition to command and control support.[2441]

To summarize, a closed national network is not just a piece of territorially segmented the Internet, or a disconnected network. Its functioning requires multiple systems and, directly or indirectly, it involves many state and private actors. It requires governance, norms, economic, and technological-scientific and educational policies to function. A closed national network requires an industrial information and technological-scientific domestic base. Moreover, it requires a political culture that is willing to limit basic freedoms and still be able to force high levels of cyber security awareness. Furthermore, its complexity means that it will take various forms depending on the nation deploying it. Here one is reminded of Alfred T. Mahan's definition of sea power which included geography and territory, the size and character of the population and the character of the government.[2442] Consequently, a closed national network requires a national strategy to become reality. The Russian version is the product of Soviet era kibernetik dreams interacting with information era threats and technologies. As a system of systems, it emphasizes the centralized state control of a territorially extensive nation through information, the nation's preparation for war, and the continuous interstate struggle in the meantime.

[2441] Cf. Scharre 2018, 220-221.

[2442] Mahan, Alfred T. The Influence of Sea Power upon History 1660-1783. Dover edition. Boston: Little, Brown and Company, 1890.

7

CONCLUSIONS

The aim of this thesis was to understand why the Russian Federation is creating a national segment of the Internet and how this segment as a closed national network could function. I decided to divide this problem into a theoretical and analytical part. The theoretical part concentrated on the ideas behind the making of strategy, and on the concepts of cyberspace, cyber power, cyber warfare, cyber strategy, and closed national networks. The analytical part concentrated on the Russian strategy to control and shape a part of cyberspace into 'a national segment of the Internet' as a case of a state creating a theoretical closed national network. I approached the research problem through six auxiliary research questions or subproblems which formed the structure of my thesis. This final chapter provides a summary of the main findings of the thesis and a conclusion. I demonstrate how the strategic cultural ideas have developed and interacted with Russian policies in a certain strategic environment to produce the national segment of the Internet as a reasonable strategic answer to perceived challenges. I review the composition and role of the most important epistemic communities involved in this process. Furthermore, I summarize the nature of the national segment of the Internet as constructed by Russia. Additionally, I summarize my interpretation of the national segment as a national system of systems of information security and defence, and the relationship of this system of systems to the theoretical closed national segment. This is followed by a discussion on the Russian understanding of cyberspace, power, and warfare, and national segments strategic meaning and possible future. I will end by reflecting upon my own research and I will present possible avenues for further research.

7.1 Strategic cultural ideas

The strategic cultural idea of an interstate struggle is related to the Russian understanding of the character of war. Its roots reach back at least into the Soviet era and it has acted as a causal or perhaps even a principled belief by providing a framework for understanding international relations. During the Soviet era it was perceived as a competition between two different political, economic, and social systems with the ultimate form of competition being a total war using strategic nuclear weapons in an eschatological war. This idea of constant competition or struggle between systems shifted in the post-Cold War era to a struggle between multiple great powers. In the 1990s 'information confrontation' became one of its forms. During peacetime this confrontation was considered as a constant struggle to influence the opponent's political elites, society, and economy with technological and psychological means. If interstate relations had moved into the initial period of war and war proper the technological and more destructive means would gain primacy.

The idea of an information struggle was defined and refined by a group of civilian and military theorists in the 2000s. Their views were affected by a geopolitics-based hope of state control over globalization, a belief in a future eschatological confrontation, and a worldview based on a struggle between political, social and economic 'kibernetik' systems with the emphasis on historical continuity. For these scholars, the information struggle became the defining form of competition between states and great powers. Information could have strategic effects and to counter those effects state-level organizational and technological information security systems must be created. The scholars did not advocate comprehensive security in the sense of broadening the sources and objects of threats but it was comprehensive in the sense of the means and actors of state power—a whole-of-state, territorial, and strategically planned response was required. Information warfare was divided into technological and psychological aspects the importance of which has fluctuated. The interstate struggle requires the mobilization of all state resources through the vertical of power.

In this view, the reward of the information struggle would be information superiority which could be achieved even in peacetime. Some theorists argued that future war would be characterised by indirect means and high tempo and would thus be resolved already in the initial phase of war. Others emphasised managed chaos or colour revolutions. Whatever the case, the technological and psychological aspects of warfare would be decisive. There were at least three different approaches to information and warfare. There were those who studied the issue in its strategic and geopolitical context—they are those whom Western scholars have called 'holistic'. But there were also those who approached IW from a systems theory point of view and those who concentrated on the operational and tactical issues—much like their Western counterparts. Furthermore, information-technological warfare has a distinct role in warfare in the Russian military thought, which is akin to the role cyber means have in Western thinking, although the Russian version includes a wider repertoire of means.

Although the Soviets had their own ideas about how military force and strategic nuclear weapons could be used to prevent military aggression, only in the 1990s did Russian and Western theoretical ideas began to converge into policies with similar basic understandings of the issue of deterrence. The concept of 'strategic deterrence' was already introduced in the 1990s but its official elaboration would be left until the 2000s. Initially and preliminary it related to strategic nuclear weapons. However, deterrence had a clear connection to the concept of the interstate struggle and its subconcept of the information struggle. In fact, even the Soviet era 'deterrence' thinking had included the use of information to prevent aggression and denial of information to protect the regime.

Strategic deterrence was given a more substantial form by General Gareev and others around 2006–2008. It was to be a continuum of creating defensive power, preventing threats from materializing, deterrence through denial and retaliation based on a complex system of state diplomatic, economic, technological, and information measures. Strategic deterrence involves all state actors. It is based on the idea of total war and thus requires the integrated functioning of strategic intelligence, political leadership, military-industrial complex, civilian administration of territorial defence, the mobilization system etc. The importance of the ideas of strategic deterrence, strategic planning, and territorial defence stems from current and future military threats, territorially bound views on security, and whole-of-state responses on a continuum of interstate struggle. This forms a framework for how the Russian defence and security elites understand military security. Most recent definitions of strategic deterrence include information and cyberspace in its sphere. Threats against the morale of the civilian population and armed forces need to be deterred. The critical information infrastructure of the information society in addition to conventional and nuclear forces must be protected. The idea of strategic deterrence thus develops and reflects the way in which the idea of interstate struggle changes.

An asymmetric response began as a solution to a strategic problem generated by the interstate struggle of the 1980s. It was an answer to the United States SDI programme via more efficient offensive weapons, preventive defensive measures, and diplomatic efforts. Moreover, it reflected the way the Soviets understood military power through the measurable strategic balance of power and cost-effective measure-countermeasure dialectics. These components have remained largely unchanged in the Russian strategic thought. During the 2000s and 2010s, the asymmetric response has been revitalized and offered as a kind of miracle cure to the Russian weaknesses contra the United States. In the contest of these proposals an asymmetric response can be described as overcoming the adversary' offensive and defensive systems while at the same time protecting one's own systems. It can be a cost-effective solution and/or an innovative technological breakthrough in the spirit of dialectical weapon–counterweapon progress. An asymmetric response is a prime example of a strategic cultural idea which is carried by epistemic communities and which resurfaces from time to time to be fitted to the current needs and environment.

From a purely military point of view, asymmetric responses have often meant ways to neutralize an adversary's superiority through technology or creative, innovative action including deception. The concept of an asymmetric response is usually related to political and strategic issues whereas asymmetric actions and the related concept of indirect means are used on the operational and tactical level. The core of the latter ideas is to evade direct use of military force against an enemy's military strengths. Military objectives can be achieved by multiple different means through the continuum on interstate relations. For most of the Russian military scholars there was little point in conclusively defining asymmetry as there were no universal asymmetric actions because conflicts differed and opponents adapted to previously used methods. Therefore, asymmetric responses and actions are not some magical tool to understand Russian strategic thinking. Moreover, the Russians are as inclined to adopt military theoretical fads as Western militaries are. Lastly, when Russians are somehow seen as inherently different, cunning, devious, and aggressive there is a fair amount of mirror-imagining, 'othering' and enemy-image building going on which does not necessarily contribute to better academic research or policy making.

The respect for state sovereignty, at least Russian sovereignty, has been a guiding principle of the Soviet and later Russian political thought. It found its expression in the information sphere as information sovereignty already in the late 1990s. However, this information sovereignty remained undefined well into the 2000s. Before it became an idea related to Russian internal sovereignty, it developed in the context of the Russian cyber diplomacy effort to create an international information security treaty that would have banned both the use of information and information systems as means (officially 'weapons') of an interstate struggle. It was also most probably discussed in the sphere of the post-Soviet security organizations where the military-political, terrorist, and criminal threats, and the threats against sovereignty intermingled with realist, geopolitical and even liberal views on state role and sovereignty. By the beginning of the 2010s the process began to produce definitions of information sovereignty and then of digital sovereignty. Information sovereignty began to denote the state's authority over information and its users on its territory and under its jurisdiction, while digital sovereignty denoted the systems, infrastructure, and economic and scientific-technological base of information sovereignty—also sometimes called technological independence. They were defined based on freedom from threats and control over national resources. As digital sovereignty has been adopted as an official concept in state documents from around 2017 it can be argued that digital sovereignty has developed from sovereignty over the information space to sovereignty in the information space and in the end to information or digital sovereignty, that is, to one of the aspects of state sovereignty.

Information and digital sovereignty are based on the idea of a unified information space and, more broadly, on the kibernetik dreams of Soviet scientists kept alive in the minds of the Russian siloviki and academicians of the scientific-technological research institutes. The societal and economic system of OGAS(U) and, on the other hand, the Soviet principles of continuity and uninterruptedness of military command, control and communications meshed in the 1990s with the Western ideas of RMA, NCW and the birth of the information society. At the same time, RuNet developed as a social and cultural space from the bottom to the top with a definite anarchical character and freedom of user which was unknown in the Soviet system. The EIP proposed a way to shape and organize these competing and sometimes conflictual processes into a state-controlled information space. This space should have delineated, controlled and protected borders, a vertical hierarchy and horizontally integrated networks. It should be a system of systems where information is gathered vertically through a feedback mechanism for the governing elites who use the information to control the state and the society. During the 2000s and 2010s the EIP continued to produce both military and civilian visions of command, control and management networks.

As was already mentioned above, the objective and prize of the information struggle is information superiority. Information superiority was already a part of the Soviet theory of a circle of command and control developed sometime in the 1970s and 1980s. Like the Western idea, the Soviet and Russian concept was initially about speed but later it emphasised knowledge and efficiency of command and control. Moreover, the Russians have developed their own theory of command and control warfare based on denying the NCW its advantage in modern warfare. The concept of information superiority is important for the Russians because it seems to explain what the West did to the Soviet Union through psychological operations and is still doing to Russia and other countries, and so it has offered an explanation and solutions for future warfare and the broader interstate struggle. Thus, the binary view on information as technological and psychological has also penetrated the idea of information superiority. However, the official documents of strategic planning or the statements of political leaders do not explicitly use the term 'information superiority' in a positive sense. It is related to domination, which is something that others pursue and can be legitimately challenged. Officially, Russia aims for parity and thus stability.

The idea of information-technological warfare was recognized by the Soviets as command and control warfare, and later in the 1990s the Russian military theorists became almost obsessed with the Western notions of NCW. During the 1990s, information warfare was generally defined by its novel means, but as time went by, the definitions began to emphasise the objective, which was the will of the opponent. This highlighted the possibility of a victory without the use of direct force. Thus, the technological component ended up as 'supporting means' in the geopolitical struggle for power. However, the military never gave up on thinking about the information-technological means in the context of preparing and fighting a war.

Arguably, Western views on the Russian understanding of IW do suffer from a certain bias. The claim that Russian IW is somehow more holistic and systematic than the Western approach is based on the implicit claim that Western IW is based on individual, fractured operations, directed against specific targets and agendas, and conducted in a relatively uncoordinated fashion. Even a cursory reading of Russian official and unofficial texts shows that this is not how Russians perceives the Western IW. The claims about the holistic and systematic nature of IW are related to only one of at least three different ways the Russians understand IW. Arguably, these claims serve certain political agendas more than an objective, scientific study of the Russian IW. However, I do not dispute the claim that outside of direct conflict the Russian information-technological activities and warfare are in theory subordinated to the information-psychological objectives.[2443] What I disagree with, based on the sources used in this study, is the claim that the Russians have managed to solve the theoretical and practical problems of IW and have built a system of perfectly functioning IW upon them.

The Russian understanding of an information-technological offensive has consolidated around a group of means which by the late 2010s includes kinetic (precision), software, hacking, electromagnetic, EMP, laser and other exotic means of attack. Consequently, the discussion has increasingly centred around what institution should be responsible for information security and what the tasks of the new 'information' troops should be. Critical information infrastructure and its resilience, integrity and security have provided substance for the Russian understanding of national information-technological or cyber defence. The concept of resilience is clearly a Western idea although its component parts were already present in the Soviet thinking. Ultimately, the protection of CII has become part of the interstate struggle.

[2443] The Russian emphasis on the psychological aspects of information warfare is the result of at least three different factors. First, as noted in this study, they interpret the fall of the Soviet Union as a result of Western IW. Secondly, this interpretation is supported by the KGB/FSB culture of 'active measures' and psychological operations, which has influenced theorists and especially geopolitically minded writers (Pynnöniemi 2019a & 2019b). And thirdly, information-psychological warfare is easier to present as an actual, foreign threat when one is needed to unite the nation. Thus, it can be argued that because Western ideas (ideology) and identities were not initially under threat after the 'victory' of the Cold War but 'cyber' (technology) was something new and interesting, Western scholars have concentrated on the technological aspects of IW. Conversely, the Russians have adopted the role of the underdog. They have approached information warfare as a Western 'technology' of the interstate struggle and, thus, as a weapon of the great power struggle. The legacy of Marxist-Leninist material dialectics might have an influence (Lalu 2014; Jonsson 2019). This stance points to one interesting and perhaps highly influential issue at the core of Russian strategic culture; namely its lack of critical self-reflection, fixation with history, and 'othering' all negative traits to the West.

The concept of an automated command and control or management system, understood in its most basic form as a system with inputs, outputs, feedback and controlling subsystems which is able to produce analysis and foresight and intended to produce faster and more efficient decisions, was introduced into the Soviet strategic thinking in the late 1950s. ASU became more than just a calculating machine. It promised to be a 'kibernetik' way of control over the human condition albeit a rigid, hierarchical and mechanistic one. During the Soviet times and later in the 1990s the idea of ASU tended to provided solutions based on integration, centralization, and control where the subject or controller would be the unitary state power.

ASUs have been conceptualized as tools but also as infrastructure and later as universal systems combining control mechanisms with the space in which they are used. Their function is based on the automation of parts of the 'cycle of command' but not on displacing humans from the loop. Creativity or the human factor has remained important for Russian military scholars, although their enthusiasm has sometimes been a bit over-interpreted by some Western scholars.[2444] The relationship of ASU to the concept of AI and related technologies, is still an open question in the sources analysed in this thesis—although there are reasons to suspect that ASUs might not fare well in future theoretical discussions.

The strategic cultural ideas discussed above for the most part had Soviet roots and were continuously developed throughout the time period under analysis. The 1990s were a defining period for modern Russia. The strength of some ideas, like the asymmetric response, has fluctuated over time. There was a period of emulation of Western ideas which was however replaced in the late 2000s with mounting criticism and a search for Russian substance for strategic cultural ideas. It is quite possible that during the 2000s and especially 2010s the Russian epistemic communities and elites turned to other sources than the West for ideas—mainly China. External events, interaction with foreign ideas, and interaction between the ideas themselves shaped the strategic cultural ideas. The Russian military and security communities did not write in a vacuum but were in constant communication with internal and external influences. When all is said and done, the main source of ideas have been the writings of American NCW and IW scholars. There might have been something inherently familiar in their texts for the Russian theorists, and, of course, they promised to offer 'a recipe for success'.

7.2 The national segment as a reasonable answer

The development of the relationship of the state and the Russian Internet can be divided into separate phases. The first phase (1991–1997) was characterized by a basically hopeful, liberal, and hands-off relationship. The Internet and 'informatization' at large was considered mostly beneficial or the government did not have the will or the resources to affect its development. The second phase (1998–2002) began when the Internet started to develop rapidly, and information warfare became an acute, although marginally understood question, mostly because of the second war in Chech-

[2444] Cf. Grau, Lester and Bartles, Charles. The Russian Way of War. Fort Leavenworth, KS.: FMSO, 2016, 57-58.

nya. Russia's relationship with the West went through crises and the government became aware of the need to regulate the 'information space.' Russia began to experience its information revolution during this time period. The basic tenets of Russian state policy towards the international cyber and/or information security were defined. They were based on territorial state sovereignty and ideas borrowed from nuclear arms control negotiations, and on the views of people affiliated with the security services. The basic forms of all strategic cultural ideas except digital sovereignty were already present. The Soviet tradition of state surveillance was re-established in cyberspace as SORM-2 was launched. The cybernetic tradition was also reflected in the proposed projects for national information management and command and control systems.

The third phase (2003–2010) was characterized by the government's efforts to manage and benefit from the informatization of the economy and the society. At the same time the regime tried to control the most negative aspects of the Internet mainly by updating and introducing new laws. Society and private industry managed to stop the most intrusive regulation and monitoring of the Internet, although other media were subjugated to the Kremlin or its oligarch allies' control. The Internet developed mostly on its own and was guided by private interests, and the state's development policies were largely dismissed or failed. The military began to pursue its own visions of the information space. The Russian regime continued to push state sovereignty as the basis for international regulation in cyberspace and classified information as a weapon. Sovereignty was also applied to domestic politics as a proto-ideology and the Soviet past began to be rehabilitated. Many of the central concepts of the latter phases, such as information sovereignty and the national segment of the Internet, were developed during this period in the context of Russian regional cyber diplomacy. The military developed the concepts of the information struggle, asymmetric response and strategic deterrence. The concept of critical infrastructure began to develop from planning and preparing for emergency situations to the protection of certain critical objects and the critical infrastructure. Moreover, Russia chose not to follow the examples set by the other great powers: It resisted the open militarization of cyberspace driven by the United States and the all-pervasive state censorship driven by China.

The fourth phase (2011–2013) began when external and internal events activated the regime to push for tighter control of the Russian Internet. The increased demand for new and old ideas grew as the elite searched for creative and innovative ways to make sense of the confusing and threatening environment and adapt to it. By 2011 the Internet had reached a significant portion of the Russian urban population and a distinct Russian Internet had formed. Before the demonstrations of 2011–2012, RuNet was mainly a platform of social interaction but it had slowly begun to challenge the regime-controlled sources of official news. Control was established mainly through laws and was in principle a vehicle for political control and censorship directed against domestic opposition. It also reflected the worsening great power relationships and the Russian negative view on the open militarization of cyberspace. During this time the ability and will of the Russian private Internet sector to resist government control began to erode. Those who did not comply were made to leave the country just as in the early 2000s. The Russian Internet was arguably beyond legal control and this was a time when the elites searched for a Russian approach to controlling it. The political debate on information and digital sovereignty arose and the idea began to be adopted into a policy, but sovereign state control was not yet a national security issue. Russia activated its global and especially regional cyber security norm diplomacy, although, at the same time some representatives of the elite began slowly to adopt Western ideas of cyber security. The increased understanding of cyber threats led to the adopting of the concept of critical information infrastructure. This trend was countered by the Chinese model, the appeal of which was partly the result of Putin's earlier 'pivot to the East'. The military pursued the development of communications, command and control systems as part of a military reform and arms procurement programme. Soviet policies of strategic planning, state mobilization, and state control over the economy were flexibly readapted.

The fifth phase (2014–) was initiated by the war in Ukraine and a definite change in the strategic environment, which led the Russian regime to seek a centralized control of the implicit manifestation of the EIP, 'national segment of the Internet', and to protect it from outside technological and psychological threats and also from internal subversion. Arguably, Russian actions were influenced by the changing global balance of power, militarization of cyberspace, their own perceived vulnerability, new technological threats, and the failure to create international cyber security norms to control the emerging threats in line with Russian interests. Multiple threats seemed to materialise at once in 2014–2015 and the West seemed poised to punish Russia for its actions—through isolation if needed. The economic and technological sanctions, stagnating economy and repeatedly failed efforts to initiate state-led growth of the ICT sector highlighted the vulnerability and weakness of Russian information-technological, or cyber, power.

Ultimately, information reached maturity and acceptance as an aspect of sovereignty, a sphere of state action and interests, and as politico-military means, ways and ends. This policy was enshrined in a series of strategic planning documents culminating in the National Programme of the Digital Economy which includes military, political, economic, and cultural aspects and which aims to shape into being a truly independent, self-sufficient, competitive, integrated, resilient and secure Russian national segment of the Internet. Russia strives to create international borders for this space through its ever-continuing cyber diplomacy initiative. In a great power interstate information struggle the national segment provides power, means for information superiority, and perhaps an asymmetric response to balance Russia's economic and technological weakness. Ideas developed in the Eurasian and Chinese context have gained influence. The regime continues to adopt laws that strengthen its control of the national information space, now with the aim of controlling information assets and information more than political activity. It has adopted the concept of integrity, resilience, and security of critical information infrastructure as the basis for a Russian understanding of national cyber security. The legacy of kibernetik ideas is merged with the Western ideas of resilience. The military has continued to develop its systems while considering both information-technological and information-psychological aspects of information security. The ultimate products of this phase are GosSOPKA, TsMUSSOP, Upravlenie, the network of SRSTs and other management networks. Which, if combined and centralized to the Kremlin, will form a modern era OGAS(U).

The above presented history raises the question as to why the elites did not really implement the ideas offered by the security services and others already in the late 1990s or 2000s? A lack of resources and a non-incentive strategic environment might have been reasons. Moreover, some members of the epistemic communities encouraged the creation of a new institutional power, the 'Ministry of Information Security', inside the regime, which the elite might not have preferred. There is no clear single point in time when the strategic cultural ideas penetrated the policies of the Russian defence and security elites. They were present already in the unofficial debates and official documents of the 2000s, however, they were not acted upon in the domestic arena in any efficient manner. The events of 2011–2012 provided the first stimulus which started the search for and reformulation of ideas to more concrete policies. The elites first deployed the ideas to solve issues of internal security and to secure their power. After 2014, as the strategic environment changed, the control of the national segment became a national security issue and the elites acted based on perceived critical security issues informed by strategic cultural ideas. Thus, I disagree with the notion that the policies of the Russian regime are just meant for internal political control. They are part of strategy to create power, prevent war and win it, if necessary.

What is then the relationship between the national segment of the Internet and the strategic cultural ideas? The idea of the interstate struggle, or more precisely the current version of the information struggle or confrontation guides Russia's approach to the national segment of the Internet. The national segment of the Internet is a at least partly the result of interaction between the ideas of an interstate struggle, digital sovereignty, strategic deterrence, a unified information space, and perhaps also of the asymmetric response. It was formulated as a response to a change in the strategic environment as the interstate struggle moved into the global information space. Information and digital sovereignty is a normative tool to control the new threats arising from that struggle. Sovereignty requires borders and these have to be defended, so the information space became the object of national security. The idea of a unified information space offered substance for this delimited and protected space. The technological protection of this space is related to the ideas concerning the critical information infrastructure and ASUs. Lastly, the unilateral disconnection, protection, and nationalization of a segment of Internet can be considered an asymmetric response to the perceived Western information-technological dominance.

The segment is directly related to Russia's national security interests. The politics related to its borders, resilience, and economic, technological, and cultural potential make sense only in the context of great power competition. Russian cyber diplomacy incorporated in the Digital Economy Programme is also a civilizational and world-order project. It is an effort to create an alternative system of Internet governance based on alternative values and power centres and thus it is an attempt to strengthen Russia's power, status, and independence. This is apparent in the way Russia is building regional norms through the CIS, CSTO and SCO. The national segment is a potential source of power as it offers a platform for scientific-technological advances, even breakthroughs, which might affect the balance-of-power between the great powers and offers Russia ways to change the current status quo. However, because the information space has so far lacked borders and, thus, juridical and practical state control, it has also been a source of danger and threats. In the Russian view, this space must be shaped and controlled so it can function as a source of power instead of a source of vulnerability. The Russian perception of the character of war is changing ever more towards a version where the borders between war and peace become increasingly blurry, and the potential enemy tries to win conflicts without the use of conventional force. The will of the population and decision-makers, and the economy have become military-political targets. Therefore, state control of the national information space and its component part, the national segment of the Internet, is imperative to succeed in the continuous great power, zero-sum struggle.

Information confrontation as part of the interstate struggle thus gives reason to build such systems as GosSOPKA, TsMUSSOP, and Upravlenie, and to adopt laws restricting the flow of information and ownership of the infrastructure in which that information resides. Information is power and, thus, critical information infrastructure is either a component part of that power or its source. No great power can leave this source unprotected or unharnessed. This means also that the 2017 Strategy of the Development of Information Society and the Programme of the Digital Economy as a state-led, national economic project makes sense as a national security strategy. The development of the national segment cannot be left to private companies, non-governmental organizations, and individuals. Although the information struggle is admittedly more about the information and its consumers than infrastructure, the services enabling the creation and dissemination of information must still be controlled. If the regulation and its autarkic tendencies improve the competitiveness of Russian ICT companies, even better—if not, that is the cost of regime security.

The increased measures to protect the national segment of the Internet and the ultimate option of disconnecting it from the global Internet are quite reasonable means of strategic deterrence. If future wars will begin with delegitimizing the enemy already in peacetime—and this includes the delegitimization of the regime in the eyes of its citizens—disconnecting the Internet makes sense. Enemy propaganda and attacks against critical infrastructure are thus denied their main attack vector. A successful deterrence by denial includes the communication to the potential opponents that their use of force and threat of it will not succeed. Moreover, as China has demonstrated with its 'Great Cannon', a state-controlled Internet, especially as interconnected as the Russian segment is, can be used to launch massive attacks against individual services or infrastructure of the Internet.[2445] These kinds of attacks and attacks launched from third countries can be combined with kinetic precision strikes and special forces operations to achieve strategic effects. The Russian leadership most certainly understands that the Internet can be weaponized. As informatization and digitalization proceed, Russia becomes as vulnerable to these attacks as any other state.

The current Russian understanding of avoiding war as a continuum of creating defensive power, preventing threats from materializing, and deterrence through denial and retaliation in a whole-of-state approach combining diverse means at the state's disposal provides good reason for shaping cyberspace. It is based on strategic level preparation of battlespace and deterrence signalling. The information space and its infrastructure need to be controlled already in peacetime because that is when information superiority is achieved on a strategic level, or at the latest in the first moments

[2445] The Citizen Lab. China's Great Cannon. Research Brief, April 2015 [Online]. Available: https://citizenlab.ca/2015/04/chinas-great-cannon/ [Accessed: 20th May 2019]; Demchak & Shavitt 2018.

of the initial phase of war. The strategic deterrence fails if the potential enemy's superiority is not already denied in peacetime. This idea is present in all strategic planning documents from the Information Security Doctrine to the Digital Economy programme. The building of deterrence requires the education of cadres, building of infrastructure, improving security and management, scientific-technological research, economic development, and international normative regulation to prevent threats and to legitimize Russian countermeasures in the case of 'the hostiles use of ICT.' Furthermore, this deterrence must be projected to outer space as the information space is ever more reliant on satellite communications. Different spheres of human action intermingle in the context of strategic deterrence.

The military-strategic reorientation of the Russian regime regarding the Internet in 2014 was not only defensive in nature. As the idea of an asymmetric response can be described as overcoming an adversary's systems while at the same time protecting one's own systems in an innovative and cost-effective manner, the control of the national segment and its disconnection from the global Internet makes sense. This is a way to shape the battlespace in such a way that a potential enemy loses its advantage and remains vulnerable. In fact, the current United States cyber strategy argues that while the United States is a superpower it is also vulnerable to cyber threats.[2446] An asymmetric response also resonates with the scientific-technological and high technology import substitution programmes and policies the Russian regime has initiated in the context of the 2014–2018 strategies and programmes. Future and disruptive technologies are at the forefront of the agenda of national scientific research. Similar efforts have been undertaken in the military sector, which proves that the Russian regime is searching for disproportionate advantages in the security sphere. The idea of an asymmetric response has thus at least two dimensions: the denial of the use of information space from advanced opponents and the search for counter-weapons. This is almost the same 'recipe' that the Soviet Union implemented in 1986-1989. However, as the history of the idea of asymmetric response has shown, it is both a tactical and political tool, promising decisive impact on the battlefield or on the balance of power. The latter can be discarded when other solutions present themselves—either a secure defence or a comfortable balance of power. Therefore, if the national segment proves to be an inefficient solution or the strategic environment changes, it might be abandoned.

The idea of information sovereignty was codified as the policy of digital sovereignty in 2017 at same time the national segment of the Internet became to denote the territorial borders of the Russian state in cyberspace. However, as was noted above, information and digital sovereignty are not synonyms. Digital sovereignty centres around the national control of the information infrastructure and technological independence. Information sovereignty requires both but is not limited to them. Information sovereignty is about the state control of information and the integrity and inviolability of the space in which that information circulates. Thus, the building blocks of information sovereignty include all the international treatises and initiatives, domestic censorship laws, doctrines, strategies, concepts and programmes adopted

[2446] The President of the United States. The National Cyber Strategy of the United States of America, September, 2018 [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [Accessed: 20th May 2019].

after 2011, and particularly after 2014, and their political, cultural, economic, societal, and military results. Perhaps the difference between external and internal sovereignty clarifies the roles of information and digital sovereignty. Information sovereignty is more about the right of the state to be free of outside interference whereas digital sovereignty is more about the state's i.e. the ruling elite's right to exploit its 'natural cyber resources'. State sovereignty is the one idea that resonates through all Russian policies and gives them undeniable reason. Information sovereignty legitimizes the top-to-bottom state control of the bottom-to-top evolved Internet. Thus, information sovereignty becomes a new aspect of state sovereignty, and the national segment anchors it to a 'physical' space.

Information sovereignty has legitimized the state-led development of the national segment of the Internet. As sovereignty is based on the balance-of-power thinking, the increased sovereignty of some implicates decreased sovereignty for others. It is then reasonable that Russian policies promote information security, and the development of infrastructure and the domestic ICT sector. A state without certain information technological resources such as a national system of encryption, domestic operating systems, and communication satellite fleet is not truly sovereign. Any dependency is a possible disproportionate and exploitable vulnerability, and thus a potential source of asymmetry. It needs to be emphasised that this aspect of information sovereignty was not always as strong as it currently is. During Medvedev's era and well into Putin's third term, Russia's dependency on foreign technology grew—and is still growing in some sectors as Chinese products enter Russian markets. Clearly then, sovereignty must be understood in a context of a question: sovereignty in relation to whom, and, thus, how much?

The development of the national segment is not only based on technological and economic potential. As Ristolainen and I have argued, through ideas presented by Russian scholars, digital sovereignty requires the delineation, control, and protection of digital borders.[2447] These functions are present in the Russia's cyber diplomatic norm-building efforts, the Information Security Doctrine, the Law on Critical Information Infrastructure and in the new so-called Law on the Sovereign Internet. Their implementation can be observed in how the state-owned companies acquire critical information infrastructure and in how the part of the infrastructure left in private hands is put under mandatory regulation and state surveillance. Moreover, data sovereignty is constructed through data localization and retention laws, and with TsMUS-SOP, GosSOPKA and SORM, the borders are finally erected. In this scheme, critical information infrastructure is the physical element of the national segment of the Internet which itself is the basis for digital sovereignty. Therefore, to summarize the current Russian approach to 'digital sovereignty', it can be understood as the extension of the authority and control of a territorial state to the national segment of the Internet, which consists of the infrastructure of the Internet and other network related ICT systems located on its territory or under its jurisdiction. A wider concept is 'information sovereignty' which additionally includes the information residing or flowing through those ICT systems and the interaction of its users, i.e. a sphere of activity.

[2447] Kukkola, Juha and Ristolainen, Mari. Projected Territoriality: A Case Study of the Infrastructure of Russian 'Digital Borders', Journal of Information Warfare, Vol. 17, No. 2 (2018), 83-100.

The national segment of the Internet replaced the unified information space as a central term as the importance of digitalization and the Internet grew. The EIP was never truly defined in the official documents and it variously included both technological and psychological aspects of information. Somewhat surprisingly, 'information space' was first defined in the international agreements in the late 2000s and early 2010s and those definitions included infrastructure, information as well as the consciousness of users. The distinction was the lack of the term 'unified' which referred to a certain way of arranging and delimiting space. Thus, the need to establish state sovereignty over a certain part of the global information space and the technology-infrastructure oriented policies of the 2010s required a more precise concept than the EIP. The national segment of the Internet, which had first referred to the domain name system and then been developed in the framework of CIS/CSTO into a political concept, was adopted for official use in the 2017 Strategy. The national segment of the Internet combined the internal way of shaping national cyberspace and the external necessity to define its borders. This is also the reason RuNet was not accepted as an official concept as it does not follow Russian territorial state borders. The national segment of the Internet is not an exclusively technological or material concept because it is also a place or sphere of activity. Therefore, the arguably Russian way of understanding infrastructure, information, and its users as a system is also present in the concept of the national segment. Thus, both digital and information sovereignty can be understood to function as systems. The idea of EIP still influences the way the optimal way of controlling and structurally arranging the national segment is understood. The technological and psychological nature of the EIP is apparent in the way that strategic planning and policy documents incorporate diplomacy, strategic communications, public affairs, economy, education, science, security and infrastructure under the concept of information. Consequently, the EIP is about the shaping of information space, not just about how the infrastructure or organizations should be arranged. This approach enables effective resilience against all information threats and enables the mobilization of the society and economy to produce potential power.

The 'unified, vertically integrated, automated, state information system' Upravlenie and the networks supporting it are the concrete manifestation of EIP and ASUs. It, and other more recent systems such as TsMUSSOP, GosSOPKA, ESPD, NSUD, the energy-sector and OPK information systems, and networks of NKTsKI and RKTsKIs, as well as national situation centres, follow the same principles of vertical control and horizontal integration. Information flows towards the national decision-making elites to establish total situation awareness and knowledge, and orders flow downwards in accordance with strategic planning and control. These systems form a system of control, not only of the information space, but also of the Russian state. The EIP and its Soviet roots resonate strongly with how these systems are being envisioned and built, although the results might deviate somewhat from the ideal.

The efforts to build the OATsSS or MTSS, and the whole system of military command and control with its hierarchical structure of command centres, a system for mobilization and territorial defence, and a system for controlling the OPK are quite reasonable if understood through the idea of EIP. Both the civilian and military solutions have definite similarities with the concepts proposed by the Russian information security theorists already at the beginning of the 2000s. A system, or more precisely a system of systems, is being built to control political, military, and economic aspects of the state and society. The systems are used as a tool for forcing the 'power vertical' onto cyberspace as the separated networks of different ministries and agencies are collected under one management. A national system of cryptography, domestic operating systems and other software solutions, and a control system over the borders of the national segment of the Internet would enforce the unity of Russian information space contra other segments of Internet.

Aspirations, intent and reality should be separated from each other. Unity is an idea, an aspiration. Any computer network where information flows freely is by its nature unified and single. The 'Russianness' of the EIP is thus a complex question. The 'shutting down' of the Internet was debated in the United States already in 2010, as has been a national monitoring systems, and the Clipper chip, i.e. a national encryption system was proposed already in the 1990s.[2448] China's 'Great Firewall' has been operational since the late 1990s.[2449] Furthermore, the idea of increasing intragovernmental cooperation, information sharing, resilience of national systems, and the whole-of-government approach all sound much like the ideas that circulated in the Western policy circles in the 2010s. The argument however is that the EIP is something more. 'Upravlenie', OATsSS etc. are more than computer networks offering information sharing and services—they are a means to control and shape cyberspace into a national segment or kibernetik system of state management. They have a distinct political, economic and social function. Furthermore, they are based on different ideas.

One reason to control and shape cyberspace according to the EIP is information superiority. This intertwining of the ideas of the EIP and information superiority was noted in Chapter 5. The information-technological and psychological aspects of this superiority are both present in Russian policies from 2011 onwards. The laws adopted against foreign media holdings, foreign supported NGOs, registration of ORIs and state blacklisting are proof of the psychological, or moral, cultural and political aspects. The technological aspect is present in import substitution and domestic production support policies, state ownership of critical information infrastructure, and in the search for scientific-technological breakthroughs. The search for superiority and its denial from potential opponents legitimizes state investment in the backbone networks, satellite communications, super and quantum computers, AIs, and encryption. It also makes it reasonable to search for allies and to create networks with them which enable the sharing of information, common situation awareness, and the joining and synchronization of assets. Information superiority has its geopolitical characteristics which become ever more important as the idea of information sovereignty spreads.

The idea of information superiority is related to military issues and the doctrine, paradigm or theory of NCW. According to this doctrine, no future conflict or war can be won without information superiority. The arms procurement programme shows that the Russian military has accepted this idea although with its own national characteristics.[2450] The idea of information superiority emphasises the need for real-time, processed knowledge made available to the decision-makers at the highest levels of

[2448] Rid 2016, 274-276.

[2449] Inkster 2016.

[2450] Cf. Persson 2016; Westerlund, Fredrik and Oxenstierna, Susanne (eds.) Russian Military Capability in a Ten-Year Perspective – 2019. Stockholm: FOI, 2019.

national and military command. NDMC, OATsSS and MTSS are a proof of how this idea has reached the Russian military and security elites. Because of the criticality of information superiority, it makes sense for the military to construct its own networks from the physical level upwards. On the issues of national security, public-private partnerships can only be a temporary solution. The military of a great power needs to control its own networks, like it has its own blue water navy, nuclear weapons and satellites. It can be argued that the urgency of information superiority can be confused with the prestige, status, and the trappings of a great power. A more critical issue is that there is a certain tension between constructing a delineated national segment of the Internet and the requirements of strategic military communications. What will happen to military communications, to a state's own and allied forces, if the national segment is disconnected? It is therefore understandable that the military has been interested in the implementation of Digital Economy Programme.

The technological and psychological aspects of the information space and warfare appear side-by-side in Russian policies, which has made it difficult to analyse the national segment as a purely technological phenomenon. However, they are distinct aspects of the same phenomena producing distinct policies and state behaviour. The concept of information security (informatsionnaia bezopasnost') in the information society and economic policies refers in part to the same real issues as the Western concept of cyber security. The Russian laws on the ensuring of integrity, resilience, and security of the CII can be read by any Western cybersecurity expert and be understood to concern cyber, not information issues. This version of cyber security has some Russian characteristics. It is state-led and controlled but depends on a Russian version of public-private partnerships. The ISPs are required by law to protect their infrastructure, share all relevant information with the state, and release control of their systems and networks to the state if the situation so requires. Moreover, they will pay for this protection themselves. The main information and cyber security actors are however the FSB, the FSO, the FSTEK and the Minkomsviaz' with its agencies. They monitor, supervise and control the federal subjects and private actors. This is cyber security with mandatory compliance and state verification.

The Russian military recognises information-technological warfare as a collection of technologies and means of using them. This mixture of more conventional means, such as computer attacks and EW, and exotic and future technologies is a distinctly Russian approach. It might produce interesting combinations, unexpected synergy, and new paths of thinking. However, military power is used based on available technology, organization, and doctrine. Based on the examination of military issues above it is safe to argue that the military has its strategic cyber forces in the GRU, and operational-tactical forces under the General Staff in the directorates, scientific institutions and the EW troops, and tactical forces in troops of various services. The Armed Forces also have psychological warfare directorates and troops which are ever more pervasive in the military organizations and resembling the Soviet era political commissar system. The ideas of information-technological warfare promoted by the military academicians resonate with how the military conducts itself. The OATsSS, MTSS, satellite communications, and field communications are built upon the principles of resilience, continuity, efficiency, and secrecy. Moreover, instead of adopting a passive defensive doctrine the Russian military has experimented with the denial of information space with its electronic 'A2/AD' capabilities and anti-satellite weapons.

Moreover, information-technological warfare has its role in mobilization, strategic deployment, and the initial phase of war—and in extraterritorial operations. It can have strategic effects, comparable to nuclear weapons, and needs to be incorporated in strategic and operational planning. Although the Armed Forces have their own tasks and probably concentrate on protecting military networks and services, the whole-of-state and government approach manifested in strategic planning and the concept of territorial defence gives reason to suspect that the military could take part in protecting civilian or at least military-industrial objects. However, the FSB's role is dominant in the peacetime.

The way the Russian decision-makers seem to promote systems and systems of systems in the area of information security becomes understandable through the Soviet tradition of ASUs. The idea of centralized systems of control is a repeating theme in the way the Russian regime has tried to shape the cyber and information space in the 2000s. After 2011, information became an object of control and automated or semi-automated systems began to be built to enable the subject, i.e. the state, to exercise that control. Networks of information collection (more than sharing) and situation centres were envisioned to manage society and the economy. A system of systems has started to take shape. Arguably, it might be just a result of a common, but not shared, idea pursued by different sectors of the government for their own ends. However, the idea has been carried over from the Soviet times by the scientific institutions now with new resources, financing, and avenues of influence at their disposal. The principles of efficiency, continuity, readiness, stability, reliability (resilience), and secrecy characterize this system of systems. It is goal-oriented and constructed for a purpose. There is friction between these principles and others upon which an information society could be built such as the efficient flow and sharing of information and the creative formation of knowledge.[2451] The dialectics of Soviet ideas and modern technology and values will most probably produce novel and unpredictable results.

The ASUs and kibernetik thinking behind these aspects have promoted the idea of systemic confrontation. Although it is difficult to find traces of this kind of theoretical thinking in the Russian policies of the 2000s and 2010s, it is arguably present in the way the defence and security elite have promoted Russia or Eurasia as a distinct entity. This entity should have its own norms, systems and information flows, and a united stance against others (the West) on how the international cyber and information space should be shaped. In practise, the borders of this system are fuzzy and the component parts i.e. states have had their own contradictory agendas. Systems theory might help to understand how the Russian elite sees the Post-Soviet space and tries to control it. If the EIP is understood as a system, then it should be defended as a system. In this context, systems theory might help to explain the Russian active and offensive actions as the interaction between systems. However, to characterize the Russian policies as based on an already ongoing information war where the borders of war and peace have blurred is at least slightly doubtful.[2452] This view excludes the presence, nature, and interaction of the other systems (great powers) in the international system. Moreover, the view offers a very particular interpretation of 'war' and interprets Russian elites' rhetorical statements as true beliefs.

[2451] Castells 2010.

[2452] As Oscar Jonsson does (Jonsson 2019, 157).

Based on the above summary of the interaction of strategic cultural ideas, strategic environment and Russian policies I argue that the national segment of the Internet is a reasonable strategic answer to perceived challenges. However, it is necessary to point out that the group of strategic cultural ideas I have chosen to analyse in this study was not exhaustive. At least the idea of geography or territoriality and the ideas of how the Russian state should be organised, governed and secured have had an influence. The information security policy, territorial defence and strategic planning are policy prescriptions derived from these. Moreover, history is itself an idea which has been constantly used to legitimize policies. These have now been included in the analysis implicitly. Moreover, politics, and history can be considered more as worldviews than causal and principled beliefs, although the borders are admittedly fuzzy. There have also been 'fads' or ideas that have come and gone out of favour, like the liberal economic ideas. Their influence has been perhaps more important in areas which were not the focus of this thesis.

7.3 Epistemic communities

Where did the ideas for the national segment of the Internet come from? Many of the ideas examined in Chapters 4 and 5 have long historical roots and their influence on the decision-making elites has waxed and waned over time. However, as Andrei Soldatov and Michael Rochilitz have demonstrated in one of the latest analysis of the security services' influence on Russian politics, it is quite difficult to tell when the actions of the Russian elites fit the ideas kept by certain communities.[2453] Did the elites really hold the same ideas or did the events and actions just support the views of those communities? The importance of 'the siloviki' cannot be dismissed, but there have also been many other sources of reasons for action. Some of them reside outside Russian borders and outside the purview of any one group or community of people. Liberal economic ideas have, for example, constantly challenged strategic cultural ideas in national planning documents. This might explain why the idea of controlling the Internet did not break through around 2006–2009 during Putin's patriotic, sovereignty-based and traditionalist great power policy and the high tide of the power of the siloviki. Although, it might have been the case that in the 2000s the Russian Internet was not yet perceived by the elites as a significant political space or a source of power and welfare. Perhaps the Russian elites were still reluctant to identify with the Chinese 'Eastern choice'. It is also possible that the Russian ideas interacted with the ideas held by epistemic communities and elites of other post-Soviet countries. In this sense the 2000s were a kind of incubation period of old Soviet ideas. During this time the Russian reactions to Western ideas, their assimilation or refutation, was the most import source of new ideas. This process made it possible to define what was meant by sovereignty and the national segment by contrasting them with Western ideas. As Russia turned away from the West, Chinese ideas and deep-rooted Soviet memories were ready to provide answers. Although, it must be pointed out, that evidence of the presence of Chinese ideas in the texts of epistemic communities chosen for this study was hard to find.

What about the people with the ideas? The most obvious case of an epistemic community providing ideas for the elites is the establishment of the cyber diplomacy team

[2453] Soldatov & Rochlitz 2018.

and the composing of the first Information Security Doctrine. Here, ex-FSB/KGB officers and military men brought with them Soviet era ideas, and by fitting new and old ideas together a reaction to the changing environment the Russian understanding of information space was established. These people were incorporated into the elite themselves in the 2000s. A second, but a related group of people were the information theorists, many with security services backgrounds, but also including civilian cybernetists, who promoted systems theoretical approach for the control of the new information space. They were also partly incorporated into the elite. A third distinct group are the military academicians, whose ideas about the changing character of war have been highly influential. Some of them have risen from the institutions to the Security Council. A fourth group are the (legacy) nuclear arms control people like Andrei Kokoshin who brought with them the idea of the asymmetric response as they became part of the decision-making elite or leading academicians in the 1990s. There have, of course, been other groups influencing Russian policies directed at shaping cyberspace. The civilian institutions, economic think tanks and forums, and lobbyist organizations quite probably have had their effect. Perhaps a cross simplification would be to argue that the siloviki carried ideas about state security and struggle, information theorists ideas about systems, military academicians ideas about deterrence, warfare and superiority, and nuclear arms control people ideas about balance and asymmetry.

Epistemic communities provided a theoretical device to legitimate the selection of sources for this thesis. They also provided a theory of how ideas held in a society transfer into the policies of the ruling regime. Although, it has not been in the centre of the thesis I have been able to demonstrate that there have been definite ‘circles’ of people who have offered their ideas concerning information security to the elites. Although others have pointed out the role of cybernetists, kagebists, gereushniks and institutchikis my analysis highlights the group of ex-KGB/FSB cryptologists and IW operators, some ex-military officers, and the cybernetists in the surviving military and civilian research institutes who have penetrated the Security Council, the diplomatic corps, and academia. Still, the secrecy of the world these men (and men they mostly are in Russia) occupy makes it difficult to claim anything specific about their influence. Moreover, it is difficult to define where an epistemic community ends and a state elite begins when the people, in addition to ideas, move back-and-forth between the academia and the halls of power. These observations point out the need to tailor any cultural approach to the political system under study.

What can be claimed is that the Russian military and civilian security communities have been in constant communication with internal and external influences. They have been quite ready to adopt foreign ideas at least in the security and defence spheres. They have been highly interested in American operations, doctrines and theories and have drawn their own conclusions from them. Sometimes Western ideas are presented as Russian ideas. On the other hand, there are those scholars who use Western primary sources and, in fact, manage to refer to somewhat obscure Western works to make their point. Thus, they offer a venue for studying the West through foreign, and sometimes revealing, eyes. Overall, there has been a constant flow of Western ideas into Russia. Some of these have been adopted, others adapted, and the rest discarded. Interestingly, Chinese ideas (expect Sun Tzu’s) are rarely if ever mentioned. The same issue can be observed with ideas from post-Soviet countries. This does not mean that there are no influences. Just that the sources used in this thesis rarely mention Chinese or post-Soviet sources. As the interest in the Russian military strategic thinking has reawakened, it is quite possible that the tide of influence of ideas is yet again turning, this time from Russia to the West.

It must be noted that only a few of the texts analysed in this thesis are critical of the official policies or offer something that is not initially based on official concepts. Moreover, the border between independent epistemic communities and the elite is somewhat vague in the area of security policy where the political allegiance to the regime is a source of resources and legitimacy and many scholars and journalist are serving or ex-officers. However, Russian scholars and officers have been left with plenty of room to discuss the substance of the officially adopted ideas at least up until 2014. It needs to be also highlighted that the adoption of ideas by the elites, understood as their appearance in strategic documents or speeches of national decision-makers, does not mean that the Russian state has acted upon those ideas. It is possible to argue that everything the strategies and programmes of the late 2010s include were already proposed in earlier documents. Therefore, the relationship between the epistemic communities, elites, policies, actual state behaviour and its efficiency is highly complex and affected by the states' ability to mobilize resources, by the elite's two-level games, and the strategic environment, among other things.

7.4 The segment as a closed national network

The national segment of the Internet is being implemented through the Doctrine of Information Security, the Strategy of the Development of Information Society and the National Programme of the Digital Economy influenced by strategic cultural ideas carried by the epistemic communities and, consequently, by the Russian security and defence elites. The deadline for 'digital sovereignty' is 2020, and for a state-controlled Internet and 'digital economy' it is 2024. Currently, the interaction of strategic cultural ideas, technology and the bottom-to-top evolved Russian Internet has produced the Russian segment of Internet which is based on a resilient, highly connected and interconnected national network with increasing state control over infrastructure. A top-to-bottom control is being forced on the bottom-to-top evolved Internet. State control consists of multiple systems to monitor, protect, and control the national networks, and systems for providing the state the means to gather information and to use that information to control the society and the economy. The systems are used as a tool for forcing 'power vertical' on cyberspace as the separated networks of different ministries and agencies are collected under one management scheme. Moreover, state owned firms are building a network of state datacentres and acquiring the CII of the Russian Internet. The Armed Forces and the MoD, together with other power ministries, are building a network of nationwide, whole-of-state situation and command centres. In principle, this project has similarities to the one unsuccessfully pushed by the Soviet cybernetists from the 1960s to 1980s.

However, this system of control is being planned and implemented by a multitude of actors with the security services in the lead—thus security overrides economic concerns. The segment is in practise a collection of barely interconnected networks, and system and services, regulation, and policies. Some of them have been in the works from the 1990s onwards. Overlapping functions, friction from trying to force control over already established networks, problems with integrating non-compatible legacy systems, crippling secrecy based on the influence of the security services, rent seeking and organizational rivalries all hinder the achievement of the 'kibernetik' dreams. The result is a Russian way to shape cyberspace, and thus it might be unique. As was argued in Chapter 3.2.2, the space Russia is shaping is malleable, but it is also resistant and contested. No single state can impose its will and power upon the whole of cyberspace for an infinite time. Soviet ideas cannot be applied in their exact old forms in the context of new technology and post-industrial economic systems. There are, however, no theoretical obstacles for building national territorial political, military, and economic management networks based on the Internet. The critical issue is whether these systems provide any kind of advantage. Can the Russian concept of ASUs, for example, provide a breakthrough synthesis with modern AI technology? Because the interplay of ideas, technology and power in the context of cyberspace continues, it is safe to argue that the policies and systems described in Chapter 6 will change and evolve in the coming years.

In Chapter 6.5 I interpreted the Russian national segment of the Internet as a national system of systems of information security and defence based on the Russian strategic cultural ideas. This segment does not yet fully exist. It is currently being shaped into being by Russian strategies, policies and laws. This approach resonates with the ideas proposed by Russian information warfare scholars who envision information space as a system, information warfare as a struggle between systems, and the controlling of that struggle as the task of a national system of command, control and management. This system of systems is composed of subsystems which are not exclusively technological. They should be understood more as technological, governance, norms, organizational, economic, and security and military instruments and functions to control and shape the technological and psychological aspects of the whole system. Admittedly, such a system of systems is an interpretation and an analytic concept, but as was argued in Chapter 6, it is something that the scholars whose writings have been analysed in this thesis, and perhaps even the elites informed by them, would recognize and understand.

I have analysed the Russian national segment as a system of systems of information security and defence through the continuum of interstate relations and threats. The system consists of seven subsystems each with their own elements, functions, and objectives. These systems include the scientific-technological basis, the national authentication and encryption system, the administrative and technical measures to remove from and restrict access to unwanted content on the Internet, targeted surveillance systems and massive Internet data traffic localization and retention systems, critical information infrastructure and its regulation, and the Russian cyber diplomacy efforts and its organizations. The seventh system controls all the others, so the system is centralized and hierarchical. I have left the analysis of the interaction between the subsystems beyond the scope of this study.

Based on my analysis I argue that the system of systems could provide a flexible and centralised way to ensure information-technological and information-psychological integrity, resilience and security of the Russian segment of Internet, and that it might even work as a deterrent. The systems theoretical logic behind this argument is that as Russia cannot move itself or destroy its opponents, it can only protect itself by building borders and by modifying itself. Systems thinking also highlights that the system of systems is a constant and fundamental part of Russian state security operating already in peacetime. Information threats can be controlled and prevented from materializing as the elite sees necessary. The system's defensive importance is not diminished if others adopt similar systems as its borders are only territorial representations in the constantly changing cyberspace which cannot be conquered. Most importantly, once this system has been planned, constructed, tested, and exercised it is basically an autonomous and independent part of the Internet. Its partial or full disconnection can be achieved with known, controllable, and acceptable risks. In 2020 Russia underwent a phase of testing and preliminary exercising.

It is important to consider this model against the reality of the Russian national segment. Thus, it becomes obvious, that there are many ways in which this Russian system of systems might fail or be vulnerable. It is also important to set this system of systems in its international context and in the context of global cyberspace. Russian cyber strategy, even its military part, cannot be disconnected from its political and economic alliances or the ways the cyberspace constantly evolves. Thus, it becomes obvious that the national segment cannot be equated with total isolationism or that Russia will not find a lasting solution to protect its information space. The way in which I have conceptualized the national segment in this thesis always leaves something outside the controlled segment. There are parts of the Russian Internet that the seventh subsystem of information security and defence system will never reach.

I have argued in Chapter 6.5 that if the Russian national segment is considered as a representation of the theoretical closed national network, a state controlled segment of the Internet that can be technically disconnected from the global Internet, that network should be able to function independently and self-sufficiently. Moreover, to function properly this network needs to be centrally and vertically controlled. However, if we compare the Russian system of systems of information security and defence to the arguments presented in Chapter 3.5 it is clear that closed national segments cannot be understood only as static technological cyber security or defence systems and technical models. They help us understand the military strategic logic of constructing them but our analysis of them will be very limited if it excludes political, normative, organizational, cultural, economic structures, elements and functions. These systems produce the substance of independence and self-sufficiency of the networks and the practical advantages or disadvantages in situation awareness, decision-making, freedom of action, and resilience. They are mobilization systems as much as they are cyber and information security systems. Moreover, closed national networks need to be analysed in the context of time, as flexible, changing, controlled and contested constructs. It is then useful to analyse them as systems of systems and to compare models between cases. Arguably, every case has its own framework which conditions the systems and their functions. From a military point of view, it is, however, important not to lose sight of the strategic issues at play. Whatever the composition and character of these systems are, the objective is to understand their military implications.

7.5 Russian cyber strategy

Based on my theoretical approach which is based on analytic realist pragmatism and modified neoclassical realism I have claimed that the ways in which a state uses power to pursue its interests, including creating more power, are influenced by ideas and it is thus that ideas shape reality through power. In other words, ideas shape the understanding of the environment, give meaning to material power, indicate acceptable and unacceptable strategic choices, and affect the interpretation of one's own and others' use of power. They give reasons for certain courses of action. Elites get their ideas primarily from epistemic communities who are the carriers of 'all knowable and proposed ideas' in a society. This system of ideas is open and changing. Furthermore, new ideas must be 'fitted' to old ones—they must make sense in the context of the old. The elites can choose the ideas which they make use of but are at the same time prisoners of their previous choices. The strategic environment might present new and threatening situations which requires the elites to find new ideas and solutions.

Cyberspace is an environment in and through which power informed by ideas can be used. It is a new environment with unknown or poorly understood potential threats. It is a man-made and governed global domain within the information environment whose distinct and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies. Human action can change cyberspace in ways it cannot change the land, air, sea or outer space. Because the object of study of my thesis was a certain way to use power, I decided to define cyber power as an ability that empowers an actor to influence others in or through cyberspace and to control and shape cyberspace to its advantage according to its preferences. This power is relative and contextual. Cyber power is defined by its resources and the environment through which it is used. It is not in any inherent way 'military' power, and only the way it is utilized, and its effects and outcomes give it a military character. Through strategy certain resources at the state's disposal can be used, among other things, to control and shape cyberspace. This strategy is a process and a policy with emergent properties as it is carried out in cyberspace and against cyberspace and other actors in it through the continuum of interstate relations. Therefore, even though a cyber strategy is not inherently military it can have intentional and unintentional military effects.

There are multiple ways that cyber power could be used in state to state relations in a military context. I tentatively defined cyber warfare as the use of force based on cyber power in or through cyberspace with a coercive intent to make political gains in the context of the continuum of interstate relations. In this thesis I chose to concentrate not on the more traditional compelling, coercive, deterring and brute force aspects but on the shaping of cyberspace as a strategic-level battlefield. More precisely, I was interested in the utilization of cyber power to control and shape cyberspace into a closed national network. A closed national network has the potential to provide a disproportionate and exploitable military advantage in cyberspace as the battlefield is shaped to favour one side or state. The military strategic importance of the shaping of cyberspace through national segments is based on the possibility of creating asymmetry. Without asymmetry, national segments would be only instruments of domestic political control and protectionist economic policies. Therefore, the connection of cyber power to warfare is two-fold: it is the potential to use force and it is also the potential to shape the space in which that force is used.

How do the Russian ideas and policies examined in Chapter 4, 5 and 6 fit the theoretical understandings of cyberspace, cyber power, cyber warfare and strategy? The drive to control and shape the national segment of the Internet, its structure, borders and the information in it conforms to the characteristics of Russian cyber power presented in Chapter 5.10. By shaping and controlling cyberspace in a technologically independent national segment, Russia, in principle, would create a measurable potential for power, negate its own vulnerabilities and weaknesses and exploit the vulnerabilities of its opponents. Power is created through the creative use of power. If the United States controls the global cyberspace, Russia must create its own space. No great power can survive in the future interstate information struggle and warfare without its own information society and economy, the ability to protect it and, conversely, without challenging the United States in its own space. The national segment of the Internet must be ordered and controlled in accordance with the principles of management, vertical control and horizontal integration ensuring the state sovereignty and power. Inside delineated, protected, and controlled information space a scientific, technological, economic and human potential can be fostered. This is a cyber strategy to create power by controlling and thus shaping cyberspace. Parity or even superiority is achieved already in peacetime which provides a deterrent and a decisive advantage in a possible, future conflict. Thus, in the light of strategic cultural ideas and policies analysed in this thesis, what Russia is currently doing in the framework of its strategies and programmes, makes sense.

The Russian ideas related to the phenomena called cyberspace, cyber power, cyber warfare and cyber strategy are ultimately not so different from the Western ones. The information infrastructure is composed of information, systems, and resources, and sometimes of users. It is as material as electromagnetic emissions can be. It forms the basis of an information space which includes the substance of information, human minds, and societies. Power in information space is measurable, relational, and can be created through human action. Power lies in the control over systems, flows, information and the opponent. It is characterised by effectiveness, efficiency, resilience (reliability and stability), flexibility and secrecy. It is based on scientific, technological, creative, spiritual, economic, and human potential. It is state power related to the continuous interstate struggle. Russian views of information-technological IW are somewhat different from the Western ones as there are at least three ways to understand IW: geopolitical, systemic, and operational-tactical. These understandings are informed by the persistent measure-countermeasure logic, derived perhaps from material dialectics. Moreover, the Russian views on IW rely on the same approach as most of the Russian public thinking on warfare as a total great power war either prevented or fought based on geography for the defence of the Motherland. In this context, the idea of plain cyber strategy is nonsensical as it is better understood and served as a part of strategic planning process.

Based on the effects of the strategic environment and the influence of strategic cultural ideas, I disagree with the interpretation that Russian policies are just tools of censorship or political control. The national segment is a response to at least the following threats: the use of the information space for terrorist and criminal purposes, interference into the internal affairs of states, the military-political use of the information space, attempts to dominate the information space and to limit the technological sovereignty of other nations. Therefore, Russian policies include aspects of building sovereignty in a new space, or sphere of activity, and thus shaping the international environment. This occurs through new digital borders, through the concept of a critical information infrastructure and resilience, through shaping and controlling the national information space in a certain way and creating military capabilities for future conflicts and warfare. It was the change in the strategic environment which made Russia strive to shape cyberspace to protect itself and to even-the-odds with more powerful adversaries supporting different political and cultural worldviews. The change of policy was not simply an autocratic reflex of Vladimir Putin and his supporters in the face of political opposition.[2454] Consequently, Russia has shifted to shaping its own national cyberspace to create power while still pursuing changes of the rules through international norm building after 2014. However, it is quite possible that the same process would have taken place without the war in Ukraine, although more slowly.

The Russian approach leads to a certain amount of friction between civilian and military strategies. As was argued above, a closed national network requires the mobilization of a wide range of state institutions and multiple different sources of potential power. Its effects are so broad that a purely military approach will fail. Conversely, a purely civilian approach will also fail as military networks are part of cyberspace, or more precisely, part of the information infrastructure that forms the backbone of the digital territory. If the battlespace changes unexpectedly under the feet of friendly forces a catastrophic failure awaits. Moreover, every closed national network is shaped into being in accordance with nation-specific strategic cultural ideas. If the ideas of the military and the defence and security elites correlate and support each other all is well. If not, then the civil-military relationships start to affect the way a closed national network is constructed and functions.

Although the Russian cyber strategy utilizes a whole-of-state approach it also has a definite military aspect. The creation of an EIP for the Armed Forces is at the heart of Russian military policy. Additionally, an asymmetric response is present in the understanding of an ever-continuing information weapon counter-weapon struggle. New technologies and creativity will hopefully provide positively disruptive solutions. The problem is how to keep this process in the framework of a cost-effective and innovative policy. Without an information-technological industrial base, it is difficult to produce cheap, secure and game changing military technologies. Moreover, without 'cyber wars' to prove testing fields for new weapons and defences on the strategic level their development is necessarily based on visions and conjecture. All this demonstrates that the use of cyber power for warfare, either as force or to shape the battlefield, is a complex issue. The Russian approach may be the new doctrine of deep battle and operations or it might be another Maginot line.

[2454] Furthermore, it shows a certain lack of imagination to think that a state's way to prepare and fight a war in the age of cyber warfare can be derived from how its secret services conduct espionage, subversion and sabotage operations.

Although, the Russian policies are for the most part threat-based, as are by definition all security policies. To approach them as an expression of a Soviet fortress mentality, or interpreting the national segment as a besieged fortress, risks missing some important features of the Russian strategy. Firstly, it is possible that Russian policies are directed by ideas with roots much farther back in history than the Soviet times. The ways to arrange state power in Russia have developed in the context of a vast, multiethnic, imperial Russia over hundreds of years. Secondly, to argue that Russia sees itself in a constant state of warfare or in active containment by the West restricts the understanding of the many directions and interests of Russian foreign and security policies. Thirdly, Russian cyber strategy has an outward directed aspect which is not focused on the West. It aims to shape the cyberspace on a global scale. The strategy is inclusive as it is expanding to Eurasia and China, possibly beyond. It promotes regional norm-building. In addition to security issues this aspect is related to the cultural, economic and social interests of a great power. Fourthly, the national segment is not only a space but a system of integrated and standardized communication networks and data resources, a system of security and management, and a system of operational, political, social and or economic control and management. It is a way to organize state sovereignty in cyberspace and, therefore, it is no more isolationist than any claim of sovereignty.

There are thus many reasons why the dreams of John Perry Barlow never came to be. In addition to the suspicion of authoritarian leaders towards the free flow of information, and the arguably Western desire to make cyberspace a domain of war, the Soviet 'kibernetik' dreams of hierarchical and centrally state controlled networks where power flows in the form of information provide one further explanation. I do not claim that Berg, Kitov, Liapunov and others dreamed of complete totalitarian control, just that their ideas have been finally adopted by those in power and fitted to their own needs. Based on the research conducted in this thesis I argue that Russia is creating a national segment of the Internet because it makes sense for the epistemic communities and the security and defence elites in the context of the current strategic environment to create a system of systems of information security and defence to manage and control their society and economy and to protect the state against internal and external threats. This system aims to produce cyber power and possibly military strategic advantages. Although the system is being built in the 21st century, it is still based on the dreams, memories, and beliefs of the people who witnessed the unexpected and unfair demise of the Soviet Union. The Russian national segment is then, at least partly, an effort to right a historical wrong with new tools—to create a digital Soviet Union that will survive the machinations of its enemies.

7.6 Reflections

How do the findings in this thesis add to or differ from the findings in previous studies on Russian information warfare? First, I have produced substance for the claim of Demchak and Dombrovski who have argued that the fragmentation of the Internet has a military aspect and that this fragmentation might benefit states seeking sovereignty. I have analysed some of the reasons behind Russia's policy of promoting information sovereignty and I have dug deep into the concept of information sovereignty to add to the research of, among others, Eneken Tikk, Mika Kerttunen and Julian Nocetti. I have shown that although the ideas of the siloviki have had a major impact on Russian cyber policies, as Soldatov and Borogan argue, the living legacy of cybernetics has had at least as powerful an influence. I have further developed the ideas of Katri Pynnöniemi on the Russian critical infrastructure. I argue that the integrity, resilience and security the CII now forms the basis of Russian understanding of state cyber security. I have added a new way to use cyber power on a strategic level, the controlling and shaping of cyberspace, to the theories advocated by Nye, Libicki and others. Furthermore, through the analysis of strategic cultural ideas I have complemented the research of Gerovich, Peters, Adamsky and Forsström by demonstrating continuity, filling in some gaps and introducing new ideas. Finally, through the study of strategic cultural ideas and theory of cyber power I have produced an alternative and more comprehensive explanation of Russian defensive cyber policies than Martti J. Kari.

It is either a sign of insightful scholarship or a sign of persistence in Russian strategic thought that in 1998 Timothy Thomas could list ten characteristics of Russian IW that are still more or less present.[2455] Thomas, however, studied ideas almost exclusively, not their implementation. Moreover, the claims by scholars like Giles, Adamsky, Heickerö, Jonsson, Blank about the 'holism' and constant continuity of the Russian IW have some truth in them but should not be taken as the whole truth. As this study brackets Russian offensive operations, I do not claim that Russian offensive information policies might not be 'holistic.' However, on the defensive side the multiplicity of actors and agendas make this claim highly suspect. Moreover, by claiming that some state thinks that it is at war with us based on the writings of academia is a claim based on false evidence. I also argue, that only by looking at Russian aggressive actions against the West, we fall prey to a multiple biases and errors of judgement.

My aim has been to capture as broad a picture of the Russian strategic cultural ideas as is possible in the context of available sources. I claim that I have succeeded well enough, but some difficult choices had to be made. For example, I have almost completely left out the statements and speeches of the elite. They are a legitimate source but would have broadened the already extensive source material even further. There is also the issue of translation. All the translations presented in this thesis are mine. There have been some difficulties in translating certain terms and I might have erred on the side of expediency—a case in point being the use of the terms struggle and confrontation. However, I believe that I have offered a more precise and comprehensive approach to these terms than previous studies.

I have tried to challenge some of the prevailing Western understandings of Russian cyber strategy or actions. The Western approach has been based on what Russia is doing to others, not on what Russia is doing to information or cyberspace or to protect itself. This 'active' and 'offensive' approach has obscured the Russian perception of 'deterrence' as constant struggle and competition. When half of the picture is missing there can be no full knowledge of the issue. Moreover, the premises of the Russian use of information security terms needs to be understood. There is a lot of intentional political maskirovka but also issues related to how the Russian scholars and the elite perceive the Western use of information against themselves.

[2455] Thomas 1998b.

Although I have claimed that the Western and Russian thinking on cyber security is quite similar, I do not claim that they are the same. For example, Russian ideas about information-technological warfare might produce interesting combinations, unexpected synergies and new paths of thinking. What is clear is that the Russians are susceptible to Western theoretical fads. The NCW and hybrid wars are a case in point. When reading Russian military and civilian journals one needs to always bear in mind that as the Russians are discussing themselves through Western examples they might get caught up in double mirror-imagining themselves.

The texts analysed in this thesis refer to China only passingly. In the 2000s some Russian authors recognized China as a possible adversary, but in the 2010s it has been mentioned only as a partner, if mentioned at all. On the official side Russia presents itself as belonging to the same political and cultural bloc with China when it comes to international information security. This would suggest some additional affinity with China in addition to rational realpolitik calculations. The problem with pointing out the Chinese influence is that the sources chosen for this study are silent on the issue. I have taken the liberty to mention China perhaps more often than the sources permit because there is enough circumstantial evidence presented in Chapter 6 of information security cooperation between the two countries. The reality of that relationship aside, I have come to believe that the Russian understanding of cyber issues cannot be understood outside the triad of the United States, China and Russia relations, and thus this thesis should be complemented with comparative studies.

I have legitimized my methodological approach in Chapter 2. The main theme characterizing my choices is the bracketing of Positivist causality. The theoretical and methodological framework of this thesis is by its nature 'eclectic'. It combines different theories and concepts of IR and Strategic Studies to study a specific problem. As such, it is vulnerable to criticism, for example, about parsimony and underlying assumptions. My answer to this challenge is an analytic realist pragmatic approach to the subject of my thesis. Thus, I take a pragmatic approach to my inquiry: I have initially engaged the subject of my study to construct a theory that has descriptive relevance to the problem at hand. I have engaged in self-reflection through dialogue with previous theoretical literature—including ontological and epistemological discourses. Furthermore, I have been open about my normative assumptions and professional interest in the subject of this thesis.

My interpretive epistemological and methodological approach can also be criticized. One could ask, what is it that makes strategic cultural ideas so enticing that they have historical staying power and have such an influence that Russia tries to shape cyberspace in a distinctly different way than other states? The problem with this approach is that there are any number of answers as previous research on ideas has shown. Russian actions could be related to, for example, Russian authoritarian political system, geopolitical factors, historical experiences or economic incentives. My approach can be challenged by all of these through empirical study. My humble goal is to understand how a set of strategic cultural ideas resonates with the policies of Russian security and military elites to create power in cyberspace by shaping the cyberspace itself.

I am cognisant of the way that I have used abduction to build a synthesis of Western and Russian ideas. Perhaps my interpretation has been distorted by the Western theories and concepts used to build my theoretical framework. Perhaps there is no system of systems of information security and defence—only fragmented bureaucratic projects informed by similar historical ideas. However, after analysing over 1,000 Russian articles I believe that there is something that makes sense in theorizing about systems and control. Moreover, I have referred to sources in Chapter 5 which explicitly refer to such systems. I do not claim that the interplay of ideas and material reality will provide a certain result, only that it makes sense from a point of view of the strategic cultural ideas to approach the Russian national segment as a system of systems of information security and defence.

Furthermore, making generalizing claims about such ideas as power is, of course, full of challenges, starting with the validity of such claims. Ideas must be understood in their temporal and political context, and the fact that they are ultimately carried and acted upon by human individuals must be recognized. The interpretations I have offered in this thesis are based on immersing myself on Russian ideas though texts produced by a distinct collection of people. My interpretations are subject to the judgement of the scientific community.

There might exist some important ideas I have left out of the analysis or incorporated incorrectly in other ideas in Chapters 4 and 5. For example, the interstate struggle includes the character of war, continuum of conflict, comprehensive security, territorial defence, and strategic planning. I have presented these as components of policy prescriptions, but they might be strategic cultural ideas of their own. I have bracketed ideas I have deemed to represent ideologies or worldviews, such as the 'besieged fortress' complex. Additionally, I have left the Russian theory of command and control largely unexplored as it is a subject of study on its own. The concepts of surprise and maskirovka as the roots of asymmetry have been studied by others, although only briefly and superficially. My thesis is not a comprehensive study of the Russian strategic thought, but I hope I have captured some important aspects of it.

I have had to leave some important issues concerning closed national networks and asymmetry beyond the scope this thesis because there was no room for them. A critically important issue for further study is the concept of structural cyber asymmetry and its analysis. Additionally, the development of the multitude of civilian systems and the vulnerability of the EIP of the Armed Forces to the possible disconnection from the global Internet of the national segment must be studied. The possibility to shape into being a closed national network with national characteristics raises multiple military strategic questions related to deterrence and escalation control which are beyond this thesis. The model of the Russian national segment as a system of systems of information security and defence provides a tool for pursuing comparative studies of other national segments. Moreover, the themes explored in this thesis should guide IR and Strategic Studies to pay more attention to the political, economic and military aspects of the shaping of cyberspace by state actors. Dominating narratives should be challenged and hidden, silent processes should be brought into the daylight.

BIBLIOGRAPHY

Finnish and English material:

Books & Academic Journals

Finnish language sources:

Berger, Heidi. Venäjän informaatio-psykologinen sodankäyntitapa terrorismin torjunnassa ja viiden päivän sodassa [Russia's information-psychological warfare in the fight against terrorism and int the Five-day war], Maanpuolustuskorkeakoulu, Johtamisen ja sotilaspedagogiikan laitos, Julkaisusarja 1, 5/2010.

Forsström, Pentti. Venäjän sotilasdoktriinien kehittyminen Neuvostoliiton hajoamisen jälkeen. [The development of Russia's military doctrines after the fall of the Soviet Union] National Defence University, Department of Warfare, Series 3: Working Paper No. 3 [Online] Available: https://www.doria.fi/bitstream/handle/10024/123521/Ven%C3%A4j%C3%A4n%20sotilasdoktriini%20ja%20sen%20kehittyminen%20Forsstr%C3%B6m%20%28netb5%29.pdf?sequence=2 [Accessed: 25th October 2018].

Forsström, Pentti. Venäjän sotilasstrategia muutoksessa. Tulkintoja Venäjän sotilasstrategian perusteiden kehityksestä Neuvostoliiton hajoamisen jälkeen. opit [The Russian military strategy under change. Interpretations on the development of the fundaments of the Russian military strategy after the fall of the Soviet Union]. Doctoral thesis. NDU Publication series 1, Research Publication No. 32. Helsinki: National Defence University, 2019.

Lalu, Petteri. Syvää vai pelkästään tiheää: neuvostoliittolaisen ja venäläisen sotataidollisen ajattelun lähtökohdat, kehittyminen, soveltaminen käytäntöön ja nykytilanne. Näkökulmana 1920- ja 1930-luvun syvän taistelun ja operaation opit [Deep or just dense: Soviet and Russian military thinking, development, application in practice and current situation. From the viewpoint of the theory of 1920s and 1930s deep battle and operation]. Doctoral thesis. NDU Publication series 1, Department of Tactics, 3/2014. Helsinki: National Defence University, 2014.

Mustajoki, Arto. Kevyt kosketus venäjän kieleen [A Slight Touch on the Russian Language]. Helsinki: Gaudeamus, 2012, 147-151.

Raitasalo, Jyri and Sipilä, Joonas. Muuttuva sota [Changing war]. Jyväskylä: Kustannusosakeyhtiö Suomen Mies, 2005.

Raitasalo, Jyri and Sipilä, Joonas. Sodan tutkimus strategian näkökulmasta [The study of war from the perspective of Strategic Studies]. In Raitasalo, Jyri and Sipilä, Joonas. Muuttuva sota [Changing war]. Jyväskylä: Kustannusosakeyhtiö Suomen Mies, 2005, 15-23.

Rantapelkonen, J. Psykologiset operaatiot. Propagandasta informaatio-operaatioihin. [Psychological operations. From propaganda to information operations]. Maanpuolustuskorkeakoulu Taktiikan laitos, Julkaisusarja 1 Taktiikan tutkimuksia N:o 1/2002. Helsinki: Edita.

Saarelainen, Jorma. Informaatiosodankäynti – venäläinen näkökulma [Information warfare - a Russian perspective]. In Saarelainen, Jorma, Alafuzoff, Georgij, Heiskanen Paavo, Tynkkynen, Vesa, Hyytiäinen, Mika, Hämäläinen, Tapani and Metteri, Jussi (Eds.) Venäjän asevoimat 2000 -luvun alussa [Russian armed forces at the beginning of the 2000s]. Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2 N:o 1/1999, 247-271.

Saarelainen, Jorma, Alafuzoff, Georgij, Heiskanen Paavo, Tynkkynen, Vesa, Hyytiäinen, Mika, Hämäläinen, Tapani and Metteri, Jussi (Eds.) Venäjän asevoimat 2000 -luvun alussa [Russian armed forces at the beginning of the 2000s]. Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2 N:o 1/1999.

Sivonen, Pekka. Suomalaisia näkökulmia strategian tutkimukseen [Finnish approaches to Strategic Studies]. Maanpuolustuskorkeakoulu, Julkaisusarja 1: Strategian tutkimuksia No. 33. Tampere: Juvenes Print, 2013.

Susiluoto, Ilmari. Suuruuden laskuoppi: Venäläisen tietoyhteiskunnan synty ja kehitys [Arithmetics of greatness: The birth and development of the Russian information society]. Juva: WSOY, 2006.

English language sources:

Aaronson, Susan A. What Are We Talking About When We Discuss Digital Protectionism? Institute for International Economic Policy, 14 July 2017 [Online] Available: https://www2.gwu.edu/~iiep/assets/docs/papers/2017WP/AaronsonIIEPWP2017-9.pdf [Accessed: 9th August 2018].

Abouzakher, Nasser (ed.) Proceedings of the 14th European Conference on Cyber Warfare & Security. Hattfield: University of Hertfordshire, 2015.

Acharya, Amitav. Global International Relations (IR) and Regional Worlds - A New Agenda for International Studies. International Studies Quarterly, Vol. 58, No. 4 (December 2014), 647–659.

Ackoff, Russell L. Ackoff's Best. His Classic Writings on Management. New York, John Wiley & Sons, Inc., 1999.

Acton, James M. Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War. International Security, Vol. 43, No. 1 (Summer 2018), 56-99.

Adamsky, Dima. Through the Looking Glass: The Soviet Military-Technical Revolution and the American Revolution in Military Affairs. Journal of Strategic Studies, Vol. 31, No. 2 (2008), 257-294.

Adamsky, Dima. The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the USA, and Israel. Stanford: Stanford University Press, 2010.

Adamsky, Dmitry (Dima). Russian Nuclear Incoherence. Journal of Strategic Studies, Vol. 37, No. 1. (2014), 91–134.

Adamsky, Dmitry (Dima). Cross-Domain Coercion: The Current Russian Art of Strategy. Proliferation Papers, No. 54, November 2015.

Adamsky, Dmitry (Dima). From Moscow with coercion: Russian deterrence theory and strategic culture, Journal of Strategic Studies, Vol. 41, No. 1-2 (2018), 33-60.

Adler, E., and Haas, P.M. Conclusion: epistemic communities, world order, and the creation of a reflective research program. International organization, Vol. 46, No. 1 (1992), 367–390.

Adler, Emanuel. The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control. International Organization, Vol. 46, No. 1, Knowledge, Power, and International Policy Coordination (Winter, 1992), 101-145.

Adler, Emmanuel. Seizing the Middle Ground: Constructivism in World Politics. European Journal of International Relations, Vol. 3, No. 3 (1997), 319-363.

Adler, Emmanuel. Constructivism and International Relations. In Carlsnaes, Walter, Risse, Thomas and Simmons, Beth A. (eds.) Handbook of International Relations. London: SAGE Publications, 2005, 95-118.

Adler, Emanuel and Vincent Pouliot. International practices. International Theory, Vol. 3 No. 1 (February 2011), 1-36.

Ahmad, Ijaz, Namal, Suneth, Ylianttila, Mika and Gurtov, Andrei. Security in Software Defined Networks: A Survey. IEEE Communication Surveys & Tutorials, Vol. 17, No. 4 (Fourth Quarter 2015), 2317-2346.

Alberts, David S. Defensive Information Warfare. Washington: NDU Press, 1996.

Alberts, David S., Gartska, John J. and Stein, Frederick P. Network Centric Warfare: Developing and Leveraging Information Superiority (2nd ed.) CCRP Publications, 2000.

Alberts, David S., Garstka, John J., Hayes, Richard E. and Signori, David A. Understanding Information Age Warfare. Washington, D.C.: CCRP, 2001.

Alberts, David S. and Papp, Daniel S. (eds.) Information Age Anthology – Volume III: The Information Age Military – Volume III. CCRP Publication Series, 2001.

Alexander, Marcus. The Internet and Democratization: The Development of Russian Internet Policy. Demokratizatsiya, The Journal of Post-Soviet Democratization, Vol. 12, No. 4 (2004), 607-627.

Allison, Roy. Reasonable Sufficiency and Changes in Soviet Security Thinking. In Frank, Willlard, C. and Gillette, Philip S. Soviet Military Doctrine from Lenin to Gorbachev, 1915-1991. Westport, Connecticut: Greenwood Press, 1992, 237-267.

Almond, Gabriel A. and Verba, Sidney. The Civic Culture: Political Attitudes and Democracy in Five Nations. Princeton, N.J.: Princeton University Press, 1963.

Andress, J. and Winterfeld, S. Cyber Warfare - Techniques, Tactics and Tools for Security Practitioners, (2nd ed.). Waltham: Syngress, 2014.

Angström, J. and Widen, J. Contemporary Military Theory: The Dynamics of War. New York: Routledge, 2015.

Arakelyan, Lilia A. The Soviet Union is Dead: Long Live the Eurasian Union. Kanet, Roger E. and Piet, Rémi (eds.) Shifting Priorities in Russia's Foreign and Security Policy. Surrey: Ashgate Publishing Limited, 2014, 141-161.

Archer, Margaret, Roy Bhaskar, Andrew Collier, Tony, Lawson and Alan Norrie (eds.) Critical Realism: Essential Readings. London and New York: Routledge, 1998.

Arbatov, Alexei and Dvorkin, Vladimir (Eds.) Missile Defese: Confrontation and Cooperation. Moscow: Carnegie Moscow Center, 2013.

Arquilla, John and Ronfeldt, David. Cyberwar is Coming. Santa Barbara: RAND, 1993.

Arquilla, John and Ronfeldt, David. The Advent Of Netwar. Santa Monica: RAND, 1996.

Arquilla, John and Ronfeldt, David. In Athena's Camp, RAND, 1997.

Arquilla, John and Ronfeldt, David. The Emergence of Noonpolitik: Toward An American Information Strategy. Santa Monica: RAND, 1999.

Art, Robert J. American foreign policy and the fungibility of force. Security Studies, Vol. 5, No. 4 (1996), 7-42.

Art, Robert J. and Greenhill, Kelly M. The Use of Force: Military Power and International Politics (8th ed). Lanham: Rowman & Littlefield Publishers inc., 2015.

Art, Robert J. Force and fungibility reconsidered, Security Studies, Vol. 8, No. 4 (1999), 183-189.

Averre, Derek. Russia, the Middle East and Syria Conflict. In Kanet, Roger E. Routledge Handbook of Russian Security. London and New York: Routledge, 2019, 399-409.

Ayson, Robert. Strategic Studies. In Reus-Smith, Christian and Snidal, Duncan (eds.) The Oxford Handbook of International Relations. Oxford University Press: Oxford, 2010, 558-575.

Babiarz, Renny. The People's Nuclear Weapon: Strategic Culture and the Development of China's Nuclear Weapons Program, Comparative Strategy, Vol. 34, No. 5 (2015), 422-446.

Bacon, Edwin. Security Council and decision-making. In Kanet, Roger E. Routledge Handbook of Russian Security. London and New York: Routledge, 2019, 119-130.

Baev, Pavel K. Defying That Sinking Feeling: Russia Seeks to Uphold Its Role in the Multistructural International System in Flux. In Stephen, Blank J. Perspectives on Russian Foreign Policy. Army War College Strategic Studies Institute (SSI), 2012, 1-24 [Online]. Available: http://ssi.armywarcollege.edu/pdffiles/pub1115.pdf [Accessed: 29th October 2018].

Baldwin, David A. Paradoxes of Power. New York: Basil Blackwell, 1989.

Baldwin, D. A. Force, fungibility, and influence. Security Studies, Vol. 8, No. 4 (1999), 173-183.

Baldwin, D. A. Power and International Relations. In Carlsnaes, Walter, Risse, Thomas and Simmons, Beth A. (eds.) Handbook of International Relations. London: SAGE Publications, 2013, 273-297.

Banerjee, Sanjoy. Rules, Agency, and International Structuration. International Studies Review, Vol. 17, No. 2 (June 2015), 274–297.

Barkanov, Boris. Natural gas. In Tsygankov, Andrei P. (ed.) Routledge Handbook of Russian Foreign Policy. London and New York: Routledge, 2018, 138-152.

Barkin, Samuel J. Realist Constructivism. International Studies Review, Vol. 5, No. 3 (September 2003), 325–342.

Barkin, Samuel J. Realist constructivism: Rethinking International Relations theory. Cambridge: Cambridge University Press, 2010.

Bardin, Jeffrey. Satellite Cyber Attack Search and Destroy. In Vacca, John. Cyber Security and IT Infrastructure Protection. Amsterdam: Syngress 2014, 309-323.

Barnett, Michael. Culture, Strategy and Foreign Policy Change: Israel's Road to Oslo. European Journal of International Relations, Vol. 5, No. 1 (1999) 5-36.

Barnett, Michael and Duvall, Raymond. Power in International Politics, International Organization, Vol. 59, No. 1 (Winter, 2005), 39-75.

Bartles, Charles K. Defense Reforms of Russian Defense Minister Anatolii Serdyukov, The Journal of Slavic Military Studies, Vol.24, No.1 (2011), 55-80.

Bartles, Charles K. Getting Gerasimov Right. Military Review, January-February 2016, 30-38.

Bateman, Aaron. The Political Influence of the Russian Security Services, The Journal of Slavic Military Studies, Vol. 27, No. 3 (2014), 380-403.

Battilega, John A. Soviet Views Of Nuclear Warfare: The Post-Cold War Interviews. In Sokolski, Henry D. Nuclear Mutual Assured Destruction, Its Origins And Practice. Carslile: Strategic Studies Institute, US Army War College, 2004, 151-174.

Bauer, Harry and Brighi, Elisabetta (eds.) Pragmatism in International Relations. Oxon: Routledge, 2009.

Baylis, John, Wirtz, James J. and Gray, Colin S. Strategy in the Contemporary World (4th ed.) Oxford: Oxford University Press, 2013.

Beaumont, Roger. Maskirovka: Soviet Camouflage, Concealment and Deception. Texas: Center for Strategic Technology, The Texas Engineering Experiment Station of the Texas ASM University System, 1982.

Bebber, Robert. Cyber power and cyber effectiveness: An analytic framework, Comparative Strategy, Vol. 36, No. 5 (2017), 426-436.

Becker, Michael E., Matthew S. Cohen, Sidita Kushi and Ian P. McManus. Reviving the Russian empire: the Crimean intervention through a neoclassical realist lens, European Security, Vol. 25, No. 1 (2016), 112-133.

Bellamy, Christopher. "Budushchaya Voyna; The Russian and Soviet View of the Military-Technical Character of Future War, Part Two" [Online]. Available: https://www.era.lib.ed.ac.uk/bitstream/1842/6892/2/504501_VOL2.pdf [Accessed: 11th November 2018].

Bendett, Samuel and Kania, Elsa B. A new Sino-Russian high-tech partnership. Authoritarian innovation in an era of great-power rivalry. ASPI Policy brief Report No. 22/2019.

Bennett, Andrew and Elman, Colin. Qualitative Research: Recent Developments in Case Study Methods. Annual Review of Political Science, Vol. 9 (2006), 457-458.

Bennett, Gordon. The Federal Security Service of the Russian Federation. Conflict Studies Research Centre, March 2000 [Online]. Available: https://www.files.ethz.ch/isn/96631/00_Mar_3.pdf [Accessed: 5th December 2018].

Benson, Vladlena and McAlaney, John. (Eds.) Emerging Cyber Threats and Cognitive Vulnerabilities. Elsevier, 2019.

Berenskoetter, Felix and Williams, M. J. Power in World Politics. London: Routledge, 2007.

Berenskoetter, Felix. Thinking about power. In Brenskoetter, Felix and Williams, M. J. Power in World Politics. London: Routledge, 2007, 1-22.

Berryman, John. "Fear and Loathing" in the Kremlin. In Kanet, Roger E. and Piet, Rémi (eds.) Shifting Priorities in Russia's Foreign and Security Policy. Surrey: Ashgate Publishing Limited, 2014, 51-71.

Betz, David. J. The more you know, the less you understand: The problem with information warfare. Journal of Strategic Studies, Vol. 29, No. 3 (2006), 505-533.

Betz, David and Stevens, Tim. Cyberspace and the State: Toward a Strategy for Cyberpower. Adelphi Series, Vol. 51, No. 424 (2011).

Betz, David. Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed, Journal of Strategic Studies, Vol. 35, No. 5 (2012), 689-711.

Biddle, S. Military Power - Explaining Victory and Defeat in Modern Battle. Princeton: Princeton University Press, 2004.

Biddle, Stephen. Military Power: A Reply, Journal of Strategic Studies, Vol. 28, No. 3 (2005), 453-469.

Biersteker, Thomas J. State, Sovereign and Territory. In Carlsnaes, Walter, Risse, Thomas and Simmons, Beth A. (eds.) Handbook of International Relations. London: SAGE Publications, 157-176.

Biscop, Sven and Whitman, Richard G. The Routledge Handbook of European Security. London: Routledge, 2013.

Bitzinger, Richard A. and Popescu, Nicu. Defence industries in Russia and China: players and strategies. EU Institute for Security Studies, Report No 38 – December 2017 [Online]. Available: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Report_38_Defence-industries-in-Russia-and-China.pdf [Accessed: 9th May 2019].

Björkdahl, Annika. Norms in International Relations: Some Conceptual and Methodological Reflections. Cambridge Review of International Affairs, Vol. 15, No. 1, (June 2002), 9-23.

Blagden, David. Induction and Deduction in International Relations. Squaring the Circle Between Theory and Evidence. International Studies Review, Vol. 18, No. 1 (June 2016), 195-213.

Blair, Bruce. The Logic of Accidental Nuclear War. Washington, DC: Brookings Institution, 1993.

Blank, Stephen J. Preparing for the Next War: Reflections on the Revolution in Military Affairs. In Arquilla, John and Ronfeldt, David. In Athena's Camp, RAND, 1997, 61-77.

Blank, Stephen. Rethinking the Concept of Asymmetric Threats in U.S. Strategy, Comparative Strategy, Vol. 23, No. 4-5 (2004), 343-367.

Blank, Stephen. Threats to and from Russia: An Assessment. Journal of Slavic Military Studies, Vol. 21, No. 3 (2008), 491-526.

Blank, Stephen J. and Weitz, Richard (Eds.) The Russian Military Today and Tomorrow: Essays in Memory of Mary FitzGerald. Army War College Strategic Studies Institute (SSI), 2010 [Online]. Available: https://ssi.armywarcollege.edu/pdffiles/PUB997.pdf [Accessed: 22th October 2018].

Blank, Stephen J. ”No Need to Threaten Us, We Are Frightened of Ourselves, ” Russia's Blueprint for a Police State, The New Security Strategy. In Blank, Stephen J. and Weitz, Richard (Eds.) The Russian Military Today and Tomorrow: Essays in Memory of Mary FitzGerald. Army War College Strategic Studies Institute (SSI), 2010, 19-149. [Online] Available: https://ssi.armywarcollege.edu/pdffiles/PUB997.pdf [Accessed: 22th October 2018].

Blank, Stephen J. (ed.) Russian Military Politics and Russia's 2010 Defense Doctrine. Army War College Strategic Studies Institute (SSI), 2011, 63-151 [Online]. Available: https://ssi.armywarcollege.edu/pdffiles/PUB1050.pdf [Accessed: 27th October 2018].

Blank, Stephen J. (2012a) The Sacred Monster: Russia as a Foreign Policy Actor. In Stephen, Blank J. Perspectives on Russian Foreign Policy. Army War College Strategic Studies Institute (SSI), 2012, 25-194 [Online]. Available: http://ssi.armywarcollege.edu/pdffiles/pub1115.pdf [Accessed: 29th October 2018].

Blank, Stephen J. (2012b) Perspectives on Russian Foreign Policy. Army War College Strategic Studies Institute (SSI), 2012, 25-194 [Online]. Available: http://ssi.armywarcollege.edu/pdffiles/pub1115.pdf [Accessed: 29th October 2018].

Blank, Stephen. Can Russia Sustain Its Military Capability? Jamestown Foundation, 13th September 2016 [Online]. Available: https://jamestown.org/program/stephen-blank-can-russia-sustain-its-military-capability/ [Accessed: 15th November 2018]

Blank, Stephen. Cyber War and Information War ál la Russe. In Perkovich, George and Levite, Ariel E. (eds.) Understanding Cyber Conflict: Fourteen Analogies. Georgetown: Georgetown University Press, 2017, 81-98.

Blank, Stephen J. (ed.) The Russian Military in Contemporary Perspective. Carlisle Barracks, PA., U.S. Army War College Press, 2019.

Bloomfield, Alan and Nossal, Kim Richard. Towards an Explicative Understanding of Strategic Culture: The Cases of Australia and Canada. Contemporary Security Policy, Vol. 28, No. 2 (2007), 286-307.

Bloomfield, Alan. Time to Move On: Reconceptualizing the Strategic Culture Debate. Contemporary Security Policy, Vol. 33, No. 3 (2012), 437-461.

Boltenkov, Dmitry. Russian MoD's ”Science Companies”. Moscow Defense Brief, No. 6 (2017), 10-12.

Booth, Ken. The Concept of Strategic Culture Affirmed. In Jacobsen, C.G. (ed.) Strategic Power: USA/USSR. New York: St Martin's Press, 1990, 121-128.

Borenstein, Eliot. Plots against Russia. Conspiracy and Fantasy after Socialism. Ithica and London: Cornell University Press, 2019.

Borghard, Erica D. and Lonergan, Shawn W. The Logic of Coercion in Cyberspace. Security Studies, Vol. 26, No. 3 (2017), 452-481.

Borghard, Erica D. and Lonergan, Shawn W. Cyber Operations as Imperfect Tools of Escalation. Strategic Studies Quarterly, Vol. 13, No. 3 (FALL 2019), 122-145.

Bouldin, Matthew. The Ivanov Doctrine and Military Reform: Reasserting Stability in Russia, Journal of Slavic Military Studies, Vol. 17, No. 4 (2004), 619-641.

Bousquet, Antoine. Cyberneticizing the American war machine: science and computers in the Cold War. Cold War History Vol. 8, No. 1 (February 2008), 77-102.

Boys, James D. The Clinton administration's development and implementation of cybersecurity strategy (1993–2001), Intelligence and National Security, Vol.33, No.5 (2018), 755-770.

Branch, Jordan. Mapping the Sovereign State: Technology, Authority, and Systemic Change. International Organization, Vol. 65 (Winter 2011), 1–36.

Brannon, Robert Russian Civil-Military Relations. Farnham, England: Routledge, 2009.

Brantly, Aaron F. The Cyber Deterrence Problem. In Minárik, T., Jakschis, R. and Lindström, L. (eds.) 10th International Conference on Cyber Conflict CyCon X: Maximising Effects. Tallinn: NATO CCD COE, 2018, 31-53.

Bratersky, Maxim. The Evolution of National Security Thinking in Post-Soviet Russia. Strategic Analysis, Vol. 40, No. 6 (2016), 513-523.

Brent, Laura. NATO's role in cyberspace. NATO Review, February 12th, 2019 [Online]. https://www.nato.int/docu/review/2019/Also-in-2019/natos-role-in-cyberspace-alliance-defence/EN/index.htm [Accessed: 1st May 2019].

Breslauer, George, Brada, Josef, Gaddy, Clifford G., Ericson, Richard, Saivetz, Carol and Winston, Victor. Russia at the End of Yel'tsin's Presidency, Post-Soviet Affairs, Vol.16, No.1 (2000), 1-32.

Brooks, Rosa. How everything became war and the military became everything. New York: Simon & Schuster, 2016.

Brooks, Stephen G. and Wohlforth, William C. Power, Globalization, and the End of the Cold War. Reevaluating a Landmark Case for Ideas. International Security, Vol. 25, No 3 (Winter 2000/2001), 5-53.

Brooks, Stephen G. and Wohlforth, William C. From Old Thinking to New Thinking in Qualitative Research. International Security, Vol. 26, No. 4 (Spring 2002), 93-111.

Brown, Chris and Ainley, Kirsten (eds.) Understanding International Relations (3rd ed.) Palgrave Macmillan: New York, 2005.

Bryant, William D. International Conflict and Cyberspace Superiority: Theory and Practice. New York: Routledge, 2016.

Buchan, Russell, Tsagourias, Nikolaos K. (eds.) Research Handbook on International Law and Cyberspace. Cheltenham: Edward Elgar Publishing, 2015.

Buchanan, Ben. Cryptography and Sovereignty, Survival, Vol. 58, No. 5 (2016), 95-122.

Budnitsky, Stanislav and Jia, Lianrui. Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. European Journal of Cultural Studies, Special Issue, 2018, 1-20.

Bueger, Christian and Gadinger, Frank. The Play of International Practice. International Studies Quarterly Vol. 59, No. 3 (2015), 449-460.

Bufacchi, V. Two Concepts of Violence. Political Studies Review, Vol. 3, No. 2 (2005) 193 - 204.

Bukkvoll, Tor. Iron Cannot Fight – The Role of Technology in Current Russian Military Theory, Journal of Strategic Studies, Vol. 34, No. 5 (2011), 681-706.

Bull, Hedley. Strategic Studies and Its Critics. World Politics, Vol. 20, No. 4 (1968), 593 – 605.

Burchill, Scott, Linklater Andrew, Devetak, Richard, Donnelly, Jack, Paterson, Matthew, Reus-Smith, Christian and True, Jacqui. Theories of International Relations (3rd), New York: Palgrave Macmillan, 2005.

Buzan, Barry, Wæver, Ole and de Wilde, Jaap: Security: A New Framework for Analysis. London: Lynne Rienne Publishers inc., 1998.

Buzan, Barry. 'Change and insecurity' reconsidered. Contemporary Security Policy, Vol. 20, No.3, 1999, 1-17.

Buzan, Barry. People, States and Fear. An agenda for international security studies in the post-cold war era. Colchester: ECPR Press, 2007.

Cadier, David and Light, Margot. Russia's Foreign Policy: Ideas, Domestic Politics and External Relations. New York: Palgrave Macmillan, 2015.

Cadier, David. Policies towards the Post-Soviet Space: The Eurasian Economic Union as an Attempt to Develop Russia's Structural Power? Cadier, David and Light, Margot (eds.) Russia's Foreign Policy. Ideas, Domestic Politics and External Relations. Basingstoke: Palgrave Macmillan, 2015, 156-174.

Caporaso, James A. Changes in the Westphalian Order: Territory, Public Authority, and Sovereignty. International Studies Review, Vol. 2, No. 2 (Summer 2000), 1-28.

Carlsnaes, Walter. Foreign Policy. In Carlsnaes, Walter, Risse, Thomas & Simmons, Beth A. (eds.) Handbook of International Relations. London: SAGE Publications, 2005, 331-349.

Carlsnaes, Walter, Risse, Thomas and Simmons, Beth A. (eds.) Handbook of International Relations. London: SAGE Publications, 2005.

Carlsnaes, Walter, Risse, Thomas and Simmons, Beth A. (Eds.) A Handbook of International Relations. London: SAGE Publications Ltd, 2013.

Carr, Jeffrey. Inside Cyber Warfare (2nd ed.) Sebastopol: O'Reilly, 2012.

Castells, Manuel. The Rise of the Network Society (2nd ed.) Chichester: Wiley-Blackwell, 2010.

Castro, Daniel and McQuinn, Alan. Unlocking Encryption: Information Security and the Rule of Law. ITIF, March 2016 [Online]. Available: http://www2.itif.org/2016-unlocking-encryption.pdf [Accessed: 11th August 2018].

Cebrowski, A. K. and Garstka, J. J. Network-Centric Warfare: Its Origin and Future. Proceedings Magazine, Vol. 124, No. 1 (1998), 28 - 35.

Cerf, Vinton G. On the Evolution of Internet Technologies. Proceedings of the IEEE, Vol. 92, No. 9, September 2004 [Online]. Available: http://www.ismlab.usf.edu/dcom/Ch5_Cerf_IEEE_2004_Evolution.pdf [Accessed: 9th August 2018].

Chandler, Daniel. Semiotics. The Basics. New York and London: Routledge, 2007.

Chapman, Bert. Military Doctrine: A Reference Handbook. California: ABC-CLIO LLC, 2009.

Checkel, Jeffrey. Ideas and International Political Change: Soviet/Russian Behavior at the End of the Cold War. New Haven: Yale University Press, 1997.

Checkel, Jeffrey. The Constructivist Turn in International Relations Theory. World Politics, Vol. 50, No. 2 (January 1998), 324-348.

Checkel, Jeffrey. Norms, Institutions, and National Identity in Contemporary Europe. International Studies Quartely, Vol. 43, No. 1 (March 1999), 83-114.

Checkel, Jeffrey. Social Learning and European Identity Change. International Organization, Vol. 55, No. 3 (Summer 2001), 553-588.

Checkland, Peter. Soft Systems Methodology: A Thirty Year Retrospective. Systems Research and Behavioral Science Syst. Res. Vol. 17 (2000), 11-58.

Chen, Jim. Cyberdeterrence by Engagement and Surprise. PRIMS, Vol. 7, No. 2 (2017), 100-107.

Chen, Jim. Effectively Exercising Deterrence in the Cyber Domain. In Chen, Jim Q. and Hurley, John S. (ed.) Proceedings of the 13th International Conference on Cyber Warfare and Security. National Defense University. Washington DC, USA. 8-9 March 2018, 120-125.

Chen, Jim Q. and Hurley, John S. (ed.) Proceedings of the 13th International Conference on Cyber Warfare and Security. National Defense University. Washington DC, USA. 8-9 March 2018.

Chernoff, Fred. Scientific Realism as a Meta-Theory of International Politics. International Studies Quarterly, Vol. 46, No. 2, (June 2002), 189–207.

Chotikul, Diane. The Soviet Theory of Reflexive Control in Historical and Psychological Perspective: A Preliminary Study. Monterey, CA: Naval Postgraduate School, 1986.

Choucri, Nazli. Cyberpolitics in International Relations. Cambridge: The MIT Press, 2012.

Choucri, Nazli and Clark, David D. Who controls cyberspace? Bulletin of the Atomic Scientists, Vol. 69, No. 5 (2013), 21-31.

Choucri, Nazli and Goldsmith, Daniel. Lost in cyberspace: Harnessing the Internet, international relations, and global security, Bulletin of the Atomic Scientists, Vol. 68, No. 2 (2012), 70-77.

Cimbala, S. J. Accidental/Inadvertent Nuclear War and Information Warfare. Armed Forces & Society, Vol. 25, No.4 (1999), 653 - 675.

Cimbala, Stephen J. The New Nuclear Disorder: Challenges to Deterrence and Strategy. London & New York: Routledge, 2015.

Cimbala, Stephen J. Nuclear deterrence and cyber warfare: coexistence or competition? Defense & Security Analysis, Vol. 33, No. 3 (2017), 193-208.

Clarke, R. A. and Knake, R. K. Cyber War: The Next Threat to National Security and What to Do About It. New York: Harper Collins, 2010.

Clarke, Richard A. and Knake, Robert K. The Fifth Domain. Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats. New York: Penguin Press, 2019.

Clough, Jonathan. A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization. Monash University Law Review, Vol. 40, No. 3 (2014), 698-736.

Cogburn, Derrick L. The Multiple Logics of Post-Snowden Restructuring of Internet Governance. In Musiani, Francesca, Cogburn, Derrick L., DeNardis, Laura and Nanette S. Levinson (eds.) The Turn to Infrastructure in Internet Governance. New York: Palgrave Macmillan, 2016, 25-45.

Collins, Jeffrey and Futter, Andrew (Eds.) Reassessing the Revolution in Military Affairs: Transformation, Evolution and Lessons Learned. New York: Palgrave Macmillian, 2015.

Connolly, Richard and Boulégue, Mathiue. Russia's New State Armament Programme. Implications for the Russian Armed Forces and Military Capabilities to 2027. Chatham House Research Paper, May 2018 [Online]. Available: https://www.chathamhouse.org/sites/default/files/publications/research/2018-05-10-russia-state-armament-programme-connolly-boulegue-final.pdf [Accessed: 29th April 2019].

Cooper, Jeffrey. Another View of the Revolution in Military Affairs, July 15, 1994 [Online]. http://ssi.armywarcollege.edu/pdffiles/00232.pdf [Accessed: 28th September 2018].

Cooper, Luke. Can contingency be 'internalized' into the bounds of theory? Critical realism, the philosophy of internal relations and the solution of 'uneven and combined development', Cambridge Review of International Affairs, Vol. 26, No. 3 (2013), 573-597.

Cooper, Julian. What If War Comes Tomorrow: Who Russia Prepares for Possible Armed Aggression, RUSI, Whitehall Report 4-16, 2016.

Cooper, Julian. Reviewing Russian Strategic Planning: The Emergence of Strategy 2020. NDC Research Review, 2012 [Online]. Available: http://www.ndc.nato.int/download/downloads.php?icode=338 [Accessed: 26th March 2019].

Cooper, Julian. (2018a) Strategic Planning, Situation Centres and the Management of Defence in Russia: An Update. Changing Character of War Centre, Pembroke College, Oxford [Online]. Available: http://www.ccw.ox.ac.uk/blog/2018/11/14/strategic-planning-situation-centres-and-the-management-of-defence-in-russia-an-update-by-julian-cooper [Accessed: 25th March 2019].

Cooper, Julian. (2018b) Russia's Invincible Weapons: Today, Tomorrow, Sometime, Never? Changing Character of War Centre, Pembroke College, Oxford [Online]. Available: http://www.ccw.ox.ac.uk/blog/2018/4/30/russias-invincible-weapons-today-tomorrow-sometime-never [Accessed: 30th October 2018].

Cottiero, Christina, Kucharski, Katherine, Olimpieva, Evgenia and Orttung, Robert W. War of words: the impact of Russian state television on the Russian Internet, Nationalities Papers, Vol.43, No.4 (2015), 533-555.

Cozette, Murielle. What Lies Ahead: Classical Realism on the Future of International Relations. International Studies Review, Vol. 10, No. 4 (December 2008), 667–679.

Collier, David, Hidalgo, Fernando Daniel and Maciuceanu, Andra Olivia. Essentially contested concepts: Debates and applications. Journal of Political Ideologies Vol. 11, No. 3 October 2006), 211–246.

Coopersmith, Jonathan. The Dog That Did Not Bark during the Night: The "Normalcy" of Russian, Soviet, and Post-Soviet Science and Technology Studies. Technology and Culture, Vol. 47, No. 3 (July 2006), 623-637.

Covington, Stephen R. The Culture of Strategic Thought Behind Russia's Modern Approaches to Warfare. Cambridge: Harvard Kennedy School, Belfer Center, 2016.

Creveld Van, M. The Transformation of War. New York: The Free Press, 1991.

Czosseck, C., Ottis, R. and Ziolkowski, K. (eds.) 4th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, 2012.

Darby, Philip. A Disabling Discipline. In Reus-Smith, Christian and Snidal, Duncan. The Oxford Handbook of International Relations. Oxford University Press: Oxford, 2010, 94-105.

Davis Cross, M.K. Rethinking epistemic communities twenty years later. Review of international studies, Vol. 39, No. 1 (2013), 137-160.

de Haas, Marcel. Relations of Central Asia with the Shanghai Cooperation Organization and the Collective Security Treaty Organization. The Journal of Slavic Military Studies, Vol.30, No.1 (2017), 1-16.

de Haas, Marcel. An analysis of Soviet, CIS and Russian military doctrines 1990–2000, The Journal of Slavic Military Studies, Vol.14, No.4 (2001), 1-34.

de Rosnay, Joël. The Macroscope A new world scientific system. New York: Harper & Row Publishers, 1975 [Online]. Available: http://pespmc1.vub.ac.be/macroscope/ [Accessed: 23rd September 2019].

Dear, Keith. Will Russia Rule the World Through AI?, The RUSI Journal, Vol. 164, No. 5-6 (2019), 36-60.

del Portillo, Inigo, Barrios, Cameron, Bruce, Crawley, Edward. Ground segment architectures for large LEO constellations with feeder links in EHF-bands. 2018 IEEE Aerospace Conference. [Online]. Available: https://www.researchgate.net/publication/326072504_Ground_segment_architectures_for_large_LEO_constellations_with_feeder_links_in_EHF-bands [Accessed: 17th May 2019].

Demchak, Chris and Dombrowski, Peter. Rise of the Cybered Westphalian Age. Strategic Studies Quarterly, Vol. 5, No. 1 (Spring 2011), 32-61.

Demchak, Chris. Cybered Conflict, Cyber Power, and Security Resilience as Strategy. In Reveron, Derek (ed.) Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Washington, D.C.: Georgetown University Press, 2012, 121-136.

Demchak, Chris and Dombrowski, Peter. Cyber Westphalia. Asserting State Prerogatives in Cyberspace. Georgetown Journal of International Affairs, Volume International Engagement on Cyber III, 2013, 29-38.

Demchak, Chris. Cybered Conflict, Cyber Power, and Security Resilience as Strategy. In: Cyberspace and National Security. Washington D.C.: Georgetown University Press, 2012, 121-136.

Demchak, Chris. Uncivil and Post-Western Cyber Westphalia Changing interstate power relations of thecybered age. The Cyber Defense Review, Vol. 1, No. 1 (SPRING 2016), 49-74.

Demchak, Chris C. and Shavitt, Yuval. China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking." Military Cyber Affairs: Vol. 3, No. 1 (2018), Article 7.

DeNardis, Laura. The Global War for Internet Governance. New Haven: Yale University Press, 2014.

Denning, Dorothy. Reflections on Cyberweapons Controls. Computer Security Journal, Vol. XVI, No. 4 (Fall 2000), 43-53.

Denning, Dorothy. Is Cyber Terror Next? In Calhoun, Craig, Price, Paul and Timmer, Ashley (eds) Understanding September. New York: The New Press, 2002.

Darczewska, Jolanta. The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study. Warsaw: Centre for Eastern Studies, 2014.

Desch, Michael C. Culture Clash. Assessing the Importance of Ideas in Security Studies. International Security, Vol. 23, No. 1 (Summer 1998), 141-170.

De Souza, Denise E. Culture, context and society – The underexplored potential of critical realism as a philosophical framework for theory and practice. Asian Journal of Social Psychology, Vol. 17 (2014), 141-151.

Devost, M. G., Houghton, B. K. and Pollard, N. A. Information terrorism: Political violence in the information age. Terrorism and Political Violence, Vol. 9, No. 1, (1997), 72 – 83.

Deyermond, Ruth. The Collective Security Treaty Organization. In Tsyganov, Andrei P. Routledge Handbook of Russian Foreign Policy. London and New York: Routledge, 2018, 421-429.

Digiser, Peter. Fourth Face of Power. The Journal of Politics, Vol. 54, No. 4 (1992), 977-1007.

Dodd, Annabel Z. The Essential Guide to Telecommunications (5th ed.) Upper Saddle River, NJ: Prentice Hall, 2012.

Dombrowski, Peter and Demchak, Chris. Cyber War, Cybered Conflict, and the Maritime Domain. Naval War College Review, Vol. 67, No. 2 (2014), 71-96.

Donaldson, Robert H., Nogee, Joseph L. and Nadkari, Vidya. The Foreign Policy of Russia: Changing Systems, Enduring Interests. New York: M.E. Sharpe, 2014.

Donaldson, Robert H. and Nadkarni, Vidya. The Foreign Policy of Russia. Changing Systems, Enduring Interests (6th ed.) New York & London: Routledge, 2019.

Donnelly, Christopher. Red Banner. The Soviet Military System in Peace and War.Coulsdon: Jane's Information Group, 1988.

Donnelly, Jack. Realism. In Burchill, Scott, Linklater Andrew, Devetak, Richard., Donnelly, Jack. Paterson, Matthew, Reus-Smith, Christian and True, Jacqui. Theories of International Relations (3rd), New York: Palgrave Macmillan, 2005, 29-54.

Duffield, John S., Farrell, Theo, Price, Richard and Desch, Michael C. Correspondence—Isms and Schisms: Culturalism versus Realism in Security Studies. International Security, Vol. 24, No. 1 (Summer 1999) 156-180.

Duffield, John S. World Power Forsaken: Political Culture, International Institutions, and German Security Policy After Unification. Stanford, CA: Stanford University Press, 1998.

Dunn Cavelty, M. From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. International Studies Review, Vol. 15, No. 1 (2013), 105 – 122.

Dunn Cavelty, Myriam and Wenger, Andreas. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, Vol. 41, No. 1 (2020), 5-32.

Dunn, John A. Lottizzazione Russian Style: Russia's Two-tier Media System, Europe-Asia Studies, Vol.66 No. 9 (2014), 1425-1451.

Dunne, Tim, Kurki, Milja and Smith, Steven (eds.) International Relations Theories: Discipline and Diversity (4th ed.) Oxford: Oxford University Press, 2013.

Duyvesteyn, I. Exploring the utility of force: some conclusions. Small Wars & Insurgencies, Vol. 19, No. 3 (2008), 423 – 443.

Echevarria II, Antulio J. Strategic Culture Is Not a Silver Bullet. Naval War College Review, Vol. 70, No. 4 (Autumn 2017), 121-124.

Edwards, Matthew (ed.) Critical Infrastructure Protection. NATO Science for Peace and Security Series. Amsterdam: IOS Press, 2014.

Eitelhuber, Norbert. The Russian Bear: Russian Strategic Culture and What it Implies for the West. Connections, Vol. 9, No. 1 (Winter 2009), 1-28.

Elkins, David J. and Simeon, Richard E. B. A Cause in Search of Its Effect, or What Does Political Culture Explain? Comparative Politics, Vol. 11, No. 2 (1979), 127-128.

Elman, Colin and Jensen, Michael A. Realism. In Williams, Paul D.: Security Studies: An Introduction (2nd ed.) New York: Routledge, 2013, 15-31.

Endresen, R. S. Hard Power in Cyberspace: CNA as a Political Means. In Pissanidis, N., Rõigas, H., Veenendaal, M. (Eds.) 8th International Conference on Cyber Conflict: Cyber Power. Tallinn: NATO CCD COE, 2016, 23-36.

Engström, Maria. Contemporary Russian Messianism and New Russian Foreign Policy, Contemporary Security Policy, Vol. 35, No. 3 (2014), 356-379.

Ericson, Richard, Lapidus, Gail, Breslauer, George, Matlock, Jack S., Starr, Frederick & Winston, Victor. Six Years After the Collapse of the USSR, Post-Soviet Affairs, Vol.14, No.1 (1998), 1-22.

Ermoshina, Ksenia and Musiani, Francesca. Migrating Servers, Elusive Users: Reconfigurations of the Russian Internet in the Post-Snowden Era. Media and Communications, Vol. 5, No. 1 (2017), 42-53.

Esin, Viktor. Russia's air-space force and armaments program. In Arbatov, Alexei and Dvorkin, Vldimir (Eds.) Missile Defense: Confrontation and Cooperation. Moscow: Carnegie Moscow Center, 2013, 147-166.

Faleg, Giovanni. Between knowledge and power: epistemic communities and the emergence of security sector reform in the EU security architecture. European Security, Vol.21, No. 2 (2012), 161-184.

Fall, Kevin R. and Stevens, Richard W. TCP/IP Illustrated, Volume 1: The Protocols (2nd ed.) Upper Saddle River NJ: Addison-Wesley, 2012.

Farrell, Theo. Constructivist Security Studies: Portrait of a Research Program. International Studies Review, Vol. 4, No. 1 (Spring 2002), 49-72.

Fast Scott, Harriet. Soviet Military Doctrine in the Nuclear Age, 1945-1985. In Frank, Willlard, C. and Gillette, Philip S. (Eds.) Soviet Military Doctrine from Lenin to Gorbachev, 1915-1991. Westport, Connecticut: Greenwood Press, 1992, 175-192.

Feaver, Peter D., Hellman, Gunther, Schweller, Randall L., Taliaferro, Jeffrey W., Wohlforth, William C., Legro, Jeffrey W. and Andrew Moravcsik. Brother, Can You Spare a Paradigm? (Or Was Anybody Ever a Realist?). International Security, Vol. 25, No. 1 (Summer 2000), 165-93.

Fernandes, Sandra. Putin's Foreign Policy towards Europe: Evolving Trends of an (Un)Avoidable Relationship. In Kanet, Roger E. and Piet, Rémi (eds.) Shifting Priorities in Russia's Foreign and Security Policy. Surrey: Ashgate Publishing Limited, 2014, 13-34.

Fierke, K. M. Constructivism. In Dunne, Tim, Kurki, Milja and Smith, Steven: International Relations Theories: Discipline and Diversity (4th ed.) Oxford: Oxford University Press, 2013, 161-178.

Finel, Bernard I. Black Box or Pandora's Box: State Level Variables and Progressivity in Realist Research Programs. Security Studies, Vol. 11, No. 2 (Winter 2001/2) 187-227.

Fink, Anya Loukianova. The Evolving Russian Concept of Strategic Deterrence: Risks and Responses. Arms Control Today, Vol. 47, No. 6 (Jul/Aug 2017), 14-20.

Finnemore, Martha and Sikkink, Kathryn. International Norm Dynamics and Political Change. International Organization, Vol. 52, No. 4, (Autumn, 1998), 887-917.

Fischerkeller, Michael. Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies, Survival, Vol.59, No.1 (February-March 2017), 103-134.

Fitzgerald, Mary. Changing Soviet Doctrine on Nuclear War. Research memorandum AD-A187 722. Alexandria, Virginia: Center for Naval Analyses, 1986.

Fitzgerald, Mary C. (1987a) Marshal Ogarkov and the New Revolution in Soviet Military Affairs. Alexandria, Virginia: CNA, 1987.

Fitzgerald, Mary C. (1987b) Marshal Ogarkov on Modern War: 1977-1985. Alexandria, Virginia: CNA, 1987.

Fitzgerald, Mary C. (1987c) Soviet views on SDI. The Carl Beck Papers in Russian and East European Studies No. 601. Pittsburgh: University of Pittsburgh Center for Russian and East European Studies, 1987.

Fitzgerald, Mary C. The Dilemma in Moscow's Defensive Force Posture. In Frank, Willlard, C. and Gillette, Philip S. Soviet Military Doctrine from Lenin to Gorbachev, 1915-1991. Westport, Connecticut: Greenwood Press, 1992, 347-362.

Fitzgerald, Mary C. The Soviet Image of Future War: The Impact of Desert Storm. In Frank, Willlard, C. and Gillette, Philip S. Soviet Military Doctrine from Lenin to Gorbachev, 1915-1991. Westport, Connecticut: Greenwood Press, 1992, 363-386.

Fitzgerald, Mary. Russian Views on IW, EW, and Command and Control: Implications for the 21st Century. CCRTS 1999. U.S. Naval War College, Rhode Island. June 29 - July 1, 1999 [Online] Available: http://www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/089fitzg.pdf [Accessed 5th August 2018].

Forrest E. Morgan, Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter and Roger Cliff. Dangerous Thresholds: Managing Escalation in the 21st Century. Santa Monica: RAND, 2008.

Forsberg, Tuomas and Haukkala, Hiski. The European Union. In Tsyganov, Andrei P. Routledge Handbook of Russian Foreign Policy. London and New York: Routledge, 2018, 269-281.

Foulon, Michael. Neoclassical Realism: Challengers and Bridging Identities. International Studies Review. Vol. 17 (2015), 635-661.

Frank, Willlard, C. and Gillette, Philip S. (Eds.) Soviet Military Doctrine from Lenin to Gorbachev, 1915-1991. Westport, Connecticut: Greenwood Press, 1992.

Freedman, Lawrence. Strategy: A History. Oxford: Oxford University Press, 2013.

Freedman, Lawrence. A Western way of war? Adelphi Papers, Vol. 38, No. 318 (2008), 11-17.

Freedman, Lawrence. The Evolution of Nuclear Strategy (3rd ed.) New York: Palgrave Macmillian, 2003.

Freedman, Lawrence. The Revolution in Strategic Affairs. The Adelphi Papers, Vol. 45, No. 379, 2006.

Freedman, Lawrence. Strategic Studies and the problem of power. In Mahnken, Thomas G. and Maiolo Joseph A. Strategic Studies: A Reader, Routledge, New York, 2014, 9-21.

Fredrichs, Brian E. Information Warfare at hthe Crossroads. Joint Forces Quarterly, Summer 1997, 97-103 [Online]. Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a529170.pdf [Accessed: 14th November 2018].

Freyberg-Inan, Annette, Ewan Harrison, and Patrick James (eds.) Rethinking Realism in International Relations: Between Tradition and Innovation.. Baltimore, MD: The Johns Hopkins University Press, 2009.

Friis, Karsten and Ringsmose, Jens (eds.) Conflict in Cyber Space: Theoretical, strategic and legal perspectives. New York: Routledge, 2016.

Frieden, Jeffry. Actors and Preferences in International Relations. In Lake, David and Powell, Robert (eds.) Strategic Choice and International Relations. Princeton: Princeton University Press, 1999, 39-76.

Friedrichs, J. and Kratochwil, F. On Acting and Knowing: How Pragmatism Can Advance International Relations Research and Methodology. International Organization, Vol. 63, No. 4 (Fall, 2009), 701-731.

Gaddis, John Lewis. The Cold War: A New History. New York: Penguin Books, 2005.

Galeotti, Mark. (2016a) Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right, Mayak Intelligence, 2016.

Galeotti, Mark. (2016b) Heavy Metal Diplomacy: Russia´s Political Use of Its Military in Europe Since 2014. ECFR, December 2016.

Galeotti, Mark. I'm Sorry for Creating the 'Gerasimov Doctrine'. Foreign Policy, 5 March 2018 [Online]. Available: https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/ [Accessed: 7th November 2018].

Gareev, Makhmut. If War Comes Tomorrow? The Contours of Future Armed Conflict. London & New York: Routledge, 1998 (org. 1995).

Gariup, Monica. European Security Culture: Language, Theory, Policy. Surrey: Ashgate, 2009.

Garthoff, Raymond L. Deterrence and the Revolution in Soviet Military Doctrine. Washington D.C.: The Brookings Institution, 1990.

Garthoff, Raymond L. New Thinking and Soviet Military Doctrine. In Frank, Willlard, C. and Gillette, Philip S. Soviet Military Doctrine from Lenin to Gorbachev, 1915-1991. Westport, Connecticut: Greenwood Press, 1992, 195-209.

Gartzke, Erik. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. International Security, Vo. 38, No. 2 (Fall 2013), 41-73.

Gartzke, E. J. and Lindsay, J. R. Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. Security Studies, Vol. 24, No. 2 (2015), 316-348.

Gartzke, Erik and Lindsay, John. Cybersecurity and Cross-Domain Deterrence: The Consequences of Complexity [draft], 2016 [Online]. Available: http://deterrence.ucsd.edu/_files/LindsayGartzke_ConsequencesofComplexity_Draft.pdf [Accessed: 16th August 2018].

Geers, Kenneth. The Cyber Threat to National Critical Infrastructures: Beyond Theory. Information Security Journal: A Global Perspective, Vol. 18, No. 1 (2009), 1 - 7.

Geers, Kenneth. Strategic Cyber Security. Tallinn: NATO CCD COE, 2011.

Geers, Kenneth (ed.) Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn: CCDCOE, 2015.

Geertz, Clifford. The Interpretation of Cultures. New York: Basic Books, 1973.

Geist, Edward. Deterrence Stability in the Cyber Age. Strategic Studies Quarterly, Vol. 9, No. 4 (Winter 2015), 44-61.

Geist, Edward M. Armageddon Insurance. Civil Defense in the United States and Soviet Union, 1945-1991. Chapel Hill: University of Northern Carolina Press, 2019.

Gelman, Harry. Reconstructing the Soviet Perspective on U.S. Global Policy. In Nerlich, Uwe (ed.) Soviet Power and Western Negotiating Policies. Volume I: The Soviet Asset: Military Power in the Competition Over Europe. Cambridge, Massachusetts: Ballinger Publishing Company, 1983, 277-305.

George, Alexander L. and Bennett, Andrew. Case Studies and Theory Development in the Social Sciences. Cambridge: MIT Press, 2004.

Gerovitch, Slava. InterNyet: why the Soviet Union did not build a nationwide computer network. History and Technology Vol. 24, No. 4 (December 2008), 335–350.

Gerovitch, Slava. From Newspeak to Cyberspeak: A History of Soviet Cybernetics. Cambridge: The MIT Press, 2002.

Giampiero, Giampiero (ed.) Security in Cyberspace. Targeting Nations, Infrastructures, Individuals. New York: Bloomsbury Academic, 2014.

Giddens, Anthony. The Constitution of Society: Outline of the Theory of Structuration. Cambridge: Polity Press, 1984.

Giles, Keir. Russia's Public Stance on Cyberspace Issues. In Czosseck, C., Ottis, R. and Ziolkowski, K. (Eds.) 4th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, 2012, 63-76.

Giles, Keir. A New Phase in Russian Military Transformation, The Journal of Slavic Military Studies, Vol. 27 No.1 (2014), 147-162.

Giles, Keir. (2016a) Handbook of Russian Information Warfare. Fellowship monograph 9. Rome: NATO Defence College, 2016.

Giles, Kier. (2016b) The Next Phase of Russian Information Warfare. Research paper. Riga: NATO STRATCOM COE, 2016.

Giles, Keir. (2016c) Russia´s ´New´ Tools for Confronting the West – Continuity and Innovation in Moscow´s Exercise of Power. Chatham House, Russia and Eurasia Programme, March 2016.

Giles, Keir and Hagestad II, William. Divided by a Common Language: Cyber Definitions in Chinese, Russian and English. In K. Podins, J. Stinissen, M. Maybaum (Eds.) 5th International Conference on Cyber Conflict 2013 - Proceedings. NATO CCD COE Publications, Tallinn, 2013, 413-429.

Giles, Keir and Monaghan, Andrew. Legality in Cyberspace: An Adversary View. The Letort Papers, Strategic Studies Institute March 2014. Carlisle, PA: U.S. Army War College, 2014.

Gill, Stephen. Power and Resistance in the New World Order (2nd ed.) New York: Palgrave Macmillan, 2008.

Glantz, David M. The Military Strategy of the Soviet Union: A History. Abingdon, Oxon: Frank Cass, 1992.

Glaser, Charles L. The Security Dilemma Revisited. World Politics, Vol. 50, No. 1 (1997), 171 – 201.

Glaser, Charles L. Rational Theory of International Politics: The Logic of Competition and Cooperation. Princeton: Princeton University Press, 2010.

Glanville, Luke. The Myth of 'Traditional' Sovereignty. International Studies Quarterly, Vol. 57 (2013), 79-90.

Glenn, Chafetz Michael Spirtas, and Benjamin Frankel. Introduction: Tracing the Influence of Identity on Foreign Policy. Security Studies, Vol. 8 (Winter 1998/99–Spring 1999), vii-xxii.

Glenn, John. Realism versus Strategic Culture: Competition and Collaboration? International Studies Review, Vol. 11, No. 3 (2009), 523-551.

Gentry, John A. Norms and Military Power: Nato's War Against Yugoslavia, Security Studies, Vol. 15, No. 2 (2006), 187-224.

Godzimirski, Jakub M. Russian national security concepts 1997 and 2000: A comparative analysis, European Security, Vol. 9, No. 4 (Winter 2000), 73-91.

Goldstein, Judith and Keohane, Robert O. (eds.) Ideas and Foreign Policy: Beliefs, Institutions, and Political Change. Ithica: Cornell University Press, 1993.

Golts, Aleksandr. Military Reform and Militarism in Russia. Washington, D.C.: The Jamestown Foundation, 2019.

Golts, Alexander M. and Putnam, Tonya L. State Militarism and Its Legacies: Why Military Reform Has Failed in Russia. International Security, Vol. 29, No. 2 (Fall 2004), 121-158.

Gompert, David C. and Libicki, Martin. Cyber War and Nuclear Peace. Survival, Vol. 61, No.4 (2019), 45-62.

Gorham, Michael S., Lunde, Ingunn and Paulsen, Amrtin (eds.) Digital Russia: The Language, Culture and Politics of New Media Communication. London & New York: Routledge, 2014.

Gorny, Eugene. A Creative History of the Russian Internet. Studies in Internet Creativity., Berlin: DVM Verlag Dr. Muller, 2009.

Gorodetsky, Gabriel. The Formulation of Soviet Foreign Policy – Ideology and Realpolitik. In Gorodetsky, Gabriel (Ed.) Soviet Foreign Policy 1917-1991 A Retrospective. London: Frank Cass, 1994, 30-44.

Gorodetsky, Gabriel (Ed.) Soviet Foreign Policy 1917-1991 A Retrospective. London: Frank Cass, 1994.

Gow, James. The Essence of Strategy: Constructivist realism and necessity. In Wilkinson, Benedict and Gow, Jameson (eds.) The Art of Creating Power: Freedman on Strategy. London: Hurst & Company, 2017, 259-278.

Grau, Lester and Bartles, Charles. The Russian Way of War. Fort Leavenworth, KS.: FMSO, 2016.

Grau, Lester W. and Bartles, Charles K. (2018a) The Russian Reconnaissance Fire Complex Comes of Age. Changing Character of War Centre, Pembroke College, Oxford [Online]. Available: http://www.ccw.ox.ac.uk/blog/2018/5/30/the-russian-reconnaissance-fire-complex-comes-of-age [Accessed: 30th October 2018].

Grau, Lester W. and Bartles, Charles K. (2018b) Factors Influencing Russian Force Moderation. Changing Character of War Centre, Pembroke College, Oxford [Online]. Available: http://www.ccw.ox.ac.uk/blog/2018/9/19/factors-influencing-russian-force-modernization-by-dr-lester-grau-and-charles-k-bartles [Accessed: 30th October 2018]. Separate territorial troops were considered in the early-2000s.

Gray, Colin S. What Rand Hath Wrought. Foreign Policy, No. 4 (Autumn 1971), 111-129.

Gray, Colin. Soviet nuclear strategy and new military thinking. In Leebaert, Derek and Dickinson, Timothy (eds.) Soviet Strategy and the New Military Thinking. Cambridge: Cambridge University Press 1992, 28-54.

Gray, Colin S. (1999a) Modern Strategy. Oxford: Oxford University Press, 1999.

Gray, Colin S. (1999b) Strategic Culture as Context: the First Generation of Theory Strikes Back. Review of International Studies, Vol. 25, No. 1 (January 1999), 49-69.

Gray, Colin S. Out of the Wilderness: Prime Time for Strategic Culture. Comparative Strategy, Vol. 26, No. 1 (2007), 1-20.

Gray, Colin, S. War, Peace and International Relations: An Introduction to Strategic History. New York: Routledge, 2007.

Green, Brendan R. and Long, Austin. The MAD Who Wasn't There: Soviet Reactions to the Late Cold War Nuclear Balance, Security Studies, Vol.26, No.4 (October-December 2017), 606-641.

Green, James A (ed.) Cyber Warfare: A multidisciplinary analysis. New York: Routledge, 2015.

Greiman, Virginia, Cyber Security and Global Governance. In Abouzakher, Nasser (ed.) Proceedings of the 14th European Conference on Cyber Warfare & Security. Hattfield: University of Hertfordshire, 2015, 71-78.

Griffiths, James. The Great Firewall of China: How to Build and Control an Alternative Version of the Internet. London: Zed Books Ltd., 2019.

Grigas, Agnia. Beyond Crimea. The New Russian Empire. New Haven: Yale University Press, 2016.

Guerlac, H. Vauban: The Impact of Science of War. In Paret, Peter (ed.) Makers of Modern Strategy from Machiavelli to the Nuclear Age. New York: Oxford University Press, 1990, 64-90.

Gunnell, John G. Realizing Theory: The Philosophy of Science Revisited. The Journal of Politics, Vol. 57, No. 4 (November 1995), 923-940.

Gustafson, K. C. Echo of Empires: Russia's Inheritance of Byzantine Security Culture. The Journal of Slavic Military Studies, Vol. 23, No. 4 (2010), 574-596.

Guzzini, Stefano. The Limits of Neorealist Power Analysis. International Organization, Vol. 47, No. 3 (1993), 443-478.

Guzzini, Stefano. Power, Realism and Constructivism. London and New York: Routledge, 2013.

Guzzini, Stefano and Leander, Anna. A Social Theory for International Relations: An Appraisal of Alexander Wendt's Theoretical and Disciplinary Synthesis. Journal of International Relations & Development, Vol. 4, No. 4, (December 2001), 316-338.

Gvosdev, Nikolas K. and Marsh, Christopher. Russian Foreign Policy: Interests, Vectors, and Sectors. Los Angeles: SAGE Publications, Inc., 2014.

Haas, Peter M. Introduction: Epistemic Communities and International Policy Coordination. International Organization, Vol. 46 (1992), 1-35.

Habermas, J., Lennox, S. and Lennox, F. The Public Sphere: An Encyclopedia Article (1964). New German Critique, No. 3 (Autumn, 1974), 49-55.

Hall, Ian. What Causes What: The Ontologies of Critical Realism (Review). International Studies Review, Vol. 11, No. 3 (September 2009), 629–630.

Hamati-Ataya, Inanna. Beyond (Post)Positivism: The Missed Promises of Systemic Pragmatism. International Studies Quarterly, Vol. 56, No. 2 (June 2012), 291-305.

Hammond, Debora. The Science of Synthesis. Exploring the Social Implications of General Systems Theory. Boulder: The University Press of Colorado, 2003.

Hammes, T. X. The Sling and the Stone: On War in the 21st Century. St Paul: Zenith Press, 2006.

Handel, M. Masters of War: Classical Strategic Thought. London: Frank Cass, 1996.

Hare, F. The Significance of Attribution to Cyberspace Coercion: A Political Perspective. In Czosseck, C., Ottis, R. and Ziolkowski, K. (eds.) 4th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, 2012, 125 - 140.

Hare, Forrest B. Precision cyber weapon systems: An important component of a responsible national security strategy? Contemporary Security Policy, Vol. 40, No. 2 (2019), 193-213.

Harknett, Richard J. and Nye, Joseph S. Jr. Correspondence – Is Deterrence Possible in Cyberspace. International Security, Vol. 42, No. 2 (2017), 196-199.

Harrop, Wayne and Matteson, Ashley. Cyber Resilience: A Review of Critical National Infrastructure and Cyber-Security Protection Measures Applied in the UK an USA The White House. In Lemieux, Frederick (ed.) Current and Emerging Trends in Cyber Operations. Policy, Strategy and Practice. New York: Palgrave Macmillian, 2015, 149-166.

Haslam, Jonathan. Near and Distant Neighbours. Oxford: Oxford University Press, 2015.

Hayden, Michael V. The Future of Things "Cyber. Strategic Studies Quarterly, Vol. 5, No. 1 (Spring 2011), 3-7.

Heickerö, Roland. Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations. Stockholm: FOI, 2010.

Heickero, Roland. Russia's Information Warfare Capabilities. In Lemieux, Frederick (ed.) Current and Emerging Trends in Cyber Operations. Policy, Strategy and Practice. New York: Palgrave Macmillian, 2015, 65-83.

Hellman, Gunther (ed.) Pragmatism and International Relations. International Studies Review, Vol. 11, No. 3 (September 2009), 638–662.

Herd, Graeme P. The Battle of ideas, Concepts and Geopolitical Projects in Central Asia: Implications for Russo-Chinese Relations? In Kanet, Roger E. and Piet, Rémi (eds.) Shifting Priorities in Russia's Foreign and Security Policy. Surrey: Ashgate Publishing Limited, 2014, 183-203.

Herspring, Dale R. Vladimir Putin and Military Reform in Russia, European Security, Vol.14, No.1 (2005), 137-155.

Herspring, Dale R. The Kremlin and the High Command: Presidential Impact on the Russian Military from Gorbachev to Putin. Lawrence, KS: University Press of Kansas, 2006.

Hill, Christopher and Light, Margot. Foreign Policy Analysis. In Light, Margot and Groom, A. J. R. International Relations: A Handbook of Current Theory. London: Bloomsbury Academic, 1985, 156-173.

Hill, Fiona. How Vladimir Putin's World View Shapes Russian Foreign Policy. In Cadier, David and Light, Margot. Russia's Foreign Policy: Ideas, Domestic Politics and External Relations. New York: Palgrave Macmillan, 2015, 42-61.

Hines, John G. and Mahoney, Donald. Defense and Counteroffensive Under the New Soviet Military Doctrine. Santa Monica: RAND Corporation, 1991.

Hines, John G., Mishulovich, Ellis M. and Shull, John F. (1995a) Soviet Intentions 1965-1985. Volume I: An Analytical Comparison of U.S.-Soviet Assessments During the Cold War. McLean, VA: The BDM Corporation, 1995.

Hines, John G., Mishulovich, Ellis M. and Shull, John F. (1995b). Soviet Intentions 1965-1985. Volume II: Soviet Post-Cold War Testimonial Evidence. McLean, VA: The BDM Corporation, 1995.

Hoffenaar, Jan and Findlay, Christopher (eds.) Military Planning For European Theatre Conflict During The Cold War. An Oral History Roundtable Stockholm, 24–25 April 2006. ETH Zurich: Center for Security Studies, 2007.

Hoffman, Frank. Strategic Culture and Ways of War: elusive Fiction or Essential Concept? Naval War College Review, Vol. 70, No. 2 (Spring 2017), 137-142.

Hoffman, David E. The Dead Hand. The Untold Story of the Cold War Arms Race and Its Dangerous Legacy. New York: Anchor Books, 2009.

Hollis, Martin and Smith, Steve. Explaining and Understanding International Relations. Oxford: Clarendon Press, 1990.

Honkova, Jana. The Russian Federation's Approach to Military Space and Its Military Space Capabilities. Arlington, VA: George Marshall Institute, 2013.

Hopf, Ted. Social Construction of International Politics: Identities and Foreign Policies, Moscow, 1955 and 1999. Ithaca, NY: Cornell University Press, 2002.

Huchthausen, Peter A. and Sheldon-Duplaix, Alexandre. Hide and Seek: The Untold Story of Cold War Naval Espionage. New Jersey, John Wiley & Sons, Inc., 2009.

Hudson, Valerie M. and Vore, Christopher S. Foreign Policy Analysis Yesterday, Today, and Tomorrow. Meshon International Studies Review, Vol. 39 (1995), 209-238.

Hurd, Ian. Constructivism. In Reus-Smith, Christian and Snidal, Duncan (eds.) The Oxford Handbook of International Relations. Oxford University Press: Oxford, 2010, 298-316.

Inkster, N. China's Cyber Power. New York: Routledge, 2016.

Inkster, Nigel. Measuring Military Cyber Power, Survival, Vol. 59, No. 4 (2017), 27-34.

Jackson, Patrick Thaddeus and Nexon, Daniel H. Constructivist Realism or Realist Constructivism. International Studies Review Vol. 6, No. 2 (2004), 337-352.

Jackson, Patrick Thaddeus. Civilizing the Enemy: German Reconstruction and the Invention of the West. Ann Arbor: University of Michigan, 2006.

Jackson, Patrick Thaddeus and Nexon, Daniel H. Paradigmatic Faults in International-Relations Theory. International Studies Quarterly Vol. 53, No. 4, (December 2009), 907-930.

Jackson, Patrick Thaddeus. Situated Creativity, or, the Cash Value of a Pragmatist Wager for IR. In Gunther, Hellman (ed.) Pragmatism and International Relations. International Studies Review, Vol. 11, No. 3 (September 2009), 656-659.

Jackson, Patrick Thaddeus. The conduct of inquiry in International Relations: philosophy of science and its implications for the study of world politics. London and New York: Routledge, 2011.

Jackson, Patrick Thaddeus. Fear of Relativism. International Studies Perspectives, Vol. 16 (2015), 13-22.

Jackson, William D. Encircled Again. Russia's Military Assesses Threats in a Post-Soviet World. Political Science Quarterly, Vol. 117, No. 3 (Autumn, 2002), 373-400.

Jacobsen, C.G. (ed.) Strategic Power: USA/USSR. New York: St Martin's Press, 1990.

Jacobsen, Kurt. Much Ado about Ideas: The Cognitive Factor in Economic Policy. World Politics, Vol. 47 (1995), 283-310.

Jaitner, Margarita and Rantapelkonen, Jari. Russian Struggle for Sovereignty in Cyberspace. Tiede ja Ase, Vol. 71 (2013), 64-89.

Jensen, Benjamin M. The role of ideas in defense planning: revisiting the revolution in military affairs. Defence Studies, Vol.18, No.3 (2018), 302-317.

Jensen, Benjamin, Valeriano, Brandon and Maness, Ryan. Fancy bears and digital trolls: Cyber strategy with a Russian twist, Journal of Strategic Studies, Vol. 42, No. 2 (2019), 212-234.

Jervis, Robert. Review: Deterrence Theory Revisited. World Politics, Vol. 31, No. 2 (January 1979), 289-324.

Jervis, Robert. Cooperation Under the Security Dilemma. World Politics, Vol. 30, No. 2 (January 1978), 167-214.

Jervis, Robert. Dilemmas About Security Dilemmas. Security Studies, Vol. 20, No. 3 (2011), 416–423.

Johnson, James. China's vision of future network-centric battlefield: Cyber, space and electromagnetic asymmetric challenges to the United States. Comparative Strategy, Vol. 37, No. 5 (2018), 373-390.

Johnston, Alastair Iain. Thinking about Strategic Culture. International Security, Vol. 19, No. 4 (Spring 1995), 32-64.

Johnston, Alastair John. Cultural Realism and Strategy in Maoist China. In Katzenstein, Peter J. (ed.) The Culture of National Security: Norms and Identity in World Politics. New York: Columbia University Press, 1996, 216-268.

Johnston, Alastair Iain. Strategic Cultures Revisited: Reply to Colin Gray. Review of International Studies, Vol. 25, No. 3 (July 1999), 519-523.

Jonathan, Joseph and Wight, Colin (eds.) Scientific Realism and International Relations. Basingstoke: Palgrave, 2010.

Jones, A. and Kovacich, G. Global Information Warfare: The New Digital Battlefield. Boca Raton: CRC Press, 2016.

Jonsson, Oscar and Seely, Robert. Russian Full-Spectrum Conflict: An Appraisal After Ukraine, Journal of Slavic Military Studies, Vol.28, No. 1 (2015), 1-22.

Jonsson, Oscar. The Understanding of War. Blurring the Lines between War and Peace. Washington, D.C.: Georgetown University Press, 2019, 33-34.

Jordan, D., Kiras, James D. Lonsdale, David J., Speller, Ian, Tuck, Christopher, Dale, Walton. Understanding Modern War. Cambridge: Cambridge University Press, 2008.

Junio, Timothy J. Military History and Fourth Generation Warfare. Journal of Strategic Studies, Vol. 32, No. 2 (2009), 243-269.

Junio, Timothy J. How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate, Journal of Strategic Studies, Vol. 36, No. 1 (2013), 125-133.

Juola, Cristina D. Venäjän puolustusteollinen yhteistyö Kiinan ja Intian kanssa 2010-luvulla. [Russia's military-industrial cooperation with China and India in the 2010s] Maanpuolustuskorkeakoulu Sotataidon laitos, Julkaisusarja 3: Työpapereita nro 9 [Online]. Available: http://www.doria.fi/bitstream/handle/10024/164170/181108_VENR_J_kiina_venaja_intia_juola_web.pdf?sequence=1&isAllowed=y [Accessed: 30th April 2019].

Kaag, John and Kreps, Sarah. Pragmatism's contributions to international relations, Cambridge Review of International Affairs, Vol. 25, No.2, 2012, 191-208.

Kaarbo, Juliet. A Foreign Policy Analysis Perspective on the Domestic Politics Turn in IR Theory. International Studies Review, Vol. 17 (2015), 189–216.

Kagan, Frederick W. and Higham, Robin (eds.) The Military History of the Soviet Union. New York: Palgrave, 2002.

Kakareka, Almantas. Detecting System Intrusion. In Vacca, John R. (ed.) Network and System Security (2nd ed.) Waltham: Syngress, 2014, 1-28.

Kaldor, Mary. New and Old Wars: Organized Violence in a Global Era (3rd edition). Stanford: Stanford University Press, 2012.

Kane, Thomas M. and Lonsdale, David J. Understanding Contemporary Strategy. New York: Routledge, 2012.

Kanet, Roger E. and Piet, Rémi (eds.) Shifting Priorities in Russia's Foreign and Security Policy. Surrey: Ashgate Publishing Limited, 2014.

Kanet, Roger E. Routledge Handbook of Russian Security. London and New York: Routledge, 2019.

Kaplan, Fred. The Wizards of Armageddon. Stanford, Calif.: Stanford University Press, 1983.

Kaplan, Fred. Dark Territory. The Secret History of Cyber War. New York: Simon & Schuster, 2016.

Kari, Martti J. Russian Strategic Culture in Cyberspace Theory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats. JYU Dissertations 122. Jyväskylä, Jyväskylän yliopisto, 2019.

Kari, Martti J. and Pynnöniemi, Katri. Theory of strategic culture: An analytical framework for Russian cyber threat perception, Journal of Strategic Studies, 2019 DOI: 10.1080/01402390.2019.1663411.

Katzenstein, Peter J. (ed.) The Culture of National Security: Norms and Identity in World Politics. New York: Columbia University Press, 1996.

Katzenstein, Peter J., Keohane, Robert O. and Krasner, Stephen D. International Organization and the Study of World Politics. International Organization, Vol. 52, No. 4 (Autumn 1998), 645-685.

Katzenstein, Peter and Sil, Rudra. Eclectic Theorizing in the Study and Practice of International Relations. In Reus-Smith, Christian and Snidal, Duncan (eds.) The Oxford Handbook of International Relations. Oxford University Press: Oxford, 2010, 109-130.

Kavanagh, Camino. The United Nations, Cyberspace and International Peace and Security – Responding to Complexity in the 21st Century. UNIDIR, 2017.

Keegan, J. A History of Warfare (2nd ed.). London: Pimlico, 2004.

Kello, Lucas. The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. International Security, Vol. 38, No. 2 (Fall 2013), 7–40.

Kern, Sean and Gaines, Charles. Expanding Combat Power Through Military Cyber Power Theory. Joint Forces Quarterly, Vol. 79, No. 4 (Quartet 2015), 88-95.

Khalilzad, Zalmay and M., White, John P. (eds.) The Changing Role of Information in Warfare. Santa Monica: RAND, 1999.

Khuel, Daniel T. Information Operations, Information Warfare, and Computer Network Attack: Their Relationship to National Security in the Information Age. International Law Studies 76. Newport, Rhode Island: U.S. Naval War College, 2002.

Kuehl, Daniel T. From Cyberspace to Cyberpower - Defining the Problem. In Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K. Cyberpower and National Security. Washington, D.C.: National Defence University Press, 2009, 24-42.

Kier, Elizabeth. Culture and French Military Doctrine Before World War II. In Katzenstein, Peter J. (ed.) The Culture of National Security: Norms and Identity in World Politics. New York: Columbia University Press, 1996, 186-215.

Kipp, Jacob W. The Methodology of Foresight and Forecasting in Soviet Military Affairs. Fort Leavenworth, KS: SASO, 1987.

Kipp, Jacob W. The Russian Military and the Revolution in Military Affairs: A Case of the Oracle of Delphi or Cassandra? Fort Leavenworth, KS: FMSO, 1995.

Kipp, Jacob W. Confronting the RMA in Russia. Military Review Vol. LXXVII - May-June 1997, No. 3, 49-55.

Kipp, Jacob W. Operational Art and the Curious Narrative on the Russian Contribution: Presence and Absence over the Last 2 Decades. In Blank, Stephen J. and Weitz, Richard (Eds.) The Russian Military Today and Tomorrow: Essays in Memory of Mary FitzGerald. Army War College Strategic Studies Institute (SSI), 2010, 193-263 [Online] Available: https://ssi.armywarcollege.edu/pdffiles/PUB997.pdf [Accessed: 22th October 2018]

Kipp, Jacob W. Russian Military Doctrine: Past, Present, and Future. In Blank, Stephen J. (ed.) Russian Military Politics and Russia's 2010 Defense Doctrine. Army War College Strategic Studies Institute (SSI), 2011, 63-151, 89 [Online]. Available: https://ssi.armywarcollege.edu/pdffiles/PUB1050.pdf [Accessed: 27th October 2018].

Kipp, Jacob W. 'Smart' Defense From New Threats: Future War From a Russian Perspective: Back to the Future After the War on Terror, The Journal of Slavic Military Studies, Vol. 27, No. 1 (2014), 36-62.

Kjellén, Jonas. Russian Electronic Warfare: Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces. FOI, 2018 [Online]. Available: https://www.foi.se/rest-api/report/FOI-R--4625--SE [Accessed: 9th March 2019].

Kim, Hyeob, Kwon, HyukJun, Kwon and Kim, Kyung Kyu. Modified cyber kill chain model for multimedia service environments. Multimedia Tools and Applications Vol. 78 (2019), 3153–3170.

Kivinen, Markku Kivinen and Cox, Terry Cox. Russian Modernisation—A New Paradigm. Europe-Asia Studies, Vol. 68, No. 1 (2016), 1-19.

Klimburg, Alexander. Mobilising Cyber Power, Survival, Vol. 53, No. 1 (2011), 41-60.

Kline, Ronald R. The Cybernetics Moment, Or Why We Call Our Age the Information Age. Baltimore: Johns Hopkins University Press, 2015.

Klinger, Janeen M. Social Science and National Security Policy. Deterrence, Coercion, and Modernization Theories. Cham: Palgrave Macmillan, 2019.

Knafo, Samuel. Critical approaches and the legacy of the agent/structure debate in international relations. Cambridge Review of International Affairs, Vol. 23, No. 3, (September 2010), 493-516.

Knight, Amy. The KGB, Perestroika, and the Collapse of the Soviet Union. Journal of Cold War Studies Vol. 5, No. 1, (Winter 2003), 67–93.

Knopf, Jeffrey W. The Fourth Wave in Deterrence Research. Contemporary Security Policy, Vol. 31, No. 1 (2010), 1–33.

Knorr, Klaus. On the uses of Military Power in the Nuclear Age. Princeton University Press, 1966.

Kokoshin, Andrei A. Soviet Strategic Thought, 1917-91. Cambridge, Massachusetts: The MIT Press, 1998.

Kolodziej, E. A. French Strategy Emergent: General Andre Beaufre: A Critique. World Politics, Vol. 19, No. 3 (1967), 417 – 444.

Konyshev, Valery and Sergunin, Alexander. Military. In Tsyganov, Andrei P. Routledge Handbook of Russian Foreign Policy. London and New York: Routledge, 2018, 168-181.

Kowert Paul A. National Identity: Inside and Out. Security Studies, Vol. 8 (Winter 1998/99–Spring 1999), 1-34.

Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K. Cyberpower and National Security. Washington, D.C.: National Defence University Press, 2009.

Krasner, Stephen. Structural Conflict. Berkeley: University of California Press, 1985.

Kratochwil, Friedrich. Sociological Approaches. In Reus-Smith, Christian and Snidal, Duncan (eds.) The Oxford Handbook of International Relations. Oxford University Press: Oxford, 2010, 444-461.

Kratochwil, Friedrich. Of False Promises and Good Bets: A Plea for a Pragmatic Approach to Theory Building (The Tartu Lecture). Journal of International Relations and Development, Vol. 10, No. 1, (March 2017), 1-15.

Krause, Keith. Conclusions: Security culture and the non-proliferation, arms control and disarmament agenda. Contemporary Security Policy, Vol. 19, No. 1 (1998), 219-239.

Kremer, Jan-Fredrik and Müller, Benedikt (eds.) Cyberspace and International Relations: Theory, Prospects and Challenges. Heidelberg: Springer, 2016.

Krepinevich, Andrew. The Military-Technical Revolution: A Preliminary Assessment. Washington: Center for Strategic and Budgetary Assessments, 2002.

Kristensen, Hans M. and Norris, Robert S. Russian nuclear forces, 2018. Bulletin Of The Atomic Scientists, 2018 Vol. 74, No 3 (2018), 185–195

Kristensen, Hans M. and Korda, Matt. Russian nuclear forces, 2019. Bulletin of the Atomic Scientists, Vol. 75, No. 2 (2019), 73-84.

Krygiel, Annette J. Behind the Wizard's Curtain: An Integration Environment for a System of Systems. CCRP Publication Series, 1999.

Kuchins, Andrew C. Mismatched Partners: US-Russia Relations after the Cold War. In Cadier, David and Light, Margot (eds.) Russia's Foreign Policy. Ideas, Domestic Politics and External Relations. Basingstoke: Palgrave Macmillan, 2015, 117-137.

Kundnani, Hans. What is the Liberal International Order. GMF, Policy Essay No. 17 (2017) [Online]. Available: http://www.gmfus.org/publications/what-liberal-international-order [Accessed: 15th July 2019].

Kuehl, Daniel. From Cyberspace to Cyberpower - Defining the Problem. In Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K. Cyberpower and National Security. Washington, D.C.: National Defence University Press, 2009, 24-42.

Kuhn, Richard D., Hu, Vincent C., Polk, Timothy W., Chang, Shu-Jen. Introduction to Public Key Technology and the Federal PKI Infrastructure. NIST, 26 February 2001 [Online]. Available: https://nvl-pubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-32.pdf [Accessed: 8th August 2018].

Kukkola, Juha. (2017a) Cyber asymmetry – Towards new strategic thinking? In Kukkola, Juha, Ristolainen, Mari and Nikkarila, Juha-Pekka. Game Changer: Structural Transformation of Cyberspace. Riihimäki: Finnish Defence Research Agency, 2017, 131-188.

Kukkola, Juha. (2018a) Russian Cyber Power and Structural Asymmetry, 13th International Conference on Cyber Warfare and Security (ICCWS), 8-9 March 2018, Washington DC, USA.

Kukkola, Juha. (2018b) The Russian Segment of Internet as a Resilient Battlefield. Presented at the International Society of Military Sciences Conference (ISMS) Warsaw, Poland, October, 18.-19., 2018.

Kukkola, Juha. (2018c) Civilian and Military Information Infrastructure and the Control of the Russian Segment of Internet. Presented in the International Conference on Military Communications and Information Systems (ICMCIS) Warsaw, Poland, May 22.-23., 2018.

Kukkola, Juha. (2018d) New guidance for preparing Russian 'digital sovereignty' released, Finnish Defence Research Agency, Research Bulletin 01 – 2018.

Kukkola, Juha and Ristolainen, Mari. Projected Territoriality: A Case Study of the Infrastructure of Russian 'Digital Borders', Journal of Information Warfare, Vol. 17, No. 2 (2018), 83-100.

Kukkola, Juha, Nikkarila, Juha-Pekka and Ristolainen, Mari. Asymmetric frontlines of cyber battlefields. Presented at International Command and Control Research and Technology Symposium (ICCRTS), Los Angeles, USA, November 6.-8., 2017.

Kukkola, Juha, Ristolainen, Mari and Nikkarila, Juha-Pekka. (2017a) Game Changer: Structural Transformation of Cyberspace. Finnish Defence Research Agency Publications 10. Riihimäki: Finnish Defence Research Agency, 2017.

Kukkola, Juha, Ristolainen, Mari and Nikkarila, Juha-Pekka. (2017b) Confrontation with a closed network nation: Open network society's choices and consequences. Presented at Military Communications (MILCOM) conference, Baltimore, USA, October 23.-25, 2017.

Kukkola, Juha, Ristolainen, Mari and Nikkarila, Juha-Pekka. Game Player. Facing the structural transformation of cyberspace. Finnish Defence Research Agency Publications 11. Riihimäki: Finnish Defence Research Agency, 2019.

Kurki, Milja. Causation in International Relations: Reclaiming Causal Analysis, Cambridge: Cambridge University Press, 2008.

Kurki, Milja and Wight, Colin. International Relations and Social Science. In Dunne, T., Kurki, M. and Smith, S. International Relations Theories: Discipline and Diversity (4th ed.) Oxford: Oxford University Press, 2013, 14-35.

Kurth, Natasha. Asia-Pacific and China. In Tsyganov, Andrei P. Routledge Handbook of Russian Foreign Policy. London and New York: Routledge, 2018, 254-268.

Kåre, Johan Mjør. Smuta: cyclical visions of history in contemporary Russian thought and the question of hegemony. Studies in East European Thought, No 70 (2018), 19–40.

Lachow, Irving. Cyber Terrorism: Menace or Myth? In Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K.: Cyberpower and National Security, National Defense University Press, Washington D.C., 2009, 437-464.

Laffey, Mark and Weldes, Jutta. Beyond Belief: Ideas and Symbolic Technologies in the Study of International Relations. European Journal of International Relations, Vol. 3, No. 2 (June 1997), 193–237.

Lake, David and Powell, Robert (eds.) Strategic Choice and International Relations. Princeton: Princeton University Press, 1999.

Lalu, Petteri. On war and perception of war in Russian thinking. Finnish Defence Research Agency Research Bulletin 3 – 2016.

Lalu, Petteri and Kivimäki, Veli-Pekka. Leading Russian Military Journal Voennaia mysl' available as whole in the EastView digital database. Finnish National Defence University Department of Warfare Series 3: Working Papers No. 15, 2019 [Online]. Available: https://www.doria.fi/bitstream/handle/10024/173304/Lalu%26Kivim%C3%A4ki_VoeannaiMysl_database_web.pdf?sequence=1&isAllowed=y [Accessed: 28th December 2019].

Lane, Ruth. Political Culture: Residual Category or General Theory? Comparative Political Studies, Vol. 25 (October 1992), 362-387.

Lango, Hans-Inge. Competing academic approaches to cyber security. In Friis, Karsten Friis and Rinsmose, Jens (eds.) Conflict in Cyber Space. Theoretical, strategic and legal perspectives. New York: Routledge 2016, 7-26.

Lantis, Jeffery S. Strategic Culture and National Security Policy. International Studies Review, Vol. 4, No. 3 (Autumn 2002), 87-113.

Lantis, Jeffrey S. Strategic Culture and Tailored Deterrence: Bridging the Gap between Theory and Practice, Contemporary Security Policy, Vol. 30, No. 3 (2009), 467-485.

Lantis, Jeffrey S. and Darryl Howlett. Strategic Culture. In John Baylis, James J. Wirtz and Coli S. Gray. Strategy in the Contemporary World (4th ed.) Oxford: Oxford University Press, 2013, 84-101.

Lantis, Jeffrey S. Strategic Cultures and Security Policies in the Asia-Pacific, Contemporary Security Policy, Vol.35, No.2 (2014), 166-186.

Lantis, Jeffrey S. Nuclear cooperation with non-NPT member states? An elite-driven model of norm contestation. Contemporary Security Policy, Vol. 39, No. 3 (2018), 399-418.

Lapointe, Thierry and Dufour, Frédérick Guillaume. Assessing the historical turn in IR: an anatomy of second wave historical sociology. Cambridge Review of International Affairs, Vol. 25, No.1 (March 2012), 97-121.

Larive□ , Maxime H. A. Debating European Security and Defense Policy: Understanding the Complexity. Surrey: Ashgate, 2014.

Larson, Doyle E. Exploiting Electronic Warfare. Air Force Magazine, July 1981.

Lawlor Russell, Alison. Strategic Anti-Access/Area Denial in Cyberspace. In Maybaum, M., Osula, A. and Lindström, L.m (Eds.) 7th International Conference on Cyber Conflict: Architectures in Cyberspace. Tallinn: NATO CCD COE Publications, 2015, 153-168.

Lawson, George and Shilliam, Robbie. Sociology and international relations: legacies and prospects. Cambridge Review of International Affairs, Vol. 23, No. 1, 2010, 69-86.

Layman, Gene A. C3CM – A Warfare Strategy. Naval War College Review, Vol. 38, No. 2 (March-April 1985), 31-42.

Lebow, Richard N. Why Nations Fight: Past and Future Motives for War. New York: Cambridge University Press, 2010.

Ledeneva, Alena V. Can Russia Modernise? Cambridge: Cambridge University Press, 2013.

Lee, S. International Reactions to U.S. Cybersecurity Policy: The BRICS undersea cable. Washington: Henry M. Jackson School of International Studies, 2016.

Leebaert, Derek and Dickinson, Timothy (eds.) Soviet Strategy and the New Military Thinking. Cambridge: Cambridge University Press, 1992.

Leffler, Melvyn P. and Westad, Odd Arne (Eds.) (2010a) The Cambridge History of The Cold War: Volume II: Crises and Détente. Cambridge: Cambridge University Press, 2010.

Leffler, Melvyn P. and Westad, Ood Arne (Eds.) (2010b) The Cambridge History of The Cold War: Volume III Endings. Cambridge: Cambridge University Press, 2010.

Legro, Jeffrey W. Culture and Preferences in the International Cooperation Two-Step. The American Political Science Review, Vol. 90, No. 1 (Mar. 1996), 118-137.

Legro, Jeffrey W. The Transformation of Policy Ideas. American Journal of Political Science, Vol. 44, No. 3 (Jul., 2000), 419-432.

Legro Jeffrey W. and Moravcsik, Andrew. Is Anybody Still a Realist? International Security, Vol. 24, No. 2 (Fall 1999), 5-55.

Legvold, Robert. Return to Cold War. Cambridge: Polity Press, 2016.

Lemieux, F. (ed.) Current and Emerging Trends in Cyber Operations. Policy, Strategy and Practice. New York: Palgrave Macmillian, 2015.

Levien, Roger and Maron, M. E. Cybernetics and Its Development in the Soviet Union. Santa Monica: RAND Corporation, 1964.

Levinson, Nanette S. and Marzouki, Meryem. International Organizations and Global Internet Governance: Interorganizational Architecture. In Musiani, Francesca, Cogburn, Derrick L., DeNardis, Laura and Nanette S. Levinson (eds.): The Turn to Infrastructure in Internet Governance. New York: Palgrave Macmillan, 2016, 47-71.

Levite, Ariel. ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies. Carnegie Endowment for International Peace, October 4th 2019 [Online]. Available: https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974 [Accessed: 5th January 2020].

Levy, Jack S. and Thompson, William R. Hegemonic Threats and Great-Power Balancing in Europe, 1495-1999. Security Studies, Vol. 14, No. 1 (January–March 2005), 1-33.

Levy, J. S. Review Roundtable. Clausewitz on Small War. The Journal of Strategic Studies, Vol. 40, No. 3 (2017), 450 – 456.

Lewis, George N. U.S. BMD Evolution Before 2000. In Arbatov, Alexei and Dvorkin, Vladimir (Eds.) Missile Defense: Confrontation and Cooperation. Moscow: Carnegie Moscow Center, 2013, 51-70.

Libel, Tamil. Explaining the security paradigm shift: strategic culture, epistemic communities, and Israel's changing national security policy. Defence Studies, Vol. 16, No. 2 (2016), 137–156.

Libicki, Martin C. What Is Information Warfare? Washington DC: National Defense University, Institute for National Strategic Studies, 1995.

Libicki, Martin C. Conquest in Cyberspace. National Security and Information Warfare. Cambridge: Cambridge University Press, 2007.

Libicki, Martin. Cyberdeterrence and Cyberwar. Santa Monica: RAND, 2009.

Libicki, Martin C. Cyberspace in Peace and War. Annapolis, Maryland: Naval Institute Press, 2016.

Libicki, Martin C. The Conversion of Information Warfare. Strategic Studies Quarterly, Vol. 11, No. 1, (Spring 2017), 49-65.

Liff, Adam. Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. Journal of Strategic Studies, Vol. 35, No. 3 (2012) 401-428.

Light, Margot. Foreign Policy Thinking. In Malcolm, Neil, Pravda, Alex, Allison, Roy and Light, Margot. Internal Factors in Russian Foreign Policy. Oxford: Oxford University Press, 1996, 33-100.

Lillienfeld, Robert. The Rise of Systems Theory: an Ideological Analysis. New York: John Wiley and Sons, 1978.

Lindsay, Jon R. Stuxnet and the Limits of Cyber Warfare, Security Studies, Vol. 22, No. 3 (2012), 365-404.

Lindsay, Jon R., Cheung, Tai Ming and Reveron, Derek S. China and Cybersecurity. Espionage, Strategy, and Politics in the Digital Domain. Oxford: Oxford University Press, 2015.

Lo, Bobo. Russia and the New World Disorder. Washington, DC: Brookings Institute Press, 2015.

Lobell, Steven N., Ripsman, Norrin M. and Taliaferro, Jeffrey W. Neoclassical Realism, the State, and Foreign Policy. Cambridge: Cambridge University Press, 2009.

Locksley, Christopher C. Concept, algorithm, indecision: Why military reform has failed in Russia since 1992. The Journal of Slavic Military Studies, Vol.14, No.1 (March 2001), 1-26.

Longhurst, Kelly. Germany and the use of force. Manchester: Manchester University Press, 2004.

Lord, Kristin M. and Sharp, Travis (ed.) America's Cyber Future Security and Prosperity in the Information Age volume II, Center for New American Security, 2011.

Luiijf, Eric, Besseling, Kim and de Graaf, Patrick. Nineteen national cyber security strategies. International Journal of Critical Infrastructure Protection, Vol. 9, No. 1-2 (2013), 3-31.

Lukes, Steven. Power: A Radical View (2nd ed.) Basingstoke: Palgrave Macmillan, 2005.

Lukin, Vladimir. The Foreign Policy of Post-Soviet Russia: A Quest for Identity, Strategic Analysis, Vol. 40, No. 6 (2016), 486-497.

Lund, Aron. Syria's Civil War. Government Victory of Frozen Conflict. FOI, December 2018 [Online]. Available: https://www.foi.se/rest-api/report/FOI-R--4640--SE [Accessed: 30th April 2019].

Luttwak, Edward N. Strategy: The Logic of War and Peace. Cambridge, Massachusetts: The Belknap Press of Harvard University Press, 2001.

Lykke, Arthur F. Toward an Understanding of Military Strategy. Military Review Vol. LXIX, No. 5, (May 1989), 2-8.

Mahan, Alfred T. The Influence of Sea Power upon History 1660-1783. Dover edition. Boston: Little, Brown and Company, 1890.

Mahnken, Thomas G. The Future of Strategic Studies. The Journal of Strategic Studies, Vol. 26, No. 1 (2003), x-xviii.

Mahnken, Thomas G. Cyber war and Cyber warfare. In Lord, Kristin M. and Sharp, Travis (ed.) America's Cyber Future Security and Prosperity in the Information Age volume II, Center for New American Security, 2011, 57-64.

Mahnken, Thomas G. and Maiolo Joseph A. Strategic Studies: A Reader, Routledge, New York, 2014.

Mahoney, James. Process Tracing and Historical Explanation. Security Studies, Vol. 24, No. 2 (2015), 200-218.

Makarychev, Andrey and Morozov, Viatcheslav. Is "Non-Western Theory" Possible? The Idea of Multipolarity and the Trap of Epistemological Relativism in Russian IR. International Studies Review, Vol. 15, No. 3 (September 2013), 328–350.

Malcolm, Neil, Pravda, Alex, Allison, Roy and Light, Margot. Internal Factors in Russian Foreign Policy. Oxford: Oxford University Press, 1996.

Maliniak, Daniel, Peterson, Susan, Powers, Ryanand and Tierney, Michael J. Is International Relations a Global Discipline? Hegemony, Insularity, and Diversity in the Field, Security Studies. Security Studies, Vol. 27, No. 3 (2018), 448-484.

Mankoff, Jeffrey. Russian Foreign Policy: The Return of Great Power Politics (2nd ed.) Lanham: Rowman & Littlefield Publishers, Inc., 2012.

March, James G. and Olsen, Johan P. The Institutional Dynamics of International Political Orders. International Organization, Vol. 52, No. 4 (Autumn 1998), 943–969.

Marten, Kimberly. The 'KGB State' and Russian Political and Foreign Policy Culture, Journal of Slavic Military Studies, Vol. 30, No. 2 (2017), 131-151.

Mattern, Janice Bially. Power in Realist Constructivist Research. International Studies Review Vol. 6, No. 2, (2004), 337-352.

Mattioli, R. The ´States(s)´of Cybersecurity. In Giampiero, G. (ed.) Security in Cyberspace. Targeting Nations, Infrastructures, Individuals. New York: Bloomsbury Academic, 2014, 23-28.

Maurer, Tim. Cyber Mercenaries. The State, Hackers, and Power. Cambridge: Cambridge University Press, 2018.

Maybaum, M., Osula, A. and Lindström, L.m (Eds.) 7th International Conference on Cyber Conflict: Architectures in Cyberspace. Tallinn: NATO CCD COE Publications, 2015.

Maximov R.V., Krupenin A.V., Sharifullin S.R., Sokolovsky S.P. Innovative Development Of Tools And Technologies To Ensure The Russian Information Security And Core Protective Guidelines. Вопросы кибербезопасности №1(29) 2014, 10-17.

McCarthy, Daniel R. Open Networks and the Open Door: American Foreign Policy and the Narration of the Internet. Foreign Policy Analysis, Volume 7, Issue 1, January 2011, Pages 89–111.

McCauley, Martin. The Soviet Union Since 1917. London and New York: Longman, 1981.

McCourt, David M. Practice Theory and Relationalism as the New Constructivism. International Studies Quarterly, Vol. 60, No. 3 (September 2016), 475–485.

MccGwire, Michael. Military Objectives in Soviet Foreign Policy. Washington, D.C.: The Brookings Institution, 1987.

McDermott, Roger N. The Restructuring of the Modern Russian Army, The Journal of Slavic Military Studies, Vol.22, No.4 (2009), 485-501.

McDermott, Roger N. Russian Perspective on Network-Centric Warfare: The Key Aim of Serdyukov's Reform. Fort Leavenforth, Kansas: FMSO, 2011.

McDermott, Roger N. The Transformation of Russia's Armed Forces. Twenty Lost Year. New York: Routledge, 2015.

McDermott, Roger. Does Russia Have a Gerasimov Doctrine? Parameters, Vol. 46, No. 1 (Spring 2016), 97-105.

McDermott, Roger N. Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. Tallinn: International Centre for Defence and Security, 2017.

McDermott, Roger, N. Brothers Disunited: Russia's Use of Military Power in Ukraine, FMSO, Kansas, 2015.

Meakins, Joss I. Squabbling Siloviki: Factionalism Within Russia's Security Services, International Journal of Intelligence and Counter Intelligence, Vol. 31, No. 2 (2018), 235-270.

Mearsheimer, John. The Tragedy of Great Power Politics. New York: Norton, 2001.

Mearsheimer, John J. Structural Realism. In Dunne, T.im, Kurki, Milja and Smith, Steven (eds.) International Relations Theories: Discipline and Diversity (4th ed.) Oxford: Oxford University Press, 2013.

Mearsheimer, John J. "Why the Ukraine Crisis Is the West's Fault," Foreign Affairs, September / October 2014, 77-89.

Menning, Bruce C. Bases of Soviet Military Doctrine. In Frank, Willlard, C. and Gillette, Philip S. Soviet Military Doctrine from Lenin to Gorbachev, 1915-1991. Westport, Connecticut: Greenwood Press, 1992, 41-59.

Merrill, Kenneth. Domains of Control: Governance of and by the Domain Name System. In Musiani, Francesca, Cogburn, Derrick L., DeNardis, Laura and Nanette S. Levinson (eds.): The Turn to Infrastructure in Internet Governance. New York: Palgrave Macmillan, 2016, 89-106.

Merton, Robert K. Social Theory and Social Structure. New York: Free Press, 1968.

Miasnikov, Eugene. The air-space threat to Russia. In Arbatov, Alexei and Dvorkin, Vladimir (Eds.) Missile Defense: Confrontation and Cooperation. Moscow: Carnegie Moscow Center, 2013, 121-146.

Milevski, Lucas. Asymmetry is Strategy, Strategy is Asymmetry. JFQ, Vol. 75, No. 4 (2014), 77-83.

Milevski, Lucas. (2016a) The Evolution of Modern Grand Strategic Thought, Oxford University Press, Oxford, 2016.

Milevski, Lukas. (2016b) The nature of strategy versus the character of war. Comparative Strategy, Vol. 35, No. 5 (2016), 438-446.

Miller, Benjamin. The Concept of Security: Should it be Redefined? The Journal of Strategic Studies, Vol. 24, No. 2 (2001), 13-42.

Milliken, Jennifer. The Study of Discourse in International Relations: A Critique of Research and Methods. European Journal of International Relations, Vol. 5, No. 2 (June 1999), 225-254.

Milton Mueller. Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace, Cambridge, UK: Polity, 2017.

Minárik, T., Jakschis, R. and Lindström, L. (eds.) 10th International Conference on Cyber Conflict CyCon X: Maximising Effects. Tallinn: NATO CCD COE, 2018.

Misenheimer, Alan Greeley. Thucydides' Other "Traps" The United States, China, and the Prospect of "Inevitable" War. Washington, D.C.: National Defence University Press, 2019.

Mitchell, Nancy. The Cold War and Jimmy Carter. In Leffler, Melvyn P. and Westad, Ood Arne (Eds.) The Cambridge History of The Cold War: Volume III Endings. Cambridge: Cambridge University Press, 2010, 66-88.

Mitchell, P. Network Centric Warfare: Coalition operations in the age of US military primacy. IISS, The Alelphi Papers, Vol. 46, No. 385, 2006.

Molander, R. C., Riddile, A. S. and Wilson, P. A. Strategic Information Warfare: A New Face of War. Santa Monica: RAND, 1996.

Molchanov, Mikhail A. The Eurasian Economic Union. In Tsyganov, Andrei P. Routledge Handbook of Russian Foreign Policy. London and New York: Routledge, 2018, 410-420.

Monaghan, Andrew. 'An enemy at the gates' or 'from victory to victory'? Russian foreign policy. International Affairs, Vol.84, No.4 (2008), 717–733.

Monaghan, Andrew. Defibrillating the Vertikal? Putin and the Russian Grand Strategy, Chatham House Research Paper, October 2014.

Monaghan, Andrew. Russian State Mobilization: Moving the Country on to a War Footing, Chatham House Research Paper, May 2016.

Monaghan, Andrew. Power in Modern Russia. Manchester: Manchester University Press, 2017.

Moravcsik, Andrew. Taking Preferences Seriously: A Liberal Theory of International Politics. International Organization, Vol. 51, No. 4, (Autumn 1997), 513–553.

Morgan, Forrest E., Mueller, Karl P., Medeiros, Evan S., Pollpeter, Kevin L. and Cliff, Roger. Dangerous Thresholds. Managing Escalation in the 21st Century. Santa Monica: RAND, 2008.

Murray, Williamson, Knox, MacGregor and Bernstein, Alvin (eds.) The Making of Strategy: Rulers, State, and War. Cambridge: Cambridge University Press, 2009.

Musiani, Francesca, Cogburn, Derrick L., DeNardis, Laura and Levinson, Nanette S. (Eds.) The Turn to Infrastructure in Internet Governance. New York: Palgrave Macmillan, 2016.

Myers, Steven Lee. The New Tsar: The Rise and Reign of Vladimir Putin. New York: Vintage Books, 2015.

Nagorski, Andrew (ed.) Global Cyber Deterrence Views from China, the U.S., Russia, India, and Norway. New York: The EastWest Institute, 2010.

Narizny, Kevin. The New Debate: International Relations Theory and American Strategic Adjustment in the 1890s. Security Studies, Vol. 11, No. 1, (Autumn 2001), 151-170.

Narizny, Kevin. On Systemic Paradigms and Domestic Politics: A Critique of the Newest Realism. International Organization, Vol. 42, No. 2, (Fall 2017), 155-190.

Nash, Roy. Explanation and quantification in educational research: the arguments of critical and scientific realism. British Educational Research Journal, Vol. 31, No. 2, (April 2005), 185-204.

Naughton, John. The evolution of the Internet: from military experiment to General Purpose Technology, Journal of Cyber Policy, Vol. 1, No. 1 (2016), 5-28.

Nauta, Frank. Logistics Implications of Maneuver Warfare. Volume 3: Soviet Offensive Concepts and Capabilities. Bethesda, Maryland: Logistics Management Institute, 1988.

Nikkarila, Juha-Pekka and Ristolainen, Mari. 'RuNet 2020' – Deploying traditional elements of combat power in cyberspace. Presented in the International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, May 15.-16., 2017.

Nikkarila, J-P., Åkesson, B., Kuikka, V., and Hämäläinen, J. Modelling Closed National Networks – Effects in Cyber Operation Capabilities. Presented at the 17th European Conference on Cyber Warfare and Security (ECCWS), 28-29 June 2018, Oslo, Norway.

Njølstad, Olav. The Collapse of superpower détente, 1975-1980. Leffler, Melvyn P. and Westad, Ood Arne (Eds.) The Cambridge History of The Cold War: Volume III Endings. Cambridge: Cambridge University Press, 2010, 135-155.

Noble, Ben and Schulmann, Ekaterina. Not Just a Rubber Stamp. Parliament and Lawmaking. In Treisman, Daniel (ed.) The New Autocracy: Information, Politics, and Policy in Putin's Russia. Washington, D.C.: Brookings Institution Press, 2018, 47-78.

Nocetti, Julian. Contest and conquest: Russia and global internet governance. International Affairs, Vol. 91, No. 1 (2015), 111-130.

Nocetti, Julian. Cyber Power. In Tsyganov, Andrei P. Routledge Handbook of Russian Foreign Policy. London and New York: Routledge, 2018, 182-198.

Norberg, Johan and Westerlund, Fredrik. Military Means for non-Military Measures: The Russian Approach to the Use of Armed Forces as Seen in Ukraine, The Journal of Slavic Military Studies, 2016 Vol. 29, NO. 4, 576-601.

Nye, Joseph. Cyber Power. Cambridge: Harvard Kennedy School, 2010.

Nye, Joseph. Deterrence and Dissuasion in Cyberspace. International Security, Vol. 41, No. 3 (2016/2017), 44-71.

Nye, Joseph. (2011a) The Future of Power. Public Affairs, New York, 2011.

Nye, Joseph. (2011b) Nuclear Lessons for Cyber Security? Strategic Studies Quarterly, Vol. 5, No. 4 (Winter 2011), 18-38.

Ó Tuathail, Gearoid and Simon Dalby (eds.) Rethinking Geopolitics London: Routledge, 1998.

O'Neil, William D. Cyberspace and Infrastructure. In Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K.: Cyberpower and National Security, National Defense University Press, Washington D.C., 2009, 113-146.

Odom, William E. The Collapse of the Soviet Military. New Haven & London: Yale University Press, 1998.

Oki, Eiji, Rojas-Cessa, Roberto, Tatipamula, Mallikarjun and Christian Vogt. Advanced Internet Protocols, Services, and Applications. Hoboken, New Jersey: John Wiley & Sons, 2012.

Oliker, Olga. Russian Nuclear Doctrine. Washington, DC: CSIS, 2016.

Oliker, Olega: Putinism, Populism and the Defence of Liberal Democrazy, Survival, Vol.59, No. 1, February – March 2017, 7-24.

Omelicheva, Mariya Y. and Zubytska, Lidiya. An Unending Quest for Russia's Place in the World: The Discursive Co-evolution of the Study and Practice of International Relations. New Perspectives, Vol. 24, No. 1, (2016), 19-51.

Onuf, Nicholas. Of Paradigms and Preferences. International Studies Quarterly, Vol. 56, No. 3 (September 2012), 626–628.

Osiander, Andreas. Sovereignty, International Relations, and the Westphalian Myth. International Organization, Vol. 55, No. 2 (Spring 2001), 251-287.

Osula, Anna-Maria and Rõigas, Henry (eds.) International Cyber Norms: Legal, Policy & Industry Perspectives. Tallinn: CCDCOE, 2016.

Oxenstierna, Susanne. The Russian Economy: Can Growth be Restored within the Economic System? FOI, 2014 [Online]. Available: https://www.foi.se/report-search/pdf?fileName=D:%5CReportSearch%5CFiles%5C7b0d3cb7-e080-447f-a4e5-2b49d669543f.pdf [Accessed: 3rd May 2019].

Oxenstierna, Susanne. Russia's Economy and Military Expenditures. In Kanet, Roger E. Routledge Handbook of Russian Security. London and New York: Routledge, 2019, 97-108.

Palmer, Diego A. Ruiz. The NATO-Warsaw Pact competition in the 1970s and 1980s: a revolution in military affairs in the making or the end of a strategic age? Cold War History, Vol. 14, No.4 (2014), 533–573.

Pape, Robert A. Bombing to Win: Air Power and Coercion in War. Ithica and London: Cornell University Press, 1996.

Parent, Joseph M. and Baron, Joshua M. Elder Abuse: How the Moderns Mistreat Classical Realism. International Studies Review, Vol. 13, No. 2 (June 2011), 193–213.

Patomaki, Heikki and Wight, Colin. After Post-positivism? The Promises of Critical Realism. International Studies Quarterly, Vol. 44, No. 2 (Jun., 2000), 213-237.

Patryk Pawlak. Reducing Uncertainties in Cyberspace through Confidence and Capacity-Building Measures. In Giacomello, Giampiero (ed.) Security in Cyberspace. Targeting Nations, Infrastructures, Individuals. New York: Bloomsbury Academic, 2014, 39-58.

Paul, C. Strategic Communications. Santa Barbara: Praeger, 2011.

Payne, Keith B. and Foster, John S. Russian strategy Expansion, crisis and conflict. Comparative Strategy, Vol. 36, No. 1 (2017), 1-89.

Perkovich, George and Levite, Ariel E. (eds.) Understanding Cyber Conflict: Fourteen Analogies. Georgetown: Georgetown University Press, 2017.

Perlman, Radia. Interconnections, Second Edition: Bridges, Routers, Switches, and Internetworking Protocols. Boston: Addison-Wesley, 2012.

Persson, Gudrun (ed.) Russian Military Capability in a Ten-Year Perspective – 2016. FOI, 2016 [Online]. Available: https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4326--SE [Accessed: 29th April 2019].

Pernik, Piret. Preparing for Cyber Conflict. Case Studies of Cyber Command. RKK ICDS, December 2018 [Online]. Available: https://icds.ee/wp-content/uploads/2018/12/ICDS_Report_Preparing_for_Cyber_Conflict_Piret_Pernik_December_2018-1.pdf [Accessed: 1st May 2019].

Perrow. Charles Normal Accidents: Living with High Risk Technologies. Princeton, NJ: Princeton University Press 1999.

Perry, Jake and Costigan, Sean S. (eds.) Cyberspaces and Global Affairs. Surrey: Ashgate, 2012.

Peters, Benjamin. How Not to Network a Nation: The Uneasy History of the Soviet Internet. The MIT Press: Cambrige, 2016.

Petersson, Bo. The eternal great power meets the recurring times of troubles: twin political myths in contemporary Russian politics. European studies, No. 30 (2013), 301-326.

Peterson, D. J. Russia and the Information Revolution. Santa Monica: RAND, 2005.

Pijenberg Muller, Lilly. How to govern cyber security? The limits of the multi-stakeholder approach and the need to rethink public-private cooperation. In Friis, Karsten and Ringsmose, Jens (eds.) Conflict in Cyber Space. Theoretical, strategic and legal perspectives. Routledge 2016, New York, 116-129.

Pissanidis, N., Rõigas, H., Veenendaal, M. (Eds.) 8th International Conference on Cyber Conflict: Cyber Power. Tallinn: NATO CCD COE, 2016.

Podins, K. Stinissen, J. and Maybaum, M. (Eds.) 5th International Conference on Cyber Conflict 2013 - Proceedings. NATO CCD COE Publications, Tallinn, 2013.

Podvig, Pavel. The Operational Status of the Russian Space-Based Early Warning System. Science & Global Security, Vol.4 (1994), 363-384.

Podvig, Pavel. History and the Current Status of the Russian Early-Warning System. Science and Global Security, Vol. 10 (2002), 21–60.

Podvig, Pavel. The Window of Vulnerability That Wasn't: Soviet Military Buildup in the 1970s--A Research Note. International Security, Vol. 33, No. 1 (Summer 2008), 118-138.

Polyakova, Alina and Boyer, Spencer P. The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition. Washington: The Brookings Institution, 2018 [Online]. Available: https://www.brookings.edu/wp-content/uploads/2018/03/fp_20180316_future_political_warfare.pdf [Accessed: 30th April 2019].

Pomerantsev, Peter and Weiss, Michael. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. New York: The Institute of Modern Russia, Inc., 2014.

Pomeranz, William E. Law and the Russian State- Russia's Legal Evolution from Peter the Great to Vladimir Putin. London and New York: Bloomsburym 2019.

Poore, Stuart. What is the context? A reply to the Gray-Johnston debate on strategic culture. Review of International Studies, Vol. 29, No. 2 (Apr. 2003), 279-284.

Popescu, Ionut C. Grand Strategy vs. Emergent Strategy in the conduct of foreign policy. The Journal of Startegic Studies, Vol. 41, No. 3, (2018), 438-460.

Popescu, Nicu and Secrieru, Stanislav (Eds.) Hacks, Leaks and Disruptions: Russian Cyber Strategies. Chaillot Papers No. 148, October 2011. Paris: European Union Institute for Security Studies, 2018.

Porche, Isaac III, Paul, Christopher, York, Michael, Serena, Chad C., Sollinger, Jerry M., Axelband, Elliot, Min, Endy Y., Held, Bruce J. Redefining Information Warfare Boundaries for an Army in a Wireless World. Santa Monica: RAND, 2013.

Porfiriev, Boris and Simons, Greg (eds.) Crisis in Russia: Contemporary Management Policy and Practice from a Historical Perspective. New York: Routledge, 2016.

Posen, Barry. The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars. Ithica: Cornell University Press, 1984.

Pouliot, Vincent. The Logic of Practicality: A Theory of Practice of Security Communities. International Organization, Vol. 62, No. 2 (Spring, 2008), 257-288.

Prakash, Pranesh, Rizk, Nagla and Souza, Carlos Affonso (eds.) Global censorship Shifting Modes, Persisting Paradigms. New Haven: Yale Law School 2015 [Online]. Available: https://law.yale.edu/system/files/area/center/isp/documents/a2k_global-censorship_2.pdf [Accessed: 14th May 2019].

Pratt, Simon. Pragmatism as Ontology, Not (Just) Epistemology: Exploring the Full Horizon of Pragmatism as an Approach to IR Theory. International Studies Review, Vol. 18, No. 3 (September 2016) 508–527.

Pynnöniemi, Katri (ed.) Russia´s Critical Infrastructures - Vulnerabilities and Possibilities, FIIA Report 35, 2012.

Pynnöniemi, Katri and Busygina, Irina. Critical infrastructure protection and Russia's hybrid regime, European Security, Vol.22, No.4 (2013), 559-575.

Pynnöniemi, Katri. (2019a) The Asymmetric Approach in Russian Security Strategy: Implications for the Nordic Countries, Terrorism and Political Violence, Vol 31, No. 1 (2019), 154-167.

Pynnöniemi, Katri. (2019b) Information-Psychological Warfare in Russian Security Strategy. In Kanet, Roger E. Routledge Handbook of Russian Security. London and New York: Routledge, 2019, 214-226.

Qu, Zhicheng, Zhang, Genxin, Cao, Haotong and Xie, Jidong. LEO Satellite Constellation for Internet of Things. IEEE Access, Vol. 5 (2017), 18391-18401.

Quirk, Joel. Historical Methods. In Reus-Smith, Christian and Snidal, Duncan (eds.) The Oxford Handbook of International Relations. Oxford University Press: Oxford, 2010, 518-536.

Ralston, Shane J. (ed.) Philosophical Pragmatism and International Relations. Plymouth, UK: Lexington Books, 2013.

Rangsimaporn, Paradorn. Russian Elite Perceptions of the Russo-Chinese 'Strategic Partnership' (1996-2001). Slovo, Vol. 18, No. 2, (Autumn 2006), 129-145.

Rantapelkonen, Jari and Salminen, Mirva (eds.) The Fog of Cyber Defence. National Defence University, Department of Leadership and Military Pedagogy, Series 2: Article Collection N:o 10. Tampere: Juvenes Print, 2013.

Rathbun, Brian. Uncertainty about Uncertainty: Clarifying a Crucial Concept for International Relations Theory. International Studies Quarterly, Vol.51, No. 3 (2007), 25-47.

Rathbun, Brian. A Rose by Any Other Name: Neoclassical Realism as the Logical and Necessary Extension of Structural Realism. Security Studies, Vol. 17, 294-332.

Rathbun, Brian C. Is Anybody Not an (International Relations) Liberal? Security Studies, Vol. 19 (2019), 2-25.

Rathbun, Brian. Politics and Paradigm Preferences: The Implicit Ideology of International Relations Scholars. International Studies Quarterly, Vol. 56, No. 3 (September 2012), 607–622.

Rattray, Gregory J. Strategic Warfare in Cyberspace. Cambridge: MIT Press, 2001.

Rattray, Gregory J. An Enviromental Approach to Understanding Cyberpower. In Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K. Cyberpower and National Security. Washington, D.C.: National Defence University Press, 2009, 253-274.

Raymond, M. Puncturing the Myth of the Internet as a Commons. Georgetown Journal of International Affairs, International Engagement to Cyber III, 2015, 57 - 68.

Reardon, R. and Choucri, N. The Role of Cyberspace in International Relations: A View of the Literature. Prepared for the 2012 ISA Annual Convention, San Diego, CA, 2012 [Online] Available: https://nchoucri.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf [Accessed: 6 August 2018].

Remmer, Vladimir. The Role of Internet Based Social Networks in Russian Protest Movement Mobilization, Central European Journal of International and Security Studies, Vol. 11, No. 1 (2017), 104-135.

Renz, Bettina and Smith, Hanna. Russia and Hybrid Warfare – Going Beyond the Label. Aleksanteri Papers 1/2016. Helsinki: Kikimora Publications, 2016.

Renz, Bettina. Russia and 'hybrid warfare'. Contemporary Politics, Vol.22, No.3 (2016), 283-300.

Renz, Bettina. Russia's Military Revival. Cambridge: Polity Press, 2018.

Reus-Smith, Christian. The Moral Purpose of the State: Culture, Social Identity, and Institutional Rationality in International Relations. Princeton: Princeton University Press, 1999.

Reus-Smith, Christian. Constructivism. In Burchill, Scott, Linklater Andrew, Devetak, Richard., Donnelly, Jack. Paterson, Matthew, Reus-Smith, Christian and True, Jacqui. Theories of International Relations (3rd), New York: Palgrave Macmillan, 2005, 188-212.

Reus-Smith, Christian and Snidal, Duncan (eds.) The Oxford Handbook of International Relations. Oxford: Oxford University Press, 2010.

Reveron, Derek (ed.) Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Washington, D.C.: Georgetown University Press, 2012.

Rid, Thomas. Cyber war will not take place. Journal of Strategic Studies, Vol. 38, No. 1 (2012), 5-32.

Rid, Thomas. Rise of the Machines: A Cybernetic History. New York: W. W. Norton & Company Inc., 2016.

Rid, Thomas. Cyber War Will Not Take Place. Oxford: Oxford University Press, 2017.

Rid, T. and Buchanan, B. Attributing Cyber Attacks. Journal of Strategic Studies, Vol. 35, No. 1 (2015), 4-37.

Rid, Thomas and McBurney, Peter. Cyber-Weapons. The RUSI Journal, Vol. 157, No. 1 (2012), 6-13.

Rindzeviciuté, Eglé. Constructing Soviet Cultural Policy: Cybernetics and Governance in Lithuania after World War II. Linköping, Linköping University, 2008.

Rieker, Pernille and Gjerde, Kristian Lundby. The EU, Russia and the potential for dialogue – different readings of the crisis in Ukraine. European Security, Vol. 25, No. 3 (2016), 304-325.

Ringsmore, Jens and Friis, Karsten (eds.). Conflict in Cyber Space: Theoretical, Strategic, and Legal Perspectives. London: Routledge, 2016.

Ripsman, Norrin M., Taliaferro, Jeffrey W. and Lobell, Steven E. Neoclassical Realist Theory of International Relations. New York: Oxford University Press, 2016.

Risse-Kappen, Thomas. Ideas Do Not Float Freely: Transnational Coalitions, Domestic Structures, and the End of the Cold War. International Organization, Vol. 48 (1994), 185-214.

Ristolainen, Mari. (2017a) Should 'RuNet 2020' be taken seriously? Contradictory views about cyber security between Russia and the West. In Scanlon, Mark and Le-Khac, Nhien-An (eds.) Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS), Dublin, Ireland, June 29.-30., 2017, 370-379.

Ristolainen, Mari. (2017b) Should "RuNet 2020" be taken seriously? Contradictory views about cybersecurity between Russia and the West. Journal of Information Warfare, Vol. 16, No. 4 (2017), 113-131.

Ristolainen, Mari and Kukkola, Juha. (2019a) Closed, safe and secure – the Russian sense of information security. In Benson, Vladlena and McAlaney, John. (Eds.) Emerging Cyber Threats and Cognitive Vulnerabilities. Elsevier, 2019, 53-71.

Ristolainen, Mari and Kukkola, Juha. (2019b) Western world order in the crosshairs? A theoretical review and application of the Russian 'information weapon'. Presented in 18th European Conference on Cyber Warfare and Security (ECCWS) University of Coimbra, Portugal, July 4.-5., 2019.

Rivera, J. Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk. In Maybaum, M. O. and Lindström, L. (eds.) 7th International Conference on Cyber Conflict: Architectures in Cyberspace. Tallinn: NATO CCD COE Publications, 2015, 7 - 24.

Roberts, Karl. The United States. In Tsyganov, Andrei P. Routledge Handbook of Russian Foreign Policy. London and New York: Routledge, 2018, 237-253.

Robinson, Linda, Helmus, Todd C., Cohen, Raphael S., Nader, Alizera, Radin, Andrew, Magnuson, Madeline and Migacheva, Katya. Modern Political Warfare: Current Practices and Possible Responses. Santa Monica, Calif.: RAND, 2018.

Roesen, Tine and Zvereva, Vera. Social network sites on the Runet. Exploring social communication. In Gorham, Michael S., Lunde, Ingunn and Paulsen, Amrtin (eds.) Digital Russia: The Language, Culture and Politics of New Media Communication. London & New York: Routledge, 2014.

Roffey, Roger. Russian Science and Technology is Still Having Problems—Implications for Defense Research. The Journal of Slavic Military Studies, Vol.26, No.2 (2013), 162-188.

Roffey, Roger: Russia's EMERCON: Managing emergencies and political stability, FOI, 2016.

Rona, Thomas. Weapon Systems and Information War. 1 July 1976. Office of the secretary of defence, Washington D.D. [Online]. Available: http://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf [Accessed: 14th August 2018].

Rose, Gideon. Neoclassical Realism and Theories of Foreign Policy. World Politics, vol. 51, no. 1 (1998), 144 – 172.

Rosen, Stephen Peter. Military Effectiveness: Why Society Matters. International Security, Vol. 19, No.4 (Spring 1995), 5-31

Rousseau, D. L., Thrall, T. A., Schulzke, M. and Sin, S. S. Democratic leaders and war: simultaneously managing external conflicts and domestic politics. Australian Journal of International Affairs, Vol. 66, No. 3 (2012), 349-364.

Rowley, Jennifer. The wisdom hierarchy: representations of the DIKW hierarchy. Journal of Information Science, Vol. 33, No. 2 (2007), 163-180.

Ruffa, Chiara. Military Cultures and Force Employment in Peace Operations. Security Studies, Vol. 26, No. 3 (2017), 391-422.

Ruggie, John Gerard. International Responses to Technology: Concepts and Trends. International Organization, Vol. 29, No. 3, International Responses to Technology (Summer, 1975), 557-583.

Ruggie, John Gerard. What Makes the World Hang Together? Neo-Utilitarianism and the Social Constructivist Challenge. International Organization, Vol. 52, No. 4, (Autumn, 1998), 855-885.

Ruggie, John Gerard, Katzenstein, Peter J., Keohane, Robert O. and Schmitter, Philippe C. Transformations in World Politics.: The Intellectual Contributions of Ernst B. Haas. Annual Reviews of Political Science, Vol. 8 (2005), 271-96.

Russell, A. L. Cyber Blockades. Washington DC: Georgetown University Press, 2014.

Russell, Stuart and Norvig, Peter. Artificial intelligence – A Modern Approach. New Jersey: Prentice Hall, 2014.

Sabillon, Regner, Cavaller, Victor and Cano, Jeimy. National Cyber Security Strategies: Global Trends in Cyberspace. International Journal of Computer Science and Software Engineering, Vol. 5, No. 5 (May 2016), 67-81.

Sadykiewicz, Michael. The Warsaw Pact Command Structure in Peace and War. Santa Monica: RAND Corporation, 1988.

Sakwa, Richard. Russian Politics and Society (4th ed.) London and New York: Routledge, 2008.

Sakwa, Richard. The Soviet collapse: Contradictions and neo-modernisation. Journal of Eurasian Studies, Vol. 4, No. 1 (2013), 65-77.

Sakwa, Richard. Dualism at Home and abroad: Russian Foreign Policy Neo-Revisionism and Bicontinentalism. Cadier, David and Light, Margot (eds.) Russia's Foreing Policy. Ideas, Domestic Politics and External Relations. Basingstoke: Palgrave Macmillan, 2015, 65-79.

Saltzman, I. Z. Growing Pains: Neoclassical Realism and Japan's Security Policy Emancipation. Contemporary Security Policy, Vol. 36, No. 3 (2015), 498 – 527.

Sanger, David E. The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. Melbourne: Scribe, 2018.

Sankaran, Jaganath. Limits of the Chinese Antisatellite Threat to the United States. Strategic Studies Quarterly, Vol. 8, No. 4 (WINTER 2014), 19-46.

Scanlon, Mark and Le-Khac, Nhien-An (eds.) Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS), Dublin, Ireland, June 29.-30., 2017.

Scharre, Paul. Army of None. Autonomous Weapons and the Future War. New York & London: W. W. Norton & Company, 2018.

Schelling, T. C. Arms and Influence. New Haven: Yale University Press, 2008.

Scheuerman, William E. Hans Morgenthau: Realism and Beyond. Cambridge, UK: Polity Press, 2009.

Schieder, Siegfried and Spindler, Manuela (eds.) Theories of International Relations. New York: Routledge, 2015.

Schieder, Siegfried. New Liberalism. In Schieder, Siegfried and Spindler, Manuela (ed.) Theories of International Relations. New York: Routledge, 2015, 107-129.

Schmidt, B. C. Realist conceptions of power. In Berenskoetter, Felix and Williams, M. J. (Eds.) Power in World Politics. London: Routledge, 2007, 43 – 61.

Schmidt, Brian C. On the History and Historiography of International Relations. In Carlsnaes, Walter, Risse, Thomas & Simmons, Beth A. (eds.): Handbook of International Relations. London: SAGE Publications, 2005, 3-22.

Schmidt, Brian. Lessons from the Past: Reassessing the Interwar Disciplinary History of International Relations. International Studies Quarterly, Vol. 42, No. 3 (September 1998), 433-459.

Schmidt, Sebastian. To Order the Minds of Scholars: The Discourse of the Peace of Westphalia in International Relations Literature. International Studies Quarterly, Vol. 55 (2011), 601–623.

Schmitt, Michael N. (ed.) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press, 2017.

Schmitt, Olivier. Strategic Users of Culture: German Decisions for Military Action. Contemporary Security Policy, Vol. 33, No. 1 (2012), 59-81.

Schoen, Fletcher and Lamb, Christopher, J. Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference. INSS Strategic Perspectives 11. Washington, DC: National Defense University.

Schreier, Fred. On Cyberwarfare. DCAF Horizon 2015 Working Paper No. 7 [Online] Available: https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf [Accessed: 10th August 2018].

Schware, Robert (ed.) E-Development: From Excitement to Effectiveness. Washington D.C.: The World Bank Group, 2004 [Online]. Available: http://documents.worldbank.org/curated/en/261151468325237852/pdf/341470EDevelopment.pdf [Accessed: 13th May 2019].

Schweller, Randall L. Deadly Imbalances. Tripolarity and Hitler's Strategy of World Conquest. New York: Columbia University Press, 1998.

Schweller, Randall L. Unanswered Threats. A Neoclassical Realist Theory of Underbalancing. International Security, Vol. 29, No. 2 (2004), 159–201.

Schweizer, P. The Soviet military goes high-tech. Orbis, Vol. 35, Issue 2 (Spring 1991).

Scott, Harriet Fast and Scott, William F. Soviet Military Doctrine. Continuity, Formulation, and Dissemination. New York: Routledge, 2019 (org. 1988).

Service, Robert. The End of the Cold War 1985-1991. New York: Public Affairs, 2015.

Shafqat, Narmeen and Masood, Ashraf. Comparative Analysis of Various National Cyber Security Strategies. International Journal of Computer Science and Information Security, Vol. 14, No. 1 (January 2016), 129-136.

Shapcott, Richard. Critical Theory. In Reus-Smith, Christian and Snidal, Duncan (eds.) The Oxford Handbook of International Relations. Oxford: Oxford University Press, 2010, 331-334.

Sharp, Travis. Theorizing cyber coercion: The 2014 North Korean operation against Sony. The Journal of Strategic Studies, vol. 40, no. 7 (2017), 898-926.

Sheldon, John B. Towards a Theory of Cyber Power: Strategic Purpose in Peace and War. In Reveron, Derek (ed.) Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Washington, D.C.: Georgetown University Press, 2012, 207-224.

Sheldon, John B. The Rise of Cyberpower. In Baylis, John, Wirtz, James J. and Gray, Colin S. Strategy in the Contemporary World (4th ed.) Oxford: Oxford University Press, 2013, 301-319.

Shevtsova, Lilia. Post-communist Russia: a historic opportunity missed. International Affairs Vol. 83(5) (2007), 891–912.

Siboni, Gabi and Kronenfeld, Sami. Iran and Cyberspace Warfare. Military and Strategic Affairs, Vol. 4, No. 3, (December 2012), 77-99.

Sil, Rudra. Simplifying Pragmatism: From Social Theory to Problem-driven Eclecticism. In Gunther, Hellman (ed.) Pragmatism and International Relations. International Studies Review, Vol. 11, No. 3 (September 2009), 648-652.

Skak, Mette. Russian strategic culture: the role of today's chekisty. Contemporary Politics, Vol. 22, No. 3 (2016), 324-341.

Slayton, R. What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. International Security, Vol. 41, No. 3 (2017), 72 - 109.

Sloan, Elinor C. Modern Military Strategy: An introduction. New York: Routledge, 2012.

Smeets, Max. A matter of time: On the transitory nature of cyberweapons, Journal of Strategic Studies, Vol. 41, No. 1-2 (2018), 6-32.

Smeets, Max and Lin, Herbert S. Offensive Cyber Capabilities: To What Ends? In Minárik, T., Jakschis, R. and Lindström, L. (eds.) 10th International Conference on Cyber Conflict CyCon X: Maximising Effects. Tallinn: NATO CCD COE, 2018, 55-72.

Smith, Martin A. A bumpy road to an unknown destination? NATO-Russia relations, 1991–2002, European Security, Vol. 11, No.4 (2002), 59-77.

Smith, Rupert. The Utility of Force: The Art of War in the Modern World. New York: Vintage Books, 2008.

Smith, Steve. Positivism and Beyond. In Smith, Steve, Booth, Ken, and Zalewski, Marysia: International theory: Positivism and Beyond. Cambridge: Cambridge University Press, 1996, 11-44.

Smith, Steve, Booth, Ken, and Zalewski, Marysia: International theory: Positivism and Beyond. Cambridge: Cambridge University Press, 1996.

Smith, Steve. The increasing insecurity of security studies: Conceptualizing security in the last twenty years, Contemporary Security Policy, Vol. 20, No. 3, 1999, 72-101.

Snyder, Jack L. The Soviet Strategic Culture: Implications for Limited Nuclear Operations. R-2154-AF. Santa Monica, RAND corporation, 1977 [Online]. Available: https://www.rand.org/content/dam/rand/pubs/reports/2005/R2154.pdf. Accessed: 28 May 2018.

Snyder, Jack. Limiting Offensive Conventional Forces: Soviet Proposals and Western Options. International Security. Vol. 12, No. 4 (Spring, 1988), 48-77.

Snyder, Glenn. Deterrence and Defence. Princeton: Princeton University Press, 1961.

Sokolski, Henry D. Nuclear Mutual Assured Destruction, Its Origins And Practice. Carslile: Strategic Studies Institute, US Army War College, 2004.

Soldatov, Andrei and Borogan, Irina. The New Nobility: The Restoration of Russia's Security State and the Legacy of the KGB. New York: Public Affairs, 2010.

Soldatov, Andrei and Borogan, Irina. Russia's Surveillance State. World Policy Journal, Vol. 30, No. 3 (Fall 2013), 23-30.

Soldatov, Andrei and Borogan, Irina. The Red Web. The Struggle Between Russia's Digital Dictators and The New Online Revolutionaries. New York: Public Affairs, 2015.

Soldatov, Andrei. The Taming of the Internet. Russian Social Science Review, Vol. 58, No. 1 (January–February 2017), 39-59.

Soldatov, Andrei and Rochlitz, Michael. The Siloviki in Russian Politics. In Treisman, Daniel (ed.) The New Autocracy: Information, Politics, and Policy in Putin's Russia. Washington, D.C.: Brookings Institution Press, 2018, 79-103.

Sondhaus, Lawrence. Strategic Culture and Ways of War. New York, Routledge, 2006.

Starr, S. H. Towards a Premilinary Theory of Cyberpower. In Kramer, F., Starr, S. and Wentz, L. (Eds.) Cyberpower and National Security. Washington D.C: National Defense University Press, 2009, 43-81.

Sterling-Folker, Jennifer. Competing Paradigms or Birds of a Feather? Constructivism and Neoliberal Institutionalism Compared. International Studies Quarterly, Vol. 44, No. 1 (March 2000), 97-119.

Sterling-Folker, Jennifer. Realist-Constructivism and Morality. International Studies Review Vol. 6, No. 2 (2004), 337-352.

Stevens, Tim. A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. Contemporary Security Policy, Vol. 33, No. 1 (2012), 148 - 170.

Stone, John. Cyber War Will Take Place! Journal of Strategic Studies, Vol. 36, No. 1 (2013), 101-108.

Stoner, Kathryn E. and McFaul, Michael A. Russian security policy towards the US. In Kanet, Roger E. Routledge Handbook of Russian Security. London and New York: Routledge, 2019, 242-256.

Storey, John (ed.) Cultural Theory and Popular Culture: A Reader (5th ed.) London: Pearson Longman, 2015.

Strachan, Hew. The Direction of War: Contemporary Strategy in Historical Perspective. New York: Cambridge University Press, 2013.

Strachan, Hew and Herberg-Rothe, Andreas. Clausewitz in the Twenty-First Century. Oxford: Oxford University Press, 2009.

Starosielski, Nicole. The Undersea Network. Durham and London: Duke University Press, 2015.

Stuart, Douglas T. Foreign-Policy Decision-Making. In Reus-Smith, Christian and Snidal, Duncan (eds.) The Oxford Handbook of International Relations. Oxford: Oxford University Press, 2010, 576-593.

Stuenkel, Oliver. Post-Western World: How Emerging Powers Are Remaking Global Order. Cambridge: Polity Press, 2016.

Sushentsov, Andrei. The Russian Response to the RMA: Military Strategy towards Modern Security Threats. In Collins, Jeffrey and Futter, Andrew (Eds.) Reassessing the Revolution in Military Affairs: Transformation, Evolution and Lessons Learned. New York: Palgrave Macmillian, 2015, 112-131.

Tanenbaum, Andrew S. and Wetherall, David J. Computer Networks (5th ed.) Boston: Prentice Hall, 2011.

Tang, Shipping. Taking Stock of Neoclassical Realism. International Studies Review, Vol. 11 (2009), 799-803.

Tannenwald, Nina. Ideas and Explanation: Advancing the Theoretical Agenda. Journal of Cold War Studies Vol. 7, No. 2 (Spring 2005), 165-173.

Tannenwald, Nina and Wohlforth, William C. Introduction: The Role of Ideas and the End of the Cold War. Journal of Cold War Studies, Vol. 7, No. 2 (Spring 2005), 3–12.

Tannenwald, Nina. Process Tracing and Security Studies. Security Studies, Vol. 24, No. 2 (2015), 219-227.

Temby, Owen. What are levels of analysis and what do they contribute to international relations theory? Cambridge Review of International Affairs, Vol. 28, No. 4 (2015), 721-742.

Tertrais, Bruno. Russia's Nuclear Policy: Worrying for the Wrong Reasons, Survival, Vol.60, No.2 (2018), 33-44.

Thomas, Timothy. Nation-state Cyber Strategies: Examples from China and Russia. In Kramer, F., Starr, S. and Wentz, L. (Eds.) Cyberpower and National Security. Washington D.C: National Defense University Press, 2009, 465-488.

Thomas, Timothy L. Russian Views on Information-Based Warfare. Airpower Journal – Special Edition 1996, 26-35.

Thomas, Timothy L. (1998a) Russia's information warfare structure: Understanding the roles of the security council, Fapsi, the state technical commission and the military, European Security, Vol. 7, No. 1 (Spring1998), 156-172.

Thomas, Timothy L. (1998b) Dialectical versus empirical thinking: Ten key elements of the Russian understanding of information operations, The Journal of Slavic Military Studies, Vol. 11, No. 1 (1998), 40-62.

Thomas, Timothy L. The Russian Understandings of Information Operations and Information Warfare. In Alberts, David S. and Papp, Daniel S. (eds.) Information Age Anthology – Volume III: The Information Age Military – Volume III. CCRP Publication Series, 2001, 777-814.

Thomas, Timothy. Is the IW Paradigm Outdated? A Discussion of U.S. IW Theory. Journal of Information Warfare, Vol. 2, No. 3 (2003), 109 – 116.

Thomas, Timothy. Russia's Reflexive Control Theory and the Military, Journal of Slavic Military Studies, Vol. 17, No. 2 (2004), 237-256.

Thomas, Timothy. Cyber Silhouettes. Shadows Over Information Operations. Fort Leavenworth, KS: Foreign Military Studies Office, 2005.

Thomas, Timothy, L. Decoding The Virtual Dragon - Critical Evolutions In The Science And Philosophy Of China's Information Operations And Military Strategy - The Art Of War And IW. Fort Leavenworth, KS: ISMS, 2007.

Thomas, Timothy L. The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia, Journal of Slavic Military Studies, Vol.22, No.1 (2009), 31-67.

Thomas, Timothy L. Russian Information Warfare Theory: The Consequences of August 2008. In Blank, Stephen J. and Weitz, Richard (Eds.) The Russian Military Today and Tomorrow: Essays in Memory of Mary FitzGerald. Army War College Strategic Studies Institute (SSI), 2010, 265-299 [Online] Available: https://ssi.armywarcollege.edu/pdffiles/PUB997.pdf [Accessed: 22th October 2018].

Timothy, Thomas L. Three Faces Of The Cyber Dragon. Fort Leavenworth, KS: ISMS, 2012.

Thomas, Timothy. (2015a) Russia Military Strategy: Impacting 21st Century Reform and Geopolitics. Fort Leavenworth: Foreign Military Studies Office, 2015.

Thomas, Timothy. (2015b) Russia´s 21st century information warfare: Working to undermine and destabilize populations, Defence Strategic Communications, Vol. 1, No. 1 (Winter 2015), 11-26.

Thomas, Timothy. (2015c) Russia's Military Strategy and Ukraine: Indirect, Asymmetric—and Putin-Led. The Journal of Slavic Military Studies, Vol. 28, No. 3 (2015), 445-461.

Thomas, Timothy. (2016a) The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking. The Journal of Slavic Military Studies, Vol. 29, No. 4 (2016), 554-575.

Thomas, Timothy. (2016b) Thinking Like a Russian Officer: Basic Factors and Contemporary Thinking on the Nature of War. Fort Leavenworth, KS., FMSO, 2016.

Thomas, Timothy. Kremlin Kontrol: Russia's Political' Military Reality. Fort Leavenworth, KS: FMSO, 2017.

Thomas, Timothy. Russia's Expanding Cyber Activities: Exerting Civilian Control While Enhancing Military Reform. In Blank, Stephen J. (ed.) The Russian Military in Contemporary Perspective. Carlisle Barracks, PA., U.S. Army War College Press, 2019, 491-574.

Thornton, Rod. Turning strengths into vulnerabilities: the art of asymmetric warfare as applied by the Russian military in its hybrid warfare concept. In Renz, Bettina and Smith, Hanna. Russia and Hybrid Warfare – Going Beyond the Label. Aleksanteri Papers 1/2016. Helsinki: Kikimora Publications, 2016, 52-60.

Tikk, Eneken and Kerttunen, Mika. The Alleged Demise of the UN GGE: An Autopsy and Eulogy. New York: Cyber Policy Institute, 2017 [Online] Available: http://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf [Accessed: 7th August 2018].

Tikk, Eneken. International Cyber Norms Dialogue as an Exercise of Normative Power. Georgetown Journal of International Affairs. 17 (2016), 47-59. 10.1353/gia.2016.0036. [upcoming] [Online] Available: (http://ict4peace.org/wp-content/uploads/2017/02/Tikk-Normative-Power.pdf) [Accessed: 17 December 2017].

Tikk, Eneken and Kerttunen, Mika. Parabasis. Cyber-diplomacy in Stalemate. Norwegian Institute of International Affairs, 2018 [Online]. Available: https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2569401/NUPI_Report_5_18_Tikk_Kerttunen.pdf?sequence=1&isAllowed=y [Accessed: 6th May 2019].

Tor, Uri. 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence, The Journal of Strategic Studies, Vol. 40, No. 1-2 (2017), 92-117.

Treisman, Daniel (ed.) The New Autocracy: Information, Politics, and Policy in Putin's Russia. Washington, D.C.: Brookings Institution Press, 2018.

Trenin, Dmitri. The End of Eurasia: Russia on the Border Between Geopolitics and Globalization. Washington, DC: The Carnegie Moscow Center, 2001.

Trenin, Dmitri. Russia's Breakout from the Post-Cold War System: The Drivers of Putin's Course. Carnegie Moscow Center, 22 December 2014.

Trenin, Dmitri. Russia Redefines Itself and Its Relations with the West. The Washington Quarterly, Vol. 30, No. 2 (2007), 95–105.

Trenin, Dmitri. Russian Foreign Policy as Exercise in Nation Building. In Cadier, David and Light, Margot (eds.) Russia's Foreign Policy. Ideas, Domestic Politics and External Relations. Basingstoke: Palgrave Macmillan, 2015, 30-41.

Tsygankov, Andrei P. Russia's Foreign Policy: Change and Continuity in National Identity (4th ed.) London: Rowman & Littlefield, 2016.

Tsygankov, Andrei (ed.) Routledge Handbook of Russian Foreign Policy. London: Taylor & Francis Ltd., 2018.

Tsypkin, Mikhail Military Influence in Russian Politics. AD-A256 718. Montrey, CA: Naval Postgraduate School [Online] Available: http://www.dtic.mil/dtic/tr/fulltext/u2/a256718.pdf [Accessed: 2nd October 2018].

Tuukkanen, Topi. Sovereignty in the Cyber Domain. In Rantapelkonen, Jari and Salminen, Mirva (eds.) The Fog of Cyber Defence. National Defence University, Department of Leadership and Military Pedagogy, Series 2: Article Collection N:o 10. Tampere: Juvenes Print, 2013, 37-45.

Twomey, Christopher P. Lacunae in the Study of Culture in International Security. Contemporary Security Policy, Vol. 29, No. 2, (August 2008), 338-357.

Ulbert, Cornelia. Social Constructivism. In Schieder, Siegfried and Spindler, Manuela (eds.) Theories of International Relations. New York: Routledge, 2015, 248-268.

Ullman, Harlan K., Wade, James P. (eds.) Shock and Awe - Achieving Rapid Dominance. Washington: National Defence University, 1996.

Uz Zaman, Rashid. Strategic Culture: A "Cultural" Understanding of War. Comparative Strategy, Vol. 28, No. 1 (2009), 68- 88.

Vacca, John R. (ed.) Network and System Security (2nd ed.) Waltham: Syngress, 2014.

Vacca, John. Cyber Security and IT Infrastructure Protection. Amsterdam: Syngress 2014.

Valeriano, Brandon and Maness, Ryan C. Cyber War versus Cyber Realities Cyber Conflict in the International System. New York: Oxford University Press, 2015.

Valeriano, Brandon, Jensen, Benjamin and Maness, Ryan C. Cyber Strategy: The Evolving Chracter of Power and Coercion. New York: Oxford University Press, 2018.

Valeriano, Brandon and Ryan C. Maness. Cyber Spillover Conflicts: Transitions from Cyber Conflict to Conventional Foreign Policy Disputes?" In Ringsmore, Jens and Friis, Karsten (eds.). Conflict in Cyber Space: Theoretical, Strategic, and Legal Perspectives. London: Routledge, 2016, 45-64.

Van Evera, Stephen. Guide to Methods for Students of Political Science. Ithica, NY: Cornell University Press, 1997.

Van Evera, Stephen. Offense, Defense, and the Causes of War. International Security, Vol. 22, No. 4 (Spring 1998), 5-43.

Vargas-Leon, Patricia. Tracking Internet Shutdown Practices: Democracies and Hybrid Regimes. In Musiani, Francesca, Cogburn, Derrick L., DeNardis, Laura & Levinson, Nanette S. (Eds.) The Turn to Infrastructure in Internet Governance. New York: Palgrave Macmillan, 2016, 167-188.

Vasquez, John A. The Realist Paradigm and Degenerative versus Progressive Research Programs: An Appraisal of Neotraditional Research on Waltz's Balancing Proposition. The American Political Science Review, Vol. 91, No. 4 (December 1997), 899-912.

Vego, Milan. Recce-Strike Complexes in Soviet Theory and Practice. Fort Leavenworth, KS: SASO, 1990.

Vego, Milan. Joint Operational Warfare: Theory and Practise, Vol. 1. Newport: US Naval War College, 2007.

Ven Bruusgaard, Kristin. Russian Strategic Deterrence. Survival, Vol. 58, No. 4 (2016), 7-26.

Vendil, Carolina. The Russian security council, European Security, Vol.10, No.2 (Summer 2001), 67-94.

Vendil Pallin, Carolina. The Russian Power Ministries: Tool and Insurance of Power, Journal of Slavic Military Studies, Vol.20, No.1 (2007), 1-25.

Vendil Pallin, Carolina. Internet control through ownership: the case of Russia, Post-Soviet Affairs, Vol. 33 No. 1, 2017, 16-33.

Vendil Pallin, Carolina. Russian information security and warfare. In Kanet, Roger E. Routledge Handbook of Russian Security. London and New York: Routledge, 2019, 203-213.

Vendil Pallin, Carolina and Oxenstierna, Susanne. Russian Think Tanks and Soft Power. FOI, August 2017 [Online]. Available: https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4451--SE [Accessed: 5th April 2019].

Vennesson, P. Is Strategic Studies narrow? Critical security and the misunderstood scope of strategy. Journal of Strategic Studies, Vol. 40, No. 3 (2017), 358 – 391.

Ventre, Daniel. Information Warfare (2nd revised ed.) Hoboken: John Wiley & Sons, 2016.

Von Heinegg, Wolff Heintschel: Legal Implications of Territorial Sovereignty in Cyberspace. In Czosseck, C., Ottis, R. and Ziolkowski, K. (Eds.) 4th International Conference on Cyber Conflict. Tallinn: NATO CCD COE Publications, 2012, 7-20.

Waltz, Edward. Information Warfare: Principles and Operations. Boston: Artech House, 1998.

Waever, Ole. The Sociology of a Not So International Discipline: American and European Developments in International Relations, International Organization, Vol. 52, No. 4, Autumn, 1998, 687-727.

Waever, Ole. Still a discipline after all these debates? In Dunne, T. Kurki, M. and Smith, S. International Relations Theories: Discipline and Diversity (4th ed.) Oxford: Oxford University Press, 2013, 300-321.

Waldner, David. Process Tracing and Qualitative Causal Inference. Security Studies, Vol. 24, No. 2 (2015), 239-250.

Waltz, Kenneth. Theory of International Politics, Boston: Addison-Wesley, 1979.

Warden, John. The enemy as a system. Airpower Journal, Vol. IX, No. 1, 1999 (Spring), 40-55.

Webb, Isaac. Russian Web Censor Cracks Down Ahead of Next Anti-Corruption Protests. Global Voices, 31 March 2017 [Online]. Available: https://globalvoices.org/2017/03/31/russian-web-censor-cracks-down-ahead-of-next-anti-corruption-protests/ [Accessed: 14th May 2019].

Weber, Cynthia. International Relations Theory: A Critical Introduction. London: Routledge, 2013.

Weber, Yaval. Petropolitics. In Tsyganov, Andrei P. Routledge Handbook of Russian Foreign Policy. London and New York: Routledge, 2018, 99-117.

Webster, Frank. Theories of the Information Society. London and New York: Routledge, 2006.

Wellman, David A. A Chip in the Curtain. Computer Technology in the Soviet Union. Washington, DC: NDU Press, 1989.

Wendt, Alexander. Social Theory of International Politics. Cambridge: Cambridge University Press, 1999.

Westerlund, Fredrik and Oxenstierna, Susanne (eds.) Russian Military Capability in a Ten-Year Perspective – 2019. Stockholm: FOI, 2019.

Whyte, Christopher, Valeriano, Brandon, Jensen, Benjamin and Maness, Ryan. Rethinking the Data Wheel: Automating Open-Access, Public Data on Cyber Conflict. In Minárik, T., Jakschis, R. and Lindström, L. (eds.)

10th International Conference on Cyber Conflict CyCon X: Maximising Effects. Tallinn: NATO CCD COE, 2018, 9-30.

Whyte, Christopher and Mazanec, Brian. Understanding Cyber Warfare. Politics, Policy and Strategy. London & New York: Routledge, 2019.

Wight, Colin. Philosophy of Social Science and International Relations. In Carlsnaes, Walter, Risse, Thomas and Simmons, Beth A. (eds.) Handbook of International Relations. London: SAGE Publications, 2005, 23-51.

Wight, Colin. After Postpositivism? The Promises of Critical Realism. International Studies Quarterly, Vol. 44, No. 2 (June 2000), 213-237.

Wight, Colin. Agents, Structures and International Relations: Politics as Ontology, Cambridge: Cambridge University Press, 2006.

Wight, Colin. A Response to Friedrich Kratochwil: Why Shooting the Messenger Does Not Make the Bad News Go Away. Journal of International Relations and Development, Vol. 10, No. 3 (September 2007), 301-315.

Westad, Odd Arne. The Cold War: A World History. London: Penguin Random House, 2017.

Wilkinson, Benedict and Gow, Jameson (eds.) The Art of Creating Power: Freedman on Strategy. London: Hurst & Company, 2017.

Williams, Michael C. Why Ideas Matter in International Relations: Hans Morgenthau, Classical Realism, and the Moral Construction of Power Politics. International Organization, Vol. 58, No. 4 (Fall 2004), 633-665.

Williams, Paul D. (ed.) Security Studies: An Introduction. London, Routledge, 2008 (2013).

Williams, Alison J., Jenkings, Neil K., Rech, Matthew F. and Woodward, Rachel. The Routledge Companion to Military Research Methods. New York: Routledge, 2016.

Wirtz, J. J. Life in the “Gray Zone”: observations for contemporary strategists. Defense & Security Analysis, Vol. 33, No. 2 (2017), 106 – 114.

Wohlforth, William C. Realism. Reus-Smith, Christian and Snidal, Duncan (eds.) The Oxford Handbook of International Relations. Oxford: Oxford University Press, 2010, 131-149.

Wolfe, Audra J. Competing with the Soviets. Science, Technology, and the State in the Cold War America. Baltimore: Johns Hopkins University Press, 2013.

Womack, James K. Soviet Correlation of Forces and Means: Quantifying Modern Operations. Master’s thesis. Fort Leavenworth, KS: U.S. Army Command and General Staff College, 1990.

World Economic Forum. The Global Risks Report 2018 – 13th Edition. Geneva: WEF.

Wortzel, Larry M. The Chinese people’s liberation army and information warfare. The Strategic Studies Institute of The United States Army War College, 2014 [Online]. Available: https://publications.armywarcollege.edu/pubs/2263.pdf [Accessed: 22th June 2019].

Wu, Chwan-Hwa and Irwin, David J. Introduction to Computer Networks and Cybersecurity. Boca Raton: CRC Press, 2013, 786-788.

Wylie, J. C. Military Strategy: A General Theory of Power Control. Annapolis, Maryland: Naval Institute Press, 2014.

Yablokov, Ilya. Fortress Russia: Conspiracy Theories in Post-Soviet Russia. Cambridge: Polity Press, 2018.

Yarynich, Valery E. C3: Nuclear Command, Control Cooperation. Washington, DC: Center for Defense Information, 2003.

Yee, Albert S. ’The Causal Effect of Ideas on Politics’. International Organization, Vol. 50 (1996), 69-108.

Yee, Albert S. Thick Rationality and the Missing “Brute Fact”. The Limits of Rationalist Incorporations of Norms and Ideas. The Journal of Politics, Vol. 59, No. 4 (November 1997), 1001-1039.

Zakaria, Fareed From Wealth to Power. The Unusual Origins of Americas World Role. Princeton: Princeton University Press, 1998.

Zhang, Nan, Krishna, Kant and Sajal K. Handbook on Securing Cyber-Physical Critical Infrastructure. Amsterdam: Elsevier, 2012.

Zins, Chaim. Conceptual Approaches for Defining Data, Information, and Knowledge. Journal of the American Society for Information Science and Technology, Vol. 58, No. 4 (2007), 479-493.

Zubok, Vladislav M. Soviet foreign policy from détente to Gorbachev, 1975-1985. In Leffler, Melvyn P. and Westad, Ood Arne (Eds.) The Cambridge History of The Cold War: Volume III Endings. Cambridge: Cambridge University Press, 2010, 89-111.

Zürn, Michael and Checkel, Jeffrey T. Getting Socialized to Build Bridges: Constructivism and Rationalism, Europe and the Nation State. International Organization, Vol. 59, No. 4 (October 2005), 1045-1079.

Webpages & News

Finnish language source:

Viestintävirasto. HAVARO havainnoi ja varoittaa tietoturvaloukkauksista. 24 May 2016 [Online] Available: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2016/05/ttn201605241520.html [Accessed: 8th August 2018].

English language source:

Alexa. Top Sites in Russia [Online]. Available: https://www.alexa.com/topsites/countries/RU [Accessed: 12th April 2019].

Aris, Ben. The Russian Economy Is Stagnating. GDP growth since the start of the year has been well below forecasts. The Moscow Times, May 28, 2019 [Online]. Available: https://www.themoscowtimes.com/2019/05/27/the-russian-economy-is-stagnating-a65760 [Accessed:28th May 2019].

Arms Control Association. The European Phased Adaptive Approach at a Glance. January 2019 [Online]. Available: https://www.armscontrol.org/factsheets/Phasedadaptiveapproach [Accessed: 30th April 2019].

Bendett, Samuel. Handicaps: weak private sector, Soviet-style bureaucracy. Helps: Great STEM education — and history. Defense One, 25 November 2019 [Online]. Available: https://www.defenseone.com/ideas/2019/11/russias-ai-quest-state-driven-even-more-chinas-can-it-work/161519/?oref=d-topstory [Accessed: 7th January 2020].

Burgess, Matt. To protect Putin, Russia is spoofing GPS signals on a massive scale. Wired, March 27, 2019 [Online]. Available: https://www.wired.co.uk/article/russia-gps-spoofing [Accessed: 1st May 2019].

BOFIT. Growth in Chinese and Russian arms exports lags growth of other major arms suppliers. BOFIT WEEKLY 2019/11 [Online]. Available: https://www.bofit.fi/en/monitoring/weekly/2019/vw201911_5/ [Accessed: 3rd May 2019].

BOFIT. Venäjä-tilastot [Russia statistics] [Online]. Available: https://www.bofit.fi/fi/seuranta/tilastot/venaja-tilastot/ [Accessed: 30th April 2019].

Carnegie Endowment for International Peace. Cyber Norms Index [Online]. Available: http://carnegieendowment.org/publications/interactive/cybernorms. [Accessed: 8th August 2018].

Center for Strategic and International Studies. Significant Cyber Incidents, September 2018 [Online]. Available: https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity [Accessed: 19th September 2018].

Cloudflare. Famous DDoS Attacks. The Largest DDoS Attacks Of All Time [Online]. Available: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/ [Accessed: 1st May 2019].

Cloudflare. What is DNS? How DNS works [Online] Available: https://www.cloudflare.com/learning/dns/what-is-dns/ [Accessed: 7th August 2018].

CSIS. Cyber From The Start podcast, multiple episodes [Online]. Available: https://www.csis.org/podcasts/cyber-start [Accessed: 28th May 2019].

Data Center Map [Online] Available: https://www.datacentermap.com/ [Accessed: 8th August 2018].

Dennis, Steven T., Brody, Ben and Frier, Sarah. Russia's Bid to Help Trump Revealed as Much Wider Than Once Known. Bloomberg, December 17, 2018 [Online]. Available: https://www.bloomberg.com/news/articles/2018-12-17/russia-waged-vast-pro-trump-social-media-plan-senate-panel-told?srnd=politics-vp [Accessed: 30th April 2019].

Dobrokhotov, Roman. Putin vs the Russian Internet - 0:1. Al Jazeera, 25 Apr 2018 [Online]. Available: https://www.aljazeera.com/indepth/opinion/putin-russian-internet-01-180424170551334.html [Accessed: 17th May 2019].

Engel, Eliot and Smith, Adam. US pulling out of the INF treaty rewards Putin, hurts NATO. CNN, February 2, 2019 [Online]. Available: https://edition.cnn.com/2019/02/01/opinions/us-pulling-out-of-the-inf-treaty-rewards-putin-hurts-nato-engel-smith/index.html?no-st=1556603190 [Accessed: 20th April 2019].

Erwin, Sandra. Air Force laying groundwork for future military use of commercial megaconstellations. SpaceNews, February 28, 2019 [Online]. Available: https://spacenews.com/air-force-laying-groundwork-for-future-military-use-of-commercial-megaconstellations/ [Accessed: 17th May 2019].

FIDH. Table Illustrating Legislative Crackdown on Rights and Freedoms of the Civil Society in Russia since 2012 (2018) [Online]. Available: https://www.fidh.org/en [Accessed: 14th May 2019].

Freedom House. Freedom on the Net 2014 - Russia [Online]. Available: https://freedomhouse.org/sites/default/files/resources/Russia.pdf [Accessed: 17th April 2019].

Freedom House. Freedom on the Net 2017: Russia, 2017 [Online]. Available: https://freedomhouse.org/report/freedom-net/2017/russia [Accessed 11 January 2018].

Freedom House. Freedom in the World 2018 – Russia. [Online]. Available: https://freedomhouse.org/report/freedom-world/2018/russia [Accessed: 25th March 2019].

GlobalSign. Certificate Authorities & Trust Hierarchies [Online]. Available: https://www.globalsign.com/en/ssl-information-center/what-are-certification-authorities-trust-hierarchies/ [Accessed: 22th June 2019].

Greenberg Andy. Cyberspies Hijacked the Internet Domains of Entire Countries. A mysterious new group called Sea Turtle targeted 40 organizations in a DNS hijacking spree, WIRED, 17th April 2019 [Online] Available: https://www.wired.com/story/sea-turtle-dns-hijacking/ [Accessed: 29th December 2019].

Grisby, Alex. Russia Wants a Deal with the United States on Cyber Issues. Why Does Washington Keep Saying No? CFR, August 27, 2018 [Online]. Available: https://www.cfr.org/blog/russia-wants-deal-united-states-cyber-issues-why-does-washington-keep-saying-no [Accessed: 1st May 2019].

Grisby, Alex. Russia, US Offer Competing Vision of Cyber Norms to the UN. Defence One, October 29, 2018 [Online]. Available: https://www.defenseone.com/politics/2018/10/russia-us-offer-competing-vision-cyber-norms-un/152382/?oref=d-river [Accessed: 25th February 2019].

Gutterman, Ivan and Grojec, Wojtek. A Timeline Of All Russia-Related Sanctions. RFE/RL, September 19, 2018 [Online]. Available: https://www.rferl.org/a/russia-sanctions-timeline/29477179.html [Accessed: 30th April 2019].

Harrison, Todd, Johnson, Kaitlyn, Roberts, Thomas G. Space Threat Assessment 2018. CSIS, April 2018 [Online]. Available: https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison_SpaceThreatAssessment_FULL_WEB.pdf [Accessed: 17th May 2019].

Hinck, Garrett. Private-Sector Initiatives for Cyber Norms: A Summary. Lawfare, June 25, 2018 [Online]. Available: https://www.lawfareblog.com/private-sector-cyber-norm-initiatives-summary [Accessed: 2nd May 2019].

Hutchins, Eric M., Clopperty, Michael J. and Amin, Rohan M. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin, 2011 [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf [Accessed: 15th August 2018].

IANA [Online]. Available: https://www.iana.org/about [Accessed: 7th August 2018].

IBM. Content Delivery Networks: A Complete Guide, 3 June 2019 [Online]. Available: https://www.ibm.com/cloud/learn/content-delivery-networks [Accessed: 17th July 2019].

ICANN. Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends, 1 October 2016 [Online]. Available: https://www.icann.org/news/announcement-2016-10-01-en [Accessed: 8th August 2018].

IGF. The Internet of Trust. Thirteenth Internet Governance Forum (IGF) 12 - 14 November 2018 Paris, France [Online]. Available: http://www.intgovforum.org/multilingual/index.php?q=filedepot_download/6037/1555 [Accessed: 2nd May 2019].

International Telecommunications Union (ITU). Global Cybersecurity Index (CGI) 2017 [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf [Accessed: 23th August 2018].

Internet Exchange Map [Online]. Available: https://www.internetexchangemap.com/ [Accessed: 14th April 2019].

Internet World Statistics [Online]. Available: https://www.internetworldstats.com/euro/ru.htm [Accessed: 10th April 2019].

Internet Society. Brief History of Internet. 1997. [Online]. Available from https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf. [Accessed 5 August 2018].

Internet Society. IXPs [Online] Available: https://www.internetsociety.org/issues/ixps/ [Accessed: 7th August 2018].

Internet Society. Internet Society Perspectives on Internet Content Blocking: An Overview, 24 March 2017 [Online]. Available: https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/ [Accessed: 15th August 2018].

Jonker, Mattjis, Pras, Aiko, Dainotti, Alberto and Sperotto, Anna. A First Joint Look at DoS Attacks and BGP Blackholing in the Wild. IMC '18, October 31-November 2, 2018, Boston, MA, USA [Online]. Available: http://www.caida.org/publications/papers/2018/dos_attacks_and_bgp/dos_attacks_and_bgp.pdf [Accessed: 1st May 2019].

Kofman, Michael. Drivers Of Russian Grand Strategy. Frivärld, 23 April 2019 [Online]. Available: https://frivarld.se/wp-content/uploads/2019/04/Drivers-of-Russian-Grand-Strategy.pdf [Accessed: 31st December 2019].

Kofman, Michael. Raiding and international brigandry: russia's strategy for great power competition. War on the Rocks, JUne 14 2018 [Online]. Available: https://warontherocks.com/2018/06/raiding-and-international-brigandry-russias-strategy-for-great-power-competition/ [Accessed: 3rd January 2019].

Kolomychenko, Maria. Exclusive: Russia opposes U.S. OneWeb satellite service, cites security concerns. Reuters, 24 October 2018 [Online]. Available: https://www.reuters.com/article/us-oneweb-russia-security-exclusive/exclusive-russia-opposes-u-s-oneweb-satellite-service-cites-security-concerns-idUSKCN1MY1P8 [Accessed: 15th April 2019].

Kruglov, Alexander. Business booming for Russia's arms trader. Asia Times, April 22, 2019 [Online]. Available: https://www.asiatimes.com/2019/04/article/business-booming-for-russias-arms-traders/ [Accessed: 3rd May 2019].

Lee, Timothy B. 40 maps that explain the internet 2 June 2014 [Online] Available: https://www.vox.com/a/internet-maps [Accessed: 7th June 2018].

Levada. Putin's approval rating [Online]. Available: https://www.levada.ru/en/ratings/ [Accessed: 27th April 2019].

LiveInternet. Statistics – Browsers, 5th December 2019 [Online]. Available https://www.liveinternet.ru/stat/ru/internet/browsers.html [Accessed: 5th December 2019].

LiveInternet. Statistics – OS, 5th December 2019 [Online]. Available https://www.liveinternet.ru/stat/ru/internet/oses.html [Accessed: 5th December 2019].

LiveInternet. Statistics – Summary, 5th December 2019 [Online]. https://www.liveinternet.ru/stat/ru/internet/summary.html [Accessed: 5th December 2019].

Luhn, Alec and Harding, Luke. Putin dismisses Panama Papers as an attempt to destabilize Russia. Guardian, April 7th, 2016 [Online]. Available: https://www.theguardian.com/news/2016/apr/07/putin-dismisses-panama-papers-as-an-attempt-to-destabilise-russia [Accessed: 1st May 2019].

Marks, Joseph. Obama's Cyber Legacy. Defence One, January 18, 2017 [Online]. Available: https://www.defenseone.com/threats/2017/01/obamas-cyber-legacy/134629/?oref=d-river [Accessed: 3rd May 2019].

McDermott, Roger. Russia's Network-Centric Warfare Capability: Tried and Tested in Syria. Eurasia Daily Monitor Volume: 15 Issue: 154 [Online]. Available: https://jamestown.org/program/russias-network-centric-warfare-capability-tried-and-tested-in-syria/ [Accessed: 18 April 2019].

McKune, Sarah. An Analysis of the International Code of Conduct for Information Security. The CitizenLab, September 28, 2015 [Online]. Available: https://citizenlab.ca/2015/09/international-code-of-conduct/ [Accessed: 2nd May 2019].

Ministry of Defence of the Russian Federation. VIII Moscow Conference on International Security [Online]. Available: https://eng.mil.ru/en/mcis/index.htm [Accessed: 9th May 2019].

Minkomsviaz'. "Nikolay Nikiforov Presented Branch Plan on Import Substitution of Software," (2015, Apr. 3). [Online]. Available: http://minsvyaz.ru/en/events/32967/. [Accessed 12 January 2018].

Mite, Valentinas. Russia: Army Resurrects Soviet-Era Red Star. RFE/RL, 28.11.2002 [Online]. Available: https://www.rferl.org/a/1101518.html [Accessed: 7th January 2020].

Mizokami, Kyle. How the Pentagon Exaggerated Russia's Cold War Super Weapons. The National Interest, June 5, 2016 [Online]. Available: https://nationalinterest.org/blog/the-buzz/how-the-pentagon-exaggerated-russias-cold-war-super-weapons-16468?page=2 [Accessed: 14th July 2019].

Moscow Times. Russia's Arms Exporter Sold $19Bln Worth of Weapons in 2018, Official Says. Moscow Times 1.11.2018. [Online] Available: https://www.themoscowtimes.com/2018/11/01/russias-arms-exporter-sold-19-billion-worth-weapons-2018-ceo-says-a63380 [Accessed: 12th April 2019].

Moscow Times. Google Began Censoring Search Results in Russia, Reports Say. The Moscow Times, February 7, 2019 [Online]. Available: https://www.themoscowtimes.com/2019/02/07/google-began-censoring-search-results-russia-reports-say-a64423 [Accessed: 29th May 2019].

Murdoch-Gibson, Sebastian. Finland's Arctic Data Cable Set to Disrupt Global Connectivity. Asia Pacific Foundation of Canada, June 19, 2018 [Online]. Available: https://www.asiapacific.ca/blog/finlands-arctic-data-cable-set-disrupt-global-connectivity [Accessed: 15th April 2019].

Nakashima, Ellen. U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms. The Washington Post, February 27, 2019 [Online]. Available: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?utm_term=.08c7444b6474 [Accessed: 3rd May 2019].

National Cyber Security Centre. Reckless campaign of cyber attacks by Russian military intelligence service exposed. October 3th, 2018 [Online]. Available: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed [18th May 2019].

NATO. Enlargement [Online]. Available: https://www.nato.int/cps/en/natolive/topics_49212.htm# [Accessed: 29th April 2019].

Newman, Lily Hay. A fishy Wikileaks dump targets Russia for a change. Wired, September 20, 2017 [Online]. Available: https://www.wired.com/story/wikileaks-spy-files-russia/ [Accessed: 1st May 2019].

Nilsen, Thomas. Russia plans to lay trans-Arctic fiber cable linking military installations. The Independent Barents Observer April 24, 2018 [Online]. Available: https://thebarentsobserver.com/en/security/2018/04/russia-slated-lay-military-trans-arctic-fibre-cable [Accessed: 15th April 2019].

Newman, Lily Hay. AI Can Help Cybersecurity – If It Can Fight Through the Hype. WIRED, 29th April 2018 [Online]. Available: https://www.wired.com/story/ai-machine-learning-cybersecurity/ [Accessed: 15th August 2018].

Oxford English Dictionary. [Online]. Available: https://en.oxforddictionaries.com [Accessed: 14th May 2019].

PCH Packet Clearing House [Online]. Available: https://www.pch.net/ixp/dir#!mt-zoom=%5B2.8284271247461907%2C-0.5148480778834943%2C-0.06895898910116116%5D [Accessed: 15th April 2019].

Plopsky, G. Russia's Big Plans for Air Defense in Eurasia: Big plans, indeed, but will they materialize? The Diplomat (2017, Apr, 7). [Online]. Available: https://thediplomat.com/2017/04/russias-big-plans-for-air-defensein-eurasia/. [Accessed 11 January 2018].

Preiherman, Yauheni. Belarus and Russia Dispute the Fundamentals of Their Relationship. Eurasian Daily Monitor, January 15, 2019 [Online]. Available: https://jamestown.org/program/belarus-and-russia-dispute-the-fundamentals-of-their-relationship/ [Accessed: 3rd May 2019].

Qrator Labs. 2019 National Internet Segments Reliability Research & Report, 5th September 2019 [Online]. Available: https://habr.com/en/company/qrator/blog/466287/ [Accessed: 5th January 2019].

RETN. Networkmap [Online]. Available: https://retn.net/networkmap/ [Accessed: 11th April 2019].

Reuters. Russia backs global use of its alternative SWIFT system. Reuters, March 19, 2019 [Online]. Available: https://uk.reuters.com/article/russia-banks-swift/russia-backs-global-use-of-its-alternative-swift-system-idUKL8N2163BU [Accessed: 17th April 2019].

RIPE NCC. Russia Country Report, April 2019 [Online]. Available: https://labs.ripe.net/country-reports/russia-country-report/view [Accessed: 11th April 2019].

RIPE NCC. The RIPE Routing Registry [Online]. Available: https://www.ripe.net/manage-ips-and-asns/db/the-ripe-routing-registry [Accessed: 7th August 2018].

RIPE NCC. Regional Internet Registry [Online] Available: https://www.ripe.net/about-us/what-we-do/regional-internet-registry [Accessed: 7th August 2018].

Root-servers.org [Online]. Available: https://root-servers.org/ [Accessed: 10th April 2019].

Rose, Frank A. Re-establishing U.S. Space Command is a great idea. Brookings, January 7, 2019 [Online]. Available: https://www.brookings.edu/blog/order-from-chaos/2019/01/07/re-establishing-u-s-space-command-is-a-great-idea/ [Accessed: 1st May 2019].

Rudesill, Dakota S. Trump's Secret Order on Pulling the Cyber Trigger. Lawfare, August 29, 2018 [Online]. Available: https://www.lawfareblog.com/trumps-secret-order-pulling-cyber-trigger [Accessed: 3rd May 2019].

Runet connectivity [Online]. Available: https://www.ididb.ru/en/runet/bgp.html [Accessed: 15th April 2019].

Schmitt, Michael and Vihul, Liis. International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms, 30 June 2017 [Online]. Available: https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/ [Accessed: 8th August 2018].

Schmitt, Eric and Gibbons-Neff, Thomas. American-Russian Relations in Syria? Less Rosy Than Trump and Putin Claim. New York Times, July 17, 2018 [Online]. Available: https://www.nytimes.com/2018/07/17/world/middleeast/american-russian-military-syria.html [Accessed: 30th April 2019].

Scoles, Sarah. Maybe Nobody Wants Your Space Internet. Wired, 15 March 2018 [Online] Available: https://www.wired.com/story/maybe-nobody-wants-your-space-internet/ [Accesswed: 8th August 2018].

Scrutton, Alistair and Mardiste, David. With an eye on Russia, Estonia seeks security in computing cloud. Reuters, 4 December 2015 [Online]. Available: https://www.reuters.com/article/us-estonia-cybersecurity/with-an-eye-on-russia-estonia-seeks-security-in-computing-cloud-idUSKBN0TN1BT20151204 [Accessed: 8th August 2018].

Seddon, Max. Inside the deal between the Kremlin and Russia's top search engine. Financial Times, December 5th 2019 [Online]. Available: https://www.ft.com/content/dce2e23c-15c5-11ea-8d73-6303645ac406 [Accessed; 5th January 2020].

Shane, Scott. Huge Trove of Leaked Russian Documents Is Published by Transparency Advocates. New York Times, January 25th, 2019 [Online]. Available: https://www.nytimes.com/2019/01/25/world/europe/russian-documents-leaked-ddosecrets.html [Accessed: 1st May 2019].

Sherman, Justin and Raymond, Mark. The U.N. passed a Russia-backed cybercrime resolution. That's not good news for Internet freedom. Washington Post, 4th December 2019 [Online]. Available: https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/ [Accessed: 5th January 2020].

SIPRI. SIPRI Military Expenditure Database 1949-2018 [Online]. Available: https://www.sipri.org/databases/milex [Accessed: 3rd May 2019].

Sozeri, Efe Kerem. Turkish Internet hit with massive DDoS attack. The Daily Dot, December 17, 2015 [Online]. Available: https://www.dailydot.com/layer8/turkey-ddos-attack-tk-universities/ [Accessed: 1st May 2019].

Statista. Information security products and services market revenue worldwide from 2011 to 2019 (in billion U.S. dollars) [Online]. Available: https://www.statista.com/statistics/305027/revenue-global-security-technology-and-services-market/ [Accessed: 24th August 2018].

Sterling, Bruce. Short History of the Internet. The Magazine of Fantasy and Science Fiction, February 1993 [Online] Available: https://www.internetsociety.org/internet/history-internet/short-history-of-the-internet/ [Accessed: 6th August 2018].

Submarine Cable Map 2018 [Online]. Available: https://www.submarinecablemap.com/#/ [Accessed: 7th August 2018].

SWIFT. Messaging and Standards [Online] Available: https://www.swift.com/about-us/discover-swift/messaging-standards [Accessed: 7th August 2018].

Tangredi, Sam J. CNO vs A2AD: Why Admiral Richardson is Right about Deconstructing the A2/AD Term, The Navalist January 2017. [Online] Available at: https://thenavalist.com/home/2017/1/8/dissecting-the-buzz-words-that-control-the-defense-debates [Accessed 19 August 2017].

The Cambridge Dictionary [Online]. Available: https://dictionary.cambridge.org/dictionary/english/resilience?q=resiliency [Accessed: 15th March 2019].

The Citizen Lab. China's Great Cannon. Research Brief, April 2015 [Online]. Available: https://citizenlab.ca/2015/04/chinas-great-cannon/ [Accessed: 20th May 2019].

The United States Cyber Command. U.S. Cyber Command History [Online]. Available: https://www.cybercom.mil/About/History/ [Accessed: 3rd May 2019].

The United States Department of Commerce, 6 January 2017 [Online]. Available: https://www.icann.org/en/system/files/correspondence/strickling-to-crocker-06jan17-en.pdf [Accessed: 8th August 2018].

The United States Department of Homeland Security. EISENSTEIN. [Online] Available: https://www.dhs.gov/einstein [Accessed: 8th August 2018].

Tucker, Patrick. China Is Still Stealing America's Business Secrets, US Officials Say. Defense One, July 26, 2018 [Online]. Available: https://www.defenseone.com/technology/2018/07/china-still-stealing-americas-business-secrets-us-officials-say/150086/ [Accessed: 1st May 2019].

Tucker, Patrick. Russia's Would-Be Windows Replacement Gets a Security Upgrade. Defense One, May 28th, 2019 [Online]. Available: https://www.defenseone.com/technology/2019/05/russias-microsoft-knockoff-gets-security-upgrade/157310/?oref=d-skybox [Accessed: 9th July 2019].

Union of Concerned Scientists, "UCS Satellite Database," 2017. [Online]. Available: http://www.ucsusa.org/nuclear-weapons/spaceweapons/ satellite-database#.Wg0WlUpl9PY. [Accessed 16 November 2017].

Wikipedia [Online]. Available: https://ru.wikipedia.org/ [Accessed: 7th March 2019].

Winter, Martin. Monitoring BGP Anomalies on the Internet. 27 July 2018. RIPE NCC. [Online]. Available: https://labs.ripe.net/Members/martin_winter/monitoring-bgp-anomalies-on-the-internet [Accessed: 7th August 2018].

Wolf, Zachary B. and Carman, JoElla. Here are all the treaties and agreements Trump has abandoned. CNN, February 1, 2019 [Online]. Available: https://edition.cnn.com/2019/02/01/politics/nuclear-treaty-trump/index.html [Accessed: 8th July 2019].

Wolff, Josephine. Borders in the Cloud. Countries are increasingly putting limits on how data travels. Slate, 20 November 2017 [Online]. Available: http://www.slate.com/articles/technology/future_tense/2017/11/countries_are_increasingly_imposing_borders_on_the_cloud.html?via=gdpr-consent [Accessed: 8th August 2018].

Zittrain, Jonathan and Sauter, Molly. Will the U.S. get an Internet "kill switch"? MIT Technology Review, March 4, 2011 [Online]. Available: https://www.technologyreview.com/s/423196/will-the-us-get-an-internet-kill-switch/ [Accessed: 3rd May 2019].

Documents & Statements

English language source:

Barlow, John Perry. A Declaration of the Independence of Cyberspace. Davos, Switzerland February 8, 1996 [Online]. Avaliable: https://www.eff.org/cyberspace-independence [Accessed: 6th August 2018].

Brooks, Rosa. Evolution of Strategic Communication and Information Operations Since 9/11: Hearing Before the Subcomm. on Emerging Threats & Capabilities of the H. Comm. on Armed Services, 112th Cong., July 12, 2011 (Statement of Rosa Ehrenreich Brooks) [Online] Available: https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1112&context=cong [Accessed: 14th August 2014].

CIA. "General Staff Academy Lectures: Principles of the Automation and Mechanization of Troop Control." Document VII-211. Prepared 6 September 1968, published October 1969; CIA/DO Intelligence Information Special Report, 11 November 1976 [Online]. Available: https://www.cia.gov/library/readingroom/docs/1976-11-11.pdf [Accessed: 6th November 2019].

Cichonski, Paul, Millar, Tom, Grance, Tim and Scarfone, Karen. Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. NIST (National Institute of Standards and Technology), 2012 [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf [Accessed: 27th September 2018].

Connolly, Gerald E. NATO @ 70: Why the Alliance Remains Indispensable. NATO Parliamentary Assembly, Report, 12th October 2019 [Online]. Available: https://www.nato-pa.int/document/2019-nato70-why-alliance-remains-indispensable-146-pctr-19-e-rev1-fin [Accessed: 5th January 2020].

CrowdStrike. Global Threat Report 2018: Blurring the lines between statecraft and tradecraft. 26 February 2018 [Online], Available: https://www.crowdstrike.com/blog/crowdstrike-2018-global-threat-report-reveals-the-trends-insights-and-threat-actors-you-need-to-know/ [Accessed: 9th August 2018].

Dans, Enrique. The Kremlin Vs. Telegram: What's Really Going On With The Messaging Service In Russia? Forbes, April 19, 2018 [Online]. Available: https://www.forbes.com/sites/enriquedans/2018/04/19/the-kremlin-vs-telegram-whats-really-going-on-with-the-messaging-service-in-russia/#17b98fe75f29 [Accessed: 29th May 2019].

Defence Intelligence Agency. Russia Military Power: Building a Military to Support Great Power Aspirations [Online]. Available: http://www.dia.mil/Military-Power-Publications/ [Accessed: 20th November 2018].

DIA. China Military Power. Modernizing a Force to Fight and Win, 2019 [Online]. Available: https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/China_Military_Power_FINAL_5MB_20190103.pdf [Accessed: 1st May 2019].

Drake, William J., Cerf, Vinton G. and Kleinwächter, Wolfgang. Future of the Internet Initiative White Paper. Internet Fragmentation: An Overview. World Economic Forum, January 2016. [Online] Available:

http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf [Accessed: 9th August 2018].

ENISA. Baseline Capabilities of National/Governmental CERTs. Update Recommendations 2012 [Online]. Available: https://www.enisa.europa.eu/publications/national-governmental-certs-enisas-recommendations-on-baseline-capabilities [Accessed: 5th August 2018].

ENISA. Definition of Cybersecurity: Gaps and overlaps in standardisation Version 1.0, December 2015 [Online] Available: https://www.enisa.europa.eu/publications/definition-of-cybersecurity [Accessed: 7th August 2018].

ENISA. ENISA Threat Landscape Report 2017: 15 Top Cyber-Threats and Trends Version 1.0. January 2018 [Online] Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017 [Accessed: 9th August 2018].

ENISA. Signalling Security in Telecom SS7/Diameter/5G EU level assessment of the current situation, March 2018 [Online] Available: https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g [Accessed: 10th August 2018].

ENISA. ENISA Threat Landscape Responding to the Evolving Threat Environment [Deliverable – 2012-09-28] [Online]. Available: https://www.enisa.europa.eu/publications/ENISA_Threat_Landscape/at_download/fullReport [Accessed: 1st May 2019].

European Commission. Conclusion of G7 Summit "Information Society Conference" DOC/95/2 of 1995-02-26 [Online]. Available: http://europa.eu/rapid/press-release_DOC-95-2_en.htm [Accessed: 24th March 2019]).

European Parliament. Countering hybrid threats: EU-NATO cooperation. Briefing, March 2017 [Online]. Available: http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599315/EPRS_BRI(2017)599315_EN.pdf [Accessed: 30th April 2019].

FireEye. M-Trends, Special Report 2018 [Online]. Available: https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf [Accessed: 15th August 2018].

Fried, Daniel. A Strategy for Central Asia. Statement Before the Subcommittee on the Middle East and Central Asia of the House International Relations Committee. Washington, DC. October 27, 2005 [Online]. Available: https://2001-2009.state.gov/p/eur/rls/rm/55766.htm [Accessed: 27th April 2019].

Godwin III, J. B., Kulpim, A., Rauscher, K. F. and Yaschenko, V. (eds.) Critical Terminology Foundations 2. Russia-U.S. Bilateral on Cybersecurity. Policy Report 2/2014. EastWest Institute and the Information Security Institute of Moscow State University [Online]. Available: https://www.files.ethz.ch/isn/178418/terminology2.pdf [Accessed: 22th June 2019].

IIFFMCG. Independent international fact-finding mission on the conflict in Georgia, report, volume I-III, 2009 [Online]. Available: http://www.mpil.de/en/pub/publications/archive/independent_international_fact.cfm [Accessed: 25th March 2019].

International Organization for Standardization. Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model. ISO/IEC 7498-1:1994. 15 June 1996 [Online] Available: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html [Accessed: 7th August 2018].

Joint Chiefs of Staff, the U.S. Department of Defence. Planner's Handbook for Operational Design, January 2011 [Online]. Available: https://www.jcs.mil/Portals/36/Documents/Doctrine/pams_hands/opdesign_hbk.pdf [Accessed: 24th January 2020].

Joint Chiefs of Staff, the U.S. Department of Defence. Information operations (Joint Publication 3-13), 2014 [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf [Accessed: 6th August 2018].

Joint Chiefs of Staff, the U.S. Department of Defence. Cyberspace operations (Joint Publication 3-12), June 8th 2018 [Online]. Available: https://fas.org/irp/doddir/dod/jp3_12.pdf [Accessed: 17th August 2018].

Joint Chiefs of Staff, the U.S. Department of Defence. Joint Operations (Joint Publication 3-0), 2017 [Online]. Available: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf [Accessed 13 October 2017].

Joint Staff J6. The Global Information Grid (GIG) 2.0 Concept of Operations Version 1.1, 11 March 2009 [Online]. Available: https://info.publicintelligence.net/DoD-GIG2-CONOPS.pdf [Accessed: 7th January 2020].

Kremlin.ru. Transcript of Press Conference with the Russian and Foreign Media, President of Russia's Official Web Portal, February 1, 2007 [English] [Online]. Available: http://en.kremlin.ru/events/president/transcripts/24026 [Accessed: 14th February 2019].

Kremlin.ru. Media Forum of Independent Local and Regional Media, President of Russia's Official Web Portal, April 24, 2014 [English] [Online]. Available: http://en.kremlin.ru/events/president/news/20858 [Accessed: 13th July 2019].

KPMG. The Changing Landscape of Disruptive Technologies. Tech hubs forging new paths to outpace the competition [Online]. Available: https://info.kpmg.us/content/dam/info/en/techinnovation/pdf/2018/tech-hubs-forging-new-paths.pdf [Accessed: 2nd May 2019].

Maurer, Tim and Morgus, Robert. Compilation of Existing Cybersecurity and Information Security Related Definitions. New America, Report October 2014 [Online]. Available: https://www.newamerica.org/cybersecurity-initiative/policy-papers/compilation-of-existing-cybersecurity-and-information-security-related-definitions/ [Accessed: 6th August 2018].

Meick, Ethan. China-Russia Military-to-Military Relations: Moving Toward a Higher Level of Cooperation. U.S.-China Economic and Security Review Commission, March 20, 2017 [Online]. Available: https://www.uscc.gov/sites/default/files/Research/China-Russia%20Mil-Mil%20Relations%20Moving%20Toward%20Higher%20Level%20of%20Cooperation.pdf [Accessed: 30th April 2019].

North Atlantic Treaty Organization (NATO). Allied Joint Doctrine for Information Operations, AJP-3.10, November 2009 [Online]. Available: https://info.publicintelligence.net/NATO-IO.pdf [Accessed: 22nd September 2018].

North Atlantic Treaty Organization (NATO). An Introduction to Operations Planning at the Operational Level - A summary of the Allied command operations comprehensive operations planning directive, 4 Oct 2013 [Online]. Available: http://www.act.nato.int/images/stories/events/2016/sfpdpe/copd_v20_summary.pdf [Accessed: 10th March 2019].

North Atlantic Treaty Organization (NATO) Cyber Defence Pledge, 8 July 2016 [Online]. Available: http://www.nato.int/cps/en/natohq/official_texts_133177.htm [Accessed: 19 August 2017].

North Atlantic Treaty Organization (NATO) Cyber Defence Pledge, 8 July 2016 [Online]. Available at: http://www.nato.int/cps/en/natohq/official_texts_133177.htm [Accessed 19 August 2017].

Office of the National Counterintelligence Executive. Foreign Spies Stealing US Economic Secrets in Cyberspace. Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011, October 2011 [Online]. Available: https://www.dni.gov/files/NCSC/documents/Regulations/Foreign_Economic_Collection_2011.pdf [Accessed: 29th May 2019].

Okinawa Charter on Global Information Society, 2000 [Online]. Available: https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html [Accessed: 2nd April 2019].

OSCE. Russian Federation Presidential Election 18 March 2018. ODIHR Election Observation Mission Final Report [Online]. Available: https://www.osce.org/odihr/elections/383577?download=true [Accessed: 17th May 2019].

Petersen, Phillip A. The Northwestern TVD in Soviet Operational-Strategic Planning. OSD Office of Net Assessment, 2014 [Online]. Available: https://bit.ly/2ZRP24b [Accessed: 29th November 2018].

RFC 4271 Y. Rekhter, T. Li, S. Hares "A Border Gateway Protocol 4 (BGP-4)" RFC 4271, January 2006.

RFC 7426 E. Haleplidis, Ed. Software-Defined Networking (SDN): Layers and Architecture Terminology RFC 7426, January 2015.

Ross, Ron, Graubart, Richard, Bodeau, Deborah and Mcquaid, Rosalie. Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems. Draft NIST Special Publication 800-160 Volume 2, 2018 [Online]. Available from: https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf [Accessed 13 June 2018].

Symantec. Symantec Global Internet Security Threat Report Trends for 2009. [Online]. Available: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf [Accessed: 1st May 2019].

The Defence Ministry of the Russian Federation. The priority tasks of the development of the armed forces of the Russian Federation, 2004 [Online]. Available: http://red-stars.org/doctrine.pdf [Accessed: 30th March 2019].

The President of the United States. International strategy for cyberspace: Prosperity, Security, and Openness in a Networked World, 2011 [Online]. Available: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [Accessed: 14th March 2019].

The President of the United States. The National Cyber Strategy of the United States of America, September, 2018 [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [Accessed: 20th May 2019].

The National Military Strategy of the United States of America. A Strategy for Today; A Vision for Tomorrow, 2004 [Online]. Available: https://www.bits.de/NRANEU/docs/NMS2004.pdf [Accessed: 27th February 2019].

The United States Department of Defence. Cyber Strategy – Summary 2018 [Online]. Available: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF [Accessed: 3rd May 2019].

The United States Department of Defence, Joint Chiefs of Staff. Joint Doctrine for Command and Control Warfare (C2W) Joint Pub 3-13.1, 7th February 1996, v. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/a357635.pdf [Accessed: 27th November 2018].

The United States Department of Defence Joint Chiefs of Staff. Net-Centric Operational Environment Joint Integrating Concept, 31 October 2005 [Online]. Available:) (https://dodcio.defense.gov/Portals/0/Documents/netcentric_jic.pdf [Accessed: 3rd March 2019].

The United States Department of Defence (U.S. DoD). Joint Publication 3-0: Joint Operations, 2017 [Online]. Available: http://www.dtic.mil/doctrine/new_pubs/jp3_0.pdf [Accessed 20 August 2017].

The United States Department of Defence (U.S. DoD). Cyberspace Operations, JP 3-12, 8th June 2018 [Online]. Available: https://fas.org/irp/doddir/dod/jp3_12.pdf [Accessed: 15th August 2018].

The United States Department of Homeland Security. Privacy Impact Assessment for EINSTEIN 3 - Accelerated (E3A) May 2016 DHS/PIA/NPPD-027 [Online]. Available: https://www.dhs.gov/publication/dhsnppdpia-027-einstein-3-accelerated [Accessed: 18th April 2019].

The United States Department of Homeland Security. Enhanced Analysis of GRIZZLY STEPPE Activity. Reference Number: AR-17-20045 February 10, 2017 [Online]. Available: https://assets.documentcloud.org/documents/3469157/Document-12-National-Cybersecurity-and.pdf [Accessed: 18th May 2019].

The United States Department of State. Soviet "Active Measure". Forgery, Disinformation, Political Operations. October 1981 [Online]. Available: https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf [Accessed: 15th November 2018].

The White House Washington. Presidential decision directive/NSC-63, May 22, 1998 [Online]. Available: https://fas.org/irp/offdocs/pdd/pdd-63.htm [Accessed: 1st May 2019].

The White House. Statement by National Security Advisor Ambassador John Bolton on Venezuela, March 29, 2019 [Online]. Available: https://www.whitehouse.gov/briefings-statements/statement-national-security-advisor-ambassador-john-bolton-venezuela-2/ [Accessed: 18th May 2019].

The White House. Fact sheet: U.S.-Russian Cooperation on Information and Communications Technology Security. June 17, 2013 [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol [Accessed: 1st May 2019].

The White House. National Cyber Strategy of the United States of America, September 2018 [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [Accessed: 3rd May 2019].

UNIDIR. The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapon Systems and Cyber Operations, No. 7 [Online]. Available: http://www.unidir.org/files/publications/pdfs/autonomous-weapon-systems-and-cyber-operations-en-690.pdf [Accessed: 24th August 2018].

UNIDIR. The Cyber Index. International Security Trends and Realities. New York and Geneva: United Nations, 2013 [Online]. Available: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf [Accessed: 1st May 2019].

United Nations General Assembly. Developments in the field of information and telecommunications in the context of international security A/RES/53/70 4 January 1999 [Online]. Available: https://digitallibrary.un.org/record/265311/files/A_RES_53_70-EN.pdf [Accessed: 24th March 2019].

United Nations General Assembly. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. A/70/174 22 July 2015 [Online]. Available: https://undocs.org/A/70/174 [Accessed: 29th March 2019].

United Nations General Assembly. Resolution adopted by the general assembly. Developments in the field of information and telecommunications in the context of international security. A/RES/53/70 4 January 1999 [Online]. Available: https://undocs.org/A/RES/53/70 [Accessed: 10th May 2019].

United Nations General Assembly. Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General. A/66/359, 14 September 2011. [Online]. Available: https://undocs.org/A/66/359 [Accessed: 2nd April 2019].

United Nations General Assembly. Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed Secretary-General. A/69/723, 13 January 2015 [Online]. Available: https://undocs.org/A/69/723 [Accessed: 2nd April 2019].

United Nations General Assembly. Developments in the field of information and telecommunications in the context of international security. A/C.1/73/L.27/, 22 October 2018 [Online]. Available: https://undocs.org/pdf?symbol=en/A/C.1/73/L.27 [Accessed: 2nd April 2019].

United Nations Office On Drugs And Crime. Comprehensive Study on Cybercrime, Draft—February 2013 [Online]. Available: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf [Accessed: 1st May 2019].

U.S. Army War College. Information Operations Primer: Fundamentals of Information Operations. November 2011 [Online] Available: http://www.au.af.mil/au/awc/awcgate/army-usawc/info_ops_primer.pdf [Accessed: 14th August 2018].

Russian material

Books, Journals & Military Periodicals

Translated in English

Abramov, Iu., Savelyev, V. and Cheremykh, V. A System for the Collection, Processing, and Transmission of Information in a Military District. Military thought – Secret version 1964, No. 2 (72). Translated and published by the Central Intelligence Agency, Intelligence Information Special Report, 20th June 1978 [Online]. Available: https://www.cia.gov/library/readingroom/docs/1978-06-20a.pdf [Accessed: 29th November 2018].

Bachkalo, B.I. and Ivanov, P.I. On the Question of Validating the Optimum Structure of a Ground Force Grouping. Military Thought No. 12 1993.

Gayvoronskii, F. New Questions of Operational Art at Its Present Stage of Development. Military Thought – Secret version 1970, No. 1 (89). Translated and published by the Central Intelligence Agency, Intelligence Information Special Report, 7th March 1974 [Online]. Available https://www.cia.gov/library/readingroom/docs/DOC_0001199073.pdf [Accessed: 5th December 2018].

Gudz, P. The Modern Theory of Tactics and Some of its Problems. Military Thought – Secret version 1970, No. 2 (90). Translated and published by the Central Intelligence Agency, Intelligence Information Special Report, 14th January 1974 [Online]. Available https://www.cia.gov/library/readingroom/docs/CIA-RDP85T00875R000300010016-7.pdf [Accessed: 5th December 2018].

Elterman, Iu. Communications in an Automated Troop Control System at the Operational Level. Military thought – Secret version 1963, No. 1 (68). Translated and published by the Central Intelligence Agency, Intelligence Information Special Report, 2nd June 1978 [Online]. Available: https://www.cia.gov/library/readingroom/docs/1978-04-20a.pdf [Accessed: 29th November 2018].

Klokotov, N. P., Kasenkov, M. M. For the Question on Military Danger. Military Thought No. 8 1991.

Manilov, V. L. Threats to Russia's National Security. Military Thought 1996 No. 1.

Pirumov, V. S. and Rodionov, M. A. Information Warfare in Armed Conflicts. Military Thought [English] No. 5 1997.

Pirumov, V. S. Two Aspects of Parity and Defensive Sufficiency. Military Thought No. 2 1992.

Povaliy, M. Military Strategy and Economics. Military Thought – Secret version 1971, No. 4. Translated and published by the Central Intelligence Agency, Foreign Press Digest, 25th March 1974 [Online]. Available: https://www.cia.gov/library/readingroom/docs/1974-01-14.pdf [Accessed: 5th December 2018].

Sayfetdinov, Kh., Kulyanitsa, A. L. Information Technology and Artificial Intelligence. Military Thought No. 5 1997.

Stishkovskiy, V. The Principal Ways of improving the quality of Military Communications. Military thought – Secret version 1970, No. 1 (89). Translated and published by the Central Intelligence Agency, Intelligence Information Special Report, 1st February 1974 [Online]. Available: https://www.cia.gov/library/readingroom/docs/1974-02-01.pdf [Accessed: 29th November 2018].)

Chernov, L., Moiseyev, V. and Kiselev, A. Some Problems in the Use of Electronic Computers. Military thought – Secret version 1962, No. 6 (67). Translated and published by the Central Intelligence Agency, Intelligence Information Special Report, 2nd June 1978 [Online]. Available: https://www.cia.gov/library/reading-room/docs/1978-06-02b.pdf [Accessed: 29th November 2018].

Sushko, N. and Puzik, V. The Marxist-Leninist Theory of Knowledge and Its Significance in the Soviet Military Science and Practice. Military Thought – Secret version 1966, No. 1. Translated and published by the Central Intelligence Agency, Selected Translations, 23th August 1966 [Online]. Available: https://www.cia.gov/library/readingroom/docs/1966-08-23e.pdf [Accessed: 5th December 2018].

Russian language sources

Автамонов П.Н., Немыкин С.А., Охтилев М.Ю., Соколов Б.В., Юсупов Р.М. Методологические и методические основы разработки и внедрения интегрированных систем поддержки принятия решений (СППР) в АСУ объектами военно-государственного управления. Информационные войны №1 (41) 2017, 39-48.

Азов, В. Концепция создания единой информационно-управляющей структуры ВС США. Зарубежное военное обозрение, № 1 (2003), 3-10.

Акулинчев, А. Б. Проблемы цифровизации военных сетей связи и пути их решения. Военная мысль, № 9 (2006), 76-80.

Александров, Михаил. Сетецентрические войны будущего и подготовка государства к их отражению. Взгляды русского военного теоретика Е. Э. Месснера. Обозреватель–observer, Ноябрь 2016 г. № 11 (322) 109-118.

Алексин, Валерий. Так считает директор Центра международных и стратегических исследований Владимир Белоус. Ответы на американские вызовы имеются. Независимое военное обозрение № 25 (198) 14.07.2000.

Алехин, Ю., Прохоров, А., Проценко, А. «Пирамида» начиналась с «воздуха». Воздушно-космическая оборона №1, 2011 г.

Алтухов, П. К. Предмет и содержание теории управления войсками. Военная мысль № 7 1975, 15-25.

Андреев, В. В., Никитин, О. Г., Марасанов, А. В. Особенности методического обеспечения обоснования состава органов управления разнородными силами и средствами радиоэлектронной борьбы объединений Сухопутных войск. Военная мысль, № 6 (2017), 51-54.

Андреев, В. Ф. Военно-стратегический паритет — объективный фактор сдерживания агрессивных сил. Военная мысль № 2 1989, 45-53.

Анureев, II. И. Расширение сфер применения кибернетики в военном деле. Военная мысль № 4 1978, 71-77.

Анисимов, Е. Г., Анисимов, В. Г., Солохов, И. В. Проблемы научно-методического обеспечения межведомственного информационного взаимодействия. Военная мысль, № 12 (2017), 45-51.

Анохин, Д. В., Зинатуллин, И. Р., Царелунга, В. В., Сафонов, В. В. О совершенствовании программного обеспечения Единой системы управления тактического звена. Военная мысль, № 4 (2018), 21-28.

Антонов С.Г., Гордеев С.В., Климов С.М., Рыжов Б.С. Модели угроз совместных информационно-технических и информационно-психологических воздействий в гибридных войнах. Информационные войны, № 2(46) 2018, 83-87.

Антонович, П. И. О сущности и содержании кибервойны. Военная мысль, № 7 (2011), 39-46.

Арбатов, Алексей. Ядерное сдерживание: реальности и химеры. Независимое военное обозрение, № 17 (377) за 14 мая я 2004 года.

Арбатов, Алексей. Совместная про никак не получается. Независимое военное обозрение, № 22 за 17 июня 2011 года.

Арбатов, Алексей. Стратегические асимметрии и системы ПРО. Независимое Военное Обозрение, № 1 20.1.2012.

Арбатов, Алексей. Большой стратегический треугольник. Независимое Военное Обозрение, № 39 2.11.2012.

Арсланов, Халил, Лихачев, Александр. Актуальные научно-практические проблемы развития ОАЦСС ВС РФ. Связь в Вооруженных Силах Российской Федерации 2015. Москва: Информационный мост 2015, 29-36.

Арсланов, Халил Абдухалимович. Перспективы развития войск связи. Российской Федерациию Федеральный справочник. Оборонно-промышленный комплекс России, Том № 10, 2014, 389-392 [Online]. Available: http://federalbook.ru/files/OPK/Soderjanie/OPK-10/III/Arslanov.pdf [Accessed: 6th March 2019].

Арсланов, Халил. На острие технического прогресса. Красная звезда, 19 октября 2018 [Online]. Available: http://redstar.ru/na-ostrie-tehnicheskogo-progressa/ [Accessed: 6th March 2019].

Артамонов, Игор, Рябцев, Роман. Асимметричный ответ России Таковым может стать развитие тактического ядерного оружия малой и сверхмалой мощности. ВПК, № 15 (483) за 17 апреля 2013 года.

Артамонов, Игорь, Рябцев, Роман. «Бог войны» XXI века Ракетно-артиллерийское вооружение должно развиваться под бесконтактные войны. ВПК, № 16 (484) за 24 апреля 2013 года.

Афанасьев, В.Г. Общество: системность, познание и управление. М: Издательство политической литературы, 1981.

Ахмадишин, И. Н., Баранюк, В. В. Организационные вопросы создания информационной службы ВС РФ. Военная мысль № 4 (2004), 45-49.

Барвиненко, В. В. Об автоматизации управления группировками Вооруженных Сил. Военная мысль № 2, 1999, 26-29.

Басистов, Владимир Анатольевич. Развитие должно быть гармоничным. Независимое военное обозрение № 40 1999.

Базылев, С. И., Дылевский, И. И., Комов, С. А., Петрунин, А. Н. Деятельность Вооруженных Сил Российской Федерации в информационном пространстве: принципы, правила, меры доверия. Военная мысль, № 6 (2012), 24-28.

Балуевский, Юрий. Генерал армии Юрий Балуевский: Генеральный штаб и задачи военного строительства. Красная звезда, 25.01.2006.

Балуевский, Юрий.. Агрессия «общечеловеческого» Военными технологиями нематериального действия у нас никто не занимается. ВПК, № 18 (584) за 20 мая 2015 года.

Балыбин, С.В., Белов, Е.Н., Федорец, В.Н. Информационная безопасность военной техники, использующей интегральные схемы иностранного производства. Военная мысль № 12 (2011), 11-21.

Балыбин, В. А., Донсков, Ю. Е., Бойко, А. А. О терминологии в области радиоэлектронной борьбы в условиях современного информационного противоборства. Военная мысль, № 9 (2013), 28-32.

Баранюк, В. В. Единое информационное пространство вс рф: проблемы создания. Военная мысль № 3 (2003), 36-38.

Барвиненко, Владимир. Война на опережение — часть I. Как противостоять сетецентрическим действиям противника. ВПК, № 24 (590) за 1 июля 2015 года.

Барвиненко, Владимир. Война на опережение — часть II Как противостоять сетецентрическим действиям противника. ВПК, № 25 (591) за 8 июля 2015 года.

Бартош, А. А. (2016a) Гибридная война: интерпретации и реальность. Независимое военное обозрение, № 35 (918) 16 сентября 2016.

Бартош, А.А. (2016b) Адаптивные стратегии информационной войны (Часть 1). Вестник академии военных наук, № 2 (55) 2016, 85-93.

Бартош, Александр. Трудно обеспечить безопасность Евразии в условиях "новой холодной войны" Независимое Военное Обозрение, № 30 (961) 18.8.2017.

Бартош, А. А. (2018a) Стратегия и контрстратегия гибридной войны. Военная мысль, № 10 2018, 5-20.

Батурин, Ю. М. Телекоммуникации и право (Вопросы стратегии). Москва: Центр “Право и СМИ”, 2000.

Безель, Яков. Этапы развития АСУ авиацией и ПВО. Воздушно-космическая сфера, № 4 (2014), 23-27.

Безуглый, А. С., Гвриленко, С. П. Об информационном моделировании в АСУВ. Военная мысль № 5 1994, 29-33.

Берг, А., Китов, А. and Ляпунов, А. Кибернетика в военном деле. Военная мысль № 2, 1961, 19-31, 19.

Веапринцев, В.Б., Манойло, А.В., Петренко, А.И., Фролов, Д.Б. Операции информационно-психологической войны: краткий энциклопедический словарь-справочник. М.: Горячая линия – Телеком, 2011.

Бец, М.О., Киселенко, В.А., Орлов, С.С. Перспективные технологические направления для развития и совершенствования облачной информационной инфраструктуры Вооруженных сил Российской Федерации. Вестник академии военных наук, № 4 (61) 2017, 74-82.

Бирюлин, Роман. Стремление к цифровому суверенитету. Красная звезда, № 136 6 декабря 2017.

Бирюков, В.В. Проблемы управления информатизацией ВС РФ. Военная мысль № 4. 1994.

Бобков, Ю. Я., Тютюнников, Н. Н. Концептуальные основы постарения АСУ Сухопутными войсками ВС РФ. М.: Палеотип, 2014.

Боков, С.И., Воронков, О.В, Чупринов, А.А. Основные принципы методологии формирования единой информационно-поисковой и аналитической системы управления развитием вооружения, военной и специальной техники. Вооружение и экономика 3 (36) / 2016 г, 54-58.

Боков, С. И., Желтухин, П. С., Пьянков, А. А. Основные подходы к созданию единого информационного пространства военно-технической политики Российской Федерации. Военная мысль, № 4 (2018), 5-12.

Бобошко, А.А., Муравьев, Н. Л., Пономарев, С.Ю. Основные проблемы автоматизации организационно-мобилизационных органов ВС РФ. Военная мысль № 6, 1999, 50-53.

Бовдунов А. Л. Неправительственные организации: сетевая война. Информационные войны, № 3(7) 2008, 30-39.

Богданов, Константин. Момент истины для «убийц авианосцев». ВПК, № 46 (362) за 24 ноября 2010 года.

Богданов, С. А. Вероятный облик вооруженной борьбы будущего. Военная мысль, № 12 2003, 2-7.

Бойко, Сергей. Формирование системы международной информационной безопасности: российские подходы и инициативы. Международная жизнь, № 5 (2018).

Бойко, Сергей. Формирование системы международной информационной безопасности: российские подходы и инициативы. Международная жизнь, №11 (2018).

Бойцов, Маркелл. Калькулятор стратегического сдерживания. Независимое военное обозрение, № 30 за 31 августа 2012 года.

Бородакий, Ю.В. Информатизация вооруженных сил. Развитие методологических основ построения информационно-управляющих систем военного назначения. Военная мысль, № 6 (2009), 33-41.

Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности xx! века (часть 1). Вопросы кибербезопасности, № 1 (1) 2013, 2-9.

Бочаров, Игорь. Парадоксы ядерного сдерживания. Независимое военное обозрение, № 15 (424) за 222 июля я 2005 года.

Брезкун, Сергей. Полемика. Подкоп под стратегическую стабильность. ВПК, № 50 за 29 декабр я 2004 года.

Будко П.А., Чихачев А.В., Баринов М.А., Винограденко А.М. Принципы организации и планирования сильносвязной телекоммуникационной среды сил специального назначения. T-Comm #6 2013, 8-12.

Буренка В.М (Общ. ред.) Толковый словарь в области военного управления, связи и информационных технологий: Военно-теоретический труд. М.: РАРАН, 2017.

Буренок, Василий. Базис сетецентрических войн – опережение, интеллект, инновации... Независимое военное обозрение, № 12 (2010).

Буренок, Василий. За рамками здравого смысла: Облик грядущих войн и новых систем вооружения определит только наука. ВПК, № 10 (478) за 12 марта 2013 года.

Буренок, Василий. О некоторых видах межгосударственного противоборства. Вестник Академии военных наук, 2(43) 2013, 15-19.

Буренок, Василий. США создают для военных нужд искусственный разум нового поколения. чем ответит Россия? ВПК, № 37 (701) за 27 сентября 2017 года.

Буренок, Василий. Интеллект по призыву. ВПК, № 46 (710) за 29 ноября 2017 года [Online]. Available: https://www.vpk-news.ru/articles/40134 [Accessed: 7th July 2019].

Бухарин, В.В. Компоненты цифрового суверенитета российской федерации как техническая основа информационной безопасности. Вестник МГИМО университета, № 6(51) 2016, 76-91.

Бурутин, А. Войны будущего станут информационными. Новые вызовы и угрозы безопасности России. Независимое военное обозрение, № 5 2008, 2-3.

Бухарин, С.Н., Цыганов, В.В. Методы и технологии информационных войн. М.: Академический проект, 2007.

Бухарин С. Н., Цыганов В.В. Ситуационный анализ в информационных войнах. информационные войны, №2 (6) 2008, 47-58.

Быстров, И. И., Козичев, В.Н., Ширманов, А.В. (2018a) Концептуальные вопросы создания интеллектуальных информационных систем обработки неструктурированной информации в автоматизированных системах военного назначения. Вестник академии военных наук, № 3 (64) 2018, 114-121.

Быстров, И. И., Козичев, В. Н., Ширманов, А. В. (2018b) Автоматизированная обработка неструктурированной информации в перспективных автоматизированных системах военного назначения: концептуальные основы. Военная мысль № 8 (2018), 54-64.

Бытьев, А.В., Смирнова, Л.А. К вопросу о научном понятии «военное управление». Вестник академии военных наук № 1 (66) 2019, 43-49.

Вайнер, А. Я. О противоборстве в сфере управления. Военная мысль № 9 1990, 12-16.

Валеев, Марат, Беломытцев, Александр. Сдерживание неопределенностью. ВПК, № 26 (690) за 12 июля 2017 года.

Варе, В. Кибернетика в управлении войсками. Военная мысль № 7 1962, 17-30.

Васильева, С.Н. (общ. ред.) Институт проблем управления им. В.А. Трапезникова Российской академии наук. Москва: ИПУ РАН, 2014 [Online]. Available: https://www.ipu.ru/sites/default/files/page_file/75%20лет%20ИПУ%20РАН.pdf [Accessed: 28th March 2019].

Ведута, Елена. Цифровая экономика приведет к экономической киберсистеме. Международная жизнь, № 10/2017.

Владимиров, Александр. Ты записался ополченцем? Незнание законов партизанской войны не освобождает от ответственности. ВПК, № 34 (649) за 7 сентября 2016 года.

Владыкин, Олег. Интернет доступен на российских кораблях. Система действует на девяти судах. Независимое военное обозрение № 23 (954) 2017.

Владимиров А.В. Информационное оружие: миф или реальность? Красная звезда № 5 (октября) 1991.

Военная мысль. «Звездные войны»: иллюзии и опасности. Военная мысль № 9 1985, 15-18.

Волкогонов, Д. «Психологическая война» империализма. Военная мысль 1975 No. 1, 67-76.

Волкогонов, Д. А. Военные вопросы в Программе КПСС. Военная мысль 1986 № 5, 3-15.

Володенков, С.В. Технологии интернет-коммуникации как фактор обеспечения информационной безопасности современного государства. Информационные войны, № 3(19) 2011, 89-95.

Вопросы Безопасности. Информационное оружие: постановка проблемы и пути решения. Вопросы Безопасности, № 3 (2000).

Воробьев, И. Н. Новое оружие и развитие принципов общевойскового боя. Военная мысль No. 11 1983, 35-45.

Воробьев, И. Н. (1984a) Новое оружие— новая тактика. Военная мысль 1984 № 2, 34-45.

Воробьев, И. Н. (1984b) Новое оружие— новая тактика. Военная мысль 1984 № 6, 47-59.

Воробьев, И. Н. Принципы формирования военной доктрины. Военная мысль № 11,12/1991.

Воробьев, И.Н. Какие войны грозят нам в будущем веке. Военная мысль № 2 (3-4) 1997, 18-24.

Воробьев, И. Н., Киселев, В. А. Стратегия непрямых действий в новом облике. Военная мысль, № 9 2006, 2-10.

Воробьев, И. Н., Киселев, В. А. Военная наука на современном этапе. Военная мысль, № 7 2008, 26-31.

Воробьев, И. Н., Киселев, В. А. От современной тактики к тактике сетецентрических действий. Военная Мысль, № 8 2011, 19-27.

Воробьев, И. Н., Киселев, В. А. (2014a) Стратегии сокрушения и измора в новом облике. Военная мусль, № 3 2014, 45-57.

Воробьев, И. Н., Киселев, В. А. (2014b) Киберпространство как сфера непрямого вооруженного противоборства. Военная мысль, № 12 (2014), 21-28.

Воронин, Станислав Николаевич, Брезкун, Сергей Тарасович. Стратегически выгодная асимметрия. Независимое военное обозрение № 36 1999.

ВПК. Кибербезопасность страны – дело всенародное. ВПК, № 11 (577) за 25 марта 2015 года.

Вус, М.А., Макаров, О.С. Стратегический вектор обеспечения международной информационной безопасности. СПб.: СПИИРАН. Изд-во «Анатолия». 2016.

Выговский, И. И., Давыдов, А. Е. Направления совершенствования организации автоматизированного управления в военной сфере. Военная мысль, № 9 (2017), 37-42.

Выпасняк, В. И. О реализации сетецентрических принципов управления силами и средствами вооруженной борьбы в операциях (боевых действиях). Военная мысль, № 12 (2009), 23-30, 27.

Выпасняк, В.И., Тиханычев, О.В. Автоматизированные системы управления войсками (силами): тенденции, методы и перспективы развития. Вестник академии военных наук, № 4 (29) 2009, 61-69.

Выпасняк, В.И., Тиханычев, О.В., Гахов, В.Р. Кибер-угрозы автоматизированным системам управления. Вестник Академии военных наук, № 1 (42) 2013, 103-109.

Гареев, Махмут Ахметович. Война и современное международное противоборство. Независимое военное обозрение, No. 1 1998.

Гареев, М. А. Стратегическое сдерживание: проблемы и решения. Красная звезда, № 183 (2008).

Гареев, М.А. Уроки и выводы из войны в Ираке. Военная мысль, № 8 2003, 68-76.

Гареев, М.А. Доклад президента Академии военных наук генерала армии М.А.Гареева. Вестник Академии военных наук, №2(3) 2003, 9-17.

Гареев, М.А. (2005a) О характере вооруженной борьбы будущего. Вестник Академии военных наук, №2, 2005, 11-14.

Гареев, М.А. (2005b) Отстаивая национальные интересы. ВПК, № 48 (115) за 21 декабря 2005 года.

Гареев, М.А. Структура и основное содержание новой военной доктрины. ВПК, № 3 (169) за 24 января 2007 года.

Гареев, М.А. Национальные интересы и национальная безопасность россии на современном этапе. Вестник Академии военных наук, №1 (22) 2008, 8-22.

Гареев, М.А. Стратегическое сдерживание: проблемы и решения. Красная звезда, № 183, 8.10.2008.

Гареев, М.А. (2009a) Проблемы стратегического сдерживания в современных условиях. Вестник Академии военных наук, № 2 (27) 2009, 19-22.

Гареев, М. А. (2009b) Проблемы стратегического сдерживания в современных условиях. Военная мысль, № 4 2009, 2-9.

Гареев, М.А. Итоги деятельности Академии военных наук за 2009 год и задачи академии на следующий год. Вестник Академии военных наук, № 1 (30) 2010, 8-18.

Гареев, М.А. Итоги деятельности Академии военных наук за 2011 год и задачи академии на 2012 год. Вестник Академии военных наук, 2(39) 2012, 6-17.

Гареев, М.А. (2013a) Итоги деятельности Академии военных наук за 2012 год и задачи академии на 2013 год. Вестник Академии военных наук, 1(42) 2013, 8-21.

Гареев, М.А. (2013b) Система знаний о войне и обороне страны на современном этапе. Вестник Академии военных наук, 2(43) 2013, 7-14.

Гареев, М.А. (2013c) Характер современных военных и невоенных угроз безопасности России и организация обороны страны. Вестник Академии военных наук, 4(45) 2013, 4-9.

Гареев, М.А. Итоги деятельности Академии военных наук за 2013 год и задачи академии на 2014 год. Вестник Академии военных наук, 1(46) 2014, 7-13.

Гареев, М.А. (2015a) Опыт Великой Отечественной войны и работа Академии военных наук по дальнейшему развитию военной науки. Вестник Академии военных наук, 2(51) 2015, 16-25.

Гареев, М.А. (2015b) В интересах обороноспособности страны. Вестник Академии военных наук 1(50) 2015, 4-9.

Гареев, М.А. (2017a) Итоги деятельности Академии военных наук за 2016 год и задачи Академии на 2017 год. Вестник Академии военных наук, 2(59) 2017, 14-22.

Гареев, М.А. (2017b) Мобилизация умов Наши руководители должны коренным образом изменить отношение к науке. ВПК, № 12 (676) за 29 марта 2017 года.

Гареев, М.А. Итоги деятельности Академии военных наук за 2017 год и задачи академии на 2018 год. Вестник Академии военных наук, № 2 (63) 2018, 6-15.

Гареев, М.А. Итоги деятельности Академии военных наук за 2018 год и задачи академии на 2019 год. Вестник Академии военных наук, 2(67) 2019, 12-18.

Герасимов, Валерий. Ценность науки в предвидении. ВПК № 8 (476) 2013, 1-3.

Герасимов, Валерий Васильевич. Приоритеты развития системы вооружения Вооруженных Сил Российской Федерации. Федеральный справочник. Оборонно-промышленный комплекс России, Том №

10, 2014, 117-120 [Online]. Available: http://federalbook.ru/files/OPK/Soderjanie/OPK-10/III/Gerasimov.pdf [Accessed: 5th March 2019].

Герасимов, В.В. Опыт стратегического руководства в Великой Отечественной войне и организация единого управления обороной страны в современных условиях. Вестник Академии военных наук, 2(51) 2015, 5-15.

Герасимов, В.В. Организация обороны Российской Федерации в условиях применения противником «традиционных» и «гибридных» методов ведения войны. Вестник Академии военных наук, № 2 (55) 2016, 19-23, 20.

Герасимов, В.В. Современные войны и актуальные вопросы обороны страны. Вестник Академии военных наук, 2(59) 2017, 9-13.

Герасимов, В.В. Мир на гранях войны: Мало учитывать сегодняшние вызовы, надо прогнозировать будущие. ВПК, № 10 (674) за 15 марта 2017 года.

Герасимов, Валерий. Векторы развития военной стратегии. Красная звезда 4.3.2019 [Online]. Available: http://redstar.ru/vektory-razvitiya-voennoj-strategii/ [Accessed: 4th March 2019].

Герасимов, Н. Н., Шакирова, Е. Ю. Социально-сетецентрические войны современности: реальность информационной эпохи. Военная мысль, № 10 (2017), 79-87.

Герасимов, В. В. О ходе выполнения указов Президента Российской Федерации от 7 мая 2012 года N603, 604 и развития Вооруженных Сил Российской Федерации. Военная мысль, № 12 (2017), 7-21.

Герасимов, В.В. Влияние современного характера вооруженной борьбы на направленность строительства и развития Вооруженных сил Российской Федерации. Приоритетные задачи военной науки в обеспечении обороны страны. Вестник академии военных наук, № 2 (63) 2018, 16-22.

Глазов, Б.И. and Ловцов, Д.А. Информационная борьба как система отношений в информационной среде. Военная мысль 1997 № 5, 36-41.

Голышко А. В., Князев К. Г. NGN: Российский сегмент. Электросвязь, № 12 2009.

Горбачев, Юрий. К вопросу о ”войне в четвертой сфере”. В США у нее иная терминология, чем в России, а задачи – всеобъемлющие. Независимое Военное Обозрение, № 14 20.4.2001.

Горбачев, Юрий. РЭБ в операциях XX и XXI века. ВПК, № 44 (61) за 17 ноября 2004 года.

Горбачев, Ю. Е. Сетецентрическая война: миф или реальность? Военная мысль, № 1 (2006), 66-76.

Горбачев, Юрий. Кибервойна уже идет. Независимое военное обозрение, № 13 (754) 2013.

Горбачев, Юрий. Борьба в электронном пространстве усиливается. Независимое военное обозрение, № 3 (2015).

Горбунов, В. Н., Богданов, С. А. Военно-стратегическое противоборство: формы и способы воздействия на экономический потенциал противника. Военная Мысль, № 12 2007, 50-59.

Горбунов, В. Н., Богданов, С. А. О характере вооруженной борьбы в XXI веке. Военная Мысль, № 3 2009, 2-15.

Горлов, А. И., Смирнов, С. С. О влиянии автоматизации на работу органов управления. Военная мысль № 12 1984, 49-55.

Горкин, А. П., Золотарев, В. А., Карев, В. М., Манилов, В.Л., Милованов, В. И. Военный энциклопедический словарь в двух томах. Москва: Большая Российская энциклопедия, 2001.

Грачев, И. А., Каргин, В. Н. Информатизация вооруженных сил. информационные технологии в автоматизированных системах военного назначения. Военная мысль, № 6 (2001), 19-22.

Грачев, И. А. Информатизация вооруженных сил. к вопросу об информационно-методической согласованности моделей военных действий. Военная мысль, № 2 (2002), 53-57.

Грачев, И. А. Принципы построения специального математического и программного обеспечения АСУ войсками (силами). Военная мысль, № 6 (2002), 64-68.

Грачева, Татьяна. Наставники плохих парней – На политическую войну Пентагон рекрутирует отщепенцев и предателей. ВПК, № 46 (612) за 2 декабря 2015 года.

Гречкоб А. А., Огарков, Н. В. (Гл. ред.) Советская Военная Энциклопедия, в 8 т. М.: Военное издательство Министерства обороны СССР, 1976—1980.

Григорьев В.Р. Информационные вирусы – Новое оружие массового поражения. Информационные войны, №3 (7) 2008, 2-29.

Гринь, В.Р. Информатизация вооруженных сил. Качество и безопасность автоматизированных систем управления войсками (силами): единство целого и частного. Военная мысль, № 12(2006), 26-31.

Гриняев, С.Н. Глобализация и информационная безопасность. Красная звезда, № 4 2.11.10.2000.

Гриняев, Сергей. Война в четвертой сфере. Превосходство в киберпространстве будет определять победу в конфликтах XXI века. Независимое военное обозрение N 42 (215) 10.11.2000.

Гриняев, С. Н. Поле битвы - киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. М.: Харвест, 2004.

Гриняев, С.Н. Глобализация и информационная безопасность. Независимое Военное Обозрение, № 221 29.11.2002.

Гришковец, Е. Формирование в США единой информационной инфраструктуры вооруженных сил. Зарубежное военное обозрение, № 3 (2018), 19-24.

Грудинин, И.В., Майбуров, Д.Г. Содержание и структура категории «информационно-управленческий ресурс отражения удара средств воздушно-космического нападения противника». Вестник академии военных наук, № 1 (62) 2018, 104-111.

Гулин, В.П. О новой концепции войны. Военная мысль № 2 (3-4) 1997, 13-17.

Дворкин, Владимир. СНВ на весах стратегической стабильности. Независимое военное обозрение, № 14 за 16 апреля 2010 года.

Дворкин, Владимир Зиновьевич. Ядерное сдерживание и договор СНВ-2. Независимое военное обозрение № 3 1997.

Дербин, Е.Л. О роли смысла в обеспечении информационной безопасности. Военная Мысль, № 11 2007, 68-77.

Дербин, Е.А. Информационная безопасность союзного государства как основа его обороноспособности в условиях непрямых действий противника. Вестник Академии военных наук, № 2 (27) 2009, 31-38.

Дербин, Е.Л. О Совершенствовании Стратегического Руководства Обороной России. Вестник Академии военных наук, № 2 (67) 2019, 46-52.

Дмитриев, А. Кибернетика и военное дело. Военная мысль № 1 1970, 89-96.

Дмитриев, А. П. Политика КПСС в области обороны и безопасности страны на современном этапе. Военная мысль № 4 1987, 58-68.

Долгополов, А. В., Богданов, С. А. Эволюция форм и способов ведения вооруженной борьбы в сетецентрических условиях. Военная мысль, № 2 (2011), 49-58.

Донсков, Ю. Е., Беседин, П. Н., Ботнев, А. К. Превосходство в управлении - обязательный фактор реализации основных закономерностей оперативного искусства. Военная мысль, № 11 (2017), 28-31, 28.

Донсков, Ю. Е., Морареску, А. Л., Беседин, П. Н. Завоевание превосходства в управлении как цель применения войск радиоэлектронной борьбы в операциях объединения Сухопутных войск. Военная мысль, № 1 (2018), 28-32.

Донсков, Ю.Е., Никитин, О. Г. Место и роль специальных информационных операций при разрешении военных конфликтов. Военная мысль, № 6 (2005), 30-34.

Донсков, Ю. Е., Фомин, В. В. Информационное превосходство: пути реализации в операциях. Военная мысль, № 11 (2003), 57-61.

Джерелиевский, Борис. Сетевые войны. ВПК, № 45 (112) за 30 ноября 2005 года.

Дружинин, В., Конторов, Д. Методика решения оперативных задач с применением средств автоматизации. Военная мысль № 1, 1970, 40-52.

Дружинин, В., Конторов, Д. Руководство и автоматизация. Военная мысль № 6 1973, 24-34.

Дружинин, В. В. and Конторов, Д. С. О некоторых новых аспектах проблемы автоматизации управления войсками. Военная мысль № 12 1975, 28-40.

Дружинин, В. В., Конторов, Д. С. Принципы создания и применения автоматизированных систем управления войсками. Военная мысль № 8 1976, 43-54.

Дугин А.Г. Теоретические основы сетевых войн. Информационные войны, № 1(5) 2008, 2-9.

Дульнев, П. А., Ковалев, В. Т., Ильин, Л. Н. Асимметричное противодействие в сетецентрической войне. Военная Мысль, № 10 2011, 3-8.

Дылевский И. Н., Комов С. А., Коротков С. В., Родионов С. Н. и Федоров А. В. Военная политика Российской Федерации в области обеспечения международной информационной безопасности. Военная мысль, № 4 2006, 2-7.

Дылевский И. Н., Комов С. А., Короткое СВ., Родионов С. Н., Федоров А. В. Военная политика Российской Федерации в области международной информационной безопасности: региональный аспект. Военная мысль № 2/2007, 32-40.

Дылевский, И. Н., Комов, С. А., Коротков, С. В., Петрунин, А. Н. Операции в киберпространстве: вопросы теории, политики и права. Военная мысль, № 8 (2011), 72-78.

Дылевский, И. Н., Запивахин, В. О., Комов, С. А., Коротков, С. В., Петрунин, А. Н. Международный режим нераспространения информационного оружия: утопия или реальность? Военная мысль, № 10 2014, 3-12.

Дылевский, И. Н., Запивахин, В. О., Комов, С. А., Коротков, С. В., Кривченко, А. А. О диалектике сдерживания и предотвращения военных конфликтов в информационную эру. Военная мысль, № 7 2016, 3-11.

Дылевский И. Н., Комов С. А., Коротков, С.В., Родионов С. Н., Полякова, Т. А., Федоров А. В. К вопросу о международно-правовой квалификации информационных операций. Военная мысль № 2 2008, 2-10.

Дылевский И. Н., Запивахин, В. О., Комов С. А., Петрунин, А. В., Эльяс, В. П. Военно-политические аспекты государственной политики Российской Федерации в области международной информационной безопасности. Военная мысль № 1/2015, 11-17.

Евстигнеев, Е. А., Вичугов, Е. С. О повышении эффективности использования ЭВМ в штабах и учреждениях. Военная мысль № 9 1977, 60-69.

Евстигнеев, Е. А., Сухоруков, Ю. С. Об основных направлениях обеспечения устойчивости автоматизированного управления войсками в операции (бою). Военная мысль № 9 1989, 42-50.

Емельянов Г.В., Стрельцов А.А. Проблемы обеспечения информационной безопасности субъектов Российской Федерации. Информационное общество, № 6 (1998), 38 - 41.

Ефремов, А.А. Формирование концепции информационного суверенитета государства. Право - Журнал Высшей школы экономики, № 1. 2017, 201–215.

Ефремов, А. А. Проблемы реализации государственного суверенитета в информационной сфере. Вестник УрФО № 2(20) / 2016, 54–60.

Ефремов, Г., Царев, В., Асатуров, С. Владимир Челомей в истории Советского ВМФ. ВПК, № 25 (291) за 1 июля 2009 года.

Ермаков, А. А., Ткачук, А. В., Мишенев, А. М. Опыт создания единой автоматизированной системы управления мобилизационным развертыванием Вооруженных Сил Российской Федерации. Военная мысль № 7 2019, 77-80.

Жованик, А. А. О роли связи в автоматизированных системах управления войсками. Военная мысль № 11 1976, 28-39.

Жованик, А. А. Космические системы связи и их использование для управления вооруженными силами. Военная мысль № 4 1983, 34-42.

Завадский, И.И. Информационная война — что это такое? Защита информации. Конфидент № 4 1996.

Зайнуплин, Р. Х. Средства массовой информации и идеологическая борьба в современных войнах. Военная мысль , № 5 1978, 16-30.

Завьялов, И. Диалектика войны и военная доктрина. Военная мысль 1975 №. 6, 23-34.

Зацаринный, А. А., Кисилев, Э. В. Некоторые подходы к формированию нормативно-технической базы единого информационного пространства России в части информационных ресурсов. Информатика и управление, Том 25 № 1 (2015), 155-167.

Зацаринный, А. А., Кисилев, Э. В. Некоторые подходы к формированию нормативно-технической базы в части требований к архитектурному построению информационных систем организаций - участников единого информационного пространства России. Информатика и управление, Том 25 № 3 (2015), 161-178.

Зацаринный, А. А., Кисилев, Э. В. Некоторые подходы к формированию обобщенной архитектуры информационных систем организаций - участников единого информационного пространства России. Информатика и управление, Том 25 № 4 (2015), 114-127.

Захаров, А. Н. Тенденции развития вооруженной борьбы. Военная мысль № 11 1991, 9-15.

Захарцев, Алексей. Федеральный антивирус: Защитникам виртуального мира требуется помощь государства- ВПК, № 3-4 (618-619) за 3 февраля 2016 года [Online]. Available: https://vpk-news.ru/articles/28996 [Accessed: 28th February 2019].

Зеленый, В. В. Основные тенденции противодействия терроризму. Военная мысль, № 10 2015, 3-14.

Зиновьев В. Н., Колдунов А. И., Груздев Н. В. Перспективы применения информационных сетей в военном деле. Информационные войны, №1 (33) 2015, 37-40.

Зиновьева, Е.С. Международное управление интернетом: проблемы, подходы, перспективы. Вестник МГИМО-Университета № 6 (15) 2010, 167-174.

Зиновьева, Е. С. Международное управление Интернетом: конфликт и сотрудничество: учеб. Пособие. М.: МГИМО-Университет, 2011.

Зиновьева, Е.С. Международно-политические аспекты развития интернета. Вестник МГИМО-Университета № 4 (31) 2013, 135-140.

Зиновьева, Е.С. Анализ внешнеполитических инициатив РФ в области международной информационной безопасности. Вестник МГИМО-Университета. № 6 (39) 2014, 47-52.

Зиновьева, Е.С. Глобальное управление Интернетом: российский подход и международная практика. Вестник МГИМО-Университета, № 4 (43) 2015, 111-117.

Зиновьева, Е.С. (2016a) Возможности России в глобальном информационном обществе. Вестник МГИМО-Университета. № 3 (48) 2016, 17-29, 19.

Зиновьева, Е.С. (2016b) Перспективные тенденции формирования международного режима по обеспечению информационной безопасности. № 4 (49) 2016, 235–247, 235.

Золотарев, Владимир. (2013a) Когда нация становится жертвой: Концептуальные основы информационно-сетевых войн. ВПК, № 17 (485) за 1 мая 2013 года.

Золотарев, Владимир. (2013b) Психологическая война уже в киберпространстве. Войска информационных операций способны обойтись без применения военной силы. ВПК, № 16 (484) за 24 апреля 2013 года.

Иванов, И. С. (ред.) Военно-политические исследования в России. М.: НП РСМД, Весь мир, 2014.

Иванов, А.А. Информатизация вооруженных сил. Информатизация Вооруженных Сил: проблемы и пути их решения. Военная мысль, № 2 (2000).

Иванов, Валерий. Поршневое управление. Чтобы достичь прорыва в разработке межвидовой АСУ, Минобороны должно сделать ставку не на кустарей, а на государственниковвпк. ВПК, № 33 (599) 2-8 сентября 2015 года.

Иванов, Павел. Плакали ваши хакеры. ВПК, № 18 (2017).

Иванов, Владимир. Армия США готовится к кибервойне. Независимое военное обозрение, № 6 (984) 2018.

Ивашов, Леонид. Удар Валдая. Выступление президента России на собрании дискуссионного клуба в Сочи стало главной мировой новостью. ВПК, № 41 (705) за 25 октября 2017 года.

Иванько, Анатолий. Эшелонированная брешь Мысль всегда будет эффективнее самого высокоточного боеприпаса. ВПК, № 12 (627) за 30 марта 2016 года.

Игнатов, В.А., Сосюра, О.В., Гусев, В.Ф. О терминологии теории военного управления. Военная мысль № 6 (11-12) 1996, 38-41.

Ильин Н.И. Эволюция информационных систем государственного управления. Информационные войны №1 (41) 2017, 54-57.

Ильин, А. П. Шакин, Д. Н. К вопросу о месте радиоэлектронной разведки, радиоэлектронной борьбы и радиоэлектронной маскировки в информационной борьбе. Военная мысль, № 1 (2008), 25-30.

Krasnaia Zvezda. Будет ли в СНГ единое информпространство? Krasnaia Zvezda № 289 1996.

Ицкович, Б.С. Формируя единое информационное пространствою Железнодорожный транспорт. 2011. № 5., 60-61.

Каберник, В.В. Проблемы классификации кибероружия. MGIMO 2 (29) 2013, 72-78.

Казарьян, Б. И. Операции, боевые действия, сетецентричная война. Военная мысль, № 2 (2010), 25-37.

Казеннов, Сергей, Кумачев, Владимир. Хочешь мира - готовься... к чему? Независимое Военное Обозрение, № 19 29.5.2015.

Казеннов, Сергей, Кумачев, Владимир. Ах, если б вам служить на суше... Независимое Военное Обозрение, № 28 7.8.2015.

Калиновский, О.Н. Дискуссионная трибуна. "Информационная война" - это война? Военная мусль, № 1 1.1.2001.

Калашников, А. О. Управление информационными рисками объектов критической информационной инфраструктуры Российской Федерации. Вопросы кибербезопасности №3(4) 2014, 35-41.

Калинин, Ю. П. Озеранскии, Л.И. Информационные сети — перспектива автоматизации процессов управления войсками. Военная мысль № 2 1997, 54-58.

Кардаш, И. Л. О совершенствовании системы территориальной обороны. Военная мысль, № 2 2014, 3-10.

Кардаш, И. Л. Новый подход к организации территориальной обороны на региональном уровне. Военная мысль, № 9 2018, 34-40.

Карпов, Е. А., Буренин, Н. И. Зюзин, Н. А. Единое военное информационное пространство: проблемы создания. Военная мысль № 8 (2004), 45.

Картаполов, А.В. Уроки военных конфликтов, перспективы развития средств и способов их ведения. Прямые и непрямые действия в современных международных конфликтах. Вестник Академии военных наук, 2(51) 2015, 26-36.

Карякин В.В. Мир вступил в эпоху войн седьмого поколения – информационно–сетевых войн. Информационные войны, № 3(19) 2011, 2-7.

Кедров, Илья. АСУ для оружия будущего. ВПК, № 36 (152) за 20 сентября 2006 года.

Кежаев, В.А. Совершенствование управления войсками: аспект информатизации. Военная мысль № 4 1996, 42-45.

Кижицкий, В. А., Завьялов, В. Е., Саваренков, С. М. Об уточнении содержания терминов "организация" и "управление" в терминологической системе теории военного управления. Военная мысль, № 10 (2014), 59-64.

Кириленко, Г. В., Тренин, Д. В. Формула безопасности от паритета к стратегической стабильности. Военная мысль № 8-9 1992.

Кириллов, В. В. Военная мощь государства: сущность, структура, проблемы. Военная мысль, № 9 (2005), 2-12.

Киселев, В. А., Воробьев, И. Н. Гибридные операции как новый вид военного противоборства. Военная мысль, № 5 2015, 41-48.

Киселев, В. А. К каким войнам необходимо готовить Вооруженные Силы России. Военная Мысль, № 3 2017, 37-46.

Ковалев В.И., Коссе Ю.В. ”Гудвилл” сша в контексте инициатив по сокращению сяс и проблемы Россиии. Информационные войны, №4 (12) 2009, 10-19.

Ковалёв В.И., Матвиенко Ю.А. «Сетецентрическая» война как новая парадигма вооружённой борьбы. Информационные войны №2 (26) 2013, 2-9.

Ковалев В.И., Малков С.Ю. Что делать, чтобы не распасться как ссср? Информационные войны, № 3(35) 2015.

Ковалев, Виктор, Малинецкий, Георгий, Матвиенко, Юрий. Концепция «сетецентрической» войны для армии России: «множитель силы» или ментальная ловушка? Экономические стратегии № 5/2013, 40-51.

Ковалев, В.И., Малинецкий, Г.Г., Матвиенко, Ю.А. Концепция «сетецентрической» войны для армии России: «множитель силы» или ментальная ловушка? Вестник Академии военных наук, 2(51) 2015, 94-100.

Козичев, В. Н., Каргин, В. Н., Ширманов, А. В., Голошев, С. П. Перспективы создания корпоративных автоматизированных информационных систем военного назначения. Военная мысль, № 20 (2015), 19-32.

Козлов, М. М. Вопросы стратегии в Советской Военной Энциклопедии. Военная мысль 1980 No. 10, 13-23.

Козлов, М. М. Сохранение военно-стратегического паритета— серьезный фактор обеспечения мира и международной безопасности. Военная № 12 1986, 3-13.

Кокошин, Андрей. "Асимметричный ответ" vs. ”Стратегической оборонной инициативы” Международная жизнь, № 7 - 8, 2007.

Кокошин, Андрей. ”Звездные войны”: ответить асимметрично. Красная звезда, № 164, 12.9.2007.

Кокошин, Андрей. Асимметричный ответ номер один. Независимое военное обозрение № 24 27.7.2007.

Кокошин, Андрей. ”Звездные войны”: как СССР ответил Рейгану. Красная звезда, № 169, 17.9.2008.

Кокошин, А. А., Герасёв, М. И. Американские планы милитаризации космоса. Военная мысль № 4 1987, 69-80.

Кокошин А. А., Ларионов В. В. Противостояние сил общего назначения в контексте обеспечения стратегической стабильности. Мировая экономика и международные отношения № 6 1988.

Кокошин, А.А. Военно-политические и экономические аспекты реформы Вооруженных Сил России. Военная мысль № 6 (11-12) (1996), 2-11.

Кокошин А. А. «Асимметричный ответ» на «Стратегическую обо-ронную инициативу» как пример стратегического планирования в сфере национальной безопасности. Международная жизнь №7 (июль-август) 2007.

Кокошин, А.А. Перспективы развития военной техносферы и будущее войн и небоевого применения военной силы. Вестник академии военных наук, № 2 (67) 2019, 26-29.

Колодяжный, В.В., Кулешов, Ю.Е., Шеховцов, Н.П. Методический подход к совершенствованию автоматизации управления войсками: информационный аспект. Вестник академии военных наук, № 1 (42) 2013, 109-115.

Колыванов, Георгий. Непонятная асимметрия. Генштаб попытался сказать новое слово в военной науке. Независимое военное обозрение N 4 3.2.2006.

Комов, С.А. О концепции информационной безопасности страны. Военная мысль № 4 1994, 12-17.

Комов, С. А. Информационная борьба в современной войне: вопросы теории. Военная мысль № 3 1996, 76-80.

Комов, С. А. О способах и формах ведения информационной борьбы. Военная мысль № 4 1997, 18-22.

Комов, С.А. О доктрине информационной безопасности Российской Федерации. Военная мысль, № 3 1998, 72-76.

Комов, С. А., Коротков, С. В., Родионов, С. Н. О военных аспектах проблемы международной информационной безопасности. Военная мысль, № 9 2003, 2-5.

Комов, С. А., Коротков, С. В., Дылевский, И. Н. Об эволюции современной американской доктрины “информационных операций”. Военная мусль, № 6 2008.

Комов, С.А. (под общ. редакцией). Международная информационная безопасность: дипломатия мира. Сборник статей. М: Военинформ, 2009.

Кондратьев, Александр. Новые возможности для нового облика. ВПК, № 45 (311) за 18 ноября 2009 года.

Кондратьев, Александр. Мнение: информатизация по-российски. ВПК, 18 января 2012 [Online]. Available: https://vpk-news.ru/news/224 [Accessed: 8th March 2019].

Коновалов, Сергей. Генеральский демарш. Независимое военное обозрение, 5 июля 2011 [Online]. Available: http://nvo.ng.ru/nvo/2011-07-05/1_demarsh.html [Accessed: 30th April 2019].

Коновченко С.В., Киселев А.Г. Информационная политика в России. Монография. М., РАГС, 2004.

Кончиц, R. H. Совершенствование управления войсками в современном бою. Военная мысль No. 9 1987, 43-50.

Копытко, В. К., Шептура, Владимир. Проблемы построения единого информационного пространства Вооруженных Сил Российской Федерации и возможные пути их решения. Военная мысль, № 10 (2011), 16-26.

Коробушин, Варфоломей. Метаморфозы стратегического сдерживания. Независимое военное обозрение, № 14 (423) за 15 апреля я 2005 года.

Коровкин С.Д. Единое информационное пространство органов государственной власти. Компетентность. 2007. № 2 (43), 26-37.

Королев, И. И., Павлов, В. Н., Ганин, А. В. Радиоэлектронно-информационная блокада - перспективный способ применения разнородных сил и средств РЭБ. Военная Мысль, № 4 2013, 16-23.

Коротков А.В., Зиновьева Е.С. Безопасность критических информационных инфраструктур в международном гуманитарном праве. Вестник МГИМО-университета, №4(19) 2011, 154-162.

Корочанский, И. Ф. Нарушение военно-стратегического равновесия — цель милитаристских приготовлений США. Военная мысль 1982 № 3, 15-22.

Коротченко, Е.Г. Об эволюции принципов военного искусства. Военная мысль № 9 1988, 22-30, 30.

Коротченко, Е.Г. Информационно-психологическое противоборство в современных условиях. Военная мысль № 1 1996, 22-28.

Коротченко, Игорь. Реорганизация совета безопасности РФ завершена. Созданная структура, по мнению Ивана Рыбкина, позволяет решать задачи любой сложности. Независимая газета, № 9 21 января 1997.

Костарев, С. В., Ефремов, О. Ю., Зверев, С. Э. Концепция сетецентрических войн в свете доктрины "Единый взгляд 2020". Военная мысль, № 1 (2014), 58-64.

Костин Н А. Теория информационной борьбы. М: ВАГШ, 1996.

Костин, Н.А. Общие основы теории информационной борьбы. Военная мысль 1997 № 3, 44-50.

Костюкевич, Н.Е. Предложения по изменению подходов к созданию (модернизации) систем и комплексов средств автоматизации управления военного назначения. Вестник академии военных наук, № 1 (54) 2016.

Костюхин А.А. и др. Словарь терминов и определений в области информационной безопасности. Москва: ГШ ВС РФ, 2008.

Крамар, Владислав. Любая война обходится дороже содержания мощной армии. ВПК, № 39 (106) за 19 октября 2005 года.

Кранс, Максим. Кибероружие в арсенале НАТО. Независимое военное обозрение, № 21 (762) 2013.

Красная звезда. Актуальные задачи развития вооруженных сил Российской Федерации. Красная звезда, 11 октябя 2003.

Красная звезда. Создается единое информационное пространство. Красная звезда. № 10 1995.

Крейдин, С.В. (1999a) Глобальное и региональное ядерное сдерживание: к системе принципов и критериев. Военная мысль № 4 1999.

Крейдин, С.В. (1999b) Дискуссионная трибуна. Проблемы ядерного сдерживания: боевая устойчивость ядерного потенциала. Военная мысль No. 4 1999.

Крикунов, Александр, Королёв, Александр. Информационные войны будущего. О необходимости адекватной защиты отечественной информационной инфраструктуры от кибератак. Военный дипломат, № 1 (2009), 94-103.

Криницкий, Ю. В. Асимметричные средства и способы ведения войны. Военная Мысль, № 11 2010, 25-30.

Круглов, В. В. Фундаментальные законы мироздания - Основа новой теории войны. Обозреватель, №8 (187) 2005.

Круглов, В. В. Новый подход к анализу современного противоборства. Военная Мысль, № 12 2006, 50-61.

Круглов, В. В. О вооруженной борьбе будущего. Военная мысль № 5 1998, 54-58.

Крутских, Андрей. Кто владеет Интернетом, тот владеет миром. Международная жизнь, № 10 (2016).

Крутских, Андрей, Стрельцов, Анатолий. Международное право и проблема обеспечения международной информационной безопасности. Международная жизнь, № 11 (2014).

Крылова, И.А. Информационные войны и безопасность России. Информационные войны №3 (39) 2016, 63-70.

Кряжев, П. Н. Развитие военно-административной территориальной структуры Вооруженных Сил Российской Федерации. Военная мысль № 11 (2011), 30-42.

Кузнецов, Н. Н. О категориях и принципах советской военной стратегии. Военная мысль 1984 No. 1, 29-40.

Кузнецов, В. И., Донсков, Ю. Е., Коробейников, А. С. О соотношении категорий "радиоэлектронная борьба" и "информационная борьба". Военная мысль, № 3 (2013), 14-20.

Кузнецов, В. И., Донсков, Ю. Е., Никитин, О. Г. К вопросу о роли и месте киберпространства в современных боевых действиях. Военная мысль № 3 (2014), 13-17.

Кузнецов, Юрий. Сто лет на охране секретов государства. Красная звезда, 2.11.2018 [Online]. Available: http://redstar.ru/sto-let-na-ohrane-sekretov-gosudarstva/ [Accessed: 17th May 2019].

Кулаков, Александр. Асимметричный ответ не спасет. Независимое военное обозрение № 25 25.7.2008.

Куликов, В. Г. О военно-стратегическом паритете и достаточности для обороны. Военная мысль № 5 1988, 3-11.

Кураленко, С. В. Тенденции изменения характера вооруженной борьбы в военных конфликтах первой половины XXI века. Военная Мысль, № 11 2012, 40-46.

Кутейников, Алексей Викторович. Проект общегосударственной автоматизированной системы управления советской экономикой (ОГАС) и проблемы его реализации в 1960-1980-х гг. Диссертации на соискание ученой степени кандидата исторических наук. Кафедра Исторической информатики Московского государственного университета имени М.В. Ломоносова. Москва, 2011 [Online]. Available: http://www.hist.msu.ru/Science/Disser/Kuteinikov.pdf [Accessed: 23rd March 2019].

Кучерявый, М.М. К осознанию информационного суверенитета в тенденциях глобального информационного пространства. Наука, новые технологии и инновации Кыргызстана № 12, 2015, 22-27.

Кучерявый, Михаил Михайлович. Информационное измерение политики национальной безопасности России в условиях современного глобального мира. Диссертация на соискание ученой степени доктора политических наук по специальности. Санкт-Петербург, 2014.

Лаврино, Г.А., Чумичкин, А.А. Опыт создания единого информационного пространства для решения задач технического оснащения Вооруженных Сил Российской Федерации. Вестник академии военных наук, № 1(26)/2009.

Ланчев, Василий. АСУ ВКО: модель для сборки. Учебные командные пункты должны лечь в основу подготовки специалистов ВКО. ВПК, № 39 (605) 14 –20 октября 2015 года.

Ласточкин, Ю. И. (ред.) Радиоэлектронная борьба в Вооруженных Силах Российской Федерации – 2018. Москва: Информационный мост, 2018 [Online]. Available: https://reb.informost.ru/2018/sod.php [Accessed: 14th March 2019].

Левин, Леонид. О законодательных мерах по обеспечению информационной безопасности Российской Федерации. Федеральный справочник 2015 [Online]. Available: http://federalbook.ru/files/BE-ZOPASNOST/soderghanie/NB_2/NB2-2015-LevinLL.pdf [Accessed: 17th May 2019].

Левшин, В. И., Неделин, А. В., Сосновский, М. Е. О применении ядерного оружия для деэскалации военных действий. Военная мысль № 3(5-6) 1999, 34-37.

Легков, К.Е. Основные теоретические и прикладные проблемы технической основы системы управления специального назначения и основные направления создания инфокоммуникационной системы специального назначения. T-Comm #6 2013, 42-46.

Легков К.Е. Организация и модели функционирования современных инфокоммуникационных сетей специального назначения. T-Comm Vol.9. #8-2015, 14-19.

Лепский В.Е. Технологии управляемого хаоса – оружие разрушения субъектности развития. Информационные войны, № 4(16) 2010, 69-78.

Лепский В.Е., Мельников А.А., Пойкин А.Е. Информационные войны за доминирование в инновационной сфере россии и на евразийском пространстве. Информационные войны, № 4(36) 2015, 12-20, 15.

Лимно, А. Н., Крысанов, М. Ф. Информационное противоборство и маскировка войск. Военная мусль, № 5 31.5.2003.

Лифшиц, А., Розенберг, В. О комплексе математического обеспечения автоматизированных систем управления войсками. Военная мысль № 6 1974, 41-48.

Лихачев, А. М., Абрамович, А. В., Присяжнюк, А. С. Концептуальные основы создания и развития автоматизированной системы управления ОАЦСС ВС РФ. Информация и космос, №2 (2016), 6-21.

Ловцов, Д. А. Информационная безопасность АСУ войсками и оружием: теоретические аспекты. Военная мысль № 6 1996, 32-38.

Лосик, О. А. Развитие оружия, боевой техники и способов боевых действий. Военная мысль № 2 1979, 12-21.

Лощилов, И. П. О новом принципе построения автоматизированных систем управления войсками. Военная мысль № 7 1977, 46-57.

Лузан, Александр. Воздушно-космическое нападение. В войнах нового поколения резко возрастает роль высокоточного оружия и средств борьбы с ним. Независимое Военное Обозрение, № 10 (846) 20.3.2015.

Лузянин, В. П. Стратегическая стабильность и многополярная модель сдерживания. Военная мысль № 8-9 1998.

Лукашкин, А.Н., Ефимов. А.И. Проблема безопасности компьютерной инфосферы стратегических оборонных систем. Военная мысль № 5, 1995 48-52.

Лутовинов, В. И. Развитие и использование невоенных мер для укрепления военной безопасности Российской Федерации. Военная мысль, № 5 (2009), 2-12.

Майоров, Леонид Сергеевич. Информация и безопасность. Развитие современных технологий как реальная угроза будущему России. Независимая газета, № 180 25 сентября 1997.

Майбуров, Д. Г., Иконников, О. В. Развитие теоретических положений информационного обеспечения управления отражением ударов средств воздушно-космического нападения противника. Военная мысль № 9 (2018), 48-53.

Макаров, Н.Е. «Характер вооруженной борьбы будущего, актуальные проблемы строительства и боевого применения Вооруженных Сил РФ в современных условиях». Вестник Академии военных наук, № 2 (31) 2010, 18-26.

Макаренко, С. И. (2017a) Перспективы и проблемные вопросы развития сетей связи специального назначения. Системы управления, связи и безопасности №2. 2017, 18-68.

Макаренко, С. И. (2017b) Динамическая модель двунаправленного информационного конфликта с учетом возможностей сторон по наблюдению, захвату и блокировке ресурса. Системы управления, связи и безопасности №1 (2017), 60-97.

Макаренко, С.И. (2017c) Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. СПб.: Науко-емкие технологии, 2017.

Макаренко, С.И., Бережнов, А.Н. Перспективы использования сетецентрических технологий управления боевыми действиями и проблемы их внедрения в вооруженных силах Российской Федерации. Вестник Академии военных наук, № 4 (37) 2011, 64-68.

Макаренко, С. И., Чукляев, И. И. Терминологический базис в области информационного противоборства. Вопросы кибербезопасности, № 1(2) 2014, 13-21.

Малин, А.С. Содержание понятия безопасность. вестник академии военных наук, № 4(21) 2007.

Малюков, Вадим. Современным войскам — современную связь. Связь в Вооруженных Силах Российской Федерации 2013. Москва: Информационный мост 2013.

Манячинский, Александр. Когда слабый побеждает сильного. Независимое военное обозрение N 47 22.12.2006.

Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны. 3-е изд., стереотип. М.: Горячая линия – Телеком, 2012.

Маркоменко, Владимир. Невидимая затяжная война. Независимое военное обозрение, № 30 1997.

Масленников, Олег. Территориальнораспределенный катастрофо-устойчивый центр обработки данных Вооружённых Сил Российской Федерации. Связь в Вооруженных Силах Российской Федерации – 2018. Москва: Информационный мост 2018.

Маслов, Алексей. Чтобы нейтрализовать военные угрозы. ВПК, № 7 (223) за 20 февраля 2008 года.

Массель Л.В., Воропай Н.И., Сендеров С.М., Массель А.Г. Киберопасность как одна из стратегических угроз энергетической безопасности России. Вопросы кибербезопасности №4(17) 2016, 2-10.

Матвиенко Ю.А. Комплексная информационная атака типа «киберстачка» на промышленную автоматизированную систему: анатомия явления и подходы к защите. Информационные войны №1 (21) 2012, 85-94.

Матвиенко, Ю.А. Невоенные угрозы как составная часть современного межгосударственного противоборства. Вестник Академии военных наук, 1(58) 2017, 35-41.

Матвичук, В. В., Хряпин, А. Л. Система стратегического сдерживания в новых условиях. Военная мысль, № 1 2010, 11-16.

Матяшов, Виктор. Войны в информационном пространстве. Защита и безопасность, № 1 (2009), 17-19.

Махутов, Н.А., Резников, Д.О., Петров, В.П. Особенности обеспечения безопасности критических Инфраструктур. Безопасность в техносфере, №1 (январь–февраль), 2014, 3-14.

Медведко, Леонид. Под эгидой Соединенных Штатов. ВПК, № 10 (226) за 12 марта 2008 года.

Медриш, М.А. (ред.) Стабильность, безопасность, отказоустойчивость глобальной инфраструктуры Интернета: технические и правовые вопросы. Москва - Лос Анджелес: ПИР-Центр, 2016.

Мельников, В.П. Информационная война и современные оружейные технологии. Информационные войны, №3 (43) 2017, 28-35.

Мейчик, Евгений. На пути к единому телекоммуникационному пространству. Россииское военное обозрение, № 9 (2009), 17-18.

Мейчик, Евгений Робертович. Перспективы развития системы связи и автоматизированных систем управления вооруженных сил. Российской Федерациию Федеральный справочник. Оборонно-промышленный комплекс России, Том № 3, 2009, 379-384 [Online]. Available: http://federalbook.ru/files/OPK/Soderjanie/OPK-6/III/meychik.pdf [Accessed: 6th March 2019].

Месснера, Е.Э. Хочешь мира, победи мятежевойну! Москва: Военный университет русский путь, 2005.

Микрюков, Василий. Победа в войне должна быть достигнута еще до первого выстрела. Независимое Военное Обозрение, № 1 15.1.2016.

Микрюков, Василий. Нездоровый сетецентризм. Отечественная военная наука находится в плену у западных догматов. ВПК, № 8 (672) за 1 марта 2017 года.

Мирошников, Алексей. Войска переходят на "цифру". Независимое военное обозрение, № 39 (2009).

Михайлов, Николай. Россия может сохранить статус великой державы. Независимое военное обозрение № 36 1998.

Михайлов, Николай. Весомые ответы на военные вызовы. Независимое военное обозрение № 16 1999.

Молитвин, А. О реализации концепции единого информационного пространства НАТО. Зарубежное военное обозрение, № 1 (2008), 23-27.

Моренков, Владислав, Тезиков, Андрей. Исторический аспект развития АСУ ПВО. Воздушно-космическая сфера, № 1 (2015), 59-64.

Морозов, С. В., Кудренко, О. А., Долин, Р. С. Основные направления развития автоматизированных систем управления военного округа. Военная мысль № 4 (2018), 29-34.

Мосиенко, Юрий Иванович. «Маневр» – Первая советская АСУВ поля боя. «Арсенал» № 3 2011 г.

Муравник В.Б., Захаренков А.И., Добродеев А.Ю. Некоторые предложения по подходу и порядку реализации политики и стратегии импортозамещения в интересах национальной безопасности и укрепления обороноспособности Российской Федерации. Вопросы кибербезопасности №1(14) 2016, 2-8.

Мухин, Владимир. Россия и НАТО вышли на дистанцию танковой атаки. Независимая газета, № 65 (6679) 2016.

Мясников, Виктор. Путин нацеливает армию на интернет. Независимое военное обозрение, № 22 (2010).

Мясников Виктор. Единая космическая система предупредит о ядерном нападении. Независимое военное обозрение, № 37 (826) 2014 [Online]. Available: http://nvo.ng.ru/nvo/2014-10-17/1_shojgu.html [Accessed: 18th April 2019].

Назаренко, В. А. Нарушение управления войсками — важная боевая задача. Военная мысль № 7 1983, 46-51.

Независимая газета. Российские системы связи остаются уязвимыми. Независимая газета, № 163 (5927) 2013.

Независимое военное обозрение. Война в киберпространстве: уроки и выводы для России. Круглый стол в редакции "Независимого военного обозрения". Независимое военное обозрение. № 46 (787) 2013 [Online]. Available: http://nvo.ng.ru/concepts/2013-12-13/1_war.html [Accessed: 4th April 2019].

Независимое военное обозрение. В бой идет новый род войск. Кибероперации приравняли к нанесению ядерного удара. Независимое военное обозрение, № 7 (938) 2017.

Независимое военное обозрение. Тыл становится передним краем Минобороны. В структуре несекретной части расходов социальная часть потеснила военную. Независимое военное обозрение, № 16 (947) 2017.

Нечитайло, Дмитрий. "Асимметричная война" исламистов. Независимое военное обозрение № 28 14.8.2006.

Ниесов, В. А. Состояние программного обеспечения автоматизированных систем управления вооруженными силами США. Военная мысль № 6 1988, 64-72.

Никитин, О. Г. Направления повышения эффективности организации боевого применения войск радиоэлектронной борьбы в операциях объединений Сухопутных войск. Военная мысль, № 5 (2017), 23-29.

Никитенко Е.Г., Сергеев Н.А. «Мягкая сила» в контексте национальной безопасности России. Информационные войны, № 3(27) 2013, 36-52.

Николаёв, Ю.А. Пчеляной, В.П., Цымбал, В.И. Реформирование Вооруженных Сил и система вооружения. Военная мысль 1998 № 2, 27-32.

Новиков, В. К. Информационное оружие – оружие современных и будущих войн. М.: Горячая линия-Телеком, 2013.

Новиков, Владимир, Голубчиков, Сергей. Олимпиада по безопасности. ВПК, № 14 (678) 12–18 апреля 2017 года.

Ноговицын, Анатолий. (2009a) Некоторые аспекты обеспечения информационной безопасности Российской Федерации. Военная мусль, № 3 2009, 24-26.

Ноговицын, Анатолий. (2009b) Некоторые аспекты обеспечения информационной безопасности российской федерации. Российское военное обозрение № 3 (62) март 2009.

Ознобищев, С. К., Потапов, В. Я., Скоков, В. В. Как готовился «асимметричный ответ» на «стратегическую оборонную инициативу» Р. Рейгана. Велихов, Кокошин и другие. М.: Институт стратегических оценок, изд. ЛЕНАНД, 2008.

Орлянский, В. И., Дульнев, П. А., Костенко, А. Н. Универсальная автоматизированная система управления войсками - принципиальное условие успешного ведения сетецентрических войн. Военная мысль, № 12 (2012), 12-20.

Павлов, Вячеслав. «СКАЙНЕТ», которого нет. Создание автоматизированной системы управления Вооруженных сил РФ – залог победы в современной войне. ВПК, № 39 (605) 14 –20 октября 2015 года.

Палий, А. И. Борьба с системами боевого управления в операциях вооруженных сил НАТО. Военная мысль № 4 1991.

Панарин, И.Н., Панарина, Л.Г. Информационная война и мир. Москва: ОЛМА-ПРЕСС, 2003.

Панарин, И.Н. Информационная война и Третий Рим. М.: 2003.

Панарин И.Н. Информационная война и дипломатия. М.:ОАО «Издательский дом «Городец», 2004.

Панарин, И.Н. Информационная война и геополитика. М.: Поколение, 2006.

Панарин, И.Н. (2008a) Инструмент внешней политики. ВПК, № 32 (248) за 13 августа 2008 года.

Панарин, И.Н. (2008b) Система информационного противоборства. ВПК, № 41 (257) за 15 октября 2008 года.

Панарин, И.Н. Первая мировая информационная война: развал СССР. СПБ: Питер, 2010.

Панарин, И.Н. СМИ, пропаганда и информационные войны. М.: Поколение, 2012.

Панков, А. В., Шевченко, С. В. Обоснование роли и формирование концептуальной модели системы интеллектуальной обработки информации в едином информационном пространстве ВС РФ. Известия СПбГЭТУ «ЛЭТИ» № 1/2018, 38-43.

Парошин, А. А. Информационная безопасность: стандартизированные термины и понятия. Владивосток: Дальневосточный федеральный университет (ДФУ), 2010.

Паршин, С. А., Гобачев, Ю. Е., Кожанов, Ю. А. Кибервойны – реалная угроза национальной безопасности? М.: КРАСАНД, 2011.

Патрушев, Николай. На сильных не нападают Крайне желательно понимать, как, а главное – зачем эволюционирует парк отечественных средств вооруженной борьбы во всей обозримой перспективе. ВПК, № 12 (480) за 27 марта 2013 года.

Пельц, Александр. Единое информационное поле для силовых структур. Красная звезда № 282 1996.

Первов, А.В. Сетецентрическая война в воздушно-космическом пространстве: миф или реальность. Вестник Академии военных наук, № 2 (31) 2010, 80-83.

Перов, Е. А., Переверзев, А. В. Проблемы цифровизации военных сетей связи и пути их решения. Военная мысль, № 9 (2006), 76-80.

Перов, Е. А., Переверзев, А. В. О перспективной цифровой системе связи Вооруженных Сил Российской Федерации. Военная мысль, № 3 (2008), 7-11.

Перфильев, Ю. Ю. Российское интернет-пространство: развитие и структура. М.: Гардарики, 2003.

Петров, Алексей, Ианин, Алексей, Карпачев, Сергей. Спасение – в цифре! Цифровизация – основной фронт мировой конкуренции. ВПК, № 31 (695) за 16 августа 2017 года.

Петрунин, А. Н. Информационное обеспечение как способ реализации государственной информационной политики в области обороны. Военная мысль, № 8 (2008), 36-44.

Печуров, С.Л. Революция в военном деле взгляд с Запада. Военная мысль № 4 (7-8) 1997, 73-80.

Печуров, С.Л. Англо-саксонская модель военной реформы: история и современность. М.: Издательство Московского университета, 2015.

Пилюгин П.Л. Проблемы определения границ в информационном пространстве. T-Comm: Телекоммуникации и транспорт. 2017. Том 11. №8, 37-44.

Пилюгин П.Л., Стрельцов А.А. Проблемы Делимитации и Демаркации Цифровой Границы. XXIII научно-практическая конференция «Комплексная защита информации», 22-24 мая 2018 [Online]. Available: https://kzi.su/files/files/materials2018/13_Pilugin.pdf [Accessed: 28th February 2019].

Пирумов В.С., Родионов М.А. Некоторые аспекты информационной борьбы в военных конфликтах. Военная мысль, 1997 № 5, 44–47.

Пирумов В. С., Родионов М. А. Некоторые аспекты информационной борьбы в военных конфликтах. Военная мысль, № 5 1997, 44-47.

Пителинский, К.В. Интернет: Единое информационное пространство, экономический инструмент, виртуальная реальность и учебный процесс. Межотраслевая информационная служба. 2006. № 3, 63-71.

Погожин, В. П. Система управления стратегическими силами и стабильность. Военная мысль № 8-9, 1992.

Поздняков, А. И. Информационная безопасность личности, общества, государства. Военная мысль № 10 1993, 13-18.

Поликарпов В.С., Поликарпова, Е.В. Новейшие информационно-коммуникационные технологии и информационный суверенитет России. Информационное противодействие угрозам терроризма, № 23 (2014), 279-284.

Поликарпов В.С., Поликарпова, Е.В. Проблема информационного суверенитета России. Информационное противодействие угрозам терроризма, № 23 (2014), 285-290.

Поликарпов В.С., Поликарпова, Е.В., Поликарпова В.А. Информационный суверенитет России, сенсорная революция, социальные сети, интернет и кибервойна. Информационное противодействие угрозам терроризма, № 23 (2014), 272-278.

Помбрик, И. Д. Обеспечение непрерывности управления войсками в современных операциях. Военная мысль № 3 1976, 50-57.

Попов, Игорь. Сете-центрическая война Пентагона. Независимое Военное Обозрение, № 9 (2004).

Попов, Игорь. Сетецентрическая война. Красная звезда, № 169 (2012).

Попов, Игорь. Военные конфликты: взгляд за горизонт: Технологическая революция в "традиционной" войне. Независимое военное обозрение, № 13 (754) 2013.

Попов И.М., Хамзатов М.М. Война будущего: концептуальные основы и практические выводы. Очерки стратегической мысли. – М.: Кучково поле, 2016.

Португальский, Р. М. О борьбе в сфере управления войсками. Военная мысль № 3 1991.

Постников, Александр. Время "автоматизированных" войн. Независимое военное обозрение, № 1 (2010).

Пощипов, И. Н. Американская концепция «управление, связь и разведка». Военная мысль № 7 1986, 63-72.

ПРАЙМ. Доходы РФ от экспорта нефти в 2018 году выросли на 38%, от газа - на 28,8%. ПРАЙМ, 06 Февраля 2019 [Online]. Available: https://1prime.ru/energy/20190206/829687892.html [Accessed: 12th April 2019].

Rambler News Service. Итоги года: рунет 2016 [Online]. Available: https://rns.online/articles/Itogi-goda-runet-2017-01-02/ [Accessed: 14th May 2019].

Рамм, Алексей. На острие экономики и автоматизации Уникальному научно-исследовательскому институту экономики, информатики и систем управления исполняется 45 лет. ВПК, № 19 (537) за 28 мая 2014 года.

Рамм, Алексей, Козаченко, Алексей, Степовой, Богдан. Военный, красивый, суверенный: армия РФ создает закрытый интернет. Вся важная информация будет храниться только на серверах Минобороны. Известия, 12 марта 2019 [Online]. Available: https://iz.ru/854961/aleksei-ramm-aleksei-kozachenko-bogdan-stepovoi/voennyi-krasivyi-suverennyi-armiia-rf-sozdaet-zakrytyi-internet [Accessed: 18th April 2019]

Рамм, Алексей, Козаченко, Алексей. Командир на автопилоте: управлять армиями поможет компьютер. В Санкт-Петербурге открывается «Штаб звездных войн». Известия, 5 июня 2019 [Online]. Available: https://iz.ru/884970/aleksei-ramm-aleksei-kozachenko/komandir-na-avtopilote-upravliat-armiiami-pomozhet-kompiuter [Accessed: 9th July 2019].

Рамм, Алексей, Козаченко, Алексей, Степовой, Богдан Код в сапогах: военные разработали боевой антивирус. Известия, 31 октября 2019 [Online]. Available: https://iz.ru/937787/aleksei-ramm-aleksei-kozachenko-bogdan-stepovoi/kod-v-sapogakh-voennye-razrabotali-boevoi-antivirus [Accessed: 7th January 2020].

Прокофьев В.Ф. Тайное оружие информационной войны: атака на подсознание. М: СИНТЕГ, 2003.

Протасов, А. А. Институт автоматизации и совершенствования управления войсками (силами): история и современность. Военная мысль, № 7 2014, 3-8.

Прудников, Д. П. Государственная информационная политика в области обороны: исходное определение. Военная мысль, № 3 (2008), 43-48.

Пядышева, Е.Б. (ред.) Приложение к журналу «Международная жизнь»: XI Международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». Гармиш-Партенкирхен, Германия 24–27 апреля 2017 года. Москва: «Международная жизнь», 2017.

Пядышева, Е.Б. (ред.) Приложение к журналу «Международная жизнь»: XII Международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности». Гармиш-Партенкирхен, Германия 16–19 апреля 2018 года. Москва: «Международная жизнь», 2018.

Раскин, А.В. Некоторые подходы по созданию единого информационно-управляющего пространства разнородных группировок войск (СИЛ). Информационные войны № 4(40) 2016, 2-5.

Раскин, А. В., Пеляк, В. С. К вопросу о сетевой войне. Военная мысль, № 3 (2005), 21-27.

Раскин, А. В., Пеляк, В. С. Сетецентрическая война - война информационной цивилизации. Военная мысль, № 4 (2008), 78-80.

Раскин, А. В., Пеляк, В. С., Вялов, С. А. Концепция сетецентрической войны: за и против. Военная мысль, № 7 (2012), 14-21.

Растопшин, Михаил. Как управлять войсками и оружием? ВПК, № 22 (39) за 16 июня 2004 года.

Растопшин, Михаил. В лабиринте асимметричных ответов. Независимое Военное Обозрение, № 17 1.6.2007.

Расторгуев, С.П. Информационная война как целенаправленное информационное воздействие информационных систем. Информационное общество, № 1 (1997), 64-66.

Расторгуев С.П. Информационная война. 2-е изд. Moscow: Радио и связь, 1999.

Расторгуев, Сергей Павлович. Введение в формальную теорию информационной войны. Москва: Вузовская книга, 2002.

Расторгуев С. П. Математические модели в информационном противоборстве. — М.: ЦСОиП, 2014.

Рипенко, Ю. Б., Волков, А. Б. О терминологии в теории управления войсками (силами) и уставных документах. Военная мысль, № 8 (2014), 10-18.

Рогова, Сергей, Есин, Виктор, Золотарева, Павел. Эксперты предлагают комплекс мер доверия по стратегическим вооружениям. Независимое военное обозрение, № 24 (384) за 02 июля 2004 года.

Роговский, Евгений. Новое кибероружие. Станут ли электронные деньги средством поражения. Независимое военное обозрение, № 8 (796) 2014.

Rodionov, I. N. On Certain Provisions of Soviet Military Doctrine. Military Thought 1991, No. 3.

Родионов, М.А. К вопросу о формах ведения информационной борьбы. Военная мысль № 2 1998, 67-70.

Ромашкина Н.П. Международная деятельность по обеспечению информационной безопасности в xxi веке. Информационные войны, 2(34) 2015, 75-88.

Росич, Ю. Ю География развития интернета в России. Dissertation. Московский государственный университет им. М. В. Ломоносова Географический факультет. Москва, 2005.

Россошанский, А. В. Информационный суверенитет и свобода слова в контексте политической модернизации в современной России. Серия «Политология. Религиоведение» 2012. № 1 (8), 19–26.

Рукшин, А.С. Геополитика и безопасность. Ядерное сдерживание: совершенствование системы управления ядерными силами. Военная мысль № 6 2000.

Рыбаченков, Владимир. Стабильность под прицелом. ВПК, № 38 (702) за 4 октября 2017 года.

Рябов, Кирилл. Мультисервисная транспортная сеть связи для министерства обороны. Военное обозрение, 13 марта 2019 [Online]. Available: https://topwar.ru/155340-multiservisnaja-transportnaja-set-svjazi-dlja-ministerstva-oborony.html [Accessed: 18th April 2019].

Рябухина, П. П., Бондуровского, В. В., Перекопского, Г. И. (Под ред.) Законодательство государств - членов ОДКБ в сфере обеспечения информационной безопасности: опыт, проблемы и перспективы гармонизации. Материалы международной научно-практической конференции. СПб.: Секретариат МПА СНГ.

Савин Л. В. Украина в сетевой войне. Информационные войны, № 3(7) 2008, 42-51.

Савин, Л. В. Сетецентричная и сетевая война. Введение в концепцию. Москва: Евразииское движение, 2011.

Савченко, В.Ф. Теория военного управления история и современность. Военная мысль № 11 2007, 50-58.

Садовничий В. А., Стрельцов А. А. Обеспечение информационной безопасности России: Теоретические и методологические основы. — Моск. центра непрерывного математического образования. М.: 2002.

Сайфетдинов, Х. И. Информационное противоборство в военной сфере. Военная мысль, № 7, 2014, 38-41.

Салманов, Г, И. Советская военная доктрина и некоторые взгляды на характер войны в защиту социализма. Военная мысль № 12 1988, 3-13.

Самохин, В. Ф., Лукьянчик, В. Н., Артюшенко, А. Н. Перспективы создания военного (боевого) интернета в рамках нового облика ВС РФ. Военная мысль, № 8 (2011), 57-64.

Самсонов, Виктор. Точка зрения. Нужна новая система коллективной безопасности, или Что сегодня может угрожать национальным интересам государств СНГ. Красная звезда 1995, № 279.

Сапожинский, В.А. Взгляды на характер операций (боевых действий) в войнах будущего. Вестник Академии военных наук, №2(3) 2003, 53-57.

Сативалдыев Р. Ш. Противодействие информационной войне как предметное содержание информационной функции государства. Правовая жизнь, Январь – март 2017, № 1 (17) [Online]. Available: http://www.tnu.tj/Hayoti%20huquqi/PZh_1_2017.pdf [Accessed: 16th March 2019].

Связь. Связь в Вооруженных Силах Российской Федерации 2013. Москва: Информационный мост 2013.

Связь. Связь в Вооруженных Силах Российской Федерации 2015. Москва: Информационный мост 2015.

Связь. Связь в Вооруженных Силах Российской Федерации 2017. Москва: Информационный мост, 2017.

Связь. Связь в Вооруженных Силах Российской Федерации 2018. Москва: Информационный мост, 2018.

Селиванов, В. В., Ильин, Ю. Д. Методические основы формирования асимметричных ответов в военно-техническом противоборстве с высокотехнологичным противником. Военная Мысль, № 9 2019, 33-41.

Сенюков, А. В. О некоторых аспектах применения кибернетики в управлении войсками. Военная мысль № 4 1979, 76-80.

Сергеев, И. Д. Основы военно-технической политики России в начале XXI Века. На Боевом Посту № 99 1998.

Сергеев, Н.А. Архитектура перспективной сетецентрической информационно-управляющей системы обеспечения национальной безопасности России в новых геополитических условиях. Информационные войны, № 2(14) 2010, 69-84.

Серебрянников, В. В. Диалектика политических и военных средств в защите социализма. Военная мысль 1988, № 10, 3-11.

Серебрянников, В. В. О понятии “война”. Военная мысль, № 10 2004, 61-65.

Серебрянников, В. В. Предотвращение войн: теория и практика. Военная мысль, № 12 2008, 2-13.

Сержантова, А.В. Современное понимание сущности и содержания войны. Вестник Академии военных наук, 2(43) 2013, 20-23.

Сивков, Константин. Хуже иприта Информационные средства ведения борьбы уже можно приравнивать к оружию массового поражения. ВПК, № 31 (499) за 14 августа 2013 года.

Сивков, Константин. Глобальный контрудар Способы нейтрализации национальной ПРО США могут быть асимметричными и весьма неординарными. ВПК, № 21 (587) за 10 июня 2015 года.

Сивков, Константин. Асимметричный «Сармат» Ракеты средней дальности – оружие малой ценности. ВПК, № 45 (709) за 22 ноября 2017 года.

Сивков, Константин. Захват будущего в теории и на практике. на форуме "АРМИЯ-2018" обсуждены проблемы психологической обороны. ВПК, № 35 за 11 сентябрь 2018.

Сивков, Константин. Противник в новом формате: Как победить без единого выстрела. № 45 (758) за 20 ноября 2018 года.

Сивков, Константин. Четвертое измерение войны. Каким должен быть Генеральный штаб информационной безопасности. ВПК, № 39 (752) за 9 октября 2018 года.

Сиволоб, Владимир Федорович, Сосновский, Михаил Евгеньевич. Реальность сдерживания. Независимое военное обозрение № 41 1999.

Сидак, А.А. Вопросы структуризации автоматизированных систем при организации защиты информации. Информационные войны №1 (45) 2018, 88-90.

Сидак, А.А. Применение метода анализа иерархии при определении критических процессов для категорирования объектов критической информационной инфраструктуры Российской Федерации. Информационные войны №2 (46) 2018, 79-82.

Симушков, А.М. Единое информационное пространство в транспортной логистикею Железнодорожный транспорт. 2009. № 10, 46-47.

Сиротинин, Евгений, Криницкий, Юрий. Партизанско-террористические войны в эпоху ядерного сдерживания. Независимое Военное Обозрение, № 20 4.6.2010.

Скиба, В. А. Синтез информационно-коммуникационного пространства эргатических систем военного назначения. Военная мысль, № 11 (2018), 39-48.

Скоков, С. И., Грушка, Л. В. Влияние концепции сетецентризма на эволюцию и функционирование системы управления Вооруженными Силами Российской Федерации. Военная мысль, № 12 (2014), 33-41.

Скокова, С.И. Сетецентрическая система управления ВС РФ и необходимые меры по ускорению развития АСУ войсками (силами). Вестник академии военных наук, № 1 (46) 2014, 52-54.

Слепцов, Михаил. DWDM-системы связи для Вооружённых сил РФ. Связь в Вооруженных Силах Российской Федерации 2017. Москва: Информационный мост 2017.

Слипченко, Владимир. Война будущего (прогностический анализ). 1999 [Online]. Available: https://www.e-reading.club/bookreader.php/112810/Slipchenko_-_Voiina_budushchego_%28prognostich-eskiii_analiz%29.html [Accessed: 14th November 2018].

Слипченко, В. И. Войны шестого поколения: оружие и военное искусство будущего. М.: ИД Вече, 2002.

Смолян, Г., Цыгичко, В., Черешкин, Д. Оружие, которое может быть опаснее ядерного. Независимая газета от 18.11.95 г. no. 3 (18 November 1995), 1–2.

Смолян, Георгий Львович, Цыгичко, Виталий Николаевич and Черешкин. Дмитрий Семенович. Куда ведет информационная супермагистраль. Независимая газета 1996, No. 33.

Соловьев, С. Л., Терехов, И. П. К вопросу о совершенствовании управления войсками. Военная мысль № 11 1980, 48-51.

Соловьев, А.В. Информационная война: теоретико-методологические и практические аспекты. Информационные войны, № 2(18) 2011, 15-22.

Соловьев, И. В., Злобин, С. М. Политика межведомственного взаимодействия - важнейшее направление решения задач обороны государства. Военная мысль № 7 (2018), 15-20.

Средин, Г. В. Проблема войны и мира в современной идеологической борьбе. Военная мысль № 7 1986, 3-13.

Стародубцев, Ю. И., Бухарин, В. В., Семенов, С. С. Техносферная война. Военная мысль, № 7 (2012), 22-31.

Старых, Геннадий. ЕСУ ТЗ: время делать следующий шаг. Независимое военное обозрение, 24 февраль 2012.

Степанова, Е. А. Асимметричный конфликт как силовая, статусная, идеологическая и структурная асимметрия. Военная Мысль, № 5 2010, 47-54.

Стишковский, В. М. Задачи и возможности военной связи. Военная мысль № 3 1977, 40-50.

Стрельцов, Анатолий Александрович. ПИР-Центр [Online]. Available: http://pircenter.org/experts/918-streltsov-anatoly-a [Accessed: 28th March 2019].

Стрельцов, А.А. Обеспечение информационной безопасности России. Теоретичнские и методологические основы. М.: МЦНМО, 2002.

Стрельцов А.А. (и др.) Организационно-правовое обеспечение информационной безопасности. М.: Академия, 2008.

Стрельцов А.А. Государственная информационная политика: основы теории. М.: МЦНМО. – 2009.

Стрельцов, А. А. Основные задачи государственной политики в области информационного противоборства. Военная мусль, № 5 2011, 18-25.

Стрельцов, Анатолий. Основные направления развития международного права вооруженных конфликтов применительно к киберпространству. VIII международный форум по международной информационной безопасности. 21-24 апреля 2014 года. Гармиш-Партенкирхен, Германия, место издания Издательство Московского университета. Москва: 2014, 52-70.

Стрельцов, А.А. Адаптация международного права безопасности к информационному пространству. Девятый международный форум «Партнерство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности» и Одиннадцатая научная конференция МИ-КИБ 20–23 апреля 2015 года. Гармиш-Партенкирхен, Германия. М.: 2015, 81-86.

Стрельцов, А.А. Применение международного гуманитарного права к вооруженным конфликтам в киберпространстве. Российский ежегодник международного права 2015. Санкт-Петербур: "Россия-Нева", 2015, 152-169.

Стрельцов, Анатолий. Применение международного гуманитарного права к вооруженным конфликтам в киберпространстве. 25.04.2016 [Online]. Available: https://digital.report/konflikt-v-kiberprostranstve/# [Accessed: 28th February 2019].

Стрельцов, Анатолий. Суверенитет и юрисдикция государства в среде информационно-коммуникационных технологий в контексте международной безопасности. Журнал Международная жизнь, № 2. 2017.

Стрельцов А.А., Пилюгин П.Л. К вопросу о цифровом суверенитете. Информатизация и связь, № 2 2016, 25-30.

Сурма, И.В. Единое информационное пространство СНГ: 20 лет спустя. Вопросы безопасности, № 5 (2015), 41-58.

Суровцева, Елена. Запад переходит в информационное наступление. Красная звезда № 109 1997.

Сухотеплый, А. П., Жилков, Е. А. Цифровая экономика. Цель номер один — технологический и цифровой суверенитет. Связь в Вооруженных Силах Российской Федерации 2018. Москва: Информационный мост 2018, 112-114.

Сычёв, С.А. Применение иррегулярных формирований в решении боевых задач. Вестник Академии военных наук, № 4 (29) 2009, 46-48.

Татаринов, В.В. Элементы сетецентрической защиты. Вестник Академии военных наук, № 1 (42) 2013, 91-94.

Тезиков, Андрей, Моренков, Владислав. АСУ ОС ПВО СНГ: сегодня и завтра. Журнал «Воздушно-космическая оборона» 17 августа, 2014 [Online]. Available: http://www.vko.ru/oruzhie/asu-os-pvo-sng-segodnya-i-zavtra [Accessed: 27th June 2016].

Тер-Арутюнянц, Г. Многополярная и асимметричная холодная война. Вестник Академии военных наук, №4(41) 2007.

Терентьева, Л.В. Концепция суверенитета государства в условиях глобализационных и информационно-коммуникационных процессов. Право. Журнал Высшей школы экономики. 2017. № 1, 187–200.

Тимошенко, Михаил. «Маневр» и маневры. Арсенал. Военно-промышленное обозрение» №6, 2010 г.

Тихонов, М.Н., Богословский, М.М. Кибернетические войны и информационная безопасность. Атомная стратегия, № 104 (2015), 15-20.

Тихонов, Александр. К единому информационному пространству. Красная звезда № 173 (2015).

Ткаченко, П. Кибернетика в управлении войсками. Военная мысль № 1 1962, 35-48.

Ткаченко, В. И., Фадеев, Ю. А. О соотношении централизованного и децентрализованного управления в Войсках ПВО страны. Военная мысль № 11 1978, 32-40.

Толмачев, А.П., Баранюк, В.В., Тютюнников, Н.Н. Информационное обеспечение управления Вооруженными силами Российской Федерации. Вестник академии военных наук, № 3 (36) 2011, 102-105.

Турко, Н. И., Гареев, М.А. Война: современное толкование теории и реалии практики. Вестник Академии военных наук, 1(58) 2017, 4-10.

Тучков Ю.Н. и др. Словарь терминов и определений в области информационной безопасности. 1-е изд Москва: ВАГШ ВС РФ, НИЦ информационной безопасности, 2008.

Тюшкевич, С. А. Разумная достаточность для обороны: параметры и критерии. Военная мысль № 5 1989, 53-61.

Устинов В. Н. Информационная мощь в стратегии национальной безопасности и проблемы информатизации российского общества. РИСИ. М., 1996.

Фаличев, Олег. Недалеко и до новой "Берлинской стены". ВПК, № 18 (184) за 16 мая 2007 года.

Фаличев, Олег. Интервью начальника академии Генштаба А. Третьяка. ВПК, 10 декабря 2012 [Online]. Available: https://vpk-news.ru/articles/13536 [Accessed: 18th March 2019].

Фаличев, Олег. Асимметричная война. Борьба с социальным неравенством – главное направление обеспечения безопасности страны. ВПК, № 9 (575) за 11 марта 2015 года.

Фаличев, Олег. Закодированы на отставаниею Проблемы отечественной микроэлектроники приходится решать с помощью «Шилки»ю ВПК, № 41 (754) за 23 октября 2018 года.

Федорова, А.В., Цигичко, В.Н. (общ. ред.) Информационные вызовы национальной и международной безопасности. М.: ПИР-Центр, 2001.

Федосов, Евгений Александрович, Спасский, Игорь Дмитриевич. Высокоточное оружие заняло место бога войны. Независимое военное обозрение № 28 1999.

Фефелов, Б.В. Информационное обеспечение системы управления войсками. Военная мысль № 1 1993, 36-39.

Фролов, Николай. Главный ТВД будущего. ВПК, № 48 (214) за 12 декабря 2007 года.

Хамзатов, М. М. Влияние концепции сетецентрической войны на характер современных операций. Военная мысль, № 7 (2006), 13-17.

Харченко, Е. Б. Проблемы безопасности инфокоммуникационных систем Вооруженных Сил Российской Федерации. Военная мысль, № 11 (2014), 14-19.

Харченко, Е. Б., Иванов, В. Г., Лукьянчик, В. Н. Научно-теоретические положения по построению технической основы системы управления Вооруженными Силами Российской Федерации. Военная мысль, № 8 (2018), 46-53.

Харченко, Е.Б., Сазыкин, А.М., Лысенков, Ю.Н. Вопросы кибербезопасности инфокоммуникационных систем специального назначения. Известия Российской Академии Ракетных и Артиллерийских Наук 97 (2017), 38-47.

Хатунцева Е.А., Хатунцев А.Б. Анализ основных тенденций развития сетей связи на телекоммуникационном рынке России. T-Comm: Телекоммуникации и транспорт, Том 10. №7. 2016, 71-74.

Хомутов, А. В. Опыт и перспективы использования концепции единой информационно-коммуникационной сети в управлении войсками. Военная мысль № 11 (2015), 17-22.

Храмчихин, Александр. Иллюзия ядерного сдерживания. ВПК, № 11/2010.

Хряпин, А. Л., Афанасьев, В. А. Слово юбилярам. Концептуальные основы стратегического сдерживания. Военная мысль, № 1 2005, 8-12.

Хряпин, А. Л., Калинкин, Д. А., Матвичук, В. В. Стратегическое сдерживание в условиях создания США глобальной системы ПРО и средств глобального удара. Военная мысль, № 1 2015, 18-22.

Цыганов, В.В., Бухарин, С.Н. Информационные войны в бизнесе и политике. М.: Академический Проект, 2007.

Цыганов, В.В., Бухарин, С.Н., Завьялов, О.Ю., Лукьянова, К.А. Национальная система информационного управления и противоборства. Информационные войны, № 2(10) 2009, 2-8.

Цыганов В.В., Бочкарева Ю.Г. Концепция системы общественной безопасности при информационных войнах. Информационные войны №3 (31) 2014, 62-70.

Цыганов, В.В., Бочкарева, Ю.Г. Эволюция социальных систем при информационной конфронтации и партийные механизмы обеспечения общественной безопасности. Информационные войны № 3(31) 2014, 12-22.

Цыганок, А.Д. Информационные войны в начале XXI века. Информационные войны, №4 (28) 2013, 17-29.

Цыганок, Анатолий. Меняется время - меняется и военная доктрина. ВПК, № 43 (209) за 7 ноября 2007 года.

Цыгичко, В., Черешкин, Д. Оружие, которое может быть опаснее ядерного. Независимая газета от 18.11.95 г.

Цыгичко В.И., Вотрин Д.С., Крутских А.В., Смолян Г.Л., Черешкин Д.С. Информационное оружие - новый вызов международной безопасности. Москва: Институт Системного Анализа Ран, 2000.

Цыгичко, Виталий. Оружие сродни ядерному. ВПК, № 42 (59) за 3 ноября 2004 года.

Цымбал, В.И. О концепции информационной войны. Информационный сборник Безопасность, № 9 (1995).

Чаднов, А. П. Роль военных сетевых технологий Вооруженных Сил Российской Федерации при создании и боевом применении высокотехнологичных систем вооружения, военной и специальной техники нового поколения. Военная мысль, № 7 (2018), 33-39, 34.

Чекинов, С. Г. Центр военно-стратегических исследований Генерального штаба Вооруженных Сил Российской Федерации история и современность. Военная мысль № 1, 2010, 3-5.

Чекинов, С.Г., Богданов, С.А. (2010a) Влияние асимметричных действий на современную военную безопасность России. Вестник Академии военных наук, № 1 (30) 2010, 46-53.

Чекинов, С. Г., Богданов, С. А. (2010b) Асимметричные действия по обеспечению военной безопасности России. Военная Мысль, № 3 2010, 13-22.

Чекинов, С. Г., Богданов, С. А. Влияние непрямых действий на характер современной войны. Военная мысль, № 1 2011, 3-13.

Чекинов, С. Г., Богданов, С. А. (2012a) Стратегическое сдерживание и национальная безопасность России на современном этапе. Военная мысль, № 3 2012, 11-20.

Чекинов, С. Г., Богданов, С. А. (2012b) Начальные периоды войн и их влияние на подготовку страны к войне будущего. Военная Мысль, № 12 2012, 14-27.

Чекинов, С. Г., Богданов, С. А. (2015a) Военное искусство на начальном этапе XXI столетия: проблемы и суждения. Военная мысль, № 1 2015, 32-43

Чекинов, С. Г., Богданов, С. А. (2015b) Прогнозирование характера и содержания войн будущего: проблемы и суждения. Военная мысль, № 10 2015, 41-49.

Чекинов, С. Г., Богданов, С. А. Военная стратегия: взгляд в будущее. Военная Мысль, № 11 2016, 3-15.

Чекинов, С. Г., Богданов, С. А. Эволюция сущности и содержания понятия “война” в XXI столетии. Военная мысль, № 1 2017, 30-43.

Чельцов, Б. Ф. Уточнение подходов к созданию системы воздушно-космической обороны государства в условиях сетецентричных войн будущего. Военная мысль, № 9 (2008), 2-10.

Чельцов, Б. Ф. Проблемы создания сетецентрической системы управления войсками, силами и средствами ВКО. Вестник Академии военных наук, № 4 (37) 2011, 56-63.

Чельцов, Борис. Вспомнив тернистый путь, подумаем о будущем. ВПК, № 13 (329) за 7 апреля 2010 года.

Червов, Н. Ф. Разоружение: кто против? Военная мысль № 12 1983, 3-15.

Черешкин, Д.С., Смолян, Г.Л., Цыгичко, В.Н. Реалии информационной войны. Конфидент. 1996. № 4.

Черкашин, Петр. Сетецентрические веяния. Замыслы советского генштаба реализуются под новым названием в пентагоне. № 45 (758) за 20 ноября 2018 года

Черная, Н.Д. Сети связи. Конспект лекций для студентов заочного отделения Специальности 210406 и 210406у “Сети связи и системы коммутации”. Самара, 2008.

Шабанов, А.П. Технология информационной поддержки аналитических структур ситуационных центров государственных организаций. Информационные войны № 1(41) 2017, 33-38.

Шаклеина, Т.А. (Сост.) Внешняя политика и безопасность современной России. 1991-2002: Хрестоматия в 4-х т. Т.IV: Документы. М.: Моск.гос.ин-т междунар.отношений (ун-т) МИД России, Российская ассоциация международных исследований, АНО "ИНО-Центр" (Информация. Наука. Образование), 2002.

Шаравин, А. А. Стратегическая стабильность в Европе системный аспект. Военная мысль № 2 1992.

Шаламберидзе Е.Г. (2011a) Непрямое противоборство в сфере военной безопасности в условиях мирного времени. Вестник Академии военных наук, № 1 (34) 2011, 20-30.

Шаламберидзе Е.Г. (2011b) Теоретические вопросы развития политики национальной обороны России в условиях мирного времени с использованием системы мер невоенного и военного характера. Вестник Академии военных наук, № 4 (37) 2011, 35-43.

Шаламберидзе Е.Г. (2012a) Национальная оборона Российской Федерации: стратегические задачи и возможные перспективы. Вестник Академии военных наук, № 4 (41) 2012, 30-37.

Шаламберидзе Е.Г. (2012b) Национальная оборона и информационная борьба государства в современных условиях мирного времени. Информационные войны, № 3(23) 2012, 11-19.

Шептура, Владимир. Единое информационное пространство ВС РФ. Защита и безопасность, № 2 (2016), 32-34.

Шеремет, Игорь. Компьютеризация как путь к победе в вооруженной борьбе. Концепция "сетецентричной войны" и особенности ее практической реализации. Независимое военное обозрение» №43 (2005).

Шеремет, Игорь. (2014a) Киберугрозы России растут — часть I. Ситуация в этой области изменяется в лучшую сторону гораздо медленнее, чем того требует развитие геополитической обстановки. ВПК, № 5 (523) за 12 февраля 2014 года.

Шеремет, Игорь. (2014b) Киберугрозы России растут — часть II. Ситуация в этой области изменяется в лучшую сторону гораздо медленнее, чем того требует развитие геополитической обстановки. № 6 (524) за 19 февраля 2014 года.

Шеремет, И.А. Обеспечение кибербезопасности в условиях развития цифровой экономики. Вестник Московского университета. Серия 25. Международные отношения и мировая политика. Т. 11. № 1 (2019), 3-19.

Шерстюк, В.П. Актуальные проблемы обеспечения информационной безопасности Российской Федерации. Военная мысль, № 6 2003, 28-32.

Шерстюк, Владислав и др. Киберстабильность: подходы, перспективы, вызовы. Международная жизнь, № 4 (2018).

Шурупов, Г. Управление войсками—на уровень современных требований. Военная мысль № 5 1979, 33-44.

Элькин, Г. И., Казанский, А. Г. Перспективы развития системы связи Вооружённых Сил Российской Федерации. Итоги деятельности Совета главных конструкторов системы связи ВС РФ. Связь в Вооруженных Силах Российской Федерации 2018. Москва: Информационный мост 2018, 28-29.

Webpages & News

Agentura.ru. В спецслужбе создали новую структуру для противодействия компьютерным Преступлениям. 12.09.2018 [Online]. Available: http://www.agentura.ru/news/28975/ [Accessed: 18th April 2019].

АиФ. Николай Никифоров: «Мы будем и дальше отстаивать свой цифровой суверенитет». № 19 06/05/2018 [Online]. Available: http://www.aif.ru/gazeta/number/37671 [Accessed: 28th February 2019].

Академия Геополитических Проблем. [Online]. Available: https://akademiagp.ru/ [Accessed: 30th March 2019].

Академия информационной самозащиты [Online]. Available: http://www.iwars.su/ [Accessed: 25th March 2019].

АКИТ. Исследование рынка Интернет-торговли в России. Результаты 1 полугодия 2017 года, 28 сентября 2017 [Online]. Available: http://www.akit.ru/ исследование-рынка-интернет-торговл/ [Accessed: 12th April 2019].

Алехина, Маргарита. Хакер из «Шалтая-Болтая» заявил о сотрудничестве с ФСБ. РБК, 9 января 2019 [Online]. Available: https://www.rbc.ru/society/09/01/2019/5c35fab59a7947185fe6da57?from=main [Accessed: 9th May 2019].

Анатолий Иванович Китов [Online]. Available: http://www.kitov-anatoly.ru/home [Accessed: 23rd March 2019].

Анненков, Андрей. «Интернет+суверенитет» рабочей группы по Интернету рассмотрела проект дорожной карты. D-Russia.ru 29 сентября 2016 [Online]. Available: http://d-russia.ru/podgruppa-internetsuverenitet-rabochej-gruppy-po-internetu-rassmotrela-proekt-dorozhnoj-karty.html [Accessed: 28th February 2019].

Анненков, Андрей. Игорь Щёголев: «Учения подтвердили недостаточную устойчивость Рунета при недружественных «целенаправленных действиях». D-Russia.ru, 17.10.2014 [Online]. Available: http://d-russia.ru/ucheniya-podtverdili-nedostatochnuyu-ustojchivost-runeta-pri-nedruzhestvennyx-celenapravlennyx-dejstviyax.html [Accessed: 29th May 2019].

Анненков, Андрей. Игорь Щёголев: безопасность Интернета и безопасность граждан должны обеспечиваться суверенитетом государств в киберпространстве. D-Russia.ru, 12.5.2015 [Online]. Available: http://d-russia.ru/igor-shhyogolev-bezopasnost-interneta-i-bezopasnost-grazhdan-dolzhny-obespechivatsya-suverenitetom-gosudarstv-v-kiberprostranstve.html [Accessed: 16th May 2019].

АНО «Цифровая Экономика». Наблюдательный совет АНО «Цифровая экономика» назвал законопроекты, которые требуют приоритетного одобрения Госдумой, 04.12.2018 [Online]. Available: https://data-economy.ru/04122018 [Accessed: 6th May 2019].

Аношин, Иван, Петухова, Людмила. Биткоин от дилера: почему россияне не купят криптовалюту без посредника. РВК, 25 января 2018 [Online]. Available: https://www.rbc.ru/money/25/01/2018/5a699d3a9a79471460896e07?from=center_5 [Accessed: 12th April 2019].

АО «НПО «Эшелон» [Online]. Available: https://npo-echelon.ru/ [Accessed: 2nd April 2019].

Артемьев, Игорь. Экономику России назвали полуфеодальной. Lenta.ru, 25 сентября 2018 [Online]. Available: https://lenta.ru/news/2018/09/25/half_feodal/ [Accessed: 3rd May 2019].

Ассоциация Коммуникационных Агентств России. Объём рекламного рынка России в 2000-2018 гг. [Online]. Available: http://www.akarussia.ru/node/7849 [Accessed: 11th April 2019].

Ассоциация электронных коммуникаций (РАЭК) [Online]. Available: https://raec.ru/statute/ [Accessed: 9th May 2019].

Ашманов, Игорь. Информационный суверенитет – новая реальность. 24.04.2013. [Online]. Available: http://eurasian-defence.ru/sites/default/files/doc/ashmanov.pdf [Accessed: 28th February 2019].

Ашманов, Игорь. Цифровая оккупация беседа о кибербезопасности, национальных интересах и сути информационной войны. Завтра 9 января 2019 [Online]. Available: http://zavtra.ru/blogs/tcifrovaya_okkupatciya [Accessed: 28th February 2019].

Безель, Я. В. Этапы развития автоматизированных систем управления авиацией и ПВО. Вестник Концерна ПВО «Алмаз – Антей», №2, 2015 [Online]. Available: http://www.almaz-antey.ru/upload/iblock/e95/e95a21ddf357267fc0137dbd3cace605.pdf [Accessed: 11th December 2018].

Балашова, Анна, Баленко, Евгения. Операторов 5G переведут на российские серверы. РБК, 2.9.2019 [Online]. Available: https://www.rbc.ru/technology_and_media/02/10/2019/5d9363d59a7947b1a00cd012 [Accessed: 7th January 2020].

Балашова, Анна, Сидоркова, Инна, Коломыченко, Мария. Правительству предложат создать глобальную спутниковую сеть за ₽299 млрд. РБК, 22 ноября 2017 [Online]. Available: https://www.rbc.ru/technology_and_media/22/11/2017/5a159bdb9a79476a55456d2b?from=center_4 [Accessed: 15th April 2019].

Балашова. Анна. Мало места большим данным: почему Москву ждет дефицит мощностей. РВК, 06 ноября 2018 [Online]. Available: https://www.rbc.ru/technology_and_media/06/11/2018/5bdc45019a79472ab0ecdbc2?from=center_2 [Accessed: 14th April 2019].

Балашова, Анна, Канаев, Петр. «Ростелеком» стал оператором реестра доменов .ru и.рф. 23 января 2018 [Online]. Available: https://www.rbc.ru/technology_and_media/23/01/2018/5a675ab29a79473a982cd704?from=main [Accessed: 10th April 2019].

Балашова, Анна, Кирьянов, Роман. Акимов объявил о создании российско-китайского конкурента OneWeb. РБК, 17.9.2019 [Online]. Available: https://www.rbc.ru/technology_and_media/17/09/2019/5d80eea69a794755e1c48c87 [Accessed: 7th January 2020]

Балашова, Анна, Посыпкина, Александра. Властям предложили штрафовать соцсети и поисковики за запрещенный контент. РБК, 22 октября 2018 [Online]. Available: https://www.rbc.ru/technology_and_media/22/10/2018/5bcda8179a79471e45ad2d1e#ws [Accessed: 9th May 2019].

Балашова, Анна, Сидоркова, Инна. Роскомнадзор выступил против выдачи частот для глобальной сети OneWeb. РВК, 14 апреля 2018 [Online]. Available: https://www.rbc.ru/technology_and_media/14/04/2018/5ad0ac9d9a794746645fa041?from=main [Accessed: 15th April 2019].

Баленко, Евгения, Кузнецова, Евгения. Исполнение законопроекта о суверенном Рунете подорожало до ₽30 млрд. РБК, 26 мая 2019 [Online]. Available: https://www.rbc.ru/technology_and_media/26/03/2019/5c98f1bd9a79476ea86fc631?from=center [Accessed: 16th May 2019].

Баленко, Евгения, Посыпкина, Александра. Не дописали: почему интернет-компании не могут исполнять «закон Яровой» РБК, 13 июля 2018 [Online]. Available: https://www.rbc.ru/technology_and_media/31/07/2018/5b5f22609a7947e1f4470779?from=main [Accessed: 14th May 2019].

Баленко, Евгения, Галимова, Наталья, Посыпкина, Александра, Балашова, Анна.. Атака изнутри: операторы протестируют закон об устойчивости Рунета. РБК, 8 февраля 2019 [Online]. Available: https://www.rbc.ru/technology_and_media/08/02/2019/5c5c51069a7947bef4503927?from=center_16 [Accessed: 1st March 2019].

Безель, Я. В. Этапы развития автоматизированных систем управления авиацией и ПВО. Вестник Концерна ПВО «Алмаз – Антей», №2, 2015 [Online]. Available: http://www.almaz-antey.ru/upload/iblock/e95/e95a21ddf357267fc0137dbd3cace605.pdf [Accessed: 11th December 2018].

Белов, Сергей. Интернет по-русски. Российская газета, 10.11.2009 [Online]. Available: https://rg.ru/2009/11/10/rf.html [Accessed: 7th March 2019].

Благовещенский, Антон. В России установлен корневой DNS-сервер. Российская газета, 04.04.2012 [Online]. Available: https://rg.ru/2012/04/04/server-site-anons.html [Accessed: 10th April 2019].

Богданов, Константин. Всю систему менять надо. ВПК, № 16 (382) за 27 апреля 2011 года.

Богданов, Юрий. Институт развития интернета укрепит цифровой суверенитет страны. ВЗГЛЯД, 12 марта 2015 [Online]. Available: https://vz.ru/society/2015/3/12/734014.html [Accessed: 9th May 2019].

Бодрик, Александр. Кибербезопасность в России: итоги 2018 года и стратегии для 2019-го. IT-Week, 4.2.2019 [Online]. Available: https://www.itweek.ru/security/article/detail.php?ID=205189 [Accessed: 17th May 2019].

Борисов, Сергей. СОИБ. Безопасность критической информационной инфраструктуры (КСИИ), 13 Августа, 2013 [Online]. Available: https://www.securitylab.ru/blog/personal/sborisov/32175.php [Accessed: 14th March 2019].

Братерский, Александр. Путинский взгляд на советских вождей. Газета, 16.6.2017 [Online]. Available: https://www.gazeta.ru/politics/2017/06/17_a_10721567.shtml [Accessed: 11th January 2020].

БРИКС. VII саммит БРИКС Уфимская декларация (Уфа, Российская Федерация, 9 июля 2015 года) [Online]. Available: http://www.brics.utoronto.ca/docs/150709-ufa-declaration-ru.pdf [Accessed: 10th May 2019].

БРИКС. Сямэньская декларация руководителей стран БРИКС (Сямэнь, Китай, 4 сентября 2017 года) [Online]. Available: http://kremlin.ru/events/president/news/55515 [Accessed: 10th May 2019].

Бутрин, Дмитрий. «Конкуренция должна происходить внизу, в экосистеме». Коммерсантъ, №227 от 10.12.2019 [Online]. Available: https://www.kommersant.ru/doc/4187705 [Accessed: 6th January 2020].

Брызгалова, Екатерина. Роскомнадзор начал блокировать страницу «МБХ медиа» в «Яндекс.Дзене». Ведомости, 23 февраля 2018 [Online]. Available: https://www.vedomosti.ru/politics/articles/2018/02/22/751870-roskomnadzor-zablokiroval-mbh-yandeksdzene [Accessed: 14th May 2019].

Валагин, Антон. Россия испытала в Сирии высокоскоростной военный интернет. RG.RU, 7 апреля 2016 [Online]. Available: https://rg.ru/2016/04/07/rossiia-ispytala-v-sirii-vysoskorostnoj-voennyj-internet.html [Accessed: 3rd May 2019].

Васильев, Алексей. Подключение к ГосСОПКА. Техвопросы. 3 апреля 2018 [Online]. Available: https://infotecs.ru/webinars/archive/?show=11430 [Accessed: 18th April 2019].

Ведомости. Клименко предупредил россиян о возможном отключении от мирового интернета. Ведомости, 29 декабря 2016 [Online]. Available: https://www.vedomosti.ru/politics/news/2016/12/29/671725-klimenko [Accessed: 16th May 2019].

Ведомости. Кто вошел в новое правительство. Полный список. Десять вице-премьеров и двадцать один министр. Ведомости, 18 мая 2018 [Online]. Available: https://www.vedomosti.ru/economics/articles/2018/05/18/768949-pravitelstvo-polnii-spisok [Accessed: 8th May 219].

Ведомости. “Ростелеком” купил компанию в сфере кибербезопасности за 1,5 млрд рублей. Ведомости, 22 мая 2018 [Online]. Available: https://www.vedomosti.ru/business/news/2018/05/22/770293-rostelekom [Accessed: 18th April 2019].

Воейков, Денис. Почему Реестр российского ПО так и не смог запустить в стране импортозамещение. CNews, 24.04.2018 [Online]. Available: http://www.cnews.ru/news/top/2018-04-24_pochemu_reestr_rossijskogo_po_tak_i_ne_smog_zapustit [Accessed: 12th April 2019].

Владыкин, Олег. Путин: Российская армия должна быть оснащена лучше зарубежных. Независимая газета, 20 декабря 2014 [Online]. Available: http://www.ng.ru/armies/2014-12-20/100_collegium.html [Accessed: 6th March 2019].

Виртуальный компьютерный музей [Online]. Available: http://www.computer-museum.ru/ [Accessed: 23rd March 2019].

Военная академия Генерального штаба Вооруженных Сил Российской Федерации. Кафедра информационной безопасности [Online]. Available: http://vagsh.mil.ru/Struktura-akademii/Kafedra-informacionnoj-bezopasnosti [Accessed: 29th March 2019].

Воентелеком. Глава ”Воентелекома”: технология блокчейн может появиться в армии России. Воентелеком, 22.08.2017 [Online]. Available: https://voentelecom.ru/news/novosti-kompanii/glava-voentelekoma-tekhnologiya-blokcheyn-mozhet-poyavitsya-v-armii-rossii/ [Accessed: 18th April 2019].

ВУНЦ СВ «ОВА ВС РФ» [Online]. Available: http://ova.mil.ru/ [Accessed: 29th March 2019].

ВЦИОМ. А если без интернета?! [Online]. Available: https://wciom.ru/index.php?id=236&uid=116148 [Accessed: 12th April 2019].

Гаврилов, Юрий. Защитят по плану Оборону расписали на пять лет вперед. Российская газета - Федеральный выпуск № 260(6831), 17.11.2015 [Online]. Available: https://rg.ru/2015/11/17/oborona-site.html [Accessed: 12th February 2019].

Гаврилов, Юрий. Глава Генштаба объяснил, как будет работать Центр управления обороной. Российская газета, 1.11.2014 [Online]. Available: https://rg.ru/2014/11/01/center-site.html [Accessed: 18th April 2019].

Газета.ru «Мы стоим перед новой угрозой» 12 апреля 2018 [Online]. Available: https://www.gazeta.ru/tech/2018/04/11/11714395/namib.shtml [Accessed: 28th March 2019].

ГАС Управление. Государственная автоматизированная информационная система ”Управление” Прикладное программное обеспечение государственной автоматизированной информационной системы «Управление» Регламент подключения и интеграции с ГАС «Управление» [Online]. Available: http://gasu.gov.ru/rest/documents/file/download?fileId=9681 [Accessed: 26th March 2019].

ГАС Управление. Государственная автоматизированная информационная система ”Управление” [Online]. Available: http://gasu.gov.ru/about [Accessed: 26th March 2019].

ГАС Управление. Прикладное программное обеспечениегосударственной автоматизированной информационной системы «Управление» [Online]. Available: http://gasu.gov.ru/preview?fileId=9681 [Accessed: 15th April 2019].

Голицына, Анастасия and Серьгина, Елизавета. Министр связи предложит правительству взять рунет под контроль. Ведомости. 26 Марта 2015. [Online]. Available: https://www.vedomosti.ru/technology/articles/2015/03/26/ministr-svyazi-predlozhit-gosudarstvu-vzyat-runet-pod-kontrol [Accessed: 4th December 2018].

Голицына, Анастасия. Совет безопасности обсудит отключение России от глобального интернета. Ведомости, 19 сентября 2014 [Online]. Available: https://www.vedomosti.ru/politics/articles/2014/09/19/suverennyj-internet [Accessed: 16th May 2019].

Голицына, Анастасия. Правительство не планирует рассматривать вопрос о суверенитете рунета. Ведомости, 31 марта 2015 [Online]. Available: https://www.vedomosti.ru/technology/articles/2015/03/31/pravitelstvo-ne-planiruet-rassmatrivat-vopros-o-suverenitete-runeta [Accessed: 16th May 2019].

Голицына, Анастасия. Институт развития интернета увольняет сотрудников. У организации начались проблемы с финансированием. Ведомости, 18 января 2017 [Online]. Available: https://www.vedomosti.ru/technology/articles/2017/01/18/673512-institut [Accessed: 17th May 2019].

Голицына, Анастасия, Серьгина, Елизавета. Министр связи предложит правительству взять рунет под контроль. Ведомости, 26 марта 2015 [Online]. Available: https://www.vedomosti.ru/technology/articles/2015/03/26/ministr-svyazi-predlozhit-gosudarstvu-vzyat-runet-pod-kontrol [Accessed: 11th April 2019].

Голицына, Анастасия, Серьгина, Елизавета, Козлов, Петр. Государство хочет контролировать маршруты интернет-трафика в стране. Ведомости, 11 февраля 2016 [Online]. Available: https://www.vedomosti.ru/politics/articles/2016/02/11/628508-gosudarstvo-hochet-kontrolirovat-rossiiskii-zarubezhnii-internet-trafik-strane [Accessed: 16th May 2019].

Голунов, Иван, Горбачев, Александр, Туровский, Даниил. «Симона» в поисках мата и порно «Медуза» выяснила, как работают сотрудники Роскомнадзора, которые занимаются цензурой в СМИ. И сколько это стоит. Meduza, 8 декабря 2017 [Online]. Available: https://meduza.io/feature/2017/12/08/simona-v-poiskah-mata-i-porno [Accessed: 15th May 2019].

Горошко, Е.И. Современные Интернет-коммуникации: структура и основные характеристики. М.: Наука, Флинта, 2012. [Online]. Available: http://www.textology.ru/article.aspx?aId=232 [Accessed: 7th March 2019].

ГосСОПКА. В 2019 году планируется уточнение нормативной базы в области кии, в том числе. 16.01.2019 [Online]. Available: http://gossopka.ru/2019/01/16 /в-2019-году-планируется-уточнение-нормат/ [Accessed: 18th April 2019].

ГосСОПКА. Нормативные документы о безопасности КИИ [Online]. Available: http://gossopka.ru/law/ [Accessed: 6th May 2019].

Грачёв, Анатолий. Технические аспекты взаимодействия с НКЦКИ. SOC-Форум, 27 ноября 2018 [Online]. Available: https://soc-forum.ib-bank.ru/files/files/SOC%202018/08_Grachev.pdf [Accessed: 9th May 2019].

Григорьев, Дмитрий. Решения от InfoTeCS. Защита от компьютерных атак, 2017 [Online]. Available: http://www.cio-sibir.ru/files/Meet/2017/10/GosSOPKA.pdf [Accessed: 10th May 2019].

Гриняев, Сергей Николаевич. Центр стратегических оценок и прогнозов [Online]. Available: http://csef.ru/ru/team/5 [Accessed: 18th March 2019].

GfK. Исследование GfK: Проникновение Интернета в России, 15 января 2019 [Online]. Available: https://www.gfk.com/ru/insaity/press-release/issledovanie-gfk-proniknovenie-interneta-v-rossii-1/ [Accessed: 10th April 2019].

ДВДМ.РУ Internet exchange (точки обмена трафиком) https://www.dwdm.ru/wiki/19 [Accessed: 15th April 2019].

Демидов, Олег, Махукова, Алёна. Инфраструктура Интернета в контексте регулирования жизненно важных услуг и критических информационных инфраструктур: обзор международного и российского опыта. CIIP Research, 2016 [Online]. Available: http://s.siteapi.org/808b25df7dd28c9.ru/docs/bf57c0ebec178d0c74fdc875e6ca39925397fd1e.pdf [Accessed: 18th April 2019].

Дрюков, Владимир. ГосСОПКА: то, о чем обычно молчат. Задачи операционной безопасности объектов КИИ в рамках функционирования центров ГосСОПКА: то, что забывают сказать. ВПК, 05 декабря 2017 [Online]. Available: https://vpk-news.ru/articles/40284 [Accessed: 15th May 2019].

Дубов, Григорий, Костина, Екатерина. В Роскомнадзоре ответили на слова Пескова о сотовой связи во Владивостоке. РБК, 12 сентября 2018 [Online]. Available: https://www.rbc.ru/society/12/09/2018/5b994abb9a79473eda33153f?from=main [Accessed: 14th April 2019].

Едовина, Татьяна “Сколково” обретет всероссийский масштаб Компании из регионов получат льготы и сервисы центра. Газета ”Коммерсантъ” №73 от 26.04.2018 [Online]. Available: https://www.kommersant.ru/doc/3614096 [Accessed: 11th April 2019].

Ефремов, А. А. Предложения для включения в проект Рекомендаций Парламентских слушаний «О совершенствовании федерального законодательства по обеспечению информационной безопасности при использовании информационно-коммуникационных технологий для оказания государственных услуг и осуществления межведомственного электронного документооборота» 28.06.2010 [Online]. Available: http://www.ifap.ru/pr/2010/n100622a.pdf [Accessed: 1st May 2019].

Жукова, Кристин, Новый, Владислав, Скоробогатько, Денис. Sailfish вносят в бюджет. Государство получило оценки стоимости перехода чиновников на отечественную ОС. Коммерсантъ, №138 от 06.08.2018 [Online]. Available: https://www.kommersant.ru/doc/3706552?from=four_tech [Accessed: 12th April 2019].

Жукова, Кристина, Скоробогатько, Денис. Гособлако выведут на рынок. IT-системам органов власти подберут операторов. Коммерсантъ, № 68 от 17.04.2019 [Online]. Available: https://www.kommersant.ru/doc/3946062?from=main_12 [Accessed: 21st April 2019].

Жукова, Кристина. ГосСОПКА сдадут под ключ. Коммерсантъ №215 от 20.11.2017 [Online]. Available: https://www.kommersant.ru/doc/3472959?from=four_tech [Accessed: 9th May 2019].

Жукова, Кристина. Российский софт отключают от заграницы. Требования к отечественному ПО ужесточают в деталях. Газета "Коммерсантъ" №229 от 12.12.2018, стр. 7 [Online]. Available: https://www.kommersant.ru/doc/3827670?from=main_11 [Accessed: 3rd May 2019].

Жукова, Кристина. Росгвардия купила российский офисный софт на 60 млн рублей. Ведомости, 30 октября 2019 [Online]. Available: https://www.vedomosti.ru/technology/articles/2019/10/30/815092-rosgvardiya [Accessed: 7th January 2020].

Жужома, Валерий Михайлович. 16 ЦНИИИ МО РФ: история и современность. Связь в Вооруженных Силах Российской Федерации – 2018. Москва: Информационный мост, 2018, 68-70 [Online]. Available: https://army.informost.ru/2018/pdf/29.pdf [Accessed: 4th March 2019].

Замахина, Татьяна. Совфед разрешил использование ВС в Сирии. Российкая Газета 30.09.2015 [Online]. Available: https://rg.ru/2015/09/30/armia-site.html [Accessed: 25th March 2019].

ЗВЕЗДА. Военный Интернет: как работают закрытые технологии министерства обороны. ЗВЕЗДА, 9 априль 2017 [Online]. Available: https://tvzvezda.ru/news/vstrane_i_mire/content/201704091018-4ygi.htm [Accessed: 18th April 2019].

Звездина, Полина. Охрана для нацпроектов: почему контроль за майским указом отдали ФСО. РБК: 26 октября 2018 [Online]. Available: https://www.rbc.ru/society/26/10/2018/5bd1b4299a7947b26916a555?from=center_5 [Accessed: 6th May 2019].

Зиновьева Елена Сергеевна. МГИМО Online. Available: https://mgimo.ru/people/zinoveva/ [Accessed: 2nd April 2019].

Зыков, Владимир. Российское шифрование протестируют на сайте госуслуг. Начато тестовое внедрение российских систем защиты интернет-трафика. Известия, 31 августа 2017 [Online]. Available: https://iz.ru/636884/sertifikat-dlia-gosuslug-i-sputnika [Accessed: 15th May 2019].

Зыков, Владимир, Кондратьев, Александр. Роскомнадзор будет оперативно получать решения судов о блокировках Для этого будет создана система электронного взаимодействия. Известия, 2 февраля 2017 [Online]. Available: https://iz.ru/news/662031 [Accessed: 14th May 2019].

Зыков, Владимир, Рамм, Алексей. (2016a) В России появился военный интернет. Закрытый сегмент передачи данных позволяет подразделениям Минобороны безопасно обмениваться секретной информацией. Известия, 19 октября 2016 [Online]. Available: https://iz.ru/news/639221 [Accessed: 18th April 2019].

Зыков, Владимир, Рамм, Алексей. (2016b) У оборонных предприятий появится свой интернет. По защищенной сети будет передаваться засекреченная техническая документация. Известия, 31 октября 2016 [Online]. Available: https://iz.ru/news/641528 [Accessed: 18th April 2019].

Иванов, Максим. Совет федерации занялся цифровым суверенитетом: Стратегии кибербезопасности наметили основные направления. Коммерсантъ № 209 от 06.11.2012 [Online]. Available: https://www.kommersant.ru/doc/2060832 [Accessed: 4th December 2018].

Иванов, Сергей. Вооруженные силы России и ее геополитические приоритеты, 2 февраля 2004 [Online]. Available: https://globalaffairs.ru/number/n_2471 [Accessed: 30th March 2019].

Известия. Роскомнадзор обновил рекомендации операторам по фильтрации трафика. Известия, 27 июня 2017 [Online]. Available: https://iz.ru/611620/2017-06-27/roskomnadzor-obnovil-rekomendatcii-operatoram-po-filtratcii-trafika [Accessed: 14th May 2019].

Известия. Путин считает, что криптовалюты несут с собой серьезные риски. Известия, 10 октября 2017 [Online]. Available: https://iz.ru/656864/2017-10-10/putin-schitaet-chto-kriptovaliuty-nesut-s-soboi-sereznye-riski [Accessed: 12th April 2019].

Институт системного анализа ФИЦ ИУ РАН [Online]. Available: http://www.isa.ru/index.php [Accessed: 3rd April 2019].

Info.nic.ru. Система доменных имен. Российский сегмент. Технические подробности, 11.4.2005 [Online]. Available: https://info.nic.ru/st/11/out_954.shtml [Accessed: 3rd April 2019].

InfraOne Research. Инфраструктура России: Индекс Развития 2019 [Online]. Available: https://bit.ly/2Fiz4GW [Accessed: 5th January 2020].

ИСТИНА webpage [Online]. Available: https://istina.msu.ru/ [Accessed: 2nd April 2019].

ITForum. XI International it-forum with BRICS and SCO participation [Online]. Available: https://itforum.admhmao.ru/2018/ [Accessed: 9th May 2019].

Казарновский, Павел, Демченко, Наталья. Роскомнадзор назвал федеральные трассы с худшей мобильной связью. РВК, 25 декабря 2018 [Online]. Available: https://www.rbc.ru/society/25/12/2017/5a40d9739a794727e1779fd2 [Accessed: 14th April 2019].

Интерфакс. Советник президента Клименко предложил ограничить в России интернет. Интерфакс, 26 января 2017 [Online]. Available: https://meduza.io/news/2017/01/26/sovetnik-putina-nazval-kitayskiy-variant-edinstvennym-sposobom-obespechit-informatsionnuyu-bezopasnost-rf [Accessed: 17th May 2019].

Калюков, Евгений. Путин подписал майский указ о развитии России до 2024 года. РБК, 7 мая 2918 [Online]. Available: https://www.rbc.ru/politics/07/05/2018/5af05f3a9a79472b558b1a4f [Accessed: 29th May 2019].

Кантышев, Павел. «Росэнергоатом» начал строить крупный дата-центр. Проектом займется близкая к «Ростелекому» компания. Ведомости, 08 апреля 2015 [Online]. Available: https://www.vedomosti.ru/technology/articles/2015/04/08/rosenergoatom-nachal-stroit-krupnii-data-tsentr [Accessed: 21st April 2019].

Кантышев, Павел. ФСБ хочет получать ключи от электронной переписки за 10 дней. Спецслужба уточнила требования к интернет-компаниям, но выполнить их будет сложно. Ведомости, 07 декабря 2017 [Online]. Available: https://www.vedomosti.ru/technology/articles/2017/12/07/744550-fsb [Accessed: 15th May 2019].

Кантышев, Павел. Партнер Усманова по киберспорту поучаствует в законе Яровой. Ведомости, 31 января 2018 [Online]. Available: https://www.vedomosti.ru/technology/articles/2018/01/31/749576-partner-usmanova [Accessed: 17th April 2019].

Кантышев, Павел. Роскомнадзор добивается блокировки IP-адресов Amazon. Ведомости, 23 марта 2018 [Online]. Available: https://www.vedomosti.ru/technology/articles/2018/03/23/754777-roskomnadzor-amazon [Accessed: 14th May 2019].

Кантышев, Павел, Болецкая, Ксения, Никольский, Алексей. Россия не будет отключена от интернета. Ведомости, 02 октября 2014 [Online]. Available: https://www.vedomosti.ru/technology/articles/2014/10/02/na-strazhe-interneta [Accessed: 16th May 2019].

Кибердемократ. Как можно снизить цены на интернет в Кыргызстане - «Элкат» 11.03.2013 [Online]. Available: http://kiber.akipress.org/news:189 [Accessed: 15th April 2019].

Кинякина, Екатерина, Жукова, Кристина. Соседи России раскритиковали закон о предустановке российского софта. Ведомости, 22 декабря 2019 [Online]. Available: https://www.vedomosti.ru/technology/articles/2019/12/22/819374-raskritikovali-zakon-po [Accessed: 7th January 2020].

Кобцев, Роман. Подключение к ГосСОПКА. Оргвопросы. 22 марта 2018 [Online]. Available: https://infotecs.ru/webinars/archive/?show=11428 [Accessed: 18th April 2019].

Кодачигов, Валерий. В России появится реестр отечественного телеком-оборудования. Реестр отечественного софта уже три года ведет Минкомсвязи. Ведомости, 14 января 2019 [Online]. Available: https://www.vedomosti.ru/technology/articles/2019/01/14/791362-reestr-otechestvennogo [Accessed: 8th May 2019].

Кодачигов, Валерий. Закон Яровой пока не работает: Для его выполнения операторам не хватает документации. Ведомости, 01 октября 2018 [Online]. Available: https://www.vedomosti.ru/technology/articles/2018/10/01/782493-zakon-yarovoi#galleries%2F140737489014365%2Fnormal%2F1 [Accessed: 1st March 2019].

Кодачигов, Валерий. Минобороны отказалось передавать операторам частоты для 5G. Без этого появление в России связи пятого поколения невозможно. Ведомости, 28 марта 2019 [Online]. Available: https://meduza.io/news/2019/03/29/minoborony-otkazalos-peredavat-operatoram-svyazi-chastoty-dlya-5g [Accessed: 7 July 2019].

Коломыченко, Мария. Шифр и меч. ФСБ собирается взять интернет-трафик на контроль. Коммерсантъ" №174 от 21.09.2016 [Online]. Available: https://www.kommersant.ru/doc/3094848 [Accessed: 9th May 2019].

Коломыченко, Мария. В интернет ввели кибервойска. Аналитики оценили количество хакеров на госслужбе. Коммерсантъ, №2 от 10.01.2017 [Online]. Available: https://www.kommersant.ru/doc/3187320?utm_source=kommersant&utm_medium=tech&utm_campaign=four [Accessed: 18th May 2019].

Коломыченко, Мария. Киберспецслужба: Сбербанк предложил создать штаб борьбы с хакерами. РБК, 1 сентября 2017 [Online]. Available: https://www.rbc.ru/technology_and_media/01/09/2017/59a9799f9a7947375702db15?from=center_7 [Accessed: 9th May 2019].

Коломыченко, Мария. Депутаты предложили защитить Рунет с помощью отечественного шифрования. РБК, 2 апреля 2019 [Online]. Available: https://www.rbc.ru/technology_and_media/02/04/2019/5ca2138a9a79477cb5e399e7 [Accessed: 9th May 2019].

Коломыченко, Мария, Линделл, Дада. Вне прослушки: почему Роскомнадзор и ФСБ судятся с операторами связи. РБК, 09 ноября 2017 [Online]. Available: http://www.rbc.ru/technology_and_media/09/11/2017/5a03187e9a7947d88f988f53?from=center_1 [Accessed: 17th April 2019].

Коломыченко, Мария, Посыпкина, Александра. Российские сим-карты запустят на чипах Samsung Отечественное шифрование нужно ФСБ для борьбы с иностранными разведками. РБК, 23 мая 2019 [Online]. Available: https://www.rbc.ru/technology_and_media/23/05/2019/5ce53a039a79471bde8de739?from=center [Accessed: 26th May 2019].

Коломыченко, Мария, Посыпкина, Александра. Иностранным производителям телеком-оборудования решили дать послабление. РБК, 22 января 2018 [Online]. Available: https://www.rbc.ru/technology_and_media/22/01/2018/5a608cfd9a79477ebc3b3e7f [Accessed: 3rd May 2019].

Комаров, Алексей. Нормативные документы по безопасности АСУ ТП, АСУ ПиТП, КСИИ, КВО, КИИ [Online]. Available: https://www.securitylab.ru/blog/personal/zlonov/144489.php [Accessed: 15th May 2019].

Комментарий Департамента информации и печати МИД России о российских оценках французской инициативы «Парижский призыв к доверию и безопасности в киберпространстве», 20.11.2018 [Online]. Available: http://www.mid.ru/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/3413302 [Accessed: 14th May 2019].

Коммерсантъ. Госдума приняла законопроект о Фонде перспективных оборонных исследований. Коммерсантъ, 28 сентября 2012 [Online]. Available: https://www.vedomosti.ru/technology/news/2012/09/28/gosduma_prinyala_zakonoproekt_o_fonde_perspektivnyh [Accessed: 17th May 2019].

Коммерсантъ. Киберугрозы сажают на CERT. В России создают центр реагирования на инциденты в сфере информационной безопасности. Коммерсантъ" №160 от 01.09.2016 [Online]. Available: http://www.kommersant.ru/doc/3077603 [Accessed: 9th May 2019].

Коммерсантъ. Герман Клименко допустил ограничение работы Microsoft в России. Коммерсантъ, 29.05.2018 [Online]. Available: https://www.kommersant.ru/doc/3643881 [Accessed: 12th April 2019].

КонсультантПлюс. К 2025 году Минпромторг России планирует довести долю электронной торговли в общем объеме торговли до 20 процентов, 18.10.2017 [Online]. Available: http://www.consultant.ru/law/hotdocs/51181.html/ [Accessed: 12th April 2019].

Координационный центр национального домена сети Интернет [Online]. Available: https://cctld.ru/ru/about/history.php [Accessed: 10th April 2019].

Координационный центр доменов .RU/.РФ «Национальный координационный центр по компьютерным инцидентам (НКЦКИ)» стал новой компетентной организацией при Координационном центре доменов .RU/.РФ, 6 августа 2019 [Online]. Available: https://cctld.ru/media/news/kc/21309/ [Accessed: 7th August 2019].

Королев, Игорь. ФСО и ФСБ получат 1,8 миллиарда на цифровую поддержку Путина и Медведева. Cnews, 21.10.2019 [Online]. Available: https://www.cnews.ru/news/top/2019-10-18_fso_i_fsb_poluchat_18_milliarda [Accessed: 7th January 2020].

Корня, Анастасия. Главным регулятором рунета становится ФСБ. Свободы в российском интернете все меньше, считают правозащитники. Ведомости, 05 февраля 2018 [Online]. Available: https://www.vedomosti.ru/politics/articles/2018/02/05/749913-regulyatorom-runeta-fsb [Accessed: 14th May 2019].

Королев, Игорь. «Ростелеком» поглотил «сердце Рунета». CNews, 06.03.2017 [Online]. Available: http://www.cnews.ru/news/top/2017-03-06_rostelekom_poglotil_serdtse_runeta [Accessed: 10th April 2019].

Космическая связь. Спутниковая группировка. [Online]. Available: https://www.rscc.ru/space/seriya-ekspress-am/ekspress-am44-11-zd/ [Accessed: 8th May 2019].

Краснушкина, Надежда. Госданным прописали архитектуру. Единая информсреда объединит сотни ГИС. Коммерсантъ" №221 от 30.11.2018 [Online]. Available: https://www.kommersant.ru/doc/3814604 [Accessed: 17th May 2019].

Кречетова, Ангелина, Харатьян, Петр. Путин подписал закон о предустановке российского софта на гаджеты. Ведомости 02 декабря 2019 [Online]. Available: https://www.vedomosti.ru/technology/articles/2019/12/02/817628-putin-podpisal-zakon [Accessed: 6th January 2020].

Круглов, Александр, Рамм, Алексей, Степовой, Богдан. Минобороны создает военное облачное хранилище Армия получит распределенную сеть для обработки секретных и служебных данных. Известия, 5 июня 2018 [Online]. Available: https://iz.ru/751658/aleksandr-kruglov-aleksei-ramm-bogdan-stepovoi/minoborony-sozdaet-voennoe-oblachnoe-khranilishche [Accessed: 5th April 2019].

Крутских Андрей Владимирович МГИМО Online. Available: https://mgimo.ru/people/krutskikh-andrey/ [Accessed: 2nd April 2019].

Ландышв, Юлия. Ростове монтируют новую систему связи для чемпионата мира по футболу. Современная радиосеть позволит надежно общаться тысячам волонтеров. Комсомольская Правда, 20 апреля 2018 [Online]. Available: https://www.rostov.kp.ru/online/news/3091086/ [Accessed: 8th May 2019].

Латухина, Кира. Спецфонд безопасности. Российская газета 25.09.2014 [Online]. Available: https://rg.ru/2014/09/24/putin-site.html [Accessed: 28th February 2019].

Латухина, Кира. Защита цифры Президент призвал вместе бороться с киберугрозой. Российская газета, 8.7.2018 [Online]. Available: https://rg.ru/2018/07/08/putin-nazval-borbu-s-kiberatakami-gosudarstvennoj-zadachej.html [Accessed: 3rd January 2019].

Латухина, Кира. Барьер для шпиона. Владимир Путин призвал ФСБ защитить Россию от кибернаступления. RG.ru, 6 марта 2019 [Online]. Available: https://rg.ru/2019/03/06/putin-prizval-fsb-zashchitit-rossiiu-ot-kibernastupleniia.html [Accessed: 28th May 2019].

ЛЕВАДА-ЦЕНТР. Общественное мнение-2018 [Online]. Available: https://www.levada.ru/cp/wp-content/uploads/2019/03/OM-2018.pdf [Accessed: 26th April 2019].

Левченко, Григорий. Интернет-омбудсмен и советник Путина открестились от защиты пользователей Сети. Republic, 11 января 2016 [Online]. Available: https://republic.ru/posts/62291 [Accessed: 8th May 2019].

Lenta.ru. Китайские хакеры стали в два раза чаще атаковать стратегические объекты России. Lenta.ru, 26 августа 2016 [Online]. Available: https://lenta.ru/news/2016/08/26/hacker_china_rus/ [Accessed: 25th May 2019].

Lenta.ru. Роскомнадзор отказался от попыток веерно заблокировать Telegram. Lenta.ru, 25 апреля 2018 [Online]. Available: https://lenta.ru/news/2018/04/25/telega/ [Accessed: 14th May 2019].

Lenta.ru. «Закон Яровой» оказался неисполним. Lenta.ru, 3 июля 2018 [Online]. Available: https://lenta.ru/news/2018/07/03/illegal/ [Accessed: 14th May 2019].

Lenta.ru. Зона.ru вошла в десятку самых активных национальных сегментов интернета. Lenta.ru, 31 марта 2004 [Online]. Available: https://lenta.ru/news/2004/03/31/domen/ [Accessed: 7th March 2019].

Лысова, Татьяна, Стеркин, Филипп, Харатьян, Кирилл. "Есть вещи пострашнее ограничения поставок". Ведомости, 8.9.2014 [Online]. Available: https://www.vedomosti.ru/newspaper/articles/2014/09/08/est-veschi-postrashnee-ogranicheniya-postavok-dmitrij#ixzz3Ci26r445 [Accessed: 14th February 2019].

Макутина, Мария. Цифровой суверенитет. Газета.Ru 19 июня 2013 [Online]. Available: https://www.gazeta.ru/politics/2013/06/19_a_5387077.shtml [Accessed: 28th February 2019].

Маркелов, Роман. В России предложили ввести платную регистрацию мобильных устройств. RG.ru, 25 января 2019 [Online]. Available: https://rg.ru/2019/01/25/v-rossii-predlozhili-vvesti-platnuiu-registraciiu-mobilnyh-ustrojstv.html [Accessed: 8th May 2019].

Мартынов, Кирилл. Откуда втекает интернет Парламентарии Клишас и Луговой предлагают россиянам самоизолироваться от глобальной сети. Новая газета, 15 декабря 2018 [Online]. Available: https://www.novayagazeta.ru/articles/2018/12/15/78947-otkuda-vtekaet-internet [Accessed: 28th February 2019].

Mediascope. Аудитория интернета, 21.11.2018 [Online]. Available: https://mediascope.net/upload/iblock/ea0/RIW2018_I-Ishunkina_21.11.2018.pdf [Accessed: 10th April 2019].

Meduza. Минобороны отказалось передавать операторам связи частоты для 5G. Meduza, 29 марта 2019 [Online]. Available: https://meduza.io/news/2019/03/29/minoborony-otkazalos-peredavat-operatoram-svyazi-chastoty-dlya-5g [Accessed: 15th April 2019].

Mil.ru. Задачи Вооруженных Сил Российской Федерации [Online]. Available: https://structure.mil.ru/mission/tasks.htm [Accessed: 28th March 2019].

Mil.ru. 4-й Центральный научно-исследовательский институт Министерства обороны Российской Федерации [Online]. Available: http://ens.mil.ru/science/SRI/infrmation.htm?id=10807%40morfOrgScience [Accessed: 4th April 2019].

Mil.ru. Главное управление связи Вооруженных Сил Российской Федерации [Online]. Available: https://structure.mil.ru/structure/ministry_of_defence/details.htm?id=9587@egOrganization [Accessed: 9th May 2019].

Mil.ru. Задачи Вооруженных Сил Российской Федерации [Online]. Available: https://structure.mil.ru/mission/tasks.htm [Accessed: 28th March 2019].

МИЭТ. Педагогический состав: Пилюгин Павел Львович [Online]. Available: https://www.miet.ru/person/50077 [Accessed: 28th February 2019].

МГИМО. [Online]. Available: https://mgimo.ru/about/ [Accessed: 28th March 2019].

Министерство Внутренних Дел Российской Федерации. Управление «К» МВД России [Online]. Available: https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii [Accessed: 6th May 2019].

Михеева, Анна. ЦБ снизит тарифы в своем аналоге системы SWIFT. РБК, 13 февраля 2018 [Online]. Available: https://www.rbc.ru/finances/13/02/2018/5a82f3019a79472864bb5ada?from=main [Accessed: 17th April 2019].

MSK-IX. [Online]. Available: https://www.msk-ix.ru/dns/ [Accessed: 10th April 2019].

Murmanlink. Магистральная сеть [Online]. Available: https://murmanlink.ru/magistralnaya-set/ [Accessed: 15th April 2019].

Наумов, В.Б. Интернет и государственный суверенитет. I Всероссийская конференция «Право и интернет: теория и практика». 1999 [Online]: Accessed: http://www.ifap.ru/pi/01/r16.htm [Accessed: 10th December 2018].

Нелюбин, Николай. От «суверенного Интернета» нет пользы никому. Это просто кипячение океана. Фонтанки.ру 8 января 2019 [Online]. Available: https://www.fontanka.ru/2019/01/08/014/ [Accessed: 5th April 2019].

Нефёдова, Мария. Эксперты Group-IB сообщают, что рунет стал чище. Хакер, 5.7.2019 [Online]. Available: https://xakep.ru/2019/07/05/runet-stats/ [Accessed: 7th July 2019].

ОГО АДЭ. Отчет о фактическом состоянии маршрутизации внутрироссийского трафика через зарубежные сети, 30 ноября 2017 [Online]. Available: http://www.rans.ru/images/news/Traffic_30112017.pdf [Accessed: 5th January 2019].

Панов, Павел, Галанина, Ангелина. Написано связью: правительство начнет контролировать интернет. За трафиком будет следить специальная государственная структура. Известия, 22 февраля 2019 [Online]. Available: https://iz.ru/848412/pavel-panov-angelina-galanina/napisano-sviaziu-pravitelstvo-nachnet-kontrolirovat-internet [Accessed: 17th May 2019].

Петелин, Герман, Баринов, Владимир. Разведка Минобороны требует от ученых неустойку в 30 млн рублей. Главное разведывательное управление отстаивает в суде свои права. Известия, 15 марта 2013 [Online]. Available: https://iz.ru/news/546680 [Accessed: 5th April 2019].

Петренко, Анатолий Иванович. Межрегиональное бюро судебных экспертиз Им. Сикорского [Online]. Available: https://www.expertsud.ru/content/view/166/39/ [Accessed: 28th March 2019].

Positive Technologies. Построение центра ГосСОПКА — краткое описание решения [Online]. Available: https://www.ptsecurity.com/upload/corporate/ru-ru/solutions/center-gossopka/PT-GosSOPKA-PB-rus.pdf [Accessed: 18th April 2019].

Посыпкина, Александра, Балашова, Анна. Одна страна — одна сеть Минкомсвязь вопреки возражениям сотовых компаний настаивает на создании единого оператора связи 5G. РБК, 14 марта 2019 [Online]. Available: https://www.rbc.ru/rbcfreenews/5cb438899a79470207aea140 [Accessed: 15th April 2019].

РАНХиГС [Online]. Available: https://www.ranepa.ru/ [Accessed: 28th March 2019].

РАЭК. Интернет в России 2014: Состояние, тенденции и перспективы развития. Москва, 2015 [Online]. Available: http://www.fapmc.ru/rospechat/newsandevents/newsagency/2015/08/item1/main/custom/00/0/file.pdf [Accessed: 10th April 2019].

РАЭК. Экономика Рунета 2015–2016. РАЭК, 2016 [Online]. Available: http://files.runet-id.com/2016/presentation-research/presentations/EconomicaRunetaItogy2016.pdf [Accessed: 10th April 2019].

РАЭК. Интернет в России в 2017 году: Состояние, тенденции и перспективы развития. М.: Типография «Форвард Принт», 2018 [Online]. Available: http://www.fapmc.ru/rospechat/activities/reports/2018/teleradio/main/custom/0/0/file.pdf [Accessed: 10th April 2019].

РАЭК. Экономика Рунета 2018. РАЭК, 2019 [Online]. Available: https://raec.ru/upload/files/ru-ec_booklet.pdf [Accessed: 12th April 2019].

РАЭК. Рунет подвел итоги года, 13 Декабря 2018 [Online]. Available: https://raec.ru/live/raec-news/10766/ [Accessed: 11th April 2019].

РБК. На Форуме «Российский софт» обсудили национальную кибербезопасность. РБК, 30 Апреля 2019 [Online]. Available: http://presscentr.rbc.ru/page5701909html [Accessed: 17th May 2019].

Резчиков, Андрей. Избежать отключения от интернета России поможет Китай. ВЗГЛЯД, 29 декабря 2016 [Online]. Available: https://vz.ru/society/2016/12/29/744236.html [Accessed: 16th May 2019].

Репин, Андрей. «Новинки Smart City» будет достраивать АО «СЗ НО «Дирекция по строительству». Коммерсант, 12 декабря 2018 [Online]. Available: https://www.kommersant.ru/doc/3827866 [Accessed: 15th April 2019].

РИА Новости. История развития Рунета. Справка, 30 сентября 2009 [Oline]. Available: https://ria.ru/20090930/186873799.html [Accessed: 7th March 2019].

РИА Новости. История развития российского Интернета. Справка, 19 сентября 2011 [Online]. Available: https://ria.ru/20110919/439857350.html [Accessed: 24th March 2019].

РИА Новости. План обороны России на 2016–2020 годы введен в действие 1 января 2016 [Online]. Available: https://ria.ru/20160101/1352552856.html [Accessed: 12th February 2019].

РИФ. 23-й Российский Интернет Форум [Online]. Available: https://2019.rif.ru/ [Accessed: 9th May 2019].

Рожков, Роман, Новый, Владислав. Telegram не сдал ключи. Роскомнадзор будет добиваться ограничения доступа к мессенджеру через суд. Коммерсантъ" №58 от 05.04.2018 [Online]. Available: https://www.kommersant.ru/doc/3593600 [Accessed: 15th May 2019].

Роскомнадзор. Выданные и аннулированные разрешения на строительство, реконструкцию, проведение изыскательских работ для проектирования и ликвидацию сухопутных линий связи при пересечении государственной границы Российской Федерации и на приграничной территории 14.01.2019 [Online]. Available: http://rkn.gov.ru/communication/register/p191/ [Accessed: 18th April 2019].

Роскомсвобода. «Китаизация» Рунета входит в активную фазу и начнётся с точек обмена трафиком, 18-8-2017 [Online]. Available: https://roskomsvoboda.org/31224/ [Accessed: 1st May 2019]; Роскомсвобода. Цифровая оборона интернета [Online]. Available: https://roskomsvoboda.org/45308/ [Accessed: 1st March 2019].

Роскомсвобода. «Китаизация» Рунета входит в активную фазу и начнётся с точек обмена трафиком. Роскомсвобода, 18.8.2017 [Online]. Available: https://roskomsvoboda.org/31224/ [Accessed: 17th May 2019].

Роскомсвобода. Итоги госрегулирования Рунета в 2018 году. Роскомсвобода, 28.12.2018 [Online]. Available: https://roskomsvoboda.org/44118/ [Accessed: 17th April 2019].

Роскомсвобода. Спутниковый трафик под надзором ФСБ. Роскомсвобода, 26.2.2019 [Online]. Available: https://roskomsvoboda.org/45251/ [Accessed: 17th May 2019].

Роскомсвобода. Telegram: год под «блокировкой». Роскомсвобода, 16.4.2019 [Online]. Available: https://roskomsvoboda.org/46556/ [Accessed: 14th May 2019].

Роскомсвобода. Интернет вещей подключат к СОРМ. Роскомсвобода, 27.03.2019 [Online]. Available: https://roskomsvoboda.org/46080/ [Accessed: 17th April 2019].

Роскомсвобода. Минпромторг хочет запретить реализацию «пакета Яровой» на иностранном оборудовании. Роскомсвобода, 7.5.2019 [Online]. Available: https://roskomsvoboda.org/46996/ [Accessed: 14th May 2019].

Роскомсвобода. «Суверенный Рунет» продолжает обрастать подзаконными актами, 29.05.2019 [Online]. Available: https://roskomsvoboda.org/47342/ [Accessed: 30th May 2019].

Роскомсвобода. Суверенное регулирование продолжает обрастать «нормативками». Роскомсвобода, 21.6.2019 [Online]. Available: https://roskomsvoboda.org/47728/ [Accessed: 8th July 2019].

Роскомсвобода. Большая российская энциклопедия не станет полноценной заменой Википедии, 7.11.2019 [Online]. Available: https://roskomsvoboda.org/51846/ [Accessed: 5th January 2020].

Роскомсвобода. Чему научили учения по Суверенному Рунету? Роскомсвобода, 24.12.2019 [Online]. Available: https://roskomsvoboda.org/53902/ [Accessed: 7th January 2020].

Роскомсвобода. Ростелеком создаст киберполигон, 06.12.2019 [Online]. Available: https://roskomsvoboda.org/53137/ [Accessed: 10th January 2020].

Российский союз промышленников и предпринимателей. Комитет по цифровой экономике [Online]. Available: http://www.rspp.ru/cc/news/60 [Accessed: 17th May 2019].

Российский союз промышленников и предпринимателей. На заседании Комитета РСПП по цифровой экономике обсудили меры господдержки импортозамещения программного обеспечения. 23 апреля 2019 [Online]. Available: http://www.rspp.ru/cc/news/60/16247 [Accessed: 17th May 2019].

Россия-24. Крым. Путь на Родину, ВГТРК, Россия-24, 15.3.2015 [Online]. Available: https://www.youtube.com/watch?v=t42-71RpRgI [Accessed: 15th March 2019].

Ростелеком. Функции Технического центра Интернет передаются компании «РТК – Центр обработки данных» 24.1.2018 [Online]. Available: http://www.rtk-dc.ru/press/rostelekom-v-voronezhe-prinyal-uchastie-v-kruglom-stole-po-voprosam-bezopasnosti-detey-v-internete8/ [Accessed: 10th April 2019].

Ростелеком. Магистральная сеть связи [Online]. Available: https://www.company.rt.ru/about/net/magistr/# [Accessed: 15th April 2019].

Ростелеком. Облачные сервисы в Цифровой трансформации, 20.2.2017 [Online]. Available: http://www.rtk-dc.ru/upload/iblock/66b/66b7243122a76c89f8f1be681cc5f0fb.pdf [Accessed: 15th April 2019].

Ростелеком. Роль ПАО «Ростелеком» в цифровой экономике. Май, 2017 [Online]. Available: https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2017/06_Saint_Petersburg/Presentations/ITU%20Workshop%2019.06%20-%20Alexei%20Borodin%202.pdf [Accessed: 17th May 2019].

РСПП. Конструктивный диалог по реализации «закона Яровой» продолжается 1 февраля 2018 [Online]. Available: http://www.rspp.ru/cc/news/32/13653 [Accessed: 1st March 2019].

Рузин, Андрей. Интернет: Россия у критической черты, CNews.ru 08.04.2004 [Online]. Available: http://www.cnews.ru/articles/internet_rossiya_u_kriticheskoj_cherty [Accessed: 7th March 2019].

RT. Чем может угрожать России активность американских военных в киберпространстве. Рамблер 28 февраля 2019 [Online]. Available: https://news.rambler.ru/other/41794660/?utm_content=rnews&utm_medium=read_more&utm_source=copylink [Accessed: 28th February 2019].

ru.map-ix.net [Online]. Available: http://ru.map-ix.net/home [Accessed: 15th April 2019].

Рябова, Вика. Владимир Путин поручил правительству обеспечить разработку национальной стратегии в области ИИ. D-Russia.ru, 27.2.2019 [Online]. Available: http://d-russia.ru/vladimir-putin-poruchil-pravitelstvu-obespechit-razrabotku-natsionalnoj-strategii-v-oblasti-ii.html [Accessed: 16th May 2019].

'Сайфетдинов' Академик 2019 [Online]. Available: https://dic.academic.ru/dic.nsf/enc_biography/ 109590 /Сайфетдинов. [Accessed: 30th January 2019].

Сафронов, Иван. «Группировка будет развернута в любом случае: с нашим участием или без него». Газета "Коммерсантъ" №33 от 25.02.2019 [Online]. Available: https://www.kommersant.ru/doc/3894154?from=author_tech [Accessed: 15th April 2019].

Сафронов, Иван, Джорджевич, Александра. На главном политическом направлении. Генерал Андрей Картаполов возглавит новый главк Минобороны. Коммерсантъ" №134 от 31.07.2018 [Online]. Available: https://www.kommersant.ru/doc/3701013 [Accessed: 18th May 2019].

Седлов, Данил. Время единорогов. Как в Рунете создается бизнес стоимостью $1 млрд. Forbes, 21.02.2019 [Online]. Available: https://www.forbes.ru/tehnologii/372571-vremya-edinorogov-kak-v-runete-sozdaetsya-biznes-stoimostyu-1-mlrd [Accessed: 12th April 2019].

Сидоркова, Инна, Дергачев, Владимир, Антонова, Елизавета. В регионах появятся центры на случай военного положения. РБК, 09 апруля 2019 [Online]. Available: https://www.rbc.ru/politics/09/04/2019/5caca4919a79475d5519d425?from=center [Accessed: 18th April 2019].

Сидоркова, Инна. Военное «Сколково»: зачем Шойгу строит технополис в Анапе. РВК, 13 марша 2018 [Online]. Available: https://www.rbc.ru/politics/13/03/2018/5a9e82869a7947860d0516ca [Accessed: 11th April 2019].

CNews. В Москве создан первый корневой сервер имен. CNews, 19.11.2003 [Online]. Available: http://www.cnews.ru/news/line/v_moskve_sozdan_pervyj_kornevoj_server_imen [Accessed: 10th April 2019].

CNews. Крупнейшие поставщики услуг ЦОД в России 2017. CNews 24.12.2018 [Online]. Available: http://www.cnews.ru/reviews/cloud2018/review_table/6df1a7366926feb538d10f26888ff71d6f0ff9cd [Accessed: 15th April 2019].

Соколов, Анатолий. Новый космический щит России. Русская Планета, 18 ноября 2015 [Online]. Available: http://rusplt.ru/society/novyiy-kosmicheskiy-schit-rossii-19771.html [Accessed: 5th March 2019].

Соколов, Анатолий. Новый космический щит России. Русская Планета, 18 ноября 2015 [Online]. Available: http://rusplt.ru/society/novyiy-kosmicheskiy-schit-rossii-19771.html [Accessed: 5th March 2019].

Стадник, Илона. Ошибка сети: что показал учебный запуск «суверенного Рунета». РБК, 26.12.2019 [Online]. Available: https://www.rbc.ru/opinions/technology_and_media/26/12/2019/5e046d649a794756d9e55596 [Accessed: 7th 2020].

Стандард. "Магистральные сети связи в России", Стандард № 9 (188) September 2018 [Online]. Available: https://www.comnews.ru/standart/issue/400 [Accessed: 11th April 2019].

SOC-Форум [Online]. Available: https://soc-forum.ib-bank.ru/ [Accessed: 9th May 2019].

Сухаревская, Алена. Нефтегазовый венчур: как работает Фонд развития интернет-инициатив. РБК, 28 апреля 2016 [Online]. Available: https://www.rbc.ru/magazine/2016/05/570fa16e9a794781cb616fa0 [Accessed: 17th May 2019].

Сухаревская, Алена. Роскомнадзор заблокировал почти триста доменов Google. Ведомости, 11 апреля 2018 [Online]. Available: https://www.vedomosti.ru/technology/articles/2018/04/11/766420-roskomnadzor-zablokiroval-google [Accessed: 14th May 2019].

Сухаренко, Александр. Кибертеррористов вычислят с ГосСОПКА. Независимая газета, 23.12.2016 [Online]. Available: http://www.ng.ru/ideas/2016-12-23/5_6893_kiber.html [Accessed: 1st May 2019].

Сухова, Светлана. "Пропагандой выиграть нельзя. Доминированием в технологиях — можно". Журнал "Огонёк" №40 от 10.10.2016 [Online]. Available: https://www.kommersant.ru/doc/3106914 [Accessed: 11th April 2019].

Tadviser. Киберпреступность и киберконфликты: Россия [Online]. Available: http://www.tadviser.ru/a/240126 [Accessed: 1st May 2019].

Tadviser. Система межведомственного электронного взаимодействия (СМЭВ) [Online]. Available: http://www.tadviser.ru/a/71478 [Accessed: 15th April 2019].

Tadviser. Государственная информационная система топливно-энергетического комплекса [Online]. Available: http://www.tadviser.ru/a/248699 [Accessed: 17th April 2019].

ТАСС. В России создана Национальная ассоциация международной информационной безопасности 10 апреля 2018 [Online]. Available: http://tass.ru/obschestvo/5111643 [Accessed: 28th March 2019].

ТАСС. Шойгу заявил, что Россия должна выработать новую теорию ведения войн. ТАСС, 18 июня 2019 [Online]. Available: https://tass.ru/armiya-i-opk/6561643 [Accessed: 2nd July 2019].

ТАСС. Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций. ТАСС, 12 мая 2014 [Online]. Available: https://tass.ru/politika/1179830 [Accessed: 18th May 2019].

ТАСС. Глава Минкомсвязи пообещал проводить ежегодные учения по обеспечению устойчивости рунета. ТАСС, 19 ноября 2014 [Online]. Available: https://digital.gov.ru/ru/events/32136/ [Accessed: 16th May 2019].

ТАСС. Система защиты Минобороны РФ от кибератак завершила тестовые испытания и будет расширена. ТАСС, 24 октября 2016 [Online]. Available: https://tass.ru/armiya-i-opk/3728399 [Accessed: 18th April 2019].

ТАСС. Военные РФ впервые отработали информационное противоборство на учениях "Кавказ". ТАСС, 14 сентября 2016 [Online]. Available: https://tass.ru/armiya-i-opk/3619816 [Accessed: 12 June 2019].

ТАСС. Юнармия России: для чего возродилось всероссийское военно-патриотическое движение. ТАСС, 22 февраля 2018 [Online]. Available: 18th May 2019].

ТАСС. Минобороны РФ увеличит число научных рот в 2018 году. ТАСС, 30 марша 2018 [Online]. Available: https://tass.ru/armiya-i-opk/5080737 [Accessed: 11th April 2019].

ТАСС. "Яндекс" запускает собственную облачную платформу. ТАСС, 5 сентября 2018 [Online]. Available: https://tass.ru/ekonomika/5523570 [Accessed: 14th April 2019].

ТАСС Путин посетит в Анапе новый военный технополис и проведет итоговое совещание по "оборонке". ТАСС, 21 ноября 2018 [Online]. Available: https://tass.ru/armiya-i-opk/5819998 [Accessed: 11th April 2019].

ТАСС. Минобороны РФ: научные роты пополнили 300 призывников по итогам осенней кампании 2018 года. ТАСС, 12 декабря 2018 [Online]. Available: https://tass.ru/armiya-i-opk/5902450 [Accessed: 18th May 2019].

ТАСС. Минобороны РФ предлагает странам ОДКБ сформировать согласованную информационную политику. ТАСС, 20 июня 2019 [Online]. Available: https://tass.ru/armiya-i-opk/6573842 [Accessed: 8th July 2019].

ТАСС. Госдума запретила военным пользоваться смартфонами на службе. ТАСС, 19 февраля 2019 [Online]. Available: https://tass.ru/obschestvo/6132986?... [Accessed: 18th May 2019].

Тадтаев, Георгий. Трамп подписал указ о создании космического командования США, РБК, 18.12.2018. [Online]. Available: https://www.rbc.ru/politics/18/12/2018/5c191a289a79473887d59637 [Accessed: 11th February 2019].

Технический центр Интернет. [Online]. Available: https://statdom.ru/ [Accessed: 10th April 2019].

Тишина, Юлия. Россия обозначит цифровые границы Власти защитят интернет-пользователей от иностранных силовиков. Коммерсантъ, №181 от 04.10.2018, 1 [Online]. Available: https://www.kommersant.ru/doc/3759627 [Accessed: 28th February 2019].

Тишина, Юлия. «Закон Яровой» вписали в инфляцию. Объемы хранения данных и затраты операторов могут вырасти. Коммерсантъ, №61 от 10.04.2017 [Online]. Available: https://www.kommersant.ru/doc/3267272 [Accessed: 14th May 2019].

Тишина, Юлия, Жукова, Кристина. Оцифрованные миллиарды. Правительство утвердило проекты «Цифровой экономики». Коммерсантъ" №2 от 10.01.2018 [Online]. Available: https://www.kommersant.ru/doc/3515334 [Accessed: 22 May 2018].

Тишина, Юлия. «Закон Яровой» сводят с реальностью Власти смягчают его условия и сроки введения. Коммерсантъ, №10 от 22.01.2018 [Online]. Available: https://www.kommersant.ru/doc/3526894 [Accessed: 14th May 2019].

Торбенко, Елена. Практика категорирования объектов КИИ. SOC форум 27 ноября 2019 [Online]. Available: https://soc-forum.ib-bank.ru/files/files/SOC%202018/05_Torbenko.pdf [Accessed: 18th April 2019].

Трифонова, Екатерина. Россия предложила разделить интернет. Независимая газета, 1 декабря 2017 [Online]. Available: http://www.ng.ru/politics/2017-12-01/3_7127_internet.html [Accessed: 15th April 2019].

Трунина, Анна. Интернет-сервисы в России обязали хранить трафик пользователей полгода. РБК, 5 февраля 2019 [Online]. Available: https://www.rbc.ru/technology_and_media/28/06/2018/5b34f94f9a79476cbd07e0e8?from=main [Accessed: 14th May 2019].

Туровский Даниил. Российские вооруженные киберсилы Как государство создает военные отряды хакеров. Meduza, 7 ноября 2016 [Online]. Available: https://meduza.io/feature/2016/11/07/rossiyskie-vooruzhennye-kibersily [Accessed: 9th May 2019].

Федеральная служба государственной статистики. ониторинг развития информационного общества в Российской Федерации [Online]. Available: http://www.gks.ru/wps/wcm/connect/rosstat_main/rosstat/ru/statistics/science_and_innovations/it_technology/ [Accessed: 10th April 2019].

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. Единый реестр [Online]. Available: https://eais.rkn.gov.ru/ [Accessed: 14th May 2019].

Федеральное агентство по печати и массовым коммуникациям приказ от 18 июля 2005 г. № 106 "О проведении открытого конкурса на выполнение работ по подготовке и проведению Второго Конкурса на присуждение ежегодной Национальной премии за вклад в развитие российского сегмента сети Интернет «ПРЕМИЯ РУНЕТА - 2005»" [Online]. Available: http://www.fapmc.ru/rospechat/docs/documents/order/2005/07/fap106.html [Accessed: 11th April 2019].

Федеральное агентство по печати и массовым коммуникациям. Российскому национальному домену «.RU» исполнилось 25 лет. 08 апреля 2019 [Online]. Available: http://www.fapmc.ru/rospechat/newsandevents/newsagency/2019/04/item4.html [Accessed: 10th April 2019].

Федеральное агентство по печати и массовым коммуникациям. Итоги премии Рунета 2017, 24 ноября 2017 [Online]. Available: http://www.fapmc.ru/rospechat/newsandevents/newsagency/2017/11/item20.html [Accessed: 8th May 2019].

Федеральный исследовательский центр «Информатика и управление» Российской Академии Наук (ФИЦ ИУ РАН) [Online]. Available: http://www.frccsc.ru/ [Accessed: 3rd April 2019].

ФГБУ Центр МИР ИТ. Устав ФГБУ Центр МИР ИТ, 22.6.2016 [Online]. Available: http://centrmirit.ru/wp-content/uploads/2017/07/Ustav-FGBU-TSentr-MIR-IT.pdf [Accessed: 8th May 2019].

ФОМ. Интернет в России: динамика проникновения. Зима 2017–2018 гг., 04 Апреля 2018г [Online]. Available: https://fom.ru/SMI-i-internet/13999 [Accessed: 10th April 2019].

Фролов, Дмитрий Борисович. Высшая школа государственного аудита [Online]. Available: http://itlaw.audit.msu.ru/ [Accessed: 28th March 2019].

ФСТЭК. Сведения о полномочиях ФСТЭК России; перечень нормативных правовых актов, определяющих эти полномочия. 28 Марта 2016 [Online]. Vailable: https://fstec.ru/obshchaya-informatsiya/polnomochiya [Accessed: 6th May 2019].

Хизриев, Арсен, Балтачева, Марина. «Используют тактику «выжженной земли». ВЗГЛЯД, 27 сентября 2013 [Online]. Available: https://vz.ru/politics/2013/9/27/652418.html [Accessed: 27th February].

Холявко, Анна. «Лаборатория Касперского» назвала мишени китайских хакеров в России. Эксперты фиксируют их возросшую активность. Ведомости, 06 декабря 2017 [Online]. Available: https://www.vedomosti.ru/technology/articles/2017/12/06/744343-hakeri-atakuyut-rossiiskie-gosudarstvennie-strukturi [Accessed: 25th May 2019].

Центр по лицензированию, сертификации и защите государственной тайны ФСБ России. Перечень средств защиты информации, сертифицированных ФСБ России [Online]. Available: http://clsz.fsb.ru/files/download/svedeniya_po_sertifikatam_22.04.doc [Accessed: 9th May 2019].

Центральный научно-исследовательский институт связи. СОРМ [Online]. Available: https://zniis.ru/focus/sorm [Accessed: 8th May 2019].

Цифровая экономика. Информационная безопасность [Online]. Available: https://data-economy.ru/security#rec34030444 [Accessed: 28th February 2019].

ЦНИИ ЭИСУ [Online]. Available: http://cniieisu.ru/ [Accessed: 5th April 2019].

Цыгичко Виталий Николаевич. Московский физико-технический институт (национальный исследовательский университет) [Online. Available: https://mipt.ru/education/chairs/parallelcomputing/persons/cigichko.php [Accessed: 5th April 2019].

Черешкин, Д. С., Смолян, Г. Л., Цыгичко, В. Н. Информационное развитие России – путь к информационному обществу. «Информационные ресурсы России» №1, 2005 [Online]. Available: http://www.aselibrary.ru/press_center/journal/irr/2005/number_1/number_1_2/digital_resources515273747787/ [Accessed: 4th March 2019].

Черненко, Елена. МИД обзаведется новым департаментом. Коммерсантъ №56 от 01.04.2019 [Online]. Available: https://www.kommersant.ru/doc/3930510 [Accessed: 6th January 2020].

Чернышова, Евгения, Михеева, Анна. В российском аналоге SWIFT появился первый зарубежный участник. РБК, 22 ноября 2018 [Online]. Available: https://www.rbc.ru/finances/22/11/2018/5bf6bbd09a79476d3e8100d5?from=main [Accessed: 17th April 2019].

Чурапченко, Евгения, Семашко, Наталья. Энергетика цифры. Коммерсантъ, 2 октября 2018 [Online]. Available: https://www.kommersant.ru/doc/3758627?query=smart%20grid [Accessed: 15th April 2019].

Шмырова, Валерия. В России хотят запретить госзакупки иностранных СХД. CNews, 8 мая 2019 [Online]. Available: http://www.cnews.ru/news/top/2019-05-08_v_rossii_zapretyat_goszakupki_inostrannyh_shd?utm_source=yxnews&utm_medium=desktop [Accessed: 9th May 2019].

Шмырова, Валерия . «Цифровая экономика» исполняет бюджет хуже всех нацпрограмм, потому что обо всем советуется с бизнесом. CNews, 11.11.2019 [Online]. Available: https://cnews.ru/news/top/2019-11-08_tsifrovaya_ekonomika_ispolnyaet [Accessed: 5th January 2020].

Эшер II. Проекты нормативных правовых актов по устойчивому Рунету [Online]. Available: https://usher2.club/helpers/stable-runet-npa-list [Accessed: 7th January 2020].

Юзбекова, Ирина. Россия уменьшит зависимость от Америки с помощью серверов из Китая. РБК, 18 августа 2014 [Online]. Available: https://www.rbc.ru/economics/18/08/2014/5424c895cbb20f353dbe0370 [Accessed: 3rd May 2019].

Яровая, Майя. Игорь Ашманов: "Сегодня информационное доминирование – это все равно, что господство в воздухе". Ain.ua 01 Мая, 2013 [Online]. Available: https://ain.ua/2013/05/01/igor-ashmanov-segodnya-informacionnoe-dominirovanie-eto-vse-ravno-chto-gospodstvo-v-vozduxe/ [Accessed: 28th February 2019].

Ястребова, Светлана. Партнер Усманова может контролировать еще одну компанию для исполнения закона Яровой. Ведомости, 13 июля 2018 [Online]. Available: https://www.vedomosti.ru/technology/articles/2018/07/13/775384-sorm-yarovoi [Accessed: 17th April 2019].

Documents & Statements

Агора. Россия. Свобода интернета 2016: на военном положении [Online]. Available: https://agora.legal/fs/a_delo2doc/8_file_2.pdf [Accessed: 14th May 2019].

Агора. Свобода интернета 2018: делегирование репрессий [Online]. Available: https://meduza.io/static/0001/Свобода-интернета-2018.pdf [Accessed: 1st March 2019].

Берг, А. И., Китов, А. И., Ляпунов, А. А. "О возможностях автоматизации управления народным хозяйством" Москва. Ноябрь 1959 [Online]. Available: http://www.kitov-anatoly.ru/naucnye-trudy/izbrannye-naucnye-trudy-anatolia-ivanovica-v-pdf/o-vozmoznostah-avtomatizacii-upravlenia-narodnym-hozajstvom [Accessed: 23rd November 2018].

Берг А. И., Китов А. И., Ляпунов А. А. Радиоэлектронику – на службу управления народным хозяйством. Коммунист № 9 1960, 21-28. [Online]. Available: http://odasib.ru/openarchive/DocumentImage.cshtml?id=Xu1_pavl_635766969644249164_16578&eid=L5_0003_0866 [Accessed: 23rd March 2019].

Выписка. ”Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации” (утв. Президентом РФ 12.12.2014 N К 1274) [Online]. Available: http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf. [Accessed 10 January 2018].

Выступление генерального секретаря ЦК КПСС М. С. Горбачёва на пресс-конференции в Рейкьявике [Online]. Available: http://perestrojka.su/documents/1986/Reykjavik.htm [Accessed: 22nd March 2019].

Gorbachev, Mikhail. Political Report of the CPSU Central Committee to the 27th Party Congress, 1986 [Online]. Available: https://archive.org/details/PoliticalReportOfTheCPSUCentralCommitteeToThe27thPartyCongress/page/n41 [Accessed: 9th November 2018].

ГОСТ 28806-90. Качество программных средств. Термины и определения [Online]. Available: https://meganorm.ru/Data2/1/4294825/4294825913.pdf [Accessed: 15th March 2019].

ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. 1992-01-01 [Online]. Available: http://docs.cntd.ru/document/gost-34-003-90 [March 17th 2019].

ГОСТ Р 51897-2011. Менеджмент риска. Термины и определения. Дата введения 2012-12-01 [Online]. Available: http://docs.cntd.ru/document/gost-r-51897-2011 [Accessed: 15th March 2019].

ГОСТ Р 56111-2014. Интегрированная логистическая поддержка экспортируемой продукции военного назначения [Online]. Available: http://cals.ru/sites/default/files/downloads/56111_.pdf [Accessed: 15th March 2019].

Доктрина. Военная доктрина Российской Федерации. 25 декабря 2014 г., № Пр-2976 [Online]. Available: http://www.scrf.gov.ru/security/military/document129/ [Accessed: 28th March 2019].

Закон РФ ”О государственной тайне” от 21.07.1993 N 5485-1 (последняя редакция) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_2481/ [Accessed: 8th May 2019].

Известия. Основные поло жения военной доктрины Российской Федерации». ноября 1993 года Совет безопасности Российской Федерации одобрил доработанный документ. Указом Президента Российской Федерации от 2 ноября 1993 года № 1833 «Основные положения военной доктрины Российской Федерации» приняты. 18th November 1993. Izveztiia 1993 No. 221 [Online]. Available: https://yeltsin.ru/uploads/upload/newspaper/1993/izv11_18_93/FLASH/index.html [Accessed: 14th Novembet 2018].

Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) [Online]. Available: https://base.garant.ru/10103000/ [Accessed: 6th May 2019].

Концепция. Концепция внешней политики Российской Федерации от 12 июля 2008 г. N Пр-1440 (утв. 12.07.2008 N Пр-1440) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_85021/ [Accessed: 30th March 2019].

Концепция. Концепция внешней политики Российской Федерации (утв. Президентом РФ 12.02.2013) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_142236/ [Accessed: 30th March 2019].

Концепция. Концепция Стратегии Кибербезопасности Российской Федераци [Проект], 2013 [Online]. Available: http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf [Accessed: 27th February 2019].

КПСС. Программа коммунистической партии советского союза. Принята XXII съездом КПСС, 1961 [Online] Available: http://leftinmsu.narod.ru/polit_files/books/III_program_KPSS_files/056.htm [Accessed: 4th December 2018].

Kremlin.ru. Президенту представлен План обороны Российской Федерации 29 января 2013 года [Online]. Available: http://www.kremlin.ru/events/president/news/17385 [Accessed: 12th February 2019].

Министерство иностранных дел Российской Федерации. (2018a) Выступление Министра иностранных дел России С.В.Лаврова на 73-й сессии Генеральной Ассамблеи ООН, Нью-Йорк, 28 сентября 2018 года [Online]. Available: http://www.mid.ru/web/guest/general_assembly/-/asset_publisher/lrzZMhfoyRUj/content/id/3359296 [Accessed: 14th May 2019].

Министерство иностранных дел Российской Федерации. (2018b) О принятии Генассамблеей ООН российской резолюции по международной информационной безопасности. 7.12.2018 [Online]. Available: http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/3437775 [Accessed: 6th May 2019].

Министерство иностранных дел Российской Федерации. (2018c) О принятии Генассамблеей ООН российской резолюции по противодействию информационной преступности, 18.12.2018 [Online]. Available: http://www.mid.ru/web/guest/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCU-Tiw2pO53/content/id/3449030 [Accessed: 14th May 2019].

Министерство иностранных дел Российской Федерации. Об итогах голосования в Генассамблее ООН по российскому проекту резолюции по противодействию киберпреступности, 30.12.2019 [Online]. Available: https://www.mid.ru/organs/-/asset_publisher/AfvTBPbEYay2/content/id/3988579 [Accessed: 6th January 2020].

Министерство обороны Российской Федерации. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве, 2011 [Online]. Available: http://ens.mil.ru/files/morf/Strategy.doc [Accessed: 30th January 2019].

Минкомсвязь. Качество связи [Online]. Available: https://geo.minsvyaz.ru/#/-1/-1/12/60.166891999990966/24.943592000000006/4 [Accessed: 14th April 2019].

Минкомсвязь. Минкомсвязь, ФСБ и Минобороны провели учения по защите российского сегмента интернета. 28 июля 2014 года [Online]. Available: https://digital.gov.ru/ru/events/31441/ [Accessed: 16th May 2019].

Минкомсвязь. Об утверждении Порядка централизованного управления сетью связи общего пользования [Проект] 23 мая 2019 г. [Online]. Available: https://regulation.gov.ru/projects#npa=91558 [Accessed: 15th May 2019].

Минкомсвязь. Единая информационнотелекоммуникационная инфраструктура органов власти [Online]. Available: https://digital.gov.ru/uploaded/presentations/prezentvopros-2tebenkovedinaya-inform-telekinfr.pdf [Accessed: 15th April 2019].

Минкомсвязь. Единую сеть передачи данных в 2016 году будут использовать 14 госорганов, 20 января 2016 [Online]. Available: https://digital.gov.ru/ru/events/34535/ [Accessed: 15th April 2019].

Минкомсвязь. Система межведомственного электронного взаимодействия (СМЭВ) [Online]. Available: https://digital.gov.ru/ru/activity/directions/49/ [Accessed: 15th April 2019].

НАМИБ. Устав Национальной Ассоциации международной информационной безопасности Протокол № 1 от «10» апреля 2018 г [Online]. Available: http://namib.online/wp-content/uploads/2018/11/Ustav_NAMIB.pdf [Accessed: 2nd January 2020].

ОДКБ. Протокол О взаимодействии государств – членов Организации Договора о коллективной безопасности по противодействию преступной деятельности в информационной сфере, от 23 декабря 2014 года [Online]. Available: http://base.spinform.ru/show_doc.fwx?rgn=77790 [Accessed: 25th February 2019].

ОДКБ. Стратегия коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года. от 14 октября 2016 года [Online]. Available: http://odkb-csto.org/documents/detail.php?ELEMENT_ID=8382 [Accessed: 25th February 2019].

Основы. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (Утверждены Президентом Российской Федерации В.Путиным 24 июля 2013 г., № Пр-1753) [Online]. Available: http://www.scrf.gov.ru/security/information/document114/ [Accessed: 30th March 2019].

Основы. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (Утверждены Президентом Российской Федерации В.Путиным 24 июля 2013 г., № Пр-1753) [Online]. Available: http://www.scrf.gov.ru/security/information/document114/ [Accessed: 30th March 2019].

Основные направления. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (утв. Президентом РФ 03.02.2012 N 803) [Online]. Available: http://www.scrf.gov.ru/security/information/document113/ [Accessed: 18th April 2019].

Поручение Президента РФ от 15.11.2011 N Пр-3400 Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов на период до 2020 года [Online]. Available: https://www.garant.ru/products/ipo/prime/doc/70041358/ [Available: 13th May 2019].

Послание Президента РФ Федеральному Собранию от 10.05.2006 [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_60109/#dst0 [Accessed: 27th March 2019].

Послание Президента РФ Федеральному Собранию от 01.03.2018 [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_291976/ [Accessed: 27th March 2019].

Посольство России в Республике Гана. Статья спецпредставителя Президента Российской Федерации по вопросам международного сотрудничества в области информационной безопасности, Посла по особым поручениям МИД России А.В.Крутских, опубликованная в газете "Коммерсант" 27 марта 2019 года [Online]. Available: https://ghana.mid.ru/ru/press-centre/news/statya_spetspredstavitelya_prezidenta_rossiyskoy_federatsii_po_voprosam_mezhdunarodnogo_sotrudniches/ [Accessed: 8th May 2019].

Постановление Правительства РФ от 28.01.2002 N 65 (ред. от 09.06.2010) "О федеральной целевой программе "Электронная Россия (2002 - 2010 годы)" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_90180/ [Accessed: 10th April 2019].

Постановление Правительство Российской Федерации от 28 января 2002 г. №65 "ФЦП «Электронная Россия (2002–2010 годы)" [Online]. Available: http://minsvyaz.ru/ru/activity/programs/6/ [Accessed: 4th March 2019].

Постановление Правительства РФ (2004a) от 30.06.2004 N 320 (ред. от 25.09.2018) "Об утверждении Положения о Федеральном агентстве связи" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_48289/ [Accessed: 8th May 2019].

Постановление Правительства РФ (2004b) от 17.06.2004 N 292 (ред. от 25.09.2018) "О Федеральном агентстве по печати и массовым коммуникациям" [Online]. Available: https://base.garant.ru/187125/ [Accessed: 22 January 2018].

Постановление Правительства РФ от 02.06.2008 N 418 (ред. от 07.02.2019) "О Министерстве цифрового развития, связи и массовых коммуникаций Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_77387/ [Accessed: 8th May 2019].

Постановление Правительства РФ (2009a) от 16.03.2009 N 228 (ред. от 28.02.2019) "О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций" (вместе с "Положением о Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций") [Online]. Available: https://base.garant.ru/195117/ [Accessed: 6th May 2019].

Постановление Правительства Российской Федерации (2009b) от 25 декабря 2009 г. № 1088 (В редакции от 02.02.2019 № 77) Положение о государственной автоматизированной информационной системе "Управление" [Online]. Available: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102134940 [Accessed: 13th May 2019].

Постановление Правительства РФ от 15.04.2014 N 313 (ред. от 29.03.2019) "Об утверждении государственной программы Российской Федерации "Информационное общество" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_162184/ [Accessed: 15th May 2019].

Постановление Правительства Российской Федерации от 27 ноября 2015 г. N 1278 О федеральной информационной системе стратегического планирования и внесении изменений в Положение о государственной автоматизированной информационной системе "Управление" [Online]. Available: http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102134940&backlink=1&&nd=102383211 [Accessed: 13th May 2019].

Постановление Правительства РФ (2018a) от 8 февраля 2018 г. № 127 Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений (с изменениями от 13 апреля 2019 г.) [Online]. Available: https://fstec.ru/component/attachments/download/1917 [Accessed: 15th May 2019].

Постановление Правительства РФ (2019a) от 2 марта 2019 г. N 234 "О системе управления реализацией национальной программы Цифровая экономика Российской Федерации" [Online]. Available: https://base.garant.ru/72190034/ [Accessed: 6th May 2019].

Постановление Правительства Российской Федерации от 30.04.2019 № 528 "Об утверждении Правил предоставления из федерального бюджета субсидии на создание и функционирование Центра мониторинга и управления сетью связи общего пользования, а также создание, эксплуатацию и развитие информационной системы мониторинга и управления сетью связи общего пользования" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_324051/ [Accessed: 17th May 2019].

Постоновление Совета Безопасности Республики Беларусь от 18 марта 2019 № 1 "О Концепции информационной безопасности Республики Беларусь" [Online]. Available: http://president.gov.by/uploads/documents/2019/1post.pdf [Accessed: 2nd April 2019].

Правительственная комиссия. (2017a) План мероприятий по направлению "Информационная инфраструктура" программы "Цифровая экономика Российской Федерации" (утв. Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 18.12.2017 N 2)) [Online]. Available: http://static.government.ru/media/files/DAMotdOImu8U89bhM7lZ8Fs23msHtcim.pdf [Accessed: 16th May 2019].

Правительственная комиссия. (2017b) План мероприятий по направлению ”Информационная безопасность” программы ”Цифровая экономика Российской Федерации” (утв. Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 18.12.2017 N 2)) [Online]. Available: http://static.government.ru/media/files/AEO92iUpNPX7Aaonq34q6BxpAHCY2umQ.pdf [Accessed: 16th May 2019].

Правительство Российской Федерации. Заседание президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам, 24 декабря 2018 [Online]. Available: http://government.ru/news/35168/ [Accessed: 8th May 2019].

Правительство Российской Федерации. (2015a) Соглашение между Правительством Российской Федерацией и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности, от 30 апреля 2015 г. N 788-р [Online]. Available: http://static.government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf [Accessed: 26th February 2019].

Правительство Российской Федерации. Временные правила администрирования домена gov.ru 2018. [Online]. Available: http://www.gov.ru/main/rsnet/page541.html. [Accessed 11 January 2018].

Правительство Российской Федерации. О «дорожных картах» по направлениям программы «Цифровая экономика Российской Федерации». 9 января 2018 [Online]. Available: http://government.ru/orders/selection/401/30895/ [Accessed: 16th May 2019].

Правительство Российской Федерации. Утверждён план мероприятий по направлению «Кадры и образование» программы «Цифровая экономика Российской Федерации» 21 февраля 2018 [Online]. Available: http://government.ru/news/31428/ [Accessed: 22 March 2018].

Правительство Российской Федерации. Информация администрации сети RSNet [Online]. Available: http://www.gov.ru/main/page5.html [Accessed: 15th April 2019].

Президент Российской Федерации. Выступление на совещании руководящего состава Вооруженных Сил Российской Федерации, 20 ноября 2000 года [Online]. Available: http://kremlin.ru/events/president/transcripts/21119 [Accessed: 19th November 2018].

Президент РФ 28 сентября 2006 г. № Пр-1649 Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз техногенного, природного характера и террористических актов [Online]. Available: https://base.garant.ru/198664/ [Accessed: 13th May 2019].

Президиум Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 24 декабря 2018 года “Паспорт национальной программы «Цифровая экономика Российской Федерации».” [Online]. Available: http://static.government.ru/media/files/urKHm0gTPPnzJlaKw3M5cNLo6gczMkPF.pdf [Accessed: 16th May 2019].

Приказ министерства связи и массовых коммуникаций Российской Федерации от 16 апреля 2014 г. N 83 Об утверждении правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. часть iii. [Online]. Available: https://rulaws.ru/acts/Prikaz-Minkomsvyazi-Rossii-ot-16.04.2014-N-83/ [Accessed: 14th May 2019].

Приказ Минкомсвязи России от 12.12.2016 N 645 ”Об утверждении Правил применения оборудования систем коммутации, включая программное обеспечение, обеспечивающего выполнение установленных действий при проведении оперативно-розыскных мероприятий. Часть I.” (Зарегистрировано в Минюсте России 13.01.2017 N 45201) [Online]. Available: https://digital.gov.ru/ru/documents/5413/ [Accessed: 9th May 2019].

Приказ Министерства связи и массовых коммуникаций Российской Федерации от 16.08.2017 г. № 422 ”О порядке функционирования и подключения к федеральной государственной информационной системе ”Федеральный ситуационный центр электронного правительства” и признании утратившим силу приказа Министерства связи и массовых коммуникаций Российской Федерации от 1 июля 2014 г. № 184” [Online]. Available: https://rg.ru/2017/10/04/minsvyaz-prikaz422-site-dok.html [Accessed: 15th April 2019].

Приказ Министерства цифрового развития, связи и массовых коммуникаций оссийской Российской Федерации от 12.12.2019 № 839 ”Об утверждении графика проведения плановых учений” [Online]. Available: https://digital.gov.ru/ru/documents/7002/https://digital.gov.ru/ru/documents/7002/ [Accessed: 7th January 2020].

Приказ Министра обороны РФ от 11 февраля 2010 г. N 70 ”Об утверждении Положения об органах информационного обеспечения Вооруженных Сил Российской Федерации” [Online]. Available: http://base.garant.ru/55170392/ [Accessed: 13th May 2019].

Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. N 31 ”Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды” (с изменениями и дополнениями) [Online]. Available: https://base.garant.ru/70690918/ [Accessed: 6th May 2019].

Приказ Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. N 239 “Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации” (ред. от 9 август 2019) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_294287/ [Accessed: 6th January 2020].

Приказ Федеральной службы по техническому и экспортному контролю от 3 апреля 2018 г. N 55 ”Об утверждении Положения о системе сертификации средств защиты информации” [Online]. Available: http://ivo.garant.ru/#/document/71942006/paragraph/1:0 [Accessed: 8th May 2019].

Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31.07.2019 № 225 “Об утверждении Положения о Центре мониторинга и управления сетью связи общего пользования” [Online]. Available: http://publication.pravo.gov.ru/Document/View/0001201911250011 [Accessed: 7th January 2020].

Приказ ФСБ России от 24.07.2018 N 366 ”О Национальном координационном центре по компьютерным инцидентам” (вместе с ”Положением о Национальном координационном центре по компьютерным инцидентам”) (Зарегистрировано в Минюсте России 06.09.2018 N 52109) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_306334/ [Accessed: 18th April 2019].

Приказ федеральная служба безопасности российской федерации № 41821 23 марта 2016 года [Online]. Available: http://www.fsb.ru/files/PDF/prikaz_182.pdf [Accessed: 6th May 2019].

Приказ ФСО России от 07.09.2016 N 443 ”Об утверждении Положения о российском государственном сегменте информационно-телекоммуникационной сети ”Интернет” (Зарегистрировано в Минюсте России 14.10.2016 N 44039) [Online]. Available: http://www.gov.ru/rsnet/pr_fso_443_07092016.pdf [Accessed: 15th April 2019].

Путин, Владимир. Совещание по вопросам развития технологий в области искусственного интеллекта. Kremlin.ru, 30 мая 2019 года [Online]. Available: http://www.kremlin.ru/events/president/news/60630 [Accessed: 9th July 2019].

Распоряжение Правительства РФ (2008a) от 17.11.2008 N 1662-р ”О Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года” (вместе с "Концепцией долгосрочного социально-экономического развития Российской Федерации на период до 2020 года"): http://www.consultant.ru/cons/cgi/online.cgi?req=doc&n=82134&base=LAW&from=308069-1847&rnd=0.6960341791725004#0577375847182553 [Accessed: 13th May 2019].

Распоряжение Правительства РФ (2008b) от 6 мая 2008 г. N 632-р Концепция формирования в Российской Федерации электронного правительства до 2010 года [Online]. Available: http://www.garant.ru/products/ipo/prime/doc/93274/ [Accessed: 13th May 2019].

Распоряжениие Правительства Российской Федерации от 20 октября 2010 г. N 1815-р Государственная программа Российской Федерации "Информационное общество (2011-2020 годы)” [Online]. Available: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102142714 [Accessed: 11th April 2019].

Распоряжение Правительства РФ от 28 мая 2012 г. №856-р. О подписании Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности [Online]. Available: https://digital.gov.ru/ru/documents/3729/ [Accessed: 29th March 2019].

Распоряжение Правительства РФ от 01.11.2013 N 2036-р (ред. от 18.10.2018) ”Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года” [Online]. Available: https://digital.gov.ru/common/upload/Strategiya_razvitiya_otrasli_IT_2014-2020_2025.pdf [Accessed: 15th May 2019].

Распоряжение Правительства Российской Федерации от 30 апреля 2015 г. N 788-р О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности [Online]. Available: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=620700#0463235836450268 [Accessed: 29th May 2019].

Распоряжение Правительства РФ от 28.07.2017 N 1632-р Об утверждении программы ”Цифровая экономика Российской Федерации” [Online]. Available: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf [Accessed: 16th May 2019].

Распоряжение Правительства РФ от 17 декабря 2019 года №3074-р “Концепция создания цифровой аналитической платформы предоставления статистических данных” [Online]. Available: http://static.government.ru/media/files/4YejV8mvcCSeGWTg2kXprmthtNbWyfrU.pdf [Accessed: 7th January 2020].

СНГ. Концепция формирования информационного пространства Содружества Независимых Государств от 18 октября 1996 года [Online]. Available: http://www.cis.minsk.by/page.php?id=7548 [Accessed: 7th March 2019].

СНГ. Модельный закон «Об основах регулирования Интернета» Межпарламентская Ассамблея государств – участников Содружества Независимых Государств, Приложение к постановлению МПА СНГ от 16.05.2011 г. № 36-9 [Online]. Available: http://www.cikrf.ru/international/docs/mpa_modzakon.html [Accessed: 3rd April 2019].

СНГ. Концепция информационной безопасности государств-участников Содружества Независимых Государств в военной сфере, 4 июня 1999 года [Online]. Available: http://www.e-cis.info/page.php?id=21396 [Accessed: 25th February 2019].

СНГ. Решение о Концепции сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности и о Комплексном плане мероприятий по реализации Концепции сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности на период с 2008 по 2010 год [Online]. Available: http://www.e-cis.info/page.php?id=20229 [Accessed: 25th February 2019].

Совет Безопасности РФ. Заседание Совета Безопасности Российской Федерации по вопросу «О противодействии угрозам национальной безопасности Российской Федерации в информационной сфере» 1 октября 2014 года [Online]. Available: http://www.scrf.gov.ru/news/allnews/831/ [Accessed: 16th May 2019].

Совет Безопасности РФ. В аппарате Совета Безопасности РФ рассмотрены вопросы развития цифровой экономики с точки зрения обеспечения национальной безопасности. 30 июня 2017 года [Online]. Available: http://www.scrf.gov.ru/news/allnews/2245/ [Accessed: 8th May 2019].

Совет Безопасности РФ. Вопросы информационной безопасности при реализации национальной программы «Цифровая экономика России» обсуждены экспертами Совета Безопасности РФ. 29 октября 2018 года [Online]. Available: http://www.scrf.gov.ru/news/allnews/2493/ [Accessed: 8th May 2019].

Совет при Президенте Российской Федерации по стратегическому развитию и национальным проектам. Паспорт национальной программы «Цифровая экономика Российской Федерации» 24 декабря 2018 [Online]. Available: http://static.government.ru/media/files/urKHm0gTPPnzJlaKw3M5cNLo6gczMkPF.pdf [Accessed: 8th May 2019].

Совет Федерации Федерального Собрания Российской Федерации. Проект стратегии кибербезопасности России направлен на формирование цифрового суверенитета страны, 27 февраля 2013 [Online]. Available: http://council.gov.ru/events/news/14575/ [Accessed: 27th February 2019].

Стратегия. Стратегия развития информационного общества в Российской Федерации (утв. Президентом РФ 7 февраля 2008 г. № Пр-212) [Online]. Available: https://rg.ru/2008/02/16/informacia-strategia-dok.html [Accessed: 13th May 2019].

Указ Президента РФ от 20 октября 1993 г. N 1686 ”О совершенствовании деятельности межведомственных комиссий Совета безопасности Российской Федерации” [Online]. Available: https://base.garant.ru/5348225/ [Accessed: 8th May 2019].

Указ Президента РФ от 23.11.1995 N Пр-1694. “Концепция формирования и развития единого информационного пространства России и соответствующих государственных информационных ресурсов” [Online]. Available: http://lawru.info/dok/1995/11/23/n453820.htm [Accessed: 23rd March 2019].

Указ Президента Российской Федерации от 24 декабря 1998 года N 1637 ”Об утверждении составов межведомственных комиссий Совета Безопасности Российской Федерации” Российская газета" No. 248 30 декабря 1998.

Указ Президента РФ от 9 сентября 2000 г. N Пр-1895. ”Об утверждении Доктрины информационной безопасности Российской Федерации” [Online]. Available: http://base.garant.ru/182535/#ixzz4x5P8ZYEp [Accessed: 21st March 2019].

Указ Президента Российской Федерации от 14 июля 2003 г. N 774 Вопросы службы специальной связи и информации при Федеральной службе охраны Российской Федерации [Online]. Available:

http://www.agentura.ru/dossier/russia/fso/docs/polojeniespecvyaz/ [Accessed: 6th May 2019].

Указ Президента РФ (2004a) от 16.08.2004 N 1082 (ред. от 26.01.2019) ”Вопросы Министерства обороны Российской Федерации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_48879/ [Accessed: 9th May 2019].

Указ Президента РФ (2004b) от 16 августа 2004 г. N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю" (с изменениями и дополнениями) [Online]. Available: https://base.garant.ru/12136635/ [Accessed: 6th May 2019].

Указ Президента РФ (2004c) от 07.08.2004 N 1013 (ред. от 27.02.2018) ”Вопросы Федеральной службы охраны Российской Федерации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_48778/ [Accessed: 9th May 2019].

Указ Президента РФ от 17.03.2008 N 351 (ред. от 22.05.2015) ”О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_75586/ [Accessed: 6th May 2019].

Указ Президента РФ от 12 мая 2009 года № 536 (2009a). Об основах стратегического планирования в РФ [Online]. Available: http://lj.rossia.org/users/anticompromat/587675.html [Accessed: 26th March 2019].

Указ Президента РФ от 12 мая 2009 года N 537 (2009b). О Стратегии национальной безопасности Российской Федерации до 2020 года Указ Президента Российской Федерации [Online]. Available: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102129631 [Accessed: 21st March 2019].

Указ Президента РБ № 60 от 01.02.2010 “О мерах по совершенствованию использования национального сегмента сети Интернет” [Online]. Available: https://belzakon.net/Законодательство/Указ_Президента_РБ/2010/3321/скачать [Accessed: 2nd April 2019].

Указ Президента РФ от 05.02.2010 N 146 “О Военной доктрине Российской Федерации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_97325/ [Accessed: 30th March 2019].

Указ Президента РФ от 06.05.2011 N 590 (ред. от 25.07.2014) "Вопросы Совета Безопасности Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_113807/ [Accessed: 6th May 2019].

Указ Президента РФ от 25.05.2012 N 715 (ред. от 18.02.2019) ”Об утверждении состава Совета Безопасности Российской Федерации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_130204/ [Accessed: 8th May 2019].

Указ Президента РФ (2013a) от 23.07.2013 N 631 (ред. от 01.07.2014) "Вопросы Генерального штаба Вооруженных Сил Российской Федерации" (вместе с "Положением о Генеральном штабе Вооруженных Сил Российской Федерации") [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_149773/ [Accessed: 9th May 2019].

Указ Президента РФ (2013b) от 15 января 2013 г. № 31с “О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации” [Online]. Available: http://www.garant.ru/products/ipo/prime/doc/70199068/ [Accessed: 15th May 2019].

Указ Президента РФ 25 декабря 2014 г., № Пр-2976. Военная доктрина Российской Федерации [Online]. Available: http://base.garant.ru/70830556/ [Accessed: 21st March 2019].

Указ Президента РФ (2015a) от 31.12.2015 N 683 “О Стратегии национальной безопасности Российской Федерации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_191669/ [Accessed: 30th March 2019].

Указ Президента Российской Федерации (2015b) от 22.05.2015 № 260 ”О некоторых вопросах информационной безопасности Российской Федерации” [Online]. Available: http://www.consultant.ru/document/Cons_doc_LAW_179963/ [Accessed 11 January 2018].

Указ Президента РФ от 5 декабря 2016 г. N 646 “Об утверждении доктриныинформационной безопасности Российской Федерации” [Online]. Available: http://rulaws.ru/president/Ukaz-Prezidenta-RF-ot-05.12.2016-N-646/ [Accessed: 21st March 2019.]

Указ Президента РФ от 30.11.2016 N 640 (2016a) “Об утверждении Концепции внешней политики Российской Федерации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_207990/ [Accessed: 30th March 2019].

Указ Президента РФ от 05.12.2016 N 646 (2016b) “Об утверждении Доктрины информационной безопасности Российской Федерации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_208191/ [Accessed: 30th March 2019].

Указ Президента РФ (2016c) от 01.12.2016 N 642 "О Стратегии научно-технологического развития Российской Федерации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_207967/ [Accessed: 16th May 2019].

Указ Президента РФ (2017a) от 09.05.2017 N 203 “О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы” [Online]. Available: https://www.garant.ru/products/ipo/prime/doc/71570570/ [Accessed: 15th May 2019].

Указ Президента РФ (2017b) от 22 декабря 2017 г. № 620 “О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации” [Online]. Available: https://www.garant.ru/products/ipo/prime/doc/71740924/ [Accessed: 18th April 2019].

Указ Президента Российской Федерации (2018a) от 7 мая 2018 г. N 204 “О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года” [Online]. Available: https://rg.ru/2018/05/08/president-ukaz204-site-dok.html [Accessed: 26th March 2019].

Указ Президента РФ (2018b) от 10 ноября 2018 г. N 648 "Об утверждении состава Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям" [Online]. Available: https://base.garant.ru/72100350/ [Accessed: 8th May 2019].

Указ Президента РФ (2018c) от 29 декабря 2018 г. № 771 ”Состав научного совета при Совете Безопасности Российской Федерации” [Online]. Available: http://www.scrf.gov.ru/about/NS_spis_organ/sost_NS/ [Accessed: 8th May 2019].

Указ Президента РФ от 10.10.2019 N 490 “О развитии искусственного интеллекта в Российской Федерации” (вместе с ”Национальной стратегией развития искусственного интеллекта на период до 2030 года”) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_335184/ [Accessed: 7th January 2020].

Федеральный закон от 03.04.1995 N 40-ФЗ (ред. от 07.03.2018) ”О федеральной службе безопасности” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_6300/ [Accessed: 9th May 2019].

Федеральный закон от 31.05.1996 N 61-ФЗ (ред. от 3.8.2018) “Об обороне” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_10591/ [Accessed: 29th March 2019].

Федеральный закон от 26.02.1997 N 31-ФЗ (ред. от 18.12.2018) “О мобилизационной подготовке и мобилизации в Российской Федерации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_13454/ [Accessed: 26th March 2019].

Федеральный конституционный закон от 30.05.2001 N 3-ФКЗ (ред. от 03.07.2016) “О чрезвычайном положении” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_31866/ [Accessed 10 June 2018].

Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 05.12.2017) “О связи” [Online]. Available: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=284294&fld=134&dst =417,0&rnd=0.1557327116187115#0 [Accessed 11 January 2018].

Федеральный конституционный закон от 30.01.2002 N 1-ФКЗ (ред. от 01.07.2017) “О военном положении” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_35227/ [Accessed 10 June 2018].

Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 18.03.2019) ”Об информации, информационных технологиях и о защите информации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_61798/ [Accessed: 8th May 2019].

Федеральный закон от 29 апреля 2008 г. N 57-ФЗ ”О порядке осуществления иностранных инвестиций в хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства” [Online]. Available: http://ivo.garant.ru/#/document/12160212/paragraph/3780:0 [Accessed: 14th May 2019].

Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 05.10.2015) ”О безопасности” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_108546/ [Accessed: 6th May 2019].

Федеральный закон от 03.12.2011 N 382-ФЗ (ред. от 5 июля 2018) ”О государственной информационной системе топливно-энергетического комплекса” [Online]. Available: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102152618 [Accessed: 17th April 2019].

Федеральный закон от 28.07.2012 N 139-ФЗ (последняя редакция) ”О внесении изменений в Федеральный закон ”О защите детей от информации, причиняющей вред их здоровью и развитию” и отдельные законодательные акты Российской Федерации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_133282/ [Accessed: 14 May 2019].

Федеральный закон (2013a) от 28 декабря 2013 г. N 398-ФЗ ”О внесении изменений в Федеральный закон ”Об информации, информационных технологиях и о защите информации” [Online]. Available: https://rg.ru/2013/12/30/extrem-site-dok.html [Accessed: 14th May 2019].

Федеральный закон (2013b) от 21 декабря 2013 г. N 369-ФЗ ”О внесении изменений в Федеральный закон ”Об оперативно-розыскной деятельности” и статью 13 Федерального закона ”О федеральной службе безопасности” [Online]. Available: https://rg.ru/2013/12/25/deatelnost-dok.html [Accessed: 14th May 2019].

Федеральный закон (2014a) от 28.06.2014 N 172-ФЗ (ред. от 31.12.2017) “О стратегическом планировании в Российской Федерации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_164841/ [Accessed: 26th March 2019].

Федеральный закон (2014b) от 05.05.2014 N 97-ФЗ (ред. от 29.07.2017) ”О внесении изменений в Федеральный закон ”Об информации, информационных технологиях и о защите информации” и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_162586/ [Accessed: 14th May 2019].

Федеральный закон (2014c) от 14.10.2014 N 305-ФЗ (последняя редакция) "О внесении изменений в Закон Российской Федерации "О средствах массовой информации" [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_169740/ [Accessed: 14th May 2019].

Федеральный закон (2014d) от 30.12.2015 N 464-ФЗ ”О внесении изменений в Закон Российской Федерации ”О средствах массовой информации” и Кодекс Российской Федерации об административных правонарушениях” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_191539/ [Accessed: 14th May 2019].

Федеральный закон (2014e) от 21 июля 2014 г. N 242-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях" [Online]. Available: http://ivo.garant.ru/#/document/70700506/paragraph/1:0 [Accessed: 14th May 2019].

Федеральный закон (2016a) от 06.07.2016 N 374-ФЗ ”О внесении изменений в Федеральный закон ”О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности” (последняя редакция) [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_201078/ [Accessed: 9th May 2019].

Федеральный закон (2016b) от 23.06.2016 N 208-ФЗ ”О внесении изменений в Федеральный закон ”Об информации, информационных технологиях и о защите информации” и Кодекс Российской Федерации об административных правонарушениях” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_200019/ [Accessed: 29th May 2019].

Федеральный закон (2016c) от 06.07.2016 N 375-ФЗ (последняя редакция) ”О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_201087/ [Accessed: 14th May 2019].

Федеральный закон (2017a) от 26.07.2017 N 187-ФЗ “О безопасности критической информационной инфраструктуры Российской Федерации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_220885/ [Accessed: 21st March 2019].

Федеральный закон (2017b) от 29 июля 2017 года № 276-ФЗ ”О внесении изменений в Федеральный закон ”Об информации, информационных технологиях и о защите информации” [Online]. Available: https://rg.ru/2017/07/30/fz276-site-dok.html [Accessed: 14th May 2019].

Федеральный закон (2017c) от 29.07.2017 N 241-ФЗ ”О внесении изменений в статьи 10.1 и 15.4 Федерального закона ”Об информации, информационных технологиях и о защите информации” [Online].

Федеральный закон от 01.05.2019 № 90-ФЗ ”О внесении изменений в Федеральный закон ”О связи” и Федеральный закон ”Об информации, информационных технологиях и о защите информации” [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_323815/ [Accessed: 8th May 2019].

ШОС. Заявление глав государств – членов Шанхайской организации сотрудничество по международной информационной безопасности. Г. Шанхай, 15 июня 2006 года [Online]. Available: http://rus.sectsco.org/ [Available: 2nd April 2019].

ШОС. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. 16 июня 2009 года. Екатеринбург. [Online]. Available: https://base.garant.ru/2571379/ [29th March 2019].

ШОС. Астанинская декларация глав государств – членов Шанхайской организации сотрудничества 9 июня 2017 года [Online]. Available: http://kremlin.ru/supplement/5206 [Accessed: 10th May 2019].

Dictionaries

Большая советская энциклопедия: в 30 т. 3-е изд. (БСЭ) / Гл. ред. А. М. Прохоров. М.: Советская Энциклопедия., 1969 – 1978 [Online]. Available: https://dic.academic.ru/dic.nsf/bse/65510/Асимметрия [Accessed: 22nd March 2019].

Википедия. [Online]. Available: https://ru.wikipedia.org/ [Accessed: 8th May 2019].

Военный энцикаопедический словарь. М.: Воениздат, 2007 [Online]. Available: http://encyclopedia.mil.ru/encyclopedia/dictionary/list.htm [Accessed: 5th April 2019].

Военный Энциклопедический Словарь, Том. I. М.: Военное издательство, 1983.

Военный Энциклопедический Словарь, Том. I. М.: Военное издательство, 1986.

Военная Энциклопедия в восьми томах, Том. I. М.: Военное издательство, 1997.

Военная энциклопедиа, Том. III. М.: Военное издательство, 1995.

Военный энциклопедический словарь в 2 томах (ВЭС). / Редкол.: А. П. Горкин, В. А. Золотарев, В. М. Карев и др. М: Большая Российская энциклопедия; Рипол классик, 2001.

Гречко, А. А., Огарков, Н. В. (Гл. ред.) Советская военная энциклопедия в восьми томах (СВЭ). М.: Военное издательство Министерства обороны СССР, 1976—1980.

Ожегов, С.И., Шведова, Н.Ю. Толковый словарь русского языка. 4-е изд., доп. М.: ООО «А ТЕМП», 2006 [Online]. Available: https://dic.academic.ru/dic.nsf/ogegova/ [Accessed: 22nd March 2019].

Прохоров, А. М. (Гл. ред.) Большой энциклопедический словарь, 2000 [Online]. Available: https://dic.academic.ru/contents.nsf/enc3p/ [March 17th 2019].

Рогозин, Д. О. (общ. Ред.) Война и мир в терминах и определениях [Online]. Available: http://www.voina-i-mir.ru [Accessed: 5th April 2019].

Соловцов, Н. Е., Шлычков, В. Р. (Общ. ред.) Энциклопедия ракетных войск стратегического назначения. М-во обороны РФ. М.: Белгород, 2009 [Online]. Available: http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=12536@morfDictionary [March 17th 2019].

Databases:

Central Intelligence Agency Library [Online]. Available: https://www.cia.gov/library/readingroom/historical-collections [Accessed: 5th December 2018].

EastView [Online]. Available: https://www.eastview.com/ [Accessed: 16th July 2019].

Electronic Dissertation Library (Russian State Library) [Online]. Available: http://sigla.rsl.ru/search.jsp?e=Cp1251&c=14i&i18n=ru&s= [Accessed: 5th December 2018].

University of Texas Libraries [Online] Available: https://guides.lib.utexas.edu/c.php?g=524005&p=3584595 [Accessed: 5th December 2018].

Wilson Center – Digital Archive [Online]. Available: https://digitalarchive.wilsoncenter.org/collection/37/end-of-the-cold-war/2 [Accessed: 5th December 2018].

Гарант.ру [Online], Available: https://base.garant.ru/ [Accessed: 16th July 2019].

КонсультантПлюс [Online]. Available: http://www.consultant.ru/ [Accessed: 16th July 2019].

Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации [Online]. Available: https://digital.gov.ru/ru/ [Accessed: 16th July 2019].

Научная электронная библиотека [Online]. Available: https://elibrary.ru/defaultx.asp [Accessed: 16th July 2019].

Официальный интернет-портал правовой информации [Online]. Available: http://pravo.gov.ru/ [Accessed: 16th July 2019].

Правителство Российскоий Федерации [Online]. Available: http://government.ru/ [Accessed: 16th July 2019].

Президента России [Online]. Available: http://www.kremlin.ru/ [Accessed: 16th July 2019].

Система обеспечения законодательной деятельности [Online]. Available: https://sozd.duma.gov.ru/ [Accessed: 16th July 2019].

Совет Безопасности Российской Федерации [Online]. Available: http://www.scrf.gov.ru [Accessed: 16th July 2019].

Федеральная служба безопасности Российской Федерации [Online]. Available: http://www.fsb.ru/ [Accessed: 16th July 2019].

Федеральная служба по техническому и экспортному контролю [Online]. Available: https://fstec.ru/ [Accessed: 16th July 2019].

National Defence University
PL 7, 00861 HELSINKI
FINLAND

Tel. +358 299 800

www.mpkk.fi

ISBN 978-951-25-3131-8 (pbk.)
ISBN 978-951-25-3132-5 (PDF)
ISSN 2342-9992 (print)
ISSN 2343-0001 (web)

Puolustusvoimat
The Finnish Defence Forces