FINNISH DEFENCE STUDIES 23

The Military Strategic Effects of the Russian National Segment of the Internet

Juha Kukkola

Finnish National Defence University 2023

FINNISH DEFENCE STUDIES 23

The Military Strategic Effects of the Russian National Segment of the Internet

Juha Kukkola

National Defence University
Helsinki 2023
FINLAND

Finnish Defence Studies is published under the auspices of the National Defence University, and the contributions reflect the fields of research and teaching of the University.

Translation by Lingsoft

ISBN 978-951-25-3328-2 (pbk.)
ISBN 978-951-25-3329-9 (pdf)
ISSN: 0788-5571

Finnish Defence Studies in open access pdf-format: *http://bit.ly/1S57Rta*

Published by

NATIONAL DEFENCE UNIVERSITY
PO. Box 7
FI-00861 Helsinki
FINLAND

www.mpkk.fi

PunaMusta Oy
Joensuu 2023

Summary

The aim of this thesis is to develop a theoretical and conceptual basis for studying structural cyber asymmetry and to examine the strategic effects of the Russian national segment of the internet. This topic is important because cyberspace is one of the domains through or into which force can be directed to achieve political ends. Methodologically this thesis is a theory-driven qualitative case study based on content analysis and abduction.

This thesis demonstrates that cyber power can be studied as a means to shape cyberspace. This approach offers a new perspective on studying the effects of national cyber strategies and the asymmetric power relationships between states. Freedom of action, common situation picture, command and control, and resilience are useful concepts for studying the relationship between closed and open national networks. These four concepts can be combined with the model of a national information security and defence system of systems to examine and compare the management and control of national networks in a novel way which takes into account the way the governance of the internet is currently changing.

This thesis argues that the structural cyber asymmetry caused by the creation of a national segment of the internet sets significant premises and frames of reference on the states' use of force in cyberspace. Structural cyber asymmetry also shapes the effects of the use force. The construction of a national segment of the internet can be compared to strategic level preparation of a cyber battlefield. The Russian national segment of the internet can, if successfully completed, change the global balance of power in cyberspace. However, the national segment, as currently envisioned, has serious vulnerabilities. Moreover, its construction will increase the interdependencies between domains, great power competition, risks of escalation, and the risk of preventive or even pre-emptive cyber strikes. The national segment of the internet increases the fragmentation of cyberspace and strengthens the norm of cyber sovereignty.

Key words: *Russia, strategy, cyber warfare, internet, asymmetry*

Contents

KEY CONCEPTS

The chapter, in which the concept is presented, derived from previous studies or defined, is marked after the definition of each concept. If the definition of the concept is unique, the references are provided.

Closed national network: A state-controlled part of cyberspace, which can be technically disconnected from the global internet but still remain capable of functioning normally with regard to services of critical importance to the nation. Its opposite is an open national network, which is not directly controlled by the state. As a rule, an open network cannot be disconnected from the global cyberspace without special preparations or serious disruptions in the critical functions of society and the economy. (Chapter 2.4)

Conflict escalation control: Regulating the intensity of the conflict that has begun by the threat or use of force in or through cyberspace with an aim to make the adversary stop using force in a manner advantageous to the actor itself and serving it in the pursuit of its political objectives, while preventing unintentional or accidental escalation. (Chapter 2.2)

Conflict prevention: Conducted as part of the state security policy, neutralisation of potential threats through any means available, without needing to resort to the threat or use of direct armed force. (Chapter 2.2)

Cyber battlefield: A military domain that can be divided into cyber battlefields to achieve tactical, operational and strategic goals. The division follows the form, objectives and goals of the operations and has not been laid down in advance. (Chapter 2.1)

Cyber deterrence: Efforts to persuade a potential opponent to refrain from using force in or from cyberspace or other space by threatening with an unbearable punishment, denying potential gains or otherwise affecting the opponent's cost-benefit calculations with cyberspace-related capabilities. (Chapter 2.2)

Cyber operation: Cyber operations can be divided into offensive and defensive operations and network maintenance operations. Offensive operations are actions carried out in or through the cyber environment with an aim to harm, i.e., to disrupt, deny, degrade or destroy, information systems or the confidentiality, integrity or availability of information contained therein. They include cyber intelligence operations to acquire information or enable the acquisition of information. Defensive operations refer to actively protecting critical information networks and information systems of a state, society or armed forces and the information contained therein from specific hostile operations. Maintenance operations are aimed at securing the general maintenance of the confidentiality, integrity and availability of state, social and/or military systems. (Chapter 2.2)

Cyber power: The ability that empowers a state to influence other states in or through cyberspace and to control and shape cyberspace to its advantage according to its preferences. (Chapter 2.1)

Cyber power resources: Cyber power resources or potential are resources or potential of mainly technological, scientific, economic, normative, doctrinal, organisational or human (professional) nature. They gain their character through their use, environment and objectives. (Chapter 2.1)

Cyberspace: A man-made and governed global space within the information environment whose distinct and unique character is based on the use of systems and services using information technology that form an interdependent networked operating environment with the purpose of creating, modifying, exchanging, and exploiting information via interconnected networks using information-communication technologies. (Chapter 2.1)

Cyber strategy: The cyber strategy means continuous planning of the use of cyber power, preparing for and using it by military and non-military means in the cyber environment to achieve national security objectives. (Chapter 2.2)

Information: Separate, non-organised facts (data) that have been set in a context and that have been structured and thus gained significance.[1]

Information environment: The aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[2] The information environment is divided into cyberspace, socio-cognitive space, information-physical space and electromagnetic space. (Chapter 2.1)

Information operations: "Operations in which, by producing, modifying or restricting access to information, the targeted entity's perceptions or activities are changed through an information and opinion environment".[3] Information operations can be implemented through the cyber domain and supported by cyber operations. (Chapter 2.2)

Information security: Usually a property associated with the confidentiality, integrity and availability of information. In this paper, information security is understood in a state-centric manner, i.e., as protecting a state against external and internal information threats, which secures the sovereignty, regional integrity, economic development, defence and security of the state. By their nature information threats can be either psychological, i.e., aimed to affect the mind, or technological, i.e., aimed against systems, devices and information stored in them. (Chapter 3.1)

---

[1] Rowley, Jennifer: The Wisdom Hierarchy: Representations of the DIKW Hierarchy. *Journal of Information Science*, Vol. 33, No. 2 (2007), pp. 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), pp. 479–493.

[2] The United States Department of Defense (U.S. DoD): *Joint Publications 3-12: Cyberspace Operations, 8th June 2018*, pp. viii. [https://fas.org/irp/doddir/dod/jp3_12.pdf], visited 17.10.2019.

[3] Sanastokeskus TSK: *Kyberturvallisuuden sanasto TSK 52*. Sanastokeskus TSK, Helsinki, 2018, pp. 29.

Military exploitation of structural cyber asymmetry: The use of coercion and brute force in cyberspace and the ability to wield such influence in or through cyberspace that forces the adversary to stop resisting against their own will, or to deny the corresponding influence on their own systems in conflict or war. (Chapter 2.2)

National segment of the internet: A manifestation of the national information security and defence system in cyberspace and an applied representation of a closed national network. Consists of the internet infrastructure, services and management systems, the necessary technological foundations and other information networks and systems which reside on a state's territory and under its sovereign jurisdiction. (Chapter 3.3)

National information security and defence system: A system of systems that provides information security for a state. A unified collection of government tools and means for delineating, building, managing and securing the national information space in the information environment. The system mobilises power from the information society and the economy for state use. The characteristics of the state concerned shape the more detailed structure, operation and objective of the system. In this paper, the system has been derived from projects aimed at managing the Russian state's national information space, the ideas of Russian information theoreticians and the characteristics of the Russian state. (Chapter 3.3)

Strategic impact: Strategic impact changes the operating environment or characteristics of states so that it tips the balance of power between them with regard to a potential future conflict. Strategic impact is related, on the one hand, to a change in the preconditions for the use of force and, on the other hand, to a change related to reaching the objective set for the use of force in the target system (state) at the strategic level. (Chapter 2.2)

Strategic level: The level of government decision-making related to the pursuit of national security objectives. The military strategic level is the level of decision-making in military leadership related to the pursuit of potential or actual objectives of war. (Chapter 1)

Structural cyber asymmetry: A characteristic of cyberspace that arises between two or more actors when the structure and rules of cyberspace are shaped so that one actor gains a disproportionate and exploitable offensive and defensive advantage over the others. (Chapter 2.4)

West: 'West' refers to the concept '*the West*' used in the English language, denoting the United States of America and its political and military allies, who opposed the Communist Soviet Union and its allies during the Cold War from the late 1940s until 1989/1991 for ideological, economic and military strategic reasons. In the period after the Cold War, the West and Western refer to the United States, Canada, Western Europe, in particular NATO and the European Union with its Member States, as well as Japan, South Korea, Australia and New Zealand. The West can be interpreted as an alliance system of the United States, a liberal democratic community of values, or in relation to the enemy image held by a certain political community, including Russia, China and radical political Islam. It can also be interpreted as a group of states that

share a certain understanding of the nature of war and approach to warfare. The term also refers to academic circles writing in English-language journals published by institutions located in the above-mentioned countries.[4]

[4] O'Hagan, Jacinta: *Conceptualizing the West in International Relations: From Spengler to Said*. Palgrace, New York, 2002, pp. 6–9; Kilcullen, David: *The Dragons and the Snakes: How the Rest Learned to Fight the West*. Oxford University Press, Oxford, 2020, pp. 7–8.

1. Introduction

"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."
M. Maigret: Treatise on Preserving the Security of States by Means of Fortresses, Paris, 1725[5]

"The information space has become one of the theatres of military operations."
Russian Defence Minister Sergei Shoigu, 25 March 2020[6]

The Russian Federation is developing a Russian national segment of the internet (*rossiĭskiĭ segment seti interneta*)[7], that can be disconnected from the global internet when certain threats are realised.[8] The project has been included in Russia's National Programme of Digital Economy adopted in 2017, aimed at achieving 'digital sovereignty' by 2024.[9] As a rule, the programme is being implemented through legislative control and acquisitions by state-owned companies, as a result of which the Russian internet, developed by civil society and business actors, is being brought under increasingly strict state control.[10] If realised, the Russian national segment of the internet can have significant political, economic and cultural impacts. As the military strategic effects of building a national segment of the internet are still largely unexplored and unknown, it is an interesting research topic from the perspective of strategic research.

The Russian project to build a national segment of the internet is linked to the fragmentation of cyberspace, which has also been referred to as 'balkanization' or 'splintering'. Fragmentation has been studied in terms of the *governance* of cyberspace since the 2010s.[11] However, the earliest discussions on the topic date back to the 1990s.[12] Chris Demchak and Peter Dombrovski, who approached the topic from the point of view of military science, called the final outcome of fragmentation the '*Cybered Westphalian Age*'. According to them, states react to threats stemming from cyberspace by creating borders in cyberspace along their geographic boundaries and by establishing

---

[5] Reference to the original in: Guerlac, H.: Vauban: The Impact of Science of War. In *Makers of Modern Strategy from Machiavelli to the Nuclear Age*. Paret, Peter (ed.). Clarendon Press, Oxford, 1990, pp. 64–90, 87.
[6] РИА новости: Шойгу рассказал, как прозападная оппозиция "лезет" на военные объекты. *РИА новости*, 25.3.2020. [https://ria.ru/20200325/1569119235.html], visited 6.5.2020.
[7] 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.
[8] ФЗ-90: 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"*. [http://www.consultant.ru/document/cons_doc_LAW_323815/], visited 8.5.2019.
[9] РП-1632: Распоряжение Правительства РФ от 28.07.2017 N 1632-р *"Об утверждении программы "Цифровая экономика Российской Федерации"*. [http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf], visited 23.01.2018.
[10] Kukkola, Juha: Civilian and Military Information Infrastructure and the Control of the Russian Segment of Internet. *Presented at The International Conference on Military Communications and Information Systems (ICMCIS) Varsova, Puola, Toukokuu 22.-23., 2018*.
[11] Choucri, Nazli: *Cyberpolitics in International Relations*. The MIT Press, Cambridge, 2012; Mueller, Milton: *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace.* Polity, Cambridge, UK, 2017; Musiani, Francesca, Cogburn, Derrick L., DeNardis, Laura & Levinson, Nanette S. (Eds.): *The Turn to Infrastructure in Internet Governance*. Palgrave Macmillan, New York, 2016.
[12] Alstyne, Marshall Van & Brynjolfsson, Erik: *Electronic Communities: Global Village or Cyberbalkans?* [https://web.mit.edu/marshall/www/papers/CyberBalkans.pdf], visited 14.9.2022.

military capabilities to operate in that space.[13] However, Demchak and Dombrovski have not explored how this development would proceed in practice. Allison Lawlor Russell's, on the other hand, has examined fragmentation though operations, i.e., cyber blockades and denial of the freedom of action. Her analysis mainly studies the subject from the point of view of the attacker, i.e., the party doing the blockading.[14]

Fragmentation has been mostly discussed from the perspectives of politics, human rights, technology or administration.[15] In the case of Russia, the control of the internet has often been seen as a political issue.[16] For example, Andrei Soldatov and Irina Borogan have argued that the Russian state's activities are reflective of domestic policy issues and 'the KGB mentality'.[17]

In general, the Russian project to build a national segment of the internet has been commented on in the media, although academic research on the subject is increasing. For example, Julian Nocetti has linked the project to building sovereignty in cyberspace.[18] Ristolainen and Rautava, on the other hand, have examined the project as a technical phenomenon from the perspective of cyberterritoriality.[19] Only recently, the Western field of research has woken up to the idea that the Russian national segment of the internet project may have a broader military strategic significance. For example, Rod Thornton and Marina Miron have argued that Russia is seeking to develop its cyber resilience against the West's AI-enhanced cyberattacks.[20] The study of global fragmentation of cyberspace at the strategic level has remained marginal with the exception of research conducted by the Finnish Defence Research Agency, which I will return to later.

On the other hand, several studies have been made on Russia's offensive cyber operations in recent years.[21] Russia's views on information warfare have also been the

---

[13] Demchak, Chris & Dombrowski, Peter: Rise of the Cybered Westphalian Age. *Strategic Studies Quarterly*, Vol. 5, No. 1 (Spring 2011), pp. 32–61.
[14] Russell, A. L.: *Cyber Blockades*. Georgetown University Press, Washington DC, 2014.
[15] Drake, William J., Cerf, Vinton G. & Kleinwächter, Wolfgang: *Future of the Internet Initiative White Paper. Internet Fragmentation: An Overview*. World Economic Forum, January 2016. [https://www.itu.int/net4/wsis/forum/2016/Agenda/Session/169], visited 9.2.2018.
[16] Freedom House: *Freedom on the Net 2017: Russia, 2017*. [https://freedomhouse.org/report/freedom-net/2017/russia], visited 11.1.2018; Аropa: *Свобода интернета 2019: план «Крепость»*. [https://2019.runet.report/assets/files/Internet_Freedom%202019_The_Fortress.pdf], visited 17.3.2020; Deibert, Ronald, Palfrey, John, Rohozinski, Rafal & Zittrain, Jonathan (eds.): *Access Controlled The Shaping of Power, Rights, and Rule in Cyberspace*. The MIT Press, Cambridge, Massachusetts, 2010.
[17] Soldatov, Andrei & Borogan, Irina: *The Red Web. The Struggle Between Russia's Digital Dictators and The New Online Revolutionaries*. Public Affairs, New York, 2015.
[18] Nocetti, Julian: Contest and conquest: Russia and Global Internet Governance. *International Affairs*, Vol. 91, No. 1 (2015), pp. 111–130.
[19] Rautava, Jori-Pekka & Ristolainen, Mari: Cyberterritory: An Exploration of the Concept *Proceedings of the 21st European Conference on Cyber Warfare and Security A Conference hosted by the University of Chester UK 16-17 June 2022*. Eze, Thaddeus, Khanand, Nabeel & Onwubiko, Cyril (eds.), pp. 239–246.
[20] Thornton, Rod & Miron, Marina: Towards the 'Third Revolution in Military Affairs'. *The RUSI Journal*, Vol. 165, No. 3 (2020), pp. 12–21.
[21] For recent studies on the subject cf. Lilly, Bilyana & Cheravitch, Joe: The Past, Present, and Future of Russia's Cyber Strategy and Forces. In 2020 *12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade*. T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, G. Visky (Eds.) NATO CCDCOE Publications, Tallinn, 2020, pp. 129–155.

focus of extensive attention. Timothy Thomas, who has been writing about the subject since the 1990s, is an undeniable authority in this field.[22] Such scholars as Mary Fitzgerald, Jakob W. Kipp, Roger N. Dermott, Dima Adamsky, Kier Giles, Oscar Jonsson, Benjamin Jensen, Brandon Valeriano and Ryan Maness have also written on the subject.[23] Only very few people have shown any interest towards Russia's *defensive* cyber strategy. Ilmari Susiluoto, Slava Gerovich and Benjamin Peters have examined the development of the Russian internet (or lack of it) by means of historical research. However, their research belongs more in the field of history and culture than in the field of military sciences.[24]

There is one exception, Martti Kari, who in his doctoral dissertation studied the cyber threat scenarios associated with the strategic culture related to the cyber environment of the Russian Federation and their impact on how Russia operates.[25] Maija Turunen and Martti Kari have also studies Russia's 'active cyber deterrence', which, according to them, is based on creating a cyberspace to be defended, developing and using offensive capabilities for communication purposes, and engaging other countries in their own solutions.[26] Similar observations were already made by Kukkola, Ristolainen and Nikkarila in 2017.[27]

In my own doctoral dissertation, *Digital Soviet Union: The Russian national segment of the internet as a closed national network shaped by strategic cultural ideas*, I presented a view on the backgrounds of Russia's cyber strategy based on neoclassical realism and strategic culture.[28] Instead of threat scenarios, the thesis examines the impact of several historically constant ideas on the Soviet Union and Russia's vision of force and using it in the information and cyber environment.

---

[22] The first article by Thomas is from 1996 (Thomas, Timothy L.: Russian Views on Information-Based Warfare. *Airpower Journal* – Special Edition 1996, pp. 26–35.)

[23] Adamsky, Dmitry (Dima): From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture. *Journal of Strategic Studies*, Vol. 41, No. 1-2 (2018), pp. 33–60; Giles, Keir: *Handbook of Russian Information Warfare*. Fellowship monograph 9. Rome: NATO Defence College, 2016; Fitzgerald, Mary: Russian Views on IW, EW, and Command and Control: Implications for the 21st Century. *Command & Control Research & Technology Symposium, 1999. U.S. Naval War College, Rhode Island. June 29 - July 1, 1999.* [http://www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/089fitzg.pdf], visited 5.8.2018; McDermott, Roger N.: *Russian Perspective on Network-Centric Warfare: The Key Aim of Serdyukov's Reform*. FMSO, Fort Leavenworth, Kansas, 2011; 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), pp. 36–62; Jonsson, Oscar: *The Understanding of War. Blurring the Lines between War and Peace*. Georgetown University Press, Washington, D.C., 2019; Jensen, Benjamin, Valeriano, Brandon & Maness, Ryan: Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies*, Vol. 42, No. 2 (2019), pp. 212–234.

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

[25] 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.

[26] Turunen, Maija & Kari, Martti J.: Cyber Deterrence and Russia's Active Cyber Defense. In *Proceedings of the 19th European Conference on Cyber Warfare and Security. A Virtual Conference hosted by University of Chester UK 25-26 June 2020*. Thaddeus Exe, Lee Speakman and Cyril Onwubiko (Eds.), pp. 526–532.

[27] Kukkola, Juha, Ristolainen, Mari & Nikkarila, Juha-Pekka: *Game Changer: Structural Transformation of Cyberspace*. Finnish Defence Research Agency, Riihimäki, 2017.

[28] Kukkola, Juha: *Digital Soviet Union. The Russian national segment of Internet as a closed national network shaped by strategic cultural ideas*. National Defence University Series 1: Research Publications No. 40. National Defence University, Helsinki, 2020a.

On the other hand, the Finnish Defence Research Agency's public research project examined the possible consequences of the Russian project. The study showed that the Russian national segment of the internet is not only a tool of political control or state-led economic policy or a response to threats.[29] According to Juha Kukkola, Mari Ristolainen and Juha-Pekka Nikkarila, a closed national network, i.e., a state-controlled part of the internet that can be technically disconnected from the global internet, can be used to gain a strategic advantage in cyberspace. This means that states can use cyber power to shape and control the changing, technology-based and man-made cyberspace according to their preferences, modifying its structure in a way that generates structural cyber asymmetry. According to Kukkola, Ristolainen and Nikkarila, Russia can thus shape the strategic cyber battlefield already during peace in order to gain a significant advantage in the initial period of a conflict and during it.[30]

The nature of structural cyber asymmetry and its strategic effects have not been sufficiently studied. In this context, strategic effects refer narrowly to deliberate changes in the conditions of the use of military force that are directly linked with the pursuit of the state's political objectives.[31] The different forms of use of force at different phases of interstate relations require more research. In particular, the ability to prevent the emergence of a military conflict, the functioning of deterrence, the management of an escalating conflict, and the ability to exploit structural asymmetry for military purposes during a conflict constitute interesting objects of study. They have previously been examined in relation to the cyber environment, but not within the framework of structural cyber asymmetry.[32]

In an earlier Finnish Defence Research Agency study, the emergence of cyber asymmetry was examined by comparing *situation awareness*, *decision-making* and *freedom of action* in offensive and defensive operations between a *closed network nation* and an *open network nation*. The analysis was based on examining attack vectors. However, closed and open networks should be studied through differences in their characteristics, not just through attack vectors. Furthermore, the concepts used in the analysis require further clarification and research. In my doctoral dissertation, I proposed that the Russian

---

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

[30] Cf. Kukkola, Ristolainen & Nikkarila (2017); Kukkola, Ristolainen & Nikkarila (2019).

[31] This definition differs from more commonly used ones. Cf. Gray, Colin S.: *Modern Strategy*. Oxford University Press, Oxford, 1999, pp. 296; Strachan, Hew: *The Direction of War: Contemporary Strategy in Historical Perspective*. Cambridge University Press, New York, 2013, pp. 191–192.

[32] These phenomena have more generally been studied by e.g., Nye, Joseph: Deterrence and Dissuasion in Cyberspace. *International Security*, Vol. 41, No. 3 (2016/2017), pp. 44–71; Cimbala, Stephen J.: Nuclear Deterrence and Cyber Warfare: Coexistence or Competition? *Defense & Security Analysis*, Vol. 33, No. 3 (2017), pp. 193–208; Chen, Jim: Cyberdeterrence by Engagement and Surprise. *PRIMS*, Vol. 7, No. 2 (2017), pp. 100–107; Libicki, M. C.: *Conquest in Cyberspace. National Security and Information Warfare*. Cambridge University Press, Cambridge, 2007; Rid, Thomas: *Cyber War Will Not Take Place*. Oxford University Press, Oxford, 2017; Gartzke, Eric & Lindsay, Jon R.: *Cross-Domain Deterrence: Strategy in an Era of Complexity*. Oxford University Press, New York, 2019; Stevens, Tim: A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy*, Vol. 33, No. 1 (2012), pp. 148–170; Valeriano, Brandon, Jensen, Benjamin & Maness, Ryan C.: *Cyber Strategy: The Evolving Chracter of Power and Coercion*. Oxford University Press, New York, 2018; Kello, Lucas: The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 7–40; Rattray, Gregory J.: *Strategic Warfare in Cyberspace*. MIT Press, Cambridge, 2001; Clarke, R. A. & Knake, R. K.: *Cyber War: The Next Threat to National Security and What to Do About It*. Harper Collins, New York, 2010.

national segment of the internet, as a real representation of the theoretical closed national network, can be examined as a system of systems of national information security and defence.[33] The model is based on Russian thinking as interpreted through the ideas of Russian strategic culture. The model provides a basis for understanding the project aimed at managing the Russian state's national information space.

1.1 Research problem and questions

The aim of this thesis is to develop a theoretical and conceptual basis for studying structural cyber asymmetry and to examine the strategic effects of the Russian national segment of the internet. Methodologically, this thesis is a theory-driven qualitative case study based on content analysis and abduction. The thesis is based on previous research, my doctoral dissertation *Digital Soviet Union* and public research conducted by the Finnish Defence Research Agency, develops it further and opens new paths for research. In this thesis, I add to the analysis of cyber asymmetry made in the Finnish Defence Research Agency papers the concept of resilience, which reflects the passive defence capability of national networks. I also replace the concepts of situational awareness and decision-making with common situation picture, and command and control, because it is impossible to analyse the previous at the strategic level without knowing the decision-makers' mindset. I have chosen freedom of action, common situation picture, command and control, and resilience as the concepts of analysis as they make it possible to examine structural cyber asymmetry through technological structures, functions and organisations rather than through subjective interpretations and modes of thinking of decision-makers that are more difficult to observe. In addition to the attack vectors, I expand the analysis to cover the characteristics of closed and open national networks to add more depth to the analysis of the differences between the networks. In addition, I deepen the analysis of my doctoral dissertation by examining the nature and strategic effects of structural cyber asymmetry.

The research problem is: does the Russian national segment of the internet create structural cyber asymmetry, how it manifests itself and what strategic effects does it have? This problem is addressed through auxiliary research questions, which also provide a structural framework for the thesis.

1. What is structural cyber asymmetry, how its existence can be examined and what is meant by strategic effects?
2. What is the Russian national segment of the internet and its relationship with the concepts of information security and defence system, and closed national network?
3. How does the Russian national segment of the internet compare with open national networks in terms of freedom of action, common situation picture, command and control, and resilience, and does the relationship contribute to structural cyber asymmetry?
4. How does structural cyber asymmetry affect the threat or use of force to achieve political objectives in different phases of interstate relations?

[33] Kukkola (2020a).

1.2 Theoretical framework and perspective

This thesis falls within the scope of international relations research and its subfield of strategic studies.[34] At the core of the problem setting for the thesis lie the interstate relations based on the use of force. The theoretical framework of the thesis is very loosely composed of the theories of neoclassical realism and constructivism and the concepts derived from previous research.[35] To save space, neoclassical realism and constructivism are not discussed in more detail in this thesis. They are discussed more closely in my doctoral dissertation, where I started the theorizing I continue in this study. The theoretical premise is that states are the key security-level actors in the international system and one of its operating environments, the cyber environment. States use non-state actors to achieve their own objectives. In this thesis, the independent activities and impacts of non-state actors are excluded from the examination. The strategic operating environment of states and the use of force gain their significance based on the beliefs of the actors involved – more specifically, the foreign and security policy decision-makers – who define what is perceived as reasonable and desirable.[36] The empirical framework for the case study is Russia's *strategic environment*, including cyberspace. According to Ripsman, Taliaferro and Lobell, the strategic environment consists of the structures based on the distribution of power in the international system, geography, technological diffusion, offence-defence balance, nature of threats, time factors, optimal modes of operation options, interpretations of the security policy elites, and beliefs.[37]

In this thesis, beliefs refer to strategic cultural ideas that are causal or principled beliefs about the threat or use of force to achieve political goals.[38] Strategic culture can be defined as a set of inter-related beliefs, standards, and assumptions or collective expectations that define what is understood by the strategic environment, and acceptable and unacceptable strategic choices.[39] The theoretical assumption is that the ideas of strategic culture *give reason* to the Russian Federation's leaders to shape a national information security and defence system and a national segment of the internet.[40]

The concepts of use of force employed in the thesis are based on the U.S. *'bargaining model of war'*, in which significant factors include the distribution of the contested resources, the relative military force of the actors involved, the costs of preparing for

---

[34] On International Relations cf. Dunne, T., Kurki, M. & Smith, S.: *International Relations Theories: Discipline and Diversity* (4th ed.) Oxford University Press, Oxford, 2013. On Strategic Studies cf. Mahnken, Thomas G.: The Future of Strategic Studies. *The Journal of Strategic Studies*, Vol. 26, No. 1 (2003), pp. x–xviii.

[35] On these theories cf. Rose, Gideon: Neoclassical Realism and Theories of Foreign Policy. *World Politics*, Vol. 51, No. 1 (1998), pp. 144–172; Rathbun, Brian: A Rose by Any Other Name: Neoclassical Realism as the Logical and Necessary Extension of Structural Realism. *Security Studies*, Vol. 17, No. 2 (2008), pp. 294–321; Ripsman, Norrin M., Taliaferro, Jeffrey W. & Lobell, Steven E.: *Neoclassical Realist Theory of International Relations*. Oxford University Press, New York, 2016.

[36] More on the theory applied in this study cf. Kukkola (2020a).

[37] Ripsman, Taliaferro & Lobell (2016), 182.

[38] Kukkola (2020a).

[39] Ripsman, Taliaferro, & Lobell (2016).

[40] On the concept of rationality cf..Banerjee, Sanjoy: Rules, Agency, and International Structuration. *International Studies Review*, Vol. 17, No. 2 (June 2015), pp. 274–297; Barkin, Samuel J.: *Realist constructivism: Rethinking International Relations Theory*. Cambridge University Press, Cambridge, 2010, pp. 66–71.

and conducting war and the uncertainty associated with the aforementioned factors.[41] These concepts based on instrumental rationality, materialism and gaming theories are integrated into the framework of neoclassical realism through the preparation and implementation of a strategy influenced by strategic cultural ideas. Based on this framework, in my doctoral dissertation I defined cyber power as the ability that empowers a state to influence other states in or through cyberspace and to control and shape cyberspace to its advantage according to its preferences.[42] From a constructivist perspective, Russia's project to build a national segment of the internet, i.e., the use of cyber power, is thus understood as a process of drafting and implementing a strategy, and structural cyber asymmetry as its theoretical and diverse final outcome in reality.

In this thesis, the national segment of the internet is discussed in the framework of system theory as a product of the system of systems of information security. The system draws its content from projects aimed at managing the Russian state's national information space, the ideas of Russian information theoreticians and the characteristics of the Russian state. It is a heuristic model intended to provide an understanding of the adaptive and complex system. The approach resonates with the Russian system theoretical thinking, focuses attention on examining national security in line with the perspective of the thesis, and makes it possible to generalise the observations made of the Russian case study into the theoretical phenomena of closed national networks and structural cyber asymmetry.

The scope of the thesis is limited to concern the Russian information security and defence system and the national segment of the internet as its representation as they appeared through public sources in the period 2017–2021. *The study focuses in particular on the impacts of the information security and defence system found in cyberspace, excluding the more extensive impacts on the national information space from the scope of the study.* It is therefore a case study seeking to understand a wider theoretical phenomenon (structural cyber asymmetry) through a single case (Russian national segment of the internet).

Some other countries, such as China, Iran and North Korea, have also developed the management of a national internet network.[43] What is special about Russia is that the state aims to use the resources of a superpower (unlike those of Iran and North Korea), to bring the originally freely developed (unlike in China) internet under state control. Furthermore, the Russian project has specific roots stemming from the strategic culture, in addition to the interests of an authoritarian regime.[44] The Russian project is seen as a typical example of a new phenomenon, and by examining this phenomenon, it is possible to create concepts for studying the management of the

---

[41] Lindsay, Jon R. & Gartzke, Erik: Politics by Many Other Means: The Comparative Strategic Advantages of Operational Domains. *Journal of Strategic Studies*, 2020 DOI: 10.1080/01402390.2020.1768372.
[42] Kukkola (2020a), 78.
[43] Williams, Martyn: How the Internet Works in North Korea. *Slate*, November 28, 2016. [https://slate.com/technology/2016/11/how-the-internet-works-in-north-korea.html], visited 28.1.2021; Article 19: Iran: *Tightening the Net 2020: After Blood and Shutdowns*. Article 19, London, 2020. [https://www.article19.org/wp-content/uploads/2020/09/TTN-report-2020.pdf], visited 28.1.2021; Nagelhus Schia, Niels & Gjesvik, Lars: The Chinese Cyber Sovereignty Concept (Part 1). *The University of Nottingham's Asia Research Institute*, September 7, 2018. [https://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-1/], visited 28.1.2021.
[44] Kukkola (2020a).

information space and internet segments in other countries as well, and for understanding structural cyber asymmetry.[45] The work does not specifically address the basics of Russian or Western military or strategic thinking. These have been discussed in the previous study.[46]

Open national networks are basically based on the prevailing way of arranging the management of the internet in the United States and Western Europe in the mid-2010s. The reason for setting this particular time frame for the thesis is the fact that the Russian national segment was a response to the prevailing situation at the time it was developed. By using a theoretical benchmark, it is possible to focus the analysis to the case of Russia and prevent the work from expanding into a general study of the management of the internet. The ongoing change in the West to bring cyberspace under sovereign control by states is acknowledged and its consequences are reverted to in later chapters.

1.3 Research methodology and sources

Answering the auxiliary research questions forms the structure of the thesis. The first chapter is the introduction. The second chapter consists of an interpretative conceptual analysis combined with a theoretical literature review. The chapter presents the key concepts, such as cyberspace, cyber power and cyber strategy. They are used to justify and make understandable the strategic significance of shaping the cyberspace. The concept analysis will continue with examining the concepts of (cyber) conflict and war, conflict prevention, deterrence, escalation and the use of force. They have been selected as key concepts of the thesis, as they provide a temporal dimension for structural cyber asymmetry and tie it as part of the strategic and military-strategic level of operations.[47] The concepts are used in Chapter 5 to examine the strategic effects.

As a new concept, Chapter 2 presents the concept of structural cyber asymmetry. In addition, it examines the relationship between theoretical open and closed national networks, and introduces the concepts and factors of analysis – freedom of action, common situation picture, command and control, and resilience – needed to examine structural cyber asymmetry. The concepts were selected based on the fact that they make it possible to examine the impacts of structural cyber asymmetry through the situational information each operations and situation requires; processing, assessment and understanding of that data; decision-making and implementation; active implementation of offensive and defensive action; and passive defence, that is, resilience. The concepts bind the work to the field of Western military research. They are used in the analysis in Chapter 4.

Chapter 3 examines system theory, Russian strategic cultural ideas, the characteristics of Russian state, the Russian national segment of the internet as a product of the

---

[45] On the Case Study method cf. Gerring, John: What Is a Case Study and What Is It Good for? *The American Political Science Review*, Vol. 98, No. 2 (May, 2004), pp. 341–354.
[46] Kukkola (2020a).
[47] On the strategic level cf. Gray, Colin S.: *War, Peace and International Relations: An Introduction to Strategic History*. Routledge, New York, 2007, pp. 40; Milevski, Lucas: *The Evolution of Modern Grand Strategic Thought*. Oxford University Press, Oxford, 2016.

national information security and defence system, and presents the model of a theoretical open national network. Chapter 4 uses the concepts of freedom of action, common situation picture, command and control, and resilience to analyse the structural cyber asymmetry between the Russian national segment of the internet and a theoretical open national network. The analysis has three phases. The first phase complements the attack vector-based analysis conducted in the previous study. The second phase compares closed and theoretical open networks through the subsystems of the system of systems of national information security and defence. The third phase is based on comparing closed and open national networks at different stages of a conflict to examine the impact of changes in network structures.

Chapter 5 analyses the impacts of structural cyber asymmetry on threat prevention, the functioning of deterrence, the management of an escalating conflict and the military exploitation of structural cyber asymmetry, drawing on the results of the previous chapter. According to the definition given in Chapter 2, strategic effects are approached through shaping the prerequisites for the use of force and examining the operations aimed at achieving military objectives. The focus is on a conflict erupting in the near future, i.e., in the 2030s, within the framework of foreseeable technological advances. Operational and tactical issues related to warfare are excluded from the analysis. Chapter 6 consists of a summary and conclusions.

As a rule, the sources used for describing Russia's national information security and defence system and internet segment are in Russian The main sources include news services such as *TASS, Izvestiia, RBK, Vedomosti* and *Kommersant*, websites representing the opposition and civil society perspective, such as *Roskomsvoboda*, *Meduza* and *Novaia gazeta*, and the official websites of the Russian administration, publishing statements and official documents from the security and defence policy elites, and online legal text services such as *KonsultantPlius* and *Garant.ru*. As regards the networks and systems of the Armed Forces, the sources used include the military journals available through the EastView database, such as *Voennaia mysl'*, *Vestnik akademii voennykh nauk* and *Voenno-promyshlennyĭ kur'er*, which are leading publications in the field, as well as the websites of the Armed Forces and the yearbooks and similar publications of the military services and branches. Blog entries by Russian cyber experts are also used as a source for the thesis. Western and English-language sources are used for supporting and verifying Russian sources when examining Russia and for providing background information for broader development trends in the internet and cyberspace. Sources were collected until spring 2021.

As a rule, the theoretical literature used in the work is of Western origin and published in English. The literature was collected from digital databases of international research articles (EBSCO, JSTOR, SAGE and Taylor & Francis). It was supplemented with a number of recent major monographs. The latest publications are from spring 2021. In Chapters 2 and 3, I use my doctoral dissertation published in 2020 as one of the main sources.

2. Cyber power and structural cyber asymmetry

This chapter describes the key concepts of the thesis, some of which are based on my earlier doctoral dissertation. The aim is to define the key concepts and to lay the foundations for their use in the analysis in later chapters. All concept presented and their definitions have been formulated with a view to the analysis made in this thesis.

2.1 Cyberspace, cyber power and cyber strategy

Information environment can be defined as the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[48] As information permeates all human domains, it is almost impossible to distinguish between the physical world, information systems, connections disseminating information, human minds and the societies based on them.[49] To facilitate analysis, in this work the information environment is divided into interconnected cyberspace, socio-cognitive space, information-physical space and electromagnetic space.[50] The socio-cognitive space refers to the human minds and the assessments, knowledge and beliefs shared by them, on which societies are based. The information-physical space refers to objects and the information contained therein, such as books, films, music, paintings and architecture, and events in physical reality on which human minds can make interpretations. The electromagnetic space refers to electromagnetic radiation that travels in free space. The division is based on the characteristics of the spaces, not the object of action or the action itself. In the information environment, the human minds are present as objects and subjects.[51]

In this thesis, *cyberspace* is defined as follows: *A man-made and governed global space within the information environment whose distinct and unique character is based on the use of systems and services using information technology that form an interdependent networked operating environment with the purpose of creating, modifying, exchanging, and exploiting information via interconnected networks using information-communication technologies.*[52] The definition highlights the nature

---

[48] The United States Department of Defense (U.S. DoD): *Joint Publications 3-12: Cyberspace Operations, 8th June 2018*, pp. viii. [https://fas.org/irp/doddir/dod/jp3_12.pdf], visited 17.10.2019.

[49] The United States Department of Defense (U.S. DoD): *Joint Publication 3-0: Joint Operations* 2017, Incorporating Change 1 22 October 2018, pp. IV-1-IV-2. [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910], visited 27.4.2020.

[50] This division corresponds to the American, Russian, and Chinese views on information environment cf. U.S. DoD JP 3-0 (2018); Bartles, C.: Sixth-generation War and Russia's Global Theatres of Military Activity. In *Russian Grand Strategy in the Era of Global Power Competition*. Monaghan, Andrew (ed.): Manchester University Press, Oxford, 2022, pp. 71–97; McReynolds, Joe: China's Military Strategy for Network Warfare. In *China's Evolving Military Strategy*. McReynolds, Joe (ed.) The Jamestown Foundation, Washington DC, 2016, pp. 195–240.

[51] Official Russian documents use the concept of information space instead of cyber space (*informat͡sionnoe prostranstvo*) which is defined as: "a collection of information resources which have been created by the subjects of the information environment, and the means of interaction of these subjects, information systems required by these means and necessary information infrastructure." (Указ-203: Указ Президента РФ от 09.05.2017 N 203 "*О Стратегии развития информационного общества в Российской Федерации на 2017 -2030 годы*". [https://www.garant.ru/products/ipo/prime/doc/71570570/], visited 15.5.2019.)

[52] For the original version of the definition cf. (Kukkola (2020a), 72.) The definition is based on e.g., Kuehl, Daniel T.: *From Cyberspace to Cyberpower - Defining the Problem*. In *Cyberpower and National Security*. Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K., National Defence University Press, Washington, D.C., 2009, pp.

of cyberspace as a plastic, i.e., a malleable space. Cyberspace is divided into physical, syntactic and semantic layers, all of which have their own rules.[53] The levels are interdependent, but they cannot be fully managed through each other, and their interaction produces difficult-to-predict consequences. It should be noted in the definition that humans belong to this space only as subjects, not as objects. The definition adopted in this thesis is based on Western research and differs, for example, from Russian definitions.[54]

Cyberspace is not a *commons* space, as the cyberspace infrastructure is largely owned by private and public bodies.[55] Parts of the cyberspace can be shaped by parties with the necessary resources, capabilities and powers for it. People can shape the cyberspace by controlling its infrastructure, software and services and the technical standards, laws and regulations that govern it. On the other hand, other actors and the cyberspace's own logic may challenge the modifications. Cyberspace cannot be destroyed or its use denied except to a limited extent (or totally from all parties). It can be restored, and its connections rerouted in new ways.

The structure of cyberspace is not homogeneous, but it consists of several networks – all of which are not connected to each other – which have different types of connections between them. In their structures, the networks have specific points, based on physical and logical structures, through which the flow of information can be controlled.[56] In summary, cyberspace is artificial, fundamentally physical, rules-based, networked, heterogeneous, plastic, regenerating and constructable, easily accessible to all actors, therefore constituting a difficult-to-attribute field with multiple players, in which power is divided and where geographical distance has lost its meaning and the concept of time is based on machine time.[57]

The essential relationship between cyberspace and the processing of information (by people through machines) and the impact of this information on people's existence makes it *an operating environment*.[58] At the same time, cyberspace interacts with other parts of the information environment. It can be influenced, and it can be used for

---

24–42, pp. 28; U.S. DoD JP 3-12 (2018), pp. I-2; Congressional Research Service: *Defense Primer: Cyberspace Operations, December 1, 2021*. [https://sgp.fas.org/crs/natsec/IF10537.pdf], visited 18.9.2022.

[53] U.S. DoD JP 3-12 (2018), I-2-I-3.

[54] Cyber space has multiple national definitions because of political interests related to the way its is defined cf. Godwin III, J. B., Kulpim, A., Rauscher, K. F. & 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, 2014, pp. 17; Dunn Cavelty, Myriam & Wenger, Andreas: Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science. *Contemporary Security Policy*, Vol. 41, No. 1 (2020), pp. 5–32.

[55] Raymond, Mark: Puncturing the Myth of the Internet as a Commons. *Georgetown Journal of International Affairs, International Engagement on Cyber III: State Building on a New Frontier*, 2013, pp. 57–68.

[56] Rattray, Gregory J.: An Environmental Approach to Understanding Cyberpower. In *Cyberpower and National Security*. Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K. (Eds.) National Defence University Press, Washington, D.C., 2009, pp. 253–274.

[57] For a list of the properties of cyber space cf. Schreier, Fred: *On Cyberwarfare*. DCAF Horizon 2015 Working Paper No. 7. [https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf], visited 27.4.2020.

[58] For the relationship between space and action cf. Sanastokeskus TSK (2018), 21; Laari, Tommi (toim.): *#kyberpuolustus. Kyberkäsikirja Puolustusvoimien henkilöstölle*. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 3: Työpapereita nro. 12, Helsinki 2019.

influencing, for example, the information physical space. When emphasising the nature of cyberspace specifically as an operating environment, the concept of *cyber domain* can be used.[59] Cyberspace is comparable to sea, land, air and space – it acts as a framework and structure of actions. At the intersection of cyberspace and operating environment lies the cyber battlefield or cyber *domain*, which is a functional concept that organises actions.[60] In this thesis, it refers to a military environment that can be divided into cyber battlefields to achieve tactical, operational and strategic goals and objectives.[61]

The power used in cyberspace is cyber power.[62] As the concept of power is controversial, complex and tied to the context and culture,[63] there is no established definition for cyber power either.[64] This thesis uses the definition I presented in my doctoral dissertation: "*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*."[65] The definition highlights the permanent, creative and constructive nature of power and forms the basis for understanding how cyberspace is managed or national segments of the internet are built. The persistence of cyber power is proportional, as other actors also make efforts to continuously shape the cyberspace. The essential thing is that, as a rule, cyber power is not offensive or defensive – or even military. Cyber power resources or potential are resources or potential of mainly technological, scientific, economic, normative, doctrinal, organisational or human (professional) nature.[66] Cyber power cannot be measured in reference to and/or outside the context in which it is used, although resources and potential can be examined separately. At the level of

---

[59] Magd, Noora: Kybertaistelutila kybertoimintaympäristön sotilaallisena ulottuvuutena. In *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, pp. 84–93.

[60] Lehto, Martti: Kybertaistelun toimintaympäristön teoreettinen tarkastelu. In *Kybertaistelu 2020*. Kuusisto, Tuija (toim.) Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2, No. 1/2014, Juvenes Print, Helsinki, 2014, pp. 67–89.

[61] Cf. Magd (2018), 90–91; Kukkola, Ristolainen & Nikkarila (2017), ix.

[62] The concept of power applied in this study differs from more traditional military ones. Cf. Wylie, J. C.: *Military Strategy: A General Theory of Power Control*. Naval Institute Press, Annapolis Maryland, 2014; Mahan, Alfred T.: *The Influence of Sea Power upon History 1660-1783*. Dover edition. Little, Brown and Company, Boston, 1890; Olsen, John Andreas: *Routledge Handbook of Air Power*. Routledge, Abingdon, Oxon, 2018.

[63] Nye, Joseph S. Jr.: *The Future of Power*. PublicAffairs, New York, 2011; Barnett, M. & Duvall, R.: Power in International Politics. *International Organization*, Vol. 59, No. 1 (2005), pp. 39–75; Guzzini, Stefano: *Power, Realism and Constructivism*. Routledge, London and New York, 2013.

[64] On previously proposed concepts cf. Kuehl (2009); Rattray (2009); Nye (2011); Demchak, Chris: Cybered Conflict, Cyber Power, and Security Resilience as Strategy. In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Reveron, Derek (ed.) Georgetown University Press, Washington, D.C., 2012, pp. 121–136; Sheldon, John B.: The Rise of Cyberpower. In *Strategy in the Contemporary World* (4th ed.) Baylis, John, Wirtz, James J. & Gray, Colin S. (Eds.) Oxford University Press, Oxford, 2013, pp. 301–319; *Valeriano, Brandon & Maness, Ryan C.: Cyber War versus Cyber Realities Cyber Conflict in the International System. Oxford University Press, New York, 2015*; Klimburg, Alexander: Mobilising Cyber Power. *Survival*, Vol. 53, No. 1 (2011), pp. 41–60, 43, 56; Whyte, Christopher & Mazanec, Brian: *Understanding Cyber Warfare. Politics, Policy and Strategy*. Routledge, London and New York, 2019, pp. 150–154.

[65] Originally proposed in Kukkola (2020a), 78. The definition is based on Endresen, R. S.: Hard Power in Cyberspace: CNA as a Political Means. In *Cyber Power*. Pissanidis, N., Rõigas, H., Veenendaal, M. (Eds.) NATO CCD COE, Tallinn, 2016, pp. 23–36, 25.

[66] Kukkola (2020a), 93; Willett, Marcus: Assessing Cyber Power. *Survival*, Vol.61, No.1 (2019), pp. 85–90; Kuusisto, Tuija: Tiedonhallinta päätöksenteossa kybertoimintaympäristössä. In *Kybertaistelu 2020*. Kuusisto, Tuija (toim.), Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2, No. 1/2014, Juvenes Print, Helsinki 2014, pp. 33–61.

principle, the use of cyber power can generate more power, as managing the properties of cyberspace itself may be a source of power.[67] Cyber power is part of the information power, which affects the information environment.

Cyber power can be used during both war and peace, and its use is based on a strategy drawn up by people.[68] In general, a strategy involves assessment, planning, preparation, power build-up, negotiation, pressure, use of force and shaping the environment in continuous interaction with other actors.[69] In the context of cyberspace, a strategy is generally understood as a plan or concept that defines the future threats, opportunities, responses, responsibilities, resources and visions facing a state.[70] From the perspective of this thesis' problem setting, such a definition is too narrow. It is useful to define cyber strategy as a practice based on *art* and experience, and competence based on knowledge that enables the use of a wide range of resources, tools and means to achieve impacts.[71] Therefore, the cyber strategy may include a dimension of military use of force but enables the use of non-military instruments and means. It should be noted that in this thesis, other actors in the cyber environment are interpreted as instruments of states' cyber strategies or variables of their strategic operating environment.[72]

Cyber strategy can, therefore, be defined as *continuous planning of the use of cyber power, preparing for and using it by military and non-military means in the cyber environment to achieve national security objectives*.[73] The concept is thus linked to the methods of the use of force in a specific environment and explains why the results of the strategy are rarely permanent and sometimes unexpected: Strategies are also made by others, and the environment has its own difficult-to-control nature that changes in time.[74] In other words, states can shape the structure and rules of the cyber environment, and structural cyber asymmetry may be one of the outcomes of shaping cyberspace.[75] As cyber power is linked with information power, the cyber strategy is part of the information strategy. The information strategy affects the information environment. The information security and defence system discussed later is a tool based on the information power of the information strategy, and it mainly affects cyberspace.

---

[67] The idea of producing power through strategy is Lawrence Freedman's (Freedman, Lawrence: *Strategy: A History*. Oxford University Press, New York, 2013, pp. xi–xii).
[68] For example China and Russia have their own military strategic concepts and way of thought. (Thomas, Timothy: Nation-state Cyber Strategies: Examples from China and Russia. In *Cyberpower and National Security*. Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K. (Eds.) National Defence University Press, Washington, D.C., 2009, pp. 465–488).
[69] Yarger, Harry R.: *Strategic Theory for the 21st Century: The Little Book on Big Strategy*. Strategic Studies Institute, U.S. Army War College, Carlisle, PA, 2006, pp. 21–23; Gray (1999), 141–150; Freedman (2013), xi–xii; Popescu, Ionut C: Grand Strategy vs. Emergent Strategy in the Conduct of Foreign Policy. *The Journal of Strategic Studies*, Vol. 41, No. 3, (2018), pp. 438–460; Strachan, Hew: Strategy in Theory, Strategy in Practice. *Journal of Strategic Studies*, Vol. 42, No. 2 (2019), pp. 171–190.
[70] Valerian, Jensen & Maness (2018), 9–10.
[71] This idea is based on Joseph Nye (Nye 2011, 40–41).
[72] On non-state actors cf. Maurer, Tim: *Cyber Mercenaries. The State, Hackers, and Power*. Cambridge University Press, Cambridge, 2018.
[73] On the concept of security cf. Miller, Benjamin: The Concept of Security: Should it be Redefined? *The Journal of Strategic Studies*, Vol. 24, No. 2 (2001), pp. 13–42.
[74] This view is based on Edward Luttwak's concept of the paradoxical nature of strategy. (Luttwak, Edward N. Strategy: *The Logic of War and Peace*. The Belknap Press of Harvard University Press, Cambridge, Massachusetts, 2001).
[75] Kukkola, Ristolainen & Nikkarila (2017).

2.2 Use of force, phases of conflict, prevention, deterrence and escalation

The use of force is tied to its context. In this thesis, the context consists of the strategic environment of states, whose temporal dimension is defined by state-to-state relations. *Interstate relations are divided into peaceful competition; intensified competition; conflict, including the initial period of war; and war* The division is based on American, Russian and Chinese thinking.[76] The phases involve specific threats, such as espionage and sabotage, local conflicts and internal disturbances, regional wars and colour revolutions, and great power wars.[77] During peaceful competition, countries openly pursue their national interests through generally accepted means, accepting *common security* as the starting point for their actions. During intensified competition, the national interests are partly opposed, the means are often non-military, and the goals are limited. A conflict can be defined as the threat or use of force not crossing the threshold of an open, declared war. The conflict is limited in terms of the means and instruments used and the scale of their use compared to a state of war. The initial period of war[78] refers to the first offensive and defensive operations executed using the capabilities established and positioned in time of peace. The main problem in the early stages of war is how to avoid being taken by surprise when a deterrence fails. Since a conflict is overshadowed by the initial period of war, it is linked to the stage of conflict rather than to the war proper. War is a state between nations in which they use open military and violent force to pursue their political objectives.[79]

In this thesis, in the context of interstate relations cyberwar is defined as a theoretical form of war conducted only in or through cyberspace.[80] Cyber warfare, on the other hand, means concrete use of intentional information network attacks to cause harm against the adversary's civilian or military infrastructure and forces as part of power politics.[81] Cyber conflict is a milder concept than war, but an extensive and even political concept. According to some theoreticians, the world is already in the phase of a continuous cyber conflict.[82]

---

[76] Mulgund, Sandeep S. & Kelly, Mark D.: Command and Control of Operations in the Information Environment. Leading with Information in Operational Planning, Execution, and Assessment. *Air & Space Power Journal*, Vol. 34 No. 4 (Winter 2020), pp. 15–26; Kofman, Michael, Fink, Anya & Edmonds, Jeffrey: *Russian Strategy for Escalation Management: Evolution of Key Concepts*. CNA, Washington, D. C., 2020; Mazarr, Michael J.: *Understanding Competition. Great Power Rivalry in a Changing International Order – Concepts and Theories*. RAND, Santa Monica, 2022.

[77] Kukkola (2020a), 361.

[78] The initial period of war has a special place in the Russian military thought cf. Kukkola (2020a), 111.

[79] On the continuum of interstate relations cf. Gray (2007); Jordan, D., Kiras, James D. Lonsdale, David J., Speller, Ian, Tuck, Christopher & Dale, Walton: *Understanding Modern War*. Cambridge University Press, Cambridge, 2008; Kane, Thomas M. & Lonsdale, David J.: *Understanding Contemporary Strategy*. Routledge, New York, 2012; Strachan (2013).

[80] Mahnken, Thomas G.: Cyber war and Cyber warfare. In *America's Cyber Future Security and Prosperity in the Information Age volume II*. Lord, Kristin M. and Sharp, Travis (ed.) Center for New American Security, 2011, pp. 57–64.

[81] Liff, Adam: Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, Vol. 35, No. 3 (2012) pp. 401–428.

[82] Libicki, Martin C.: *Cyberspace in Peace and War*. Naval Institute Press, Annapolis, Maryland, 2016; Whyte & Mazanec (2019).

Cyber operations can be divided into offensive and defensive operations and network maintenance operations.[83] *Offensive Cyber Operations* (OCO) are activities carried out in or through the cyber environment with an aim to harm, i.e., to disrupt, deny, degrade or destroy information systems or the confidentiality, integrity or availability of information contained therein. They include cyber intelligence operations to acquire information or enable the acquisition of information but exclude efforts to cause immediate damage to targeted systems. *Defensive Cyber Operations* (DCO) refer to actively protecting critical information networks and information systems of a state, society or armed forces and the information contained therein from specific hostile operations. Therefore, cyber defence does not refer to military networks or actions carried out by armed forces only.[84] Maintenance operations are aimed at securing the general maintenance of the confidentiality, integrity and availability of state, social and/or military systems.[85]

Cyber operations are operational and tactical forms of use of force. At the strategic level, the different forms of use of force are linked to the phases of the conflict, although they also have an independent nature. The mildest form of the use of force is conflict prevention. *In this work, conflict prevention, conducted as part of the state security policy, refers to the neutralisation of potential threats through any means available, without needing to resort to the threat or use of direct armed force.* The definition is partly based on the fact that armed force falls within the sphere of defence policy and strategy. Therefore, in this thesis, defence policy is defined as the part of state policy addressing the use or threat of force, including the assessment of threats, planning, and preparation for and the execution of the threat or use of force. The military strategy is thus subordinate to the defence policy. The context of conflict prevention is a state of peace or an intensified competitive situation in which the threat has not yet materialised.

Conflict prevention relates to intelligence to detect potential threats, communications, persuasion, engagement, alliance policy, diplomacy and non-military coercion or threatening with it. In this thesis, they are collectively called *persuasion*.[86] Persuasion is understood more broadly than as 'positive attraction'. It includes exerting pressure without threat or use of direct force. With regard to cyber actions, conflict prevention can be considered to relate to intelligence, achieving early warning, persuasion, and shaping the operating environment to prevent potential threats.[87] One essential measure is cyber diplomacy, which refers to using diplomatic means to safeguard the interests of a state in cyberspace, mainly through building capabilities, increasing trust and developing norms and standards.[88]

---

[83] The definition is based on U.S. DoD JP 3-12 (2018), II-2–II-9.
[84] Andress, Jason & Winterfeld, Steve: *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners. (*2nd ed.*)* Syngress, Waltham. 2014, pp. 196; Liff (2012), 404.
[85] The definition is based on U.S. DoD JP 3-12 (2018), II-2–II-9.
[86] On persuasion cf. Nye (2011).
[87] On these actions cf. Libicki, Martin C.: *Cyberdeterrence and Cyberwar.* RAND, Santa Monica, 2009; Libicki (2016); Nye (2016/2017); Lewis, James Andrew: *Rethinking Cybersecurity*. A Report of the CSIS Technology Policy Program. Rowman & Littlefield, New York, London, 2018; Brantly, Aaron Franklin: *The Decision to Attack. Military and Intelligence Cyber Decision-Making.* University of Georgia Press, Athens, Georgia, 2016; Libicki, Martin C.: The Conversion of Information Warfare. *Strategic Studies Quarterly*, Vol. 11, No. 1, (Spring 2017), pp. 49–65.
[88] Manantan, Mark Bryan F.: Advancing Cyber Diplomacy in the Asia Pacific: Japan and Australia. *Australian Journal of International Affairs,* Vol.75, No.4 (2021), pp. 432–459.

Power politics refers to the English term *coercion*, which is understood as an umbrella concept of deterrence and compellence.[89] According to Thomas Schelling, power politics differs from *brute force*, which is based on unilateral destruction or takeover by using military force. In power politics, the element of negotiation is always present.[90] The aim is, by manipulating the amount (pain) and likelihood (fear) of costs, to make a subject refrain from, interrupt or take certain kind of action. *Compellence* refers to efforts to make the subject do something that it would not otherwise do. Deterrence, on the other hand, is aimed at making a potential opponent refrain from action. This can be achieved either by threatening with a punishment (*deterrence by punishment*) or by letting the target understand that it would not benefit from its actions (*deterrence by denial*). The concept of deterrence in particular has long historical roots and, today, different variations of it guide the security and defence policy of the United States, Russia and China alike.[91]

Theoretically, in essence deterrence consists of capabilities, credibility, a degree of uncertainty and communication. The basic idea of deterrence is to affect an opponent's cost-benefit calculations. Therefore, the subject of deterrence has the final decision on how to respond to deterrence. The subject must know and understand the existence and nature of the threat. The underlying assumption is that the subject is rational and that the parties share the interest to avoid war, if possible. In general, both deterrence and compellence are based on the idea that the subject believes that it will avoid the consequences if it acts or refrains from acting as the opponent wants. The threatening party can enhance its credibility by demonstrating that it is prepared to make sacrifices even before the subject responds, or the party publicly commits itself to specific 'red lines', i.e., ties its hands. Since the whole deterrence may suffer from too specific thresholds under which the opponent may operate freely, it is possible to attach a degree of indefiniteness, that is, uncertainty, to the thresholds.[92] Although the logic of the deterrence theory is generally recognised as firm, the views differ strongly regarding its practical requirements and implementation.[93]

The content and effectiveness of cyber deterrence is a contested issue.[94] The most common arguments against the effectiveness of cyber deterrence are as follows:

---

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

[90] Schelling (2008), 2–5.

[91] Gat, Azar: *War in Human Civilization*. Oxford University Press, Oxford, 2006, pp. 92–93; Chase, Michael S. & Chan, Arthur: *China's Evolving Approach to "Integrated Strategic Deterrence"* RAND Corporation, Santa Monica, 2016; Bruusgaard, Kristin Ven: Russian Concept of Deterrence. In *Russian Concept of Deterrence in Contemporary and Classic Perspective*. Pentti Forsström (ed.) National Defence University, Department of Warfare, Series 2: Research Reports No. 11, Helsinki, 2022, pp. 9–20; The United States Department of Defence (U.S. DoD): *Fact Sheet: 2022 National Defense Strategy*. [https://media.defense.gov/2022/Mar/28/2002964702/-1/-1/1/NDS-FACT-SHEET.PDF], visited 19.9.2022.

[92] On deterrence theory cf. Kaplan, Fred: *The Wizards of Armageddon*. Stanford University Press, Stanford, California, 1991; Freedman, Lawrence: *The Evolution of Nuclear Strategy* (3rd ed.) Palgrave Macmillian, New York, 2003; Jervis, Robert: Review: Deterrence Theory Revisited. *World Politics*, Vol. 31, No. 2 (January 1979), pp. 289–324; Knopf, Jeffrey W.: The Fourth Wave in Deterrence Research. *Contemporary Security Policy*, Vol. 31, No. 1 (2010), pp. 1–33.

[93] Glaser, Charles L.: Why do Strategists Disagree about the Requirements of Strategic Deterrence? In *Nuclear Arguments: Understanding the Strategic Nuclear Arms and Arms Control Debates*. Eden, Lynn & Miller, Steven E. (Eds.) Cornell University Press, Ithica, NY, 1989, pp. 109–171.

[94] Cf. Libicki (2016); Geist, Edward: Deterrence Stability in the Cyber Age. *Strategic Studies Quarterly*, Vol. 9, No. 4 (Winter 2015), pp. 44–61; Valeriano, Jensen & Maness (2018).

- In terms of impact, cyber weapons[95] (or equivalent) are not comparable to nuclear weapons on which the deterrence theory was originally based.
- It is difficult and time-consuming to attribute cyberattacks, so it may be difficult to execute deterrence by punishment within the time frame its political legitimacy would require.
- State and non-state actors are likely to respond differently to deterrence.
- Concealing of capabilities weakens the credibility of deterrence because threatening with cyber weapons is difficult without revealing the real capabilities.
- Cyber weapons are difficult to manufacture for storage, they do not preserve well, and their impact is difficult to reproduce, as it is relatively easy for the subject to remedy its vulnerabilities and change its systems.
- The proportionality of deterrence is difficult to measure because it is difficult to obtain sufficient information about potential targets. This may lead to unintentional or accidental escalation.
- With regard to cyberattacks, there are no international standards to increase mutual understanding and transparency, which would at least help deterrence communication.
- Threatening with a cyberattack requires preparation, which may be interpreted as an actual attack.
- Cyber deterrence cannot be built upon *deterrence stability*, since mutually assured destruction (or *disruption*) cannot be guaranteed, or a deterrent built in such a way that it would not constitute a security dilemma for the other party.[96]
- It is impossible to assess or calculate the adversary's 'cyber weapons' and their impact on the target or its surroundings with sufficient reliability.[97]

According to the current view, cyber deterrence by punishment seems difficult to implement. Deterrence by denial, on the other hand, seems more promising. The development of technology and attribution methods, the lessons learned from real cyber operations and the evolution of cyber security technologies and principles have balanced the difference between attacks 'that always get through' and defence.[98] Since defence remains vulnerable and it is difficult to prevent the attacker from trusting its capability to attack, deterrence by denial has begun to be built upon resilience, or denial of impacts.[99] Cyber resilience can be defined as "*the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include*

---

[95] On the definition of cyber weapon cf. Friis, Karsten & Ringsmose, Jens: *Conflict in Cyber Space. Theoretical, strategic and legal perspectives*. Routledge, New York, 2016.
[96] On the concept of security dilemma cf. Jervis, R.: Dilemmas About Security Dilemmas. *Security Studies*, Vol. 20, No. 3 (2011), pp. 416–423.
[97] On the criticism of cyber deterrence cf. Libicki (2009), pp. xiv–xix; Liff (2012), 417–422; Andress & Winterfeld (2014), 92–96; Geist (2015); Chen (2017); Valeriano, Jensen & Maness (2018); Brantly, Aaron F.: The Cyber Deterrence Problem. In *10th International Conference on Cyber Conflict CyCon X: Maximising Effects*. Minárik, T., Jakschis, R. & Lindström, L. (eds.) NATO CCD COE, Tallinn, 2018, pp. 31–53; Leuprecht, Christian, Szeman, Joseph & Skillicorn, David B.: The Damoclean Sword of Offensive Cyber: Policy Uncertainty and Collective Insecurity. *Contemporary Security Policy*, Vol. 40, No. 3 (2019), pp. 382–407.
[98] Libicki (2017); Lewis (2018); Sharp, Travis: Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony. *The Journal of Strategic Studies*, Vol. 40, No. 7 (2017), pp. 898–926.
[99] Cf. Libicki (2016), 269–272.

cyber resources".[100] The basic idea of the concept is that, despite successful attacks, systems are able to recover quickly or to resume their functions to a limited extent. This minimises the impacts (risk) and maximises the adversary's costs. The likelihood of a successful attack remains unchanged, but the impacts are minimised. According to Gratzke and Lindsay, resilience also includes deceiving the attacker.[101] In other words, cyber resilience changes considerably the concept of deterrence by denial. As the weakness of the approach has been proposed passivity, i.e., allowing the attacker to act freely.[102]

In recent years, the blurring of the line between war and peace in interstate relations in the West has generated efforts to extend the deterrence theory to active, non-military and target-specific actions ('*tailored deterrence*'), including cyber operations.[103] Deterrence could be based on repeated, lighter, yet harmful countermeasures. Their effect would be cumulative over time, thus slowly modifying the attacker's behaviour.[104] Examples include sanctions against individuals and institutions, and 'naming and shaming'.[105] In recent years, cyber deterrence thinking has branched out to include a so-called active defence or forward defence.[106] It means penetrating the opponent's networks, conducting intelligence gathering operations and preparing for carrying out a *preventive* or *pre-emptive* strike. The first type of strike is based on the idea of beginning a war at an opportune moment for oneself before the adversary becomes stronger. The latter is based on the will to be the aggressor rather than the defender in an inevitable war.[107] A pre-emptive first strike in particular is thought to have a deterrent effect, as it sends the potential aggressor a message that its targets are vulnerable to a strike attaining the initiative.[108] Furthermore, it has been proposed that cyber deterrence would not necessarily require a cyber response or equal countermeasures to influence the adversary's calculations.[109] This is referred to as *cross-domain deterrence*. In such a case, the use of divergent methods and environments supports the formation of general deterrence.[110]

---

[100] Ross, Ron, Graubart, Richard, Bodeau, Deborah & Rosalie McQuaid: *Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems*. Draft NIST Special Publication 800-160 Volume 2, 2018. [https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf], visited 1.5.2020.

[101] Gartzke, Erik J. & Lindsay, Jon R.: Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies*, Vol. 24, No. 2 (2015), pp. 316–348.

[102] Wilner, Alex S.: US Cyber Deterrence: Practice Guiding Theory. *Journal of Strategic Studies*, Vol.43, No.2 (2020), pp. 245–280.

[103] Kramer, Franklin D. & Teplinsky, Melanie J.: *Cybersecurity and Tailored Deterrence*. Atlantic Council, Washington DC., 2013.

[104] Wilner (2020).

[105] Braw, Elisabeth & Brown, Gary: Personalised Deterrence of Cyber Aggression. *The RUSI Journal*, Vol.165, No.2 (2020), pp. 48–54.

[106] On this concept and criticism of it cf. Klimburg, Alexander: Mixed Signals: A Flawed Approach to Cyber Deterrence. *Survival*, Vol.62, No.1 (2020), pp. 107–130.

[107] Mueller, Karl P., Castillo, Jasen J. & Morgan, Forrest E. (et al.): *Striking First: Preemptive and Preventive Attack in U.S. National Security Policy*. RAND, Santa Monica, 2006.

[108] Libicki (2016), 84; Harknett, Richard J. & Nye, Joseph S. Jr.: Correspondence – Is Deterrence Possible in Cyberspace. *International Security*, Vol. 42, No. 2 (2017), pp. 196–199.

[109] Tor, Uri: 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence. *The Journal of Strategic Studies*, Vol. 40, No. 1-2 (2017), pp. 92–117.

[110] Gartzke & Lindsay (2019).

In the absence of a shared, generally accepted definition of cyber deterrence[111], for pragmatic reasons, cyber deterrence is defined in this thesis as *efforts to persuade a potential opponent not to use force in or from cyberspace or other space by threatening with an unbearable punishment, preventing potential gains or otherwise affecting the adversary's cost-benefit calculations with cyberspace-related capabilities*. Cyber deterrence constitutes a part of a state's general deterrence strategy, in which the boundaries of the operational domains are volatile. Cyber deterrence is also associated with protecting a state from threats in a wider information environment, and it interacts with other domains and methods. Cyber deterrence can thus be part of the cross-domain deterrence.[112] The concept is accepted to include not only the threat but also the use of military and non-military force not crossing the threshold of the use of armed, violent force to affect the cost-benefit calculations in a preventive manner.[113]

The use of force also involves the concept of escalation. The RAND study on escalation theory defines it as "an increase in the intensity or scope of conflict that crosses threshold(s) considered significant by one or more of the participants."[114] Escalation may refer to changes in the intensity, expansion of activities, or the marginal conditions of the political objectives or conflicts. Escalation may happen accidentally, through misunderstanding or intentionally. Accidental escalation is based on unintentional actions. Misunderstanding derives from interpreting non-escalatory actions as escalatory.[115] Intentionality is related to the concept of escalation control, i.e., one of the parties seeking to escalate or prevent the escalation of a conflict in order to gain an advantage over the others.[116] The objective of escalation control is to achieve escalation *dominance*. It means a condition in which one party has the ability to escalate the situation in a manner beneficial to them, while the other parties cannot respond, or they could but their response would weaken their position or be too costly.[117] The goal may be to gain an advantage, prevent a threat, avoid loss or communicate about objectives and thresholds in a war that is still *a limited war*.[118]

Generally speaking, escalation is linked with the concept of deterrence, since deterrence is often based on efforts to prevent the situation from developing in a disadvantaged direction. However, deterrence and escalation management should not be confused with one another. By definition, deterrence cannot be linked to the time of war, as use of open military force has already taken place. In other words, deterrence is associated with the potential of using force and the pre-conflict situation, while escalation management is related to the use of force, compellence and conflict situations.[119]

---

[111] Wilner (2020).
[112] Lindsay & Gartzke (2019).
[113] On armed, violent use of force cf. Schmitt, Michael N. (ed.): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, Cambridge, 2013, pp. 107, 141–142.
[114] Morgan, Forrest E., Mueller, Karl P., Medeiros, Evan S., Pollpeter, Kevin L. & Cliff, Roger: *Dangerous Thresholds: Managing Escalation in the 21st Century*. RAND, Santa Monica, 2008, pp. 15–16, xi.
[115] Ibid., 24-26.
[116] Ibid., 31–33.
[117] Morhan et al. (2008), 15–16; Freedman (2003), 205.
[118] Schelling (2008), 135.
[119] The idea of a deterrence in war is based on nuclear weapons and the promise of unbearable pain – not in the management of the intensity of the conflict. (Snyder, Glenn H.: Deterrence and Power. *The Journal of Conflict Resolution*, Vol. 4, No. 2 (1960), pp. 163–178).

In literature about cyberwarfare, escalation has been connected to the concept of escalation dominance or cross-domain escalation, which has been considered to mean an inadvertent or accidental *spill-over* of a conflict from cyberspace into the realms of conventional or nuclear warfare.[120] Escalation management has been considered to be difficult in the cyber domain due to its properties.[121] In particular, the proneness of cyberattacks to escalate has been explained by the fact that any reciprocal strikes against critical infrastructure or strategic nuclear command and control systems and their consequences may expand in an uncontrollable manner.[122] Diversion attacks by third parties, intended to cause a conflict or even a war between great powers, have also been proposed as a source of escalation. It has also been feared that the great powers focusing on prevention and offensive actions in their cyberwarfare doctrine will increase the risk of escalation.[123] On the other hand, it has been proposed that states do not have at their disposal the kind of cyber capabilities or willingness to use the kind of capabilities the use of which could lead to escalation.[124] It has also been argued that the constant interstate competition and hostile interaction in cyberspace do not follow the same escalation model as potential and intermittent conflict situations.[125]

Considering the above, in this thesis escalation management and control of a conflict refers to *regulating the intensity of the conflict that has begun by the threat or use of force in or through cyberspace with an aim to make the adversary stop using force in a manner advantageous to oneself or in a way serving the pursuit of one's political objectives, while preventing unintentional or accidental escalation.*

Coercive use of force is the extreme form of cyber use of force. Similar theoretical and practical challenges have largely been associated with it as with deterrence, including the following:

- Cyberattacks do not have a similar impact in terms of permanence or scale as conventional or nuclear weapons.[126] At the strategic level, cyber coercion lacks a clear link between the impact and the party using compellence, a sense of

---

[120] Maness, R. C. & Valeriano, B.: Cyber spillover conflicts: Transition from cyber conflict to conventional foreign policy disputes. In *Conflict in Cyber Space: Theoretical, strategic and legal perspectives*. Routledge, New York, 2016, pp. 45–64.
[121] Libicki (2016), 276.
[122] Cimbala, S. J.: Accidental/Inadvertent Nuclear War and Information Warfare. *Armed Forces & Society*, Vol. 25, No.4 (1999), pp. 653–675; 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), pp. 56–99.
[123] Klare, Michael T.: Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation. *Arms Control Today*, November 2019. [https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation], visited 30.4.2020.
[124] Borghard, Erica D. & Lonergan, Shawn W.: Cyber Operations as Imperfect Tools of Escalation. *Strategic Studies Quarterly*, Vol. 13, No. 3 (Fall 2019), pp. 122–145. Cf. also Valeriano, Jensen & Maness (2018), 88.
[125] Fischerkeller, Michael P. & Harknett, Richard J.: Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation. *The Cyber Defense Review*, Special Edition: International Conference on Cyber Conflict (CYCON U.S.), November 14-15, 2019, pp. 267–287.
[126] Libicki (2009), xiv-xv; Libicki (2016), 201.

imminence and the ability to clearly demonstrate the costs of non-compliance.[127]

- The impacts of cyberattacks are slow, indirect and, so far, have failed to rise to a more serious level than that of espionage, sabotage or provocation, i.e., to the level of killing people.[128]
- The use of cyber weapons must be accompanied by the use of other weapons to achieve a coercive effect.[129]

Based on their own statistical research, Valeriano, Jensen and Maness have argued that cyber operations have achieved the desired results in only 5.7% of the cases.[130] According to the opposing views, cyberattacks can affect the critical information infrastructure, vital functions of society, military command and control systems or the political leadership's capacity to act so that it defeats the opponent's ability and willingness to resist.[131] Those who believe in cyber power usually justify their arguments by the fundamental dependence of society and the armed forces on information technology.

Since causing direct destruction – not to mention killing – by cyber force has remained a theoretical phenomenon, and because it is practically impossible to achieve permanent dominance, i.e., establish ownership of the domain, in cyberspace, the use of brute force has not played a significant role when examining the use of strategic-level force in earlier research. Martin Libicki has argued that 'the correlation of forces' cannot be the basis for superiority in cyberspace, as the offensive cyber forces are not set against each other in cyberspace.[132] In practice, it is impossible to use brute force successfully in a cyber environment for as long as the target has even a theoretical opportunity to deny the use of the operating environment from the aggressor or the defender can manage without a cyber environment. In this case, the aggressor cannot achieve the ability to control or destroy the adversary.

Taking into account the above-mentioned views, in this thesis, the use of coercive cyber force is examined as *the use of coercive means and brute force in cyberspace and the ability to wield such influence in or through cyberspace that forces the adversary to stop resisting against its own will, or to deny the same influence on one's own systems*. Such a use of force is associated with an open state of war between state actors. It may involve using several strategies, such as *attrition*, *destruction*, *disruption* or *decapitation*.[133] In this thesis, the use of coercive

---

[127] Whyte & Mazanec (2019), 131.
[128] Rid (2017).
[129] Mahnken (2011), 61–62.
[130] Valeriano, Jensen & Maness (2018), 17.
[131] Rattray (2001); Clark & Knake (2010); Geers, Kenneth: *Strategic Cyber Security*. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2011.
[132] Libicki (2016).
[133] The first one is based on the attrition of the opponent's power through a series of operations directed at the military power, critical functions of the society, or military support functions of the opponent. The second one is based on the destruction of the opponent's military capabilities with one strike to achieve a swift conclusion to the conflict. The third one is based on the paralyzing the military capabilities and will of the opponent by striking its vulnerabilities and destabilizing its cohesion. The fourth one is based on the destruction of civil and military leadership of the opponent. (Valeriano, Jensen & Maness (2018); Sloan, Elinor C.: *Modern Military Strategy: An introduction.* Routledge, New York, 2012).

force is examined within the framework of military exploitation of structural cyber asymmetry.[134]

The consequences and opportunities of using cyber power are related to the concept of strategic effect. According to Colin S. Gray, it may refer to the impact of a specific behaviour on achieving the objectives of the conflict. In other words, it is not a property of an instrument or behaviour, but a consequence caused by it. Usually, the impacts are targeted against the adversary's capacities, will or resources.[135]

The strategic effect is linked to the target and context, since it is decisive how the target reacts to the impact.[136] The impact is not necessarily one-way-only or permanent, but the target may try to change the relationship, for example, by protecting its weaknesses. The situation may also change or influencing may be combined with other factors that have a decisive effect.[137] In other words, the effects are seen as the impact caused in the adversary – or in a system – by an offensive, identifiable action, and not by negotiation.[138] It should be noted that the strategic effects of cyber weapons have been called into question since the 2010s.[139] It has been understood that the development of cyber weapons that cause real destruction requires state-level resources and long preparation, which often go to waste. In addition, cyber weapons have been considered to be mainly suitable as first-strike weapons and to quickly lose their usefulness after the conflict has begun.[140]

However, Harknett and Smeets have proposed that long-term cyber campaigns can achieve strategic effects without the use of military force, based on the cumulative impact of individual operations not crossing the threshold of the use of armed force.[141] Kello, on the other hand, has argued that the development of cyber technology will change the functioning of the whole international system, for example, by increasing uncertainty, imbalance and the number of actors involved.[142] Ben Buchanan has argued that the real use of cyber power is based on signalling and shaping the operating environment through information gathering rather than on compellence and deterrence.[143] The strategic effect can also be potential. It may relate to a

---

[134] On structural cyber asymmetry cf. chapter 2.4.
[135] Gray (2009), 19.
[136] On the concept of effect cf. Vego, Milan: Effects-Based Operations: A Critique. *Joint Forces Quarterly,* Vol. 41, No. 2 (2006), pp. 51–57; Correll, John T.: The Assault on EBO. The Cardinal Sin of Effects-Based Operations Was That It Threatened the Traditional Way of War. *Air Force Magazine*, Vol. 96, No. 1 (January 2013), pp. 50–53; Sloan (2012).
[137] Byman, Daniel L. & Waxman, Matthew C.: Kosovo and the Great Air Power Debate. *International Security*, Vol. 24, No. 4 (Spring 2000), pp. 145–171.
[138] Klinger, Janeen M.: *Social Science and National Security Policy. Deterrence, Coercion, and Modernization Theories*. Palgrave Macmillan, Cham, Switzerland, 2019.
[139] Liff (2012); Stevens (2012); Gartzke, Erik: Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth. *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 41–73; Gartzke & Lindsay (2015), 316–348; Libicki (2016); Nye (2016/2017), 51; Rid (2017), 167-179; Sharp (2017); Lewis (2018); Valeriano, Jensen & Maness (2018).
[140] Geist (2015); Libicki (2016); Clarke, Richard A. & Knake, Robert K.: *The Fifth Domain. Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Press, New York, 2019.
[141] Harknett & Smeets (2022).
[142] Kello, Lucas: *The Virtual Weapon and International Order*. New Haven, Yale University Press, 2017.
[143] Buchanan, Ben: *The Hacker and The State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press, Cambridge, 2020.

future-oriented defence policy or military strategy or to the functioning of the operation of the defence system as a whole.[144]

Taking into account the definition of cyber power above and the discussion related to its strategic effects, it is justified to expand the definition of strategic effects to also include the operating environment shared by the actors, as the change in the operating environment also affects states. From this perspective, *strategic effect changes the operating environment or characteristics of states so that it tips the balance of power between them with regard to a potential future conflict. Strategic impact is related, on the one hand, to a change in the preconditions for the use of force and, on the other hand, to a change related to reaching the objective set for the use of force in the target system (state) at the strategic level.*

Shaping the operating environment or the battlefield is not part of Schelling's original division of power politics, but it is a justified addition as regards cyberspace, where it is possible to shape the framework for interstate interaction in terms of the use of force. It can, therefore, be claimed that strategic effects can emerge in all phases of interstate relations in relation to conflict prevention, deterrence, escalation management and control, and military exploitation of asymmetry.

2.3 Structural cyber asymmetry

Within the sphere of Western military theory, the roots of the term 'asymmetry' date back to the 1970s, even though the matter itself is as old as warfare itself.[145] According to Hew Strachan, each conflict has asymmetric characteristics because there are strengths and vulnerabilities in the power of parties involved in conflicts.[146] Furthermore, the concept of strategy, an integral part of military conflicts, is based on exploiting the opponent's weaknesses.[147] In the 1990s and 2000s, the concept of asymmetric warfare was intertwined with discussions on the revolution in warfare.[148] The discussions were driven by the change observed in the nature of warfare, which included the weakening of states, the strengthening of non-state actors, the emergence of the information society and the increasing significance of cultural factors.[149] Within the framework of the fight against terrorism in the 2000s, asymmetry began to be understood as warfare between non-state actors and a great power or alliance, where

---

[144] Cf. e.g., Gibson, Irving M.: The Maginot Line. *The Journal of Modern History*, Vol. 17, No. 2 (Jun., 1945), pp. 130–146.

[145] On the history of the concept of asymmetry cf. Blank, Stephen: Rethinking the Concept of Asymmetric Threats in U.S. Strategy. *Comparative Strategy*, Vol. 23, No. 4-5 (2004), pp. 343–367; Freedman (2013), 52; Arreguín-Toft, Ivan: Contemporary Asymmetric Conflict Theory in Historical Perspective. *Terrorism and Political Violence*, Vol. 24, No. 4 (2012), pp. 635–657.

[146] Strachan (2013), 22.

[147] Freedman (2013), 227; Strachan (2013), 22; Milevski, Lucas: Asymmetry is Strategy, Strategy is Asymmetry. *JFQ*, Vol. 75, No. 4 (2014), pp. 77–83, 78.

[148] Cf. Raitasalo, Jyri: *Constructing War and Military Power After the Cold War: The Role of the United States in the Shared Western Understandings of War and Military Power in the Post-Cold War Era*. National Defence College, Series 1, Strategic Research No. 21, Helsinki, 2005.

[149] Creveld Van, M.: *The Transformation of War*. The Free Press, New York, 1991; Keegan, J. A.: *History of Warfare* (2nd ed.) Pimlico, London, 2004; Kaldor, Mary: *New and Old Wars: Organized Violence in a Global Era* (3rd edition). Stanford University Press, Stanford, 2012.

the parties even had a differing view of the nature and duration of the war.[150] When the U.S. Armed Forces adopted the Joint Operations Doctrine, they developed an understanding that any operating environment may have critical weaknesses that the opponent can exploit to circumvent the strengths of other operating environments.[151] As a kind of an antidote to the free exploitation of operating environments, an A2/AD (*anti-access and area denial*) doctrine was created. It was considered a way by which the adversaries of the U.S. aimed to prevent the free exploitation of operational domains.[152] The most recent manifestation of asymmetry is related to the concept of hybrid warfare, which is associated with, for example, Russia's actions in connection with the war in Ukraine. In this context, asymmetry is linked with acquiring a strategic advantage by using means that differ from open use of armed force and generally accepted methods of warfare in a way that makes it difficult for the targeted state to respond.[153]

Various elements have been associated with asymmetric warfare. For example, Lawrence Freedman has specified three different types of asymmetry, i.e., power, means and interests.[154] The first type relates to the differences in the military power of the parties, the second to the methods used by the other party that give it an advantage, and the third to the difference of interests, which is related to the other party's stronger will or a different view of the nature of the war being conducted. Correspondingly, according to Ivan Arreguin-Toft, asymmetry is based not on vulnerabilities, or differences in power and methods but on a different understanding of war, the troop structure guided by this understanding and internal political factors.[155] Emily Goldman and Andrew Ross have argued that, as states strive to *offset* the superiority of more powerful states, they develop specific capabilities and conceptual innovations, at the same time producing asymmetry.[156] Jesse Chace, on the other hand, has argued that asymmetric warfare should be based on the use of imagination.[157]

The debate on asymmetry has also affected the development of theoretical framework related to cyber warfare. As a rule, cyber threats and the related non-state actors have

---

[150] Cf. Evans, M.: Elegant Irrelevance Revisited: A Critique of Fourth-Generation Warfare. *Contemporary Security Policy*, Vol. 26, No. 2 (2005), pp. 242–249; Hammes, T. X.: *The Sling and the Stone: On War in the 21st Century*. Zenith Press, St Paul, 2006; Smith, Rupert: *The Utility of Force: The Art of War I the Modern World*. Vintage Books, New York, 2008; Echevarria, Antulio J.: Deconstructing the Theory of Fourth-Generation War. *Contemporary Security Policy*, Vol. 26, No. 2 (2005), pp. 233–241.

[151] The United States Department of Defense (U.S. DoD), Joint Staff Force Development (J7): *Cross-Domain Synergy in Joint Operations: Planner's Guide*, 14 January 2016. [http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cross_domain_planning_guide.pdf?ver=2017-12-28-161956-230], visited 14.4.2020.

[152] Biddle, Stephen & Oelrich, Ivan: Future Warfare in the Western Pacific: Chinese Antiaccess / Area Denial, U.S. AirSea Battle, and Command of the Commons in East Asia. *International Security*, Vol. 41, No. 1 (2016), pp. 7–48.

[153] Renz, Bettina & Smith, Hanna: *Russia and Hybrid Warfare: Going Beyond the Label*. Aleksanteri Papers 1/2016. Aleksanteri Institute, Helsinki, 2016; Thomas, Timothy: 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), pp. 554–575.

[154] Freedman, Lawrence: Asymmetric Wars. *Adelphi Papers*, Vol. 38, No. 318 (1998), pp. 33–48.

[155] Arreguin-Toft, Ivan: How the Weak Win Wars: A Theory of Asymmetric Conflict. *International Security*, Vol. 26, No. 1 (2001), pp. 93–128.

[156] Goldman, Emily O. & Ross, Andrew, L.: Conclusion: The Diffusion of Military Technology and Ideas – Theory and Practice. In *The Diffusion of Military Technology and Ideas*. Goldman, Emily O. & Eliason, Leslie C. (eds.) Stanford University Press, Stanford, CA, 2003, pp. 371–403.

[157] Chase, Jesse: Defining Asymmetric Warfare: A Losing Proposition. *Joint Forces Quarterly*, Volume 61 (2nd Quarter 2011), pp. 115–120.

been defined as asymmetric.[158] The concept of critical infrastructure has highlighted the vulnerability of information societies to attacks by non-state and state actors made using relatively small resources.[159] Cyber warfare itself has been called unconventional and asymmetric.[160] On the other hand, some people feel that the asymmetry of cyberattacks has been exaggerated.[161]

Others focused their attention to the asymmetry produced by the cyber environment instead of the attacks and actors. According to Martin Libicki, because of its digitalisation, the United States is very dependent on the internet and therefore vulnerable, but on the other hand, this also makes it strong, as most of the software used in the world comes from the United States. Libicki also states that nations are quite dependent on the expertise of 'third parties', i.e., international information security companies.[162] In general, however, the Western perspective on cyber asymmetry emphasises the threat caused by it and interprets it as resulting from the characteristics of cyberspace, not from its structures or the balance of power.[163]

Exploring the question of asymmetry is not the exclusive right of Western military science. In today's Russia, asymmetry has been seen as an opportunity for both the strong and the weak. Both can strive for maximum benefits with minimal costs, using creativity, cunning or new technologies. In Russian thinking, asymmetry is linked to calculations of the correlation of forces[164], in which asymmetry can be considered a qualitative divergent, orthogonal and discontinuous variable. Asymmetric actions neutralise or offset (*nivelirovat'*) the opponent's technological superiority. The current Russian military command has shown great interest in the concept of asymmetry.[165] The concept of '*stratagem*', historically related to Chinese military theory, is also very close to the Western and Russian meanings given to asymmetry. In addition, Chinese thinking has highlighted the meaning of 'assassin's maces', based on weapons technology, which can be used for striking at the opponent's weak point.[166]

---

[158] Kaplan, Fred: *Dark Territory. The Secret History of Cyber War*. Simon & Schuster, New York, 2016; Lewis, James A.: National Perceptions of Cyber Threats. *Strategic Analysis*, Vol. 38, No. 4 (2014), pp. 566–578.
[159] Cf. e.g., Clarke & Knake (2010); Clarke & Knake (2019).
[160] NATO: *Allied Joint Doctrine for Cyberspace Operations, AJP-3.20, Edition A Version 1, January 2020*. NATO Standardization Office (NSO), 2020. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf], visited 13.7.2020.
[161] Mahnken (2011), 61–62; Liff (2012); Gartzke & Lindsay (2015); Slayton, R.: What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. *International Security*, Vol. 41, No. 3 (2017), pp. 72–109.
[162] Libicki (2016), 201-209.
[163] Cf. Thomas, Timothy: *Cyber Silhouettes. Shadows Over Information Operations*. Foreign Military Studies Office, Fort Leavenworth, KS, 2005.
[164] Cf. Reach, Clint, Kilambi, Vikram & Cozad, Mark: *Russian Assessments and Applications of the Correlation of Forces and Means*. RAND, Santa Monica, 2020.
[165] Kukkola, Juha: Oveluuden lupaus. *Asymmetria, epäsuoruus ja ei-sotilaalliset toimenpiteet uuden venäläisen sotataidon kiintopisteinä*. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 2: Tutkimusselosteita nro 22, Helsinki, 2022.
[166] Puranen, Matti: *Informaatioherruus. Kiinan sotilasstrategia ja sodan kuva kylmän sodan jälkeen*. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 2: Tutkimusselosteita nro 21, Helsinki, 2022.

The definition of the concept of asymmetry has been considerably more challenging than examining its forms or consequences. In 2001, Steven Metz and Douglas Johnson proposed that asymmetry is: "In the realm of military affairs and national security, […] acting, organizing, and thinking differently than opponents in order to maximize one's own advantage, exploit an opponent's weaknesses, attain the initiative, or gain greater freedom of action."[167] In the context of cyberspace, one of the most interesting definitions of asymmetry is by Oehmen et al. They define asymmetry as: "disproportionate, exploitable imbalance between actors related to, but not limited to, resources, *level of effort*, risk, or consequences in an attack."[168] Among the imbalances in capabilities, Oehmen et al. include the ability to manipulate the terrain to disproportionally favour the defender, which is a useful addition from the perspective of this thesis.

Based on the aforementioned military and cyber warfare-related definitions of asymmetry, we can claim that asymmetry has at least seven different forms. Firstly, asymmetry can be based on the relative imbalance of material resources. Secondly, asymmetry can be based on relatively basic differences in characteristics. The third form of asymmetry is based on differences in the will, interests, understanding of the nature of war and objectives between the parties to the conflict. The fourth form of asymmetry is related to space and is an environmental characteristic that affects the position of the actors involved. It enables or restricts the actor's ability to observe its environment, project force or protect its resources. Fifthly, asymmetry can be based on time. Time can be understood as the actors having a different sense of time[169], or it can also be understood as a resource, as the actor may have either more or less time for achieving its goals than the opponent.[170] On the battlefield, time can be switched with space.

The sixth form of asymmetry is information that can be understood as part of all forms of asymmetry or as an independent form. The characteristics of information – its topicality, completeness or integrity – may serve as coefficients for resources or properties.[171] It can be controlled and it is possible to gain information superiority over an opponent.[172] In fact, information can be seen as asymmetric in its basic nature because it constantly changes and receives new forms, is unpredictable and gains its

---

[167] Metz, S. & Johnson, D. I.: *Asymmetry and U.S. Military Strategy L Definition, Background, and Strategic Concepts*. U. S. Army Strategic Studies Institute: Carlisle, 2001, pp. 3–4, 5–6.
[168] Oehmen, Christopher & Multari, Nicholas: *AiR: Asymmetry in Resilience: Report on the First Meeting on Asymmetry in Resilience for Complex Cyber Systems*, U.S. Department of Energy, 2014, pp. 4. [https://cybersecurity.pnnl.gov/documents/AiR_1.0_Final_Report.pdf], visited 15.4.2020.
[169] On cyclical and linear time cf. Hanska, Jan: *Times of war and war over time: the roles time and timing play in operational art and its development according to the texts of renowned theorists and practitioners*. Doctoral Dissertation. National Defence University Series 1: Research Publications No. 12, Helsinki, National Defence University, 2017.
[170] This view corresponds to the premises of the theory of network centric warfare cf. Alberts, David S., Gartska, John J. & Stein, Frederick P.: *Network Centric Warfare: Developing and Leveraging Information Superiority* (2nd ed.). CCRP Publications, 2000.
[171] Mingers, John & Standing, Craig: What is Information? Toward a Theory of Information as Objective and Veridical. *Journal of Information Technology*, Vol. 33 (2018), pp. 85–104.
[172] Cf. e.g., The United State Department of Defence (U.S. DoD): *Joint Publication 3-13: Information Operations*; 27 November 2012 Incorporating Change 1 20 November 2014. [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf], visited 11.1.2021.

significance when its environment changes.[173] The seventh form of asymmetry is imagination. It is an extreme enabler and creates asymmetry based on human creativity and its ability to manipulate reality.[174]

Governments can shape the information environment by using information power. The use of this power can take many different forms, one of which is the national system of systems of information security and defence. In this work, the system refers to an analytical model that combines the policies and projects aimed at managing a state's information space into a single entity. It is a unified collection of government tools and means for delineating, building, managing and securing the national information space, and for mobilising resources in the information environment. The nature of this system will be reverted to in more detail later. At this stage, it suffices to say that it contributes to channelling cyber power to shaping cyberspace and, further, to producing structural cyber asymmetry.

From a theoretical point of view, any state is capable of using its cyber power potential to shape and control the mutable, technology-based and man-made cyberspace in the preferred direction. Shaping the cyber space may produce a closed national network – or a national segment of the internet. It is a state-controlled part of the cyberspace, which can be technically disconnected from the global internet but still remain capable of functioning normally with regard to services of critical importance to the nation.[175] It is important to understand that closing the national network does not necessarily mean disconnecting all traffic. It can be done in steps and flexibly by controlling traffic to, from and inside the network.[176]

The opposite of a closed national network is an open national network, which is not directly controlled by the state, and, as a rule, cannot be disconnected from the global cyberspace without special preparations or serious disruptions in the critical functions of society and the economy. The term national network is generally used to refer to a set of different systems and networks located in a given geographical area and operated by private and public actors under the legal control of a given state.

The relationship between closed and open networks may lead to structural cyber asymmetry. In their previous study, Kukkola, Ristolainen and Nikkarila examined the relative offensive and defensive capability of closed and open national networks through offensive and defensive cyber operations conducted through different interfaces.[177] In such a conflict, operations may be conducted through interfaces officially designated for traffic (*designated interface*), as well as through unofficial connections

---

[173] Cf. Вепринцев, В.Б., Манойло, А.В., Петренко, А.И. & Фролов, Д.Б.; *Операции информационно-психологической войны: краткий энциклопедический словарь-справочник*. Горячая линия – Телеком, Москва., 2011, с. 22–23.

[174] Cf. Тюшкевич, С. А.: *О законах войны вопросы военной теории и методологии*. Проспект, Москва, 2017, с. 45–47.

[175] Kukkola (2020a), 94–95.

[176] Kukkola, Ristolainen & Nikkarila (2017), 52. Closing process is a more comprehensive concept than closing a network. It refers to the ways in which the standards, technologies, and management and technical solutions to nationally control the confidentiality, integrity and availability of data transfer, storage, and manipulation are developed and deployed.

[177] Kukkola, Ristolainen & Nikkarila (2017), 96.

(*non-designated interfaces*), through *third-party networks* and from inside the national network (*insider interface*). Designated interfaces are monitored and regulated points of traffic exchange points. In theory, traffic through these interfaces can be tracked and attributed, and the interfaces can be disconnected at will. Non-designated interfaces are unregulated and possibly illegal interfaces, which nevertheless technically allow traffic from and into national networks. These may include mobile networks and satellite-based internet services. Third party networks are not directly connected to either open or closed networks, but they can act as launch or intermediate stations for attacks. Insider interfaces require physical connections to the target network using USB, side-channel techniques or other media. The analysis also included a theory and model of using internal, sequential and centrally derived traffic filtering and control levels in the closed national network.

Kukkola, Ristolainen and Nikkarila's analysis was based on a comparison of *the freedom of movement*, *situation awareness* and *decision-making* between the routes of attack.[178] The result of the analysis was that a nation that has closed its network has a disproportionate and exploitable advantage, because it is easier to defend a closed network and to attack an open network from the closed one.[179] Based on their studies, Kukkola, Ristolainen and Nikkarila argued that if a state or a number of states decide to build a closed national network, they will gain a significant strategic advantage vis-à-vis those countries that leave their national networks open.[180] They are thus conducting strategic shaping of the battlefield.

This observation is the foundation of structural cyber asymmetry. States are able to shape the structure of cyberspace in a way that provides a disproportionate advantage if potential opponents refrain from countermeasures. *In other words, structural cyber asymmetry is a characteristic of cyberspace that arises between two or more actors when the structure and rules of cyberspace are shaped so that one actor gains a disproportionate and exploitable offensive and defensive advantage over the others.*[181] It should be noted that the effects of structural cyber asymmetry interact with a wider information environment.

2.4 Analysis concepts of structural cyber asymmetry

In this thesis, the intersection point of cyberspace with other information environments (socio-cognitive, electromagnetic and information-physical) is examined as *digital territory* and battlefield. The concept of digital territory makes it possible to map cyberspace, examine its elements to find asymmetry, and define the subject of the controlling and shaping cyber power. The starting point is that technical images of the network alone do not reveal how networks are managed and controlled or what their military strategic function is. At its simplest, digital territory refers to information infrastructure built and managed by humans. At its most complex, it refers to the social and non-social structures that make the information infrastructure relevant.

---

[178] Ibid.
[179] Ibid.
[180] Kukkola, Ristolainen, & Nikkarila (2017); Kukkola, Ristolainen, & Nikkarila (2019).
[181] The concept of structural cyber asymmetry derives from a conference paper written by Juha-Pekka Nikkarila and Mari Ristolainen (Nikkarila, Juha-Pekka & 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).*

The map of a digital territory contains technical, functional, normative, economic, military and political elements. In them, technically free flow of information meets human control. There is no single way of mapping a digital territory; it must be done on a case-by-case basis. In this thesis, the elements of digital territory are treated as subsystems of information security and defence (see Section 3.1) and a closed national network or national segment of the internet as one of its real representations. The relationships between the different concepts are described in Appendix 1.

Even though structural cyber asymmetry is related to the resources of the actor (state), it is not a direct consequence of their use, but a characteristic of cyberspace resulting from the change in the digital territory and the position of the actors in relation to each other. As such, structural cyber asymmetry is not an offensive or defensive characteristic; it can be both. It cannot be created directly, but by influencing the digital territory through technology, *governance*, standards and policies. These are methods of cyber strategy.

In this thesis, the exploitable and disproportionate advantage offered by structural cyber asymmetry to one actor over another is examined through the concepts of freedom of action, common situation picture, command and control, and resilience. Using these concepts, it is possible to examine the impacts of potential structural asymmetry and to verify them in qualitative terms. To put it simply, they are dependent variables that indicate the existence or absence of asymmetry. This set-up is illustrated in Figure 1.

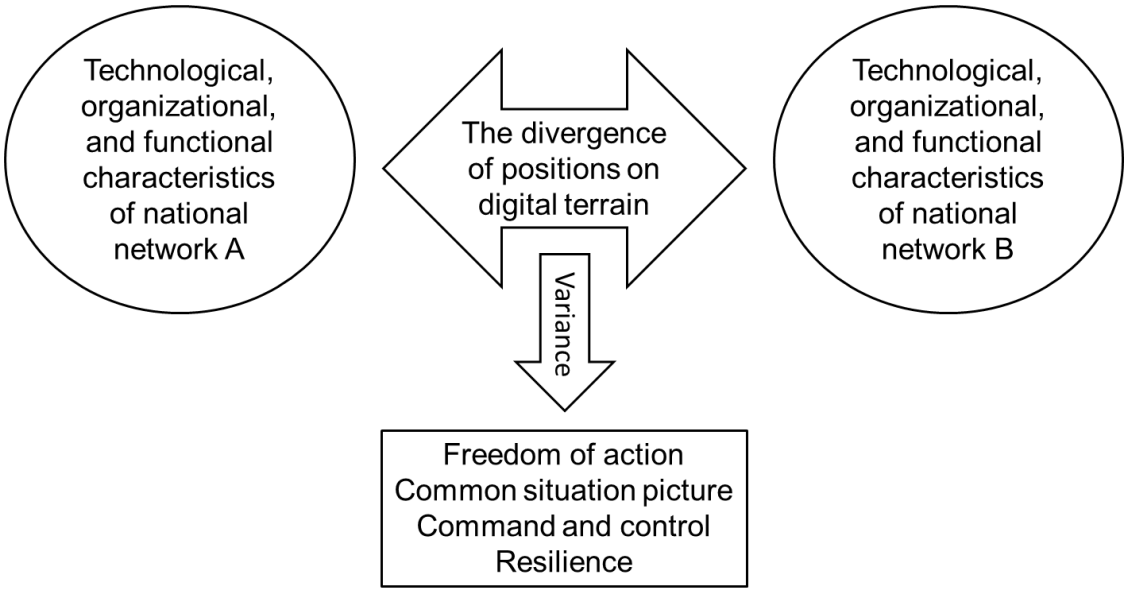

Figure 1: Manifestation of structural cyber asymmetry

By comparing the freedom of action, common situation picture, command and control, and resilience of national networks between the parties, it is possible to make observations on disproportionate and exploitable advantages. To put it simply, in this thesis the above-mentioned concepts refer to the technological, organisational and functional characteristics of closed and open national networks that can affect both

the offensive and defensive capabilities. In other words, the capabilities of the actual 'cyber forces' are excluded from the examination.

2.4.1 Freedom of action

Historically, the freedom of manoeuvre has been considered one of the key concepts of warfare in the Western, Soviet and Russian theory of warfare alike.[182] Movement is an essential part of the manoeuvre-warfare theory, which emphasises destabilising and confusing the opponent instead of degrading or destroying the main combat force.[183] *The freedom of action* is a more general concept than freedom of manoeuvre and simply means freedom to act in a certain domain while at the same time contesting the enemy's freedom of action. The concept is better suited to cyberspace, as there 'movement' is tied to user privileges and connections and is not continuous in the same way as in physical domains.[184] Movement is also discontinuous because the force has no persistence and the actions can shift between the different layers of cyberspace.[185] In a cyber domain, the parties to the conflict may be present and operate in the same space. Their forces do not actually cross paths. In other words, there are no two forces constantly manoeuvring in relation to each other and influencing each other. The terrain is variable, and the concepts of 'inner and outer frontlines' are practically meaningless. Therefore, traditional material calculations of the correlation of forces lose their meaning because there is no space or time where to position troops against each other.[186] Furthermore, at the operational and strategic level, the concept of freedom of action detaches the acts of directing and manoeuvring forces from 'fire', gun mounts and ammunition, which refer to physically destroying, paralysing or degrading the adversary. This is important to take into account because the law of conservation of energy does not exist or functions differently in cyberspace than in the physical domain.[187] In other words, physical destruction of the target is replaced by affecting the targeted system through effects causing changes, which reflects the effects-based approach to operations.[188]

In cyberspace, the aggressor's ability to achieve its goals is based on at least one vulnerability that the defender has not recognised in its own systems.[189] In cyberspace, the aggressor's freedom of action and the consequent scope of influencing depend on

---

[182] Liddell Hart, B. H.: *Strategy* (2nd rev. ed.) Meridian, New York, 1991, pp. 323–328; Fuller, J. F. C.: *The Foundations of the Science of War*. A Military Classic Reprint (org. 1925). U.S. Army Command and General Staff College Press, Fort Leavenworth, Kansas, 1993; Svechin, Aleksandr A.: *Strategy*. East View Information Services, Minneapolis, Minnesota, 1992, pp. 276–278; Isserson, G. S.: G. S. *Isserson and the War of the Future: Key Writings of a Soviet Military Theorist*. Richard W. Harrison (trans., ed.). McFarland & Company, Jefferson, NC, 2016, pp. 61–65, 288.
[183] Lind, William S.: *Maneuver Warfare Handbook*. Westview Press, Boulder, Colorado, 1985, pp. 6–7.
[184] Kiviharju, Mikko & Huttunen, Mika: Kybertaktiikkaa – Yleisten periaatteiden soveltuvuudesta kybertoimintaympäristössä. In *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, pp. 161–180, 167.
[185] Kiviharju & Huttunen (2018), 170–171.
[186] Cf. Kallberg, Jan & Cook, Thomas S.: The Unfitness of Traditional Military Thinking in Cyber. Four Cyber Tenets That Undermine Conventional Strategies. *IEEE Access*, Vol. 5, 2017, pp. 8126–8130.
[187] On the tactical level of cyber operations cf. Kantola, Harry, Huttunen, Mika & Kiviharju, Mikko: Taistelun elementit kybertoimintaympäristössä. In *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, pp. 142–152, 143.
[188] Mälkki, Juha: Vaikutusperusteisen operatiivisen ajattelun (EBAO) sotataidolliset lähtökohdat. *Tiede ja Ase*, Vol 69 (2010), pp. 7–31.
[189] Libicki (2009), xiv; Libicki (2016), 51–52.

the attack surface, the depth of defence, the time available, the novelty of the means used and the defender's passive and active countermeasures.[190] In the initial situation, the defender has, in principle, full freedom of action, since it controls the operating conditions and structure of the space to be defended.[191] In practice, however, at the level of the national network, the defender's freedom of action is always limited due to, for example, legislation, competencies and technical solutions. In addition, the defender cannot affect the attack if it does not detect it being prepared and is thus, principally, the responding party. In addition, the aggressor may be able to close out the defender from its own systems, or the defender may modify or close them, thus locally and temporally denying the freedom of action from both parties. Therefore, protection becomes an integral part of freedom of action and the struggle over it at the operational and strategic level of the cyber battlefield.

The freedom of action in cyberspace also differs from other operating domains in the sense that it can be seen as 'a chain' or continuum of operations or as countermeasures. These chains include the *'cyber kill-chain'*[192] and its various versions as well as different cyber security processes. So, it is more a question of a process than movement. In cyber combat operations, a process is set against another process. The aggressor reconnoitres the target, creates malware or other means to gain access to the target, penetrates the target, acquires the required operating rights at the target, maintains its presence, and performs the task.[193] Defence makes efforts aimed at eliminating vulnerabilities, encrypting the systems, deceiving any attackers, detecting and preventing attacks, removing attackers from the systems, and restoring functionalities.[194] It is also essential that the freedom of action cumulates and may lead to the adversary being unable to respond to new events. However, this inability is often temporally and locally limited and temporary, as services can often be restored to a normal state after the operation has ended or after the destroyed systems have been replaced with new ones and the services have been rebuilt.[195] In other words, in cyberspace the freedom of action increases the opportunities to influence and the significance of effects but is not a permanent property or ability.

In cyberspace, the freedom of action of both the attacker and the defender is the sum of the margins of cyberspace and each actor's user privileges (capabilities). *Therefore,*

---

[190] Kärkkäinen, Anssi: Kyberpuolustuksen taistelukenttä nyt ja tulevaisuudessa. In *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, pp. 72–83, 81; Taillat, Stéphane: Disrupt and Restraint: The Evolution of Cyber Conflict and the Implications for Collective Security. *Contemporary Security Policy*, Vol. 40, No. 3 (2019), pp. 368–381, 372–373.
[191] Kiviharju & Huttunen (2018), pp. 170–171.
[192] Cf. Kim, Hyeob, Kwon, HyukJun & Kim, Kyung Kyu: Modified Cyber Kill Chain Model for Multimedia Service Environments. *Multimedia Tools and Applications*, Vol. 78 (2019), pp. 3153–3170.
[193] Hutchins, Eric M., Cloppert, Michael J. & Amin, Rohan M.: *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* [https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf], visited 29.6.2020; Kim, Kwon & Kim (2019); MITRE: *ATT&CK Matrix for Enterprise.* [https://attack.mitre.org/matrices/enterprise/], visited 29.6.2020.
[194] National Institute of Standards and Technology (NIST): *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, February 12, 2014.* [https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf], visited 29.6.2020; Andress & Winterfeld (2014).
[195] Kiviharju & Huttunen (2018), 168–169. The views on the permanent effects of cyber operations and destructive power differ markedly between theorists cf. Ashraf, Cameran: Defining cyberwar: towards a definitional framework. *Defense & Security Analysis*, Vol. 37, No. 3 (2021), pp. 274–294.

the freedom of action in cyberspace or cyber battlefield is defined as the ability to execute offensive and defensive cyber operations in one's own and an adversary's networks and to deny an adversary the ability to do the same. Regarding the freedom of action, the object of analysis is the impact of the boundaries and internal structure of closed and open national networks on the actors' ability to affect the targets or to deny that effect and the actors' ability to operate in the networks. This thesis only deals with how the network structure affects the situation, i.e., access to national networks and opportunities to operate in them.

2.4.2 Common situation picture

Situational awareness refers to analysed, structured, and continuously updated aggregated information about the status of a domain.[196] In other words, situational awareness is topical, temporally and locally limited data, a collection of situational information on the past and present, which is collected in an information system and presented to support decision-making. Situational awareness may also include a component related to assessing future developments. *A common situation picture, on the other hand, is the information available for the shared use of one or more users. It is a mutually understood model and description of the information that affects the interpretation of a situation*. A common situation picture requires coordinating structures (organisation), actions (processes - service architecture) and information (data contents and data models) to produce well-functioning information flows.[197] A good situational awareness system enables making decisions quicker and with more certainty.[198]

The concept of situational awareness has been used above all by theoreticians of *Network Centric Warfare (NCW)* in the context of cyber and information warfare.[199] Martin Libicki has defined *situational awareness*[200] as knowing the disposition, location and general intentions of the enemy forces, which enables more effective planning, prevents surprise and makes it possible to surprise the adversary.[201] In other words, perfect situational awareness contains information of all items of military significance on the battlefield, including the intentions of the other players involved.[202] According to NCW thinking, one of the factors behind making and implementing decisions that are better and quicker than those made by the adversary, and thus the foundation of information superiority, is having an accurate and up-to-date situation picture. Theoretically, this superiority, the importance of which is recognised by American, Russian and Chinese theoreticians alike, should lead to victory on a modern battlefield. In

---

[196] Kuusisto, Rauno: *Tilannekuvasta täsmäjohtamiseen. Johtamisen tietovirrat kriisin hallinnan verkostossa*. Liikenne- ja viestintäministeriön julkaisuja 81/2005, Helsinki, 2005; Rantanen, Hannu: *Tilannekuvan tuottaminen, hyödyntäminen ja jakaminen - Kriittinen nykytilan tarkastelu*. Aluehallintovirastojen julkaisuja 42/2018, Vaasa, 2018.
[197] Kuusisto (2005), 9–14.
[198] Kuusisto, Rauno: *Aspects On Availability: A Teleological Adventure Of Information In The Lifeworld*. Doctoral Dissertation. Series / National Defence College, Department of Tactics and Operations Art. 1, 2004.
[199] Cf. e.g., Alberts, David S. & Papp, Daniel S. (eds.): *The Information Age Anthology – Volumes I-III*. CCRP Publication Series, 1997–2000.
[200] In English and in military context s*ituation awareness* (SA) often refers to Mica Endsley's model of dynamic decision making. (Endsley, M. R.: Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, Vol. 37, No. 1 (1995), pp. 32–64.)
[201] Libicki, Martin C.: *What Is Information Warfare?* National Defense University, Institute for National Strategic Studies, Washington, D.C., 1995, pp. 5.
[202] Alberts, David: The Future of Command and Control with DBK. In *Dominant Battlespace knowledge*. Libicki, Martin & Johnson, Stuart E. (eds.) NDU Press Book, Washington, D.C., 1995, pp. 29.

theory, it transforms information into an effective power and multiplies the impact of material power.[203] Unlike the freedom of action, situational awareness is not dependent on the situation picture of the opposing party, since both the attacker and the defender can theoretically have a perfect situation picture related to their own task. On the other hand, one party may have a better situation picture than the other, and this may, in principle, lead to quicker and better decisions and, going forward, to victory.

Cyber security situation awareness refers to an aggregate description of "the availability and security situation of information systems at a specific point in time and the prevailing status of the cyber environment."[204] In cyberspace, the forming of a situation picture is restricted by the complexity of the operating environment; changing topology; the attacks blending in with other data; anonymity; machine speed; potentially long interval between attacks and their impacts; and technical challenges related to the processing and sharing of data.[205] Therefore, due to the nature of cyberspace, the forming of a situation picture and situational awareness requires several sources of information; highly automated and rapid data collection, retention, processing and analysis; sharing and integration of information between systems and organisations; filtering data from a technical level and presenting it in a form suited for the higher levels of decision-making; and protecting information and systems from manipulation and disruptions.[206]

The situation picture is a significant part of cyber warfare. It enables detecting deviations in the systems and, on the other hand, operations in target networks.[207] Without knowledge of the target system, it is practically impossible to conduct a cyberattack.[208] The defender is also dependent on the situation picture: If they do not know about the attack, they cannot defend themselves against it. One can only prevent attacks one is aware of. The command-and-control process requires accurate and timely information to enable centralised C2 and decentralised operations in the cyber battlespace.[209] From the perspective of decision-making, identifying the origin of attacks is important, and the accuracy of the cyber situation picture plays an important role in attributing attacks.[210]

---

[203] Hayes, Richard E. & Alberts, David S.: *Power to the Edge. Command… Control… in the Information Age*. CCRP, 2005, pp. 172–173; Wortzel, Larry M.: *The Chinese People's Liberation Army And Information Warfare*. Strategic Studies Institute and U.S. Army War College Press, Carlisle Barracks, PA, 2014; Kukkola (2020a).
[204] Sanastokeskus TSK (2018), 22.
[205] Kott, Alexander, Wang, Cliff, Erbacher, Robert F. (Eds.): *Cyber Defense and Situational Awareness*. Springer International Publishing, London, 2014.
[206] Kuusisto (2014); Matthews, Earl D., Arata, Harold J. III & Hale, Brian L.: Cyber Situational Awareness. *The Cyber Defense Review*, Vol. 1, No. 1 (Spring 2016), pp. 35–46, 40; Multinational Experiment 7: *Outcome 3 – Cyber Domain Objective 3.4 Cyber Situational Awareness Standard Operating Procedure. Version 1.0, 1 December 2012*. [https://www.hsdl.org/?view&did=760553], visited 6.7.2020; NATO: *Military Strategic Level Decision Making within a (Future) Framework of Cyber Resilience*. STO-TR-SAS-116, 24.8.2020. NATO Unclassified Rel To PFP. DOI: 10.14339/STO-TR-SAS-116.
[207] Kärkkäinen (2018).
[208] Brantly (2016).
[209] Lehto, Martti & Limnéll, Jarno: Kybersodankäynnin kehityksestä ja tulevaisuudesta. *Tiede- ja Ase*, Vol. 75 (2017), pp. 179–212, 199.
[210] Rid, T. & Buchanan, B.: Attributing Cyber Attacks. *Journal of Strategic Studies*, Vol. 35, No. 1 (2015), pp. 4–37; Lin, Herbert: Attribution of Malicious Cyber Incidents: From Soup to Nuts. *Journal of International Affairs*, Vol. 70, No. 1 (Winter 2016), pp. 75–137.

Analysing situational awareness in the context of cyberspace is, in principle, challenging, as it is formed in a cognitive dimension, i.e., in the decision-maker's minds.[211] On the other hand, the structures, processes and data contents and models as well as data flows required for a unified situation picture can be examined externally.[212] Therefore, the items defined as targets of analysis in regard to the common situation picture are the processes, organisations and technology related to the collection, formation, analysis, sharing and monitoring of situational information.[213]

2.4.3 Command and control

To put is simply, command and control is related to the achievement of the organisation's objectives and goals. In the United States Armed Forces, the concept *command and control* involves a process consisting of planning, preparation, implementation and assessment associated with all phases of the process.[214] *Command* includes the aspects of authority, responsibility, decision-making and leadership.[215] *Control* includes the aspects of guidance, feedback, information and communication, i.e., is an instrument of *command*.[216] In the Soviet Union, the term *control* used by Norbert Wiener, the inventor of cybernetics, was translated into *upravlenie*, which meant regulation, administration or management to reach a set target state.[217] In Russian military thinking, the command and control (*upravlenie voiskami*) includes the collection and analysis of information; decision-making; command, planning; organisation and maintenance of cooperation and support functions; leading the process of preparing troops for battle; organising the control and support of lower echelons; direct command of combat operations; and maintaining the morale of the troops.[218]

Decision-making is an integral part of command and control. According to Said Elbanna, in decision-making research, the level of decision-making has been considered to define the characteristics of decision-making.[219] According to Yarger, strategic decision-making seeks to influence and shape the future environment.[220] In terms of

---

[211] Cf. e.g., Siukonen, Veikko: *APT-Operaation inhimilliset tekijät: Operaation tarkastelu päätöksenteon näkökulmasta*. Jyväskylän yliopisto, Tietojenkäsittelytiede, Master's thesis, 2019.
[212] Cf. e.g., Timonen, Jussi: *A Common Operating Picture for Dismounted Operations and Situation Room Environments*. Doctoral Dissertation. National Defence University Series 1: Research Publications No. 19, Helsinki, 2018.
[213] Koskinen-Kannisto, Anne: *Situational Awareness Concept In A Multinational Collaboration Environment Challenges in the Information Sharing Framework*. Doctoral Dissertation. National Defence University Department of Military Technology Series 1, n:o 31, Helsinki, 2013, pp. 198–199.
[214] The United States Department of Defense (U.S. DoD): *DOD Dictionary of Military and Associated Terms, December 2020*: Command and control, pp. 40. [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2020-06-18-073638-727], visited 11.1.2021.
[215] Pigeau, Ross, & McCann, Carol: Re-conceptualizing Command and Control. *Canadian Military Journal*, Vol. 3, No 1. (Spring 2002), pp. 53–63.
[216] The Department of the Army of the United States of America: *ADP 6-0 31 July 2019. Mission Command: Command and Control of Army Forces*. Headquarters Department of the Army, Washington D.C., 2019.
[217] Rindzeviciuté, Eglé: *Constructing Soviet Cultural Policy: Cybernetics and Governance in Lithuania after World War II*. Doctoral Dissertation. Linköping University, Linköping, 2008.
[218] *Военный энциклопедический словарь (ВЭС)*: Управление войсками (силами) [http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=10705@morfDictionary], visited 3.7.2020.
[219] Elbanna, Said: Strategic Decision-Making: Process Perspectives. *International Journal of Management Reviews*, Vol. 8 No. 1 (2006), pp. 1–20.
[220] Yarger (2006), 21–23.

military science and art, strategic decision-making, and command and control are associated with the achievement of the objectives of war.[221] In a situation where the time and resources available are limited, John Boyd's OODA Loop (Observe-Orient-Decide-Act) has been used to model decision-making.[222] According to the model, an individual continuously observes his surroundings, reacting if necessary, and orients himself using his inner models, makes decisions and acts. The aim is to get inside the adversary's command and control cycle more rapidly and destabilise them.[223]

The information technology used in support of command and control has been considered to improve the quality and speed of making and executing decisions.[224] The execution of command and control is also influenced by the way it is implemented. In centralised decision-making, information is collected into a single point where the decision is made, and the orders are then forwarded to those executing them. In decentralised decision-making, there are several decision-makers who share a common goal and situational information. A centralised C2 system is vulnerable but cost-effective. A decentralised one, on the other hand, supports the benefits gained from networking, such as self-synchronisation, but it is restricted by geography and interdependencies between functions.[225] A centralised C2 system is rigid and slow to respond at a tactical level, and as a closed system it can, theoretically, sink into entropy.[226] A decentralised system may be flexible, but networking increases complexity and the possibility of disruptions and unpredictable incidents.[227] Theoretically, under conditions of perfect communications and optimally functioning systems, decentralised decision-making is based on better knowledge and is faster than centralised decision-making.[228] Between a centralised and decentralised system, lies a stove-piped system which, in principle, is the weakest solution for achieving common goals, because it minimises the exchange of information, and the decision-making does not serve the common goal. In addition, it is the most vulnerable command and control model in terms of organisation.[229]

In the cyber environment, decision-making and command and control have their own characteristics. Decision-making and execution are affected by anonymity and lack of

---

[221] Gray, Colin S.: *Strategy and Politics*. Routledge, New York, 2016.
[222] Olsen (2012); Bryant, David J.: Rethinking OODA: Toward a Modern Cognitive Framework of Command Decision Making. *Military Psychology*, Vol. 18, No. 3 (2006), pp. 183–206, 185–187, 185–187; Osinga, Frans: 'Getting' A Discourse on Winning and Losing: A Primer on Boyd's 'Theory of Intellectual Evolution'. *Contemporary Security Policy*, Vol. 34, No. 3 (2013), pp. 603–624.
[223] Hammond, Grant T.: *The Mind of War. John Boyd and American Security*. Smithsonian Books, Washington, D.C., 2001, pp. 165; Osinga (2013), pp. 618–619.
[224] Molloy, Steve & Schwenk, Charles R.: The Effects of Information Technology on Strategic Decision Making. *Journal of Management Studies*, Vol. 32, No. 3 (1995), pp. 283–311.
[225] Athans, Michael: Command and Control (C2) Theory: A Challenge to Control Science. *IEEE Transactions on Automatic Control*, Vol. AC-32, No. 4 (April 1987), pp. 286–293; Van Bezooijen, B. J. A., Essens, P. J. M. D. & Vogelaar, A. L. W.: Military Self-synchronization: An Exploration of the Concept. *11TH ICCRTS, Coalition Command and Control in The Networked Era 27 September 2006*.
[226] Hammond (2001), 164–165.
[227] Perrow, Charles: *Normal Accidents: Living with High Risk Technologies (*updated edition*)*. Princeton University Press, Princeton, 1999.
[228] Lee, Tony S., Ghosh, Sumit & Nerode, Anil: Asynchronous, Distributed, Decision-Making Systems with Semi-Autonomous Entities: A Mathematical Framework. *IEEE Transactions On Systems, Man, And Cybernetics—Part B: Cybernetics*, Vol. 30, No. 1, February 2000, pp. 206–212.
[229] Hitchins, D. K.: A General Theory of Command and Control. *1989 Third International Conference on Command, Control, Communications and Management Information Systems, Bournemouth, UK, 1989*, pp. 111–126.

transparency, uncertainty, complexity, speed of situations (machine time), authority issues and cooperation factors, and the emphasised importance of information.[230] Command and control in cyberspace is completely dependent on systems and networks – operations taking place in cyberspace cannot be commanded from outside the space. Systems must be flexible and adaptable, which requires decentralised support infrastructure and a certain degree of autonomy.[231] The increasing complexity of C2 environments may lead to uncontrolled emergent phenomena if the interaction between decision-makers, exchange of information and decision-making rules are not controlled.[232]

C2 systems allow defenders to monitor traffic, detect deviations, change the structure of networks and prevent unwanted traffic.[233] Command connections are also critical to success in terms of attacks. Attackers are aware of the defender's ability to control the operating environment and try to decentralise, conceal, hide from sight and mask their connections. C2 systems themselves may be the target of manipulation and attacks.[234]

In other words, C2 is tied to the organisation, processes, the environment, technology and the objective of the system. Since this research paper focuses on differences between national networks, attention – in the broad sense of the word –is paid to systems used for information management, decision-making support and execution at the strategic, operational and tactical level. When it comes to national networks, the role of private operators and cooperation between the public and private sector must also be taken into account.[235] In other words, the analysis of command and control focuses on *command and control structures, i.e., on where and in what context decisions are made, and processes, i.e., how decisions are made and communicated, and technology that enables these structures and processes*.[236] The structures, processes and technology are assessed through the speed, accuracy and control they provide.

---

[230] Smeets, Max & Work, J.D.: Operational Decision-Making for Cyber Operations: In Search of a Model. *The Cyber Defense Review*, Vol. 5, No. 1 (2020), pp. 95–112; Chen, Jim Q.: A Strategic Decision-Making Framework in Cyberspace. In *Developments in information security and cybernetic wars*. Sarfraz, Muhammad (ed.) IGI Global, Hershey, PA, 2019, pp. 64–75; Brantly (2016).

[231] Carvalho, M., Eskridge, T. C., Ferguson-Walter, K. & Paltzer, N.: MIRA: A Support Infrastructure for Cyber Command and Control Operations. *2015 Resilience Week (RWS), Philadelphia, PA, 18-20 Aug. 2015*.

[232] Ma, Lin & Wang, Chaowei: Study of Decision-making Progress and Its Emergence in System of Systems. *2012 Prognostics & System Health Management Conference (PHM-2012 Beijing) 23-25 May 2012, Beijing, China*.

[233] Gardiner, Joseph, Cova, Marco & Nagaraja, Shishir: *Command & Control. Understanding, Denying and Detecting.* University of Birmingham, February 2014. [https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf], visited 2.7.2020. The concept of *Moving Target Defence* is based on the continuous changing of the configuration of cyber systems. This allows the defender to change the reconnaissance, attack, and monitoring and defence surface of the protected system. (Sengupta, Sailik, Chowdhary, Ankur, Sabur, Abdulhakim, Alshamrani, Adel, Huang, Dijiang & Kambhampati, Subbarao: A Survey of Moving Target Defenses for Network Security. *IEEE Communications Surveys & Tutorials 2020*, [https://arxiv.org/abs/1905.00964v2], visited 11.1.2021.

[234] Hartmann, Kim & Steup, Christoph: Hacking the AI – the Next Generation of Hijacked Systems. In *2020 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade*. Jančárkova, Lindström, L., Signoretti, M., Tolga, I. & Visky, G. (eds.). CCD COE Publications, Tallinn, 2020, pp. 327–349.

[235] The United States' Cyberspace Solarium Commission report summarises this issue (Cyberspace Solarium Commission: *End Report,* March 2020.
[https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view], visited 1.7.2020.).

[236] The evaluation of the quality or correctness of the decision making would require data on the intentions and results of cyber policies which are not available in the context of this study. (Howard, Ronald & Abbas, Ali E.: *Foundations of Decision Analysis*. Pearson, London, 2015).

2.4.4 Resilience

In cyberspace, it is almost impossible to permanently destroy an attacker's offensive capabilities or to seek complete defence.[237] Both the attacker and the defender base their actions on the same space the continuous operation of which they must guarantee. An operational cyberspace works like a fortress or a friendly area that neutralizes the threat, ensures the control of resources and processes, and provides an opportunity to achieve freedom of action in one's own space. This requires resilience.

The concept of resilience lacks an internationally shared meaning, and it has even become a contested concept.[238] Resilience has usually been employed to refer to the return to a normal state, but when examining complex adaptive systems, such as cyberspace, it is difficult to define what is meant by normal. According to Alexander Kott, resilience can be studied as a low sensitivity to disruptions, ability to reduce the impacts of disruptions or to prevent their spread, ability to neutralise cyber impacts or ability to adapt to such impacts.[239] Resilience lies between stability and antifragility, the former being related to the maintenance of functions and the latter to them being remedied to a stronger level than before. However, it should be noted that, following the adaptation, the system's objectives or operating principles should not change to a significant extent, or otherwise the system loses its original character.

Cyber resilience has become an important part of national cyber strategies.[240] Cyber resilience should deny the opponent the advantages they seek with their attacks by strengthening the resilience of the national critical infrastructure. For example, Martin Libicki argues for the kind of cyber resilience that includes redundancy, prioritisation, diversity, rapid response capability, *loose couplings*, cyber-safe attitudes, testing, analysis and continuous technical development.[241] In Russia, the 'Act on sovereign internet' of 2019 made resilience (*ustoičhivost'*)[242] one of the basic elements of the Russian internet alongside security and integrity.[243] In Russia, the focus of the concept of resilience has shifted from the set of norms for protecting the critical infrastructure to cyberspace, and is strongly associated with the set of concepts used in the contexts of information warfare, and C2 warfare.[244]

The concept of cyber resilience being used in this thesis was defined in Chapter 2.2. as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources. In other

---

[237] Libicki (2009), 59–61; Nye (2016/2017).
[238] Fjäder, Christian: The Nation-state, National Security and Resilience in the Age of Globalisation. *Resilience*, Vol.2, No.2 (2014), pp. 114–129; Humbert, Clemence & Joseph, Jonathan: Introduction: The Politics of Resilience: Problematising Current Approaches. *Resilience*, Vol. 7, No. 3 (2019), pp. 215–223.
[239] Kott, Alexander: *Information Warfare and Organizational Decision-Making.* Artech House, London, 2007, pp. 216.
[240] Cyber Solarium Commission (2020).
[241] Libicki (2016), 176.
[242] Kukkola (2020a). In military context cyber resilience has been described as the ability of an ICT network to support command and control during a cyber-attack. Resilience is based on survivability, reliability, and noise tolerance. (Коцыняк М.А., Кулешов И.А., Кудрявцев А.М. & Лаута О.С.: Киберустойчивость Информационнотелекоммуникационной Сети. Бостон-спектр, Санкт-Петербург, 2015, с. 7–8).
[243] ФЗ-90 (2019).
[244] Pynnöniemi, Katri & Busygina, Irina: Critical Infrastructure Protection and Russia's Hybrid Regime. *European Security*, Vol.22, No.4 (2013), pp. 559–575; Kukkola (2020a), pp. 241.

words, it refers to the services and systems constituting cyberspace, with components related to network and information technology.[245] Cyber resilience differs from defence because it is based on minimising risks and on recovery, and not on active measures to protect a target, in principle fully, from harmful impacts.[246] Resilience has similarities with deterrence by denial, since it is based on defeating the opponent's efforts and minimising impacts.[247] Resilience differs from security, which is based on the lack of threats, since resilience accepts the continuous presence of the risk of threats as a basis for preparation and adaptation.[248] In other words, the analysis of resilience focuses on critical information infrastructure and the conditions for its continued operation in open and closed national networks. Another subject that emerges as a subject of analysis are the systems and methods used to guarantee the continued operation of the critical information infrastructure.[249]

[245] Ross, Graubart, Bodeau, & Mcquaid (2018); Cf. myös Vlacheas, Panagiotis T., Stavroulaki, Vera, Demestichas, Panagiotis, Cadzow, Scott & Slawomir Gorniak: *Ontology and taxonomies of resilience*. ENISA, 2011. [https://www.enisa.europa.eu/publications/ontology_taxonomies/at_download/fullReport], visited 1.5.2020.
[246] Fjäder (2014).
[247] Gartzke & Lindsay (2015).
[248] Joseph, Jonathan: Resilience as Embedded Neoliberalism: A Governmentality Approach. *Resilience*, Vol. 1, No. 1 (2013), pp. 38–52.
[249] Geers, Kenneth: The Cyber Threat to National Critical Infrastructures: Beyond Theory. *Information Security Journal*: A Global Perspective, Vol. 18, No. 1 (2009), pp. 1–7.

3. Russian national segment of the internet

This chapter answers the research question: What is the Russian national segment of the internet and its relationship with the concepts of information security and defence system and closed national network? The chapter describes the basics of general system theory, certain factors of Russian strategic culture and the characteristics of the Russian state as well as the development of the Russian national segment of the internet, which is used as a basis for shaping the model for the system of systems of national information security and defence. At the end of this chapter, the characteristics of a theoretical open national network are presented.

3.1 Systems thinking and strategic cultural ideas

Systems thinking is helpful for structuring the cyber environment.[250] According to systems approach, phenomena should be approached from the perspective of the relationships between their constituent parts, the principles of organisation and in terms of wholes rather than as individual items.[251] According to Peter Checkland, in the *systems approach*, the world is seen to consist of *structured wholes* that are able to preserve their identity and integrity in relation to their environment. Systems cannot be observed directly, but the task of the researcher is to examine the reality and define the systems.[252]

According to systems thinking, systems can be mechanical, biological or social.[253] Systems have also been divided into closed and open systems, depending on whether they exchange matter, energy or information with their environment or not.[254] The most open systems are complex adaptive systems that evolve and change with their environment.[255] In other words, systems thinking can be equally applied to material and technological systems and forms of human activity.

According to Talcott Parsons, who emphasises the functionality of social systems, systems have four types of primary functions: adaptation, goal-attainment, integration and pattern-maintenance.[256] Niklas Luhmann, on the other hand, has argued that each system has been built around a unique process.[257] In any case, all social systems can refer to historically unique governance mechanisms that supervise and control the

---

[250] Hammond, Debora: *The Science of Synthesis. Exploring the Social Implications of General Systems Theory*. The University Press of Colorado, Boulder, 2003.
[251] Weinberg, Gerald M.: *An Introduction to General Systems Thinking*. Dorset House Publishing, New York, 2001.
[252] Checkland, Peter: *Systems thinking, Systems Practice*. John Wiley & Sons ltd., New York, 1993; Checkland, Peter: Soft Systems Methodology: A Thirty-Year Retrospective. *Systems Research and Behavioral Science Syst. Res*. 17 (2000), pp. 11–58.
[253] Checkland (2000).
[254] Cf. Heylighen, Francis: *Web Dictionary of Cybernetics and Systems*. [http://pespmc1.vub.ac.be/ASC/INDEX-ASC.html], visited 23.9.2019.
[255] Bousquet, Antoine & Curtis, Simon: Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations. *Cambridge Review of International Affairs*, Vol. 24, No. 1 (March 2011), pp. 43–62.
[256] Parsons, Talcott: *Social Systems and the Evolution of Action Theory*. Free Press, New York, 1977.
[257] Luhmann (1995).

state of society, steering it in the preferred direction based on feedback. This allows the division of the system into functional systems (politics, economy, law, etc.)[258] and dismantling them into regimes of organisations and rules.[259]

According to the 'soft' systems approach applied in this thesis, social systems can be found and defined by researchers, and no *a priori* functions are set for them.[260] Based on this approach, a system is understood as *an entity of interactive objects that has boundaries in relation to other systems, internal interrelationships and principles of organisation, and a function and goal.*[261] The definition was chosen based on the fact that the object of interest in the thesis is an organised system, created for a specific purpose by humans or created through human activity, with technological components.[262]

Systems can be examined as entities consisting of subsystems. Such a *system of systems* is composed of multiple subsystems, the interactions of which enable the pursuit of goals which no individual subsystem can achieve alone.[263] Each subsystem has its own functions, they can operate on their own, have their own *management* mechanisms, and are often separate but interconnected, by means of exchanging information, for example.[264] According to Boardman and Sauser, systems of systems are characterised by autonomy, independent subsystems, diverse internal interconnections, internal diversity and emergence.[265] The more complex[266] systems, and systems of systems are, and the more compact the *couplings* between their component parts are, the more likely it is that the systems function unpredictably or produce unexpected results.[267] An information security and defence system, to be presented later, is seen as a *goal-seeking*[268] system of systems, i.e., it receives information-based positive or negative feedback on its operation in relation to its environment and is thus able to modify its own operations, environment or other systems with increasing efficiency to achieve its goal.[269]

---

[258] Habermas, Jürgen: Talcott Parsons: Problems of Theory Construction. *Social Inq*. Vol 51, No. ¾ (1981), pp. 173–196; Luhmann, Niklas: *Social Systems*. Stanford University Press, Stanford, Cal., 1995.
[259] Esmark, Anders: The Functional Differentiation of Governance: Public Governance Beyond Hierarchy, Market and Networks. *Public Administration*, Vol. 87, No. 2 (2009), pp. 351–370.
[260] Checkland (2000).
[261] This definition is based on de Rosnay (Rosnay, Joël de: *The Macroscope A new world scientific system*. Harper & Row, Publishers, New York, 1975. [http://pespmc1.vub.ac.be/macroscope/], visited 23.9.2019).
[262] On system typology cf. Ackoff, Russell L.: *Ackoff's Best. His Classic Writings on Management*. John Wiley & Sons, Inc., New York, 1999.
[263] Meentemeyer, Scott M., Sauser, Brian & Boardman, John: Analysing a System of Systems Characterisation to Define System of Systems Engineering Practices. *International Journal of System of Systems Engineering*, Vol. 1, No. 3, 2009, pp. 329–346; Krygiel, Annette J.: *Behind the Wizard's Curtain: An Integration Environment for a System of Systems*. CCRP Publication Series, 1999, pp. 33–34.
[264] Maier, Mark W.: Research Challenges for Systems-of-Systems. *IEEE International Conference on Systems, Man and Cybernetics Waikoloa, HI, USA, October 10-12, 2005, pp.* 3149–3154.
[265] Emergency means not deductive from a priori elements. (Boardman, John & Sauser, Brian: System of Systems – the meaning of. *IEEE/SMC International Conference on System of Systems Engineering, Los Angeles, CA, USA, 2006).*
[266] On complexity cf. Thurner, Stefan, Hanel, Rudolf & Klimek, Peter: *Introduction to the Theory of Complex Systems*. Oxford, Oxford University Press, 2018; Perrow (1999)).
[267] Perrow (1999).
[268] Ackoff (1999), 52.
[269] Heylighen, Francis, Joslyn Cliff & Turchin Valentin: What are Cybernetics and Systems Science? *Principia Cybernetica Web (Principia Cybernetica, Brussels), 1999*. [http://pespmc1.vub.ac.be/CYBSWHAT.html], visited 7.7.2020.

Based on the above, it can be argued that the values and beliefs held by a government may affect what kind of social governance systems the government develops and make it possible for external researchers to create models of these systems. In fact, several Russian civilian and military researchers structure the information space as a system, as a struggle between information warfare systems, and the control of that struggle as one of the missions of the national command and control system.[270] In this context, many of them have put forward the idea of a state information security system the purpose of which is to prevent both psychological and technological threats against society and the state. Such a system would consist of several subsystems and would be of a cross-administrative and centrally managed nature.

The underlying reasons for this kind of thinking include the ideas of Russia's strategic culture I examined in my doctoral dissertation.[271] In Russia, systems approach has a long history in cybernetics, which played an important role in Soviet sciences during the Cold War.[272] Systems thinking reflects the way international politics is seen as a confrontation between competing systems, where the class struggle has today been replaced by the struggle over the world order tied to great power interests.[273] Currently, the most important form of struggle is the information struggle (*informat͡sionnoe protivoborstvo*), which makes it possible to gain strategic superiority even during peace. Information struggle involves the idea of digital or information sovereignty, which has been developing as part of Russian legal thinking since the 1990s. It gives the state authority over information, information technology and systems, and their users/consumers in its own territory and makes them elements of sovereignty. The idea of information struggle has its information psychological and information technology aspects. The former emphasises influencing the human mind, and the latter command and control warfare and system (cyber) warfare, and the opportunities offered by technology to seek countermeasures against a more technologically advanced opponent. The idea of information superiority is also divided into psychological and technological aspects, of which the former is undoubtedly more important for Russian theoreticians, and it is sought at the strategic level.[274] The idea of a unified information space (*edinoe informat͡sionnoe prostranstvo*), describing a national, unified cyberspace that is controlled by a system of management and control systems, offers a tool for the information struggle. The management of the space is based on vertical control through automated management and control systems, and horizontal integration, centralisation, delineation of borders in cyberspace and scientific-technological self-sufficiency.

---

[270] These include E. A. Derbin, S. A. Komov, E. G. Shalamberidze, D. T͡sereshkin, G. Smoljan, V. Tsygit͡sko, A. A. Sidak, Ju. G. Bot͡skareva, V.K. Novikov, S. I. Makarenko, H. I. Saiifetdinov, V. Kruglov, V. V. T͡syganov, S. N. Bukharin, A. V. Manoilo, and I. Panarin. Their writings have been analysed in Kukkola (2020a).
[271] The following summaries of strategic cultural ideas are based on Kukkola (2020a).
[272] Susiluoto (2006); Peters (2016); Vasara, Antti: *Theory of Reflexive Control: Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy*. Finnish Defence Studies 22. National Defence University, Helsinki, 2020.
[273] Kukkola (2020a).
[274] The psychological side of information warfare is related to the theory of reflexive control cf. Thomas, Timothy: Russian Military Thought: Concepts and Elements. MITRE Corporation, McLean VA, 2019; Vasara (2020).

When it comes to the security threat posed by the idea of a continuous struggle, the idea of strategic deterrence – a Russian interpretation of the Western deterrence thinking – provides a broader scope of response than the use of information. It is based on the idea of preventing threats, avoiding war and controlling the course of conflict by military and non-military means. When it is not possible to build deterrence relying on the balance of power, the idea of an asymmetric response (*asimmetrichnyĭ otvet*) provides a cost-effective option for neutralising the opponent's power, protecting one's own weaknesses and increasing own power. It has its roots in Russian military theory, which emphasises cunning, creativity, deception and concealment. All the above ideas explain why Russian government believes that closing the information space and building a national segment of the internet appears *reasonable*, especially if other countries do not undertake similar action.[275]

Since social systems are linked to the societal, economic and political characteristics of a specific society, in this thesis the concept of a system of systems is applied by combining the Russian strategic cultural ideas of the state-controlled information space and information system with the Russian state's actual projects to control the national information space (Chapter 3.3) and the Russian state's characteristics into a systems theory model. The model can also be applied to examining other countries, but only as a basis for an analytical framework. The outcome is called a national information security and defence system. *A national information security and defence system refers to a system of systems providing information security. It is a unified collection of government tools and means for delineating, building, managing and securing the national information space in the information environment. The system mobilises power from the information society and the economy for state use.* It is comprised of functional subsystems that produce, adapt, guide and control information, and related structures, processes and users within a state. As a rule, the system is understood as a tool for exercising power by the state elites – especially in the case of authoritarian states.[276]

The information security and defence system produces internal and external security. Internal security refers to internal state order and external security refers to defence.[277] In this context, information security is understood in a state-centric manner, i.e., as protection of a state against external and internal information threats, which secures the sovereignty, regional integrity, economic development, defence and security of the state.[278] Information threats against a state can be roughly divided into psychological and technological ones. In this work, the main focus will be on the latter, which include cyber warfare and cyber operations.[279] As the information space and cyberspace are constantly changing due to technological and societal developments, the

---

[275] Other explanations might be the need of authoritarian political leaders to protect themselves and their interests, the mentality of the leadership, or Russia's geography and history.
[276] The elite are a group of people who make the decisions on the use of force and on how to respond to threats in a state. (Kukkola 2020a).
[277] On internal and external security cf. Eriksson, Johan & Rhinard, Mark: The Internal–External Security Nexus: Notes on an Emerging Research Agenda. *Cooperation and Conflict*, Special Issue On The Internal-External Nexus, Vol. 44, No. 3 (September 2009), pp. 243–267.
[278] The definition is based on the Russian information security doctrine. (Указ-646 (2016)). On the concept of security more generally cf. Smith, Steve: The increasing insecurity of security studies: Conceptualizing security in the last twenty years. *Contemporary Security Policy*, Vol. 20, No. 3 (1999), pp. 72–101; Williams, Paul D. (ed.): *Security Studies: an Introduction*. Routledge, London, 2008.
[279] Kukkola (2020a).

information security and defence system must be adaptive and complex.[280] Only in its extreme form will it cover the entire information space of society. Usually, a free or less regulated space is left outside it. The operation of the information security and defence system is manifested as observable phenomena, the most significant and comprehensive element of which in cyberspace is a national segment of the internet, i.e., a closed network. By studying the properties of the national segment of the internet, it is possible to model the subsystems of the information security and defence system.

3.2 Characteristics of the Russian state

This chapter presents the characteristics of the Russian state that affect the properties of the subsystems of the national information security and defence system and thus the analysis of the relationship between national segments of the internet (closed networks) and open networks made in Chapter 4. Russia's foreign and security political behaviour has been explained by, for example, rational great power behaviour or longing for superpower status; the geopolitical thinking of the elites; the mentality or interests of the elites and security organisations; the internal political system (*sistema*)[281]; and the personality of President Vladimir Putin.[282] Although researchers disagree on the intentions behind the Russian foreign and security policy, there is a strong consensus regarding the national behaviour that, since President Putin's second term (2004–2008) at the latest, Russia has been actively seeking to restore its great power status and to create an economic, political and military alliance system in its geographical neighbourhood, protecting its interests by various means, use of force included, in its neighbouring areas. After 2013, the relationship between Russia and the West deteriorated as a result of the war in Ukraine, and Russia has increasingly focused its earlier efforts to establish alliances against the West or parallel with Western alliances to a strategic partnership with China. On the other hand, Russia has attempted to destabilise and weaken the parties it considers as its opponents, i.e., the United States, NATO and the EU, using, inter alia, cyber-assisted information operations. It has denied the existence of its own cyber capabilities, but cyber capabilities are clearly a part of Russia's strategic deterrence and escalation control during conflict.[283]

Russia is an autocratic, presidentially governed country with a formal parliamentary democracy.[284] Law has mostly been employed as a tool for the exercise of power by

---

[280] On the adaptability and complexity of human systems cf. Waldrop, Mitchell M.: *The Emerging Science at the Edge of Order and Chaos*. Touchstone, New York, 1992, pp. 11–12. For example, Anderson et al. have defined as the main elements of complex systems agents, non-linear interconnections, self-organization, emergence, and coevolution of the systems and its environment. (Anderson, Ruth A., Crabtree, Benjamin F., Steele, David J. & McDaniel, Reuben R, Jr.: Case Study Research: The View from Complexity Science. *Qualitative Health Research*, Vol. 15, No. 5 (May 2005), pp. 669–685, 673).

[281] Ledeneva, Alena V.: *Can Russia Modernise?* Cambridge University Press, Cambridge, 2013.

[282] Cadier, David & Light, Margot (Eds.): *Russia's Foreign Policy. Ideas, Domestic Politics and External Relations*. Palgrave Macmillan, Basingstoke, 2015; Oliker, Oleg: Putinism, Populism and the Defence of Liberal Democrazy. *Survival*, Vol.59, No. 1 (February – March 2017), pp. 7–24; Tsygankov, Andrei P. (Ed.) *Routledge Handbook of Russian Foreign Policy*. Routledge, London and New York, 2018; Donaldson, Robert H. & Nadkarni, Vidya: *The Foreign Policy of Russia. Changing Systems, Enduring Interests* (6th ed.) Routledge, New York & London 2019; Kanet, Roger E. & Piet, Rémi (Eds.): *Shifting Priorities in Russia's Foreign and Security Policy*. Ashgate Publishing Limited, Surrey, 2014.

[283] Lilly & Cheravitch (2020); Maurer (2018); Bruusgaard (2022).

[284] Sakwa, Richard: *The Putin Paradox*. I. B. Taurus, London, 2020, pp. 97–98; Treisman (2018); Oliker (2017).

the state leaders, and the Russian judiciary is under the control of the political leadership and does not enjoy the confidence of the people.[285] The protection of property rights against crime and state arbitrariness is weak.[286] Putin is surrounded by a group of influential individuals in institutional or financial positions who are dependent on him.[287] The positions of power in the presidential administration and ministries have varied over time, depending on the political skills of the persons directing them.[288] In practice, the upper and lower houses of the country's bicameral parliament are under the control of representatives or individuals of the party United Russia affiliated with Vladimir Putin.[289] However, the Russian political system is not totalitarian and seeks to take into account the needs of citizens to maintain popular support.[290] The state's social spending and indirect income transfers through state-owned companies to citizens are a factor legitimising the central government.[291] According to various researchers, the primary security interest of Russian leadership lies in the continuity of administration and preserving the popular support of the state leadership.[292] Officially, the Russian state is based on institutions, but within and alongside them networks, personal relations, informal power, negotiations and bargaining define the positions of power and the control over resources.[293]

The characteristics of the Russian state have changed over time. For example, it was believed that the security services had risen to the leading position in Russia during Putin's first two periods. Since then, it seems that the established role of the security services has become that of the supplier and disseminator of information.[294]On the other hand, the militarisation of Russian society has accelerated since 2014. The government has also intensified its efforts to strengthen the unity of the people and its

---

[285] Pomeranz, William E.: *Law and the Russian State: Russia's Legal Evolution from Peter the Great to Vladimir Putin*. Bloomsbury, London & New York, 2019, pp. 148–149, 164–165.
[286] Becker, Uwe & Vasileva, Alexandra: Russia's Political Economy Re-conceptualized: A Changing Hybrid of Liberalism, Statism and Patrimonialism. *Journal of Eurasian Studies*, Vol. 8, No. 1 (January 2017), pp. 83–96.
[287] Konyshev, Valery & Sergunin, Alexander: Military. In *Routledge Handbook of Russian Foreign Policy*. Tsyganov, Andrei P. (ed.) Routledge, London and New York, 2018, pp. 168–181; Vendil, Carolina: The Russian Security Council. *European Security*, Vol.10, No.2 (Summer 2001), pp. 67–94; Mankoff, Jeffrey: *Russian Foreign Policy: The Return of Great Power Politics* (2nd ed.) Rowman & Littlefield Publishers, Inc., Lanham, 2012, pp. 55–56; Gvosdev, Nikolas K. & Marsh, Christopher: *Russian Foreign Policy: Interests, Vectors, and Sectors*. SAGE Publications, Inc., Los Angeles, 2014, pp. 35–36; Bacon, Edwin: Security Council and decision-making. In *Routledge Handbook of Russian Security*. Kanet, Roger E. (ed.) Routledge, London and New York, 2019, pp. 119–130.
[288] Konyshev & Sergunin (2018); Vendil (2001); Mankoff (2012), 55–56; Gvosdev & Marsh (2014), 35–36; Bacon (2019).
[289] On elections cf. Noble, Ben & Schulmann, Ekaterina: Not Just a Rubber Stamp. Parliament and Lawmaking. In *The New Autocracy: Information, Politics, and Policy in Putin's Russia.* Treisman, Daniel (ed.) Brookings Institution Press, Washington, D.C., 2018, pp. 47–78; Sakwa (2020), 87–89.
[290] Oliker (2017); Robinson, Neil & Milne, Sarah: Populism and political development in hybrid regimes: Russia and the development of official populism. *International Political Science Review*, Vol. 38, No. 4, pp. 412–425.
[291] Sokhey, Sarah Wilson: What Does Putin Promise Russians? Russia's Authoritarian Social Policy. *Orbis*, Vol. 64, No. 3 (2020), pp. 390–402.
[292] Cadier & Light (2015), 8–9; Treisman (2018); Donaldson & Nadkarni (2019), 429; The Finnish Ministry of Defence: *Russia of Power*. Punamusta, Helsinki, 2019, pp. 17.
[293] Ledeneva (2013).
[294] Marten, Kimberly: The 'KGB State' and Russian Political and Foreign Policy Culture. *Journal of Slavic Military Studies*, Vol. 30, No. 2 (2017), pp. 131–151; Soldatov, Andrei: From the "New Nobility" to the KGB. *Russian Politics and Law*, Vol. 55, No. 2 (2017), pp. 133–146.

relationship with the state launched around 2007 through patriotic education and controlling how historical events are interpreted.[295] The activities of national and international NGOs and free media have been restricted, the operation of foreign media has been made more difficult or foreign ownership of media assets has been hindered.[296]

The state plays an important role in the economy through the distribution of energy revenues and the large state-owned companies. The characteristics of the Russian political and economic system include *ad hoc* approach to crises and the patron-client system. These features lead to administrative stove-piping, lack of investments and strategic projects being led directly by the administration, opaqueness, lack of responsibility, and 'gimmicky' campaigns and projects rather than deliberate development.[297] Due to the above-mentioned characteristics, the widespread grey and black economy, and Russia's state-centred active financial and ownership policy, corruption has become a systematic feature of Russian society.[298] The impacts of corruption are further reinforced by the administrative branches competing over resources and power. In general, private and public operators compete in an opaque manner over the resources distributed by the state, and oligarchs close to the power play an important role in business life.[299] In terms of cyberspace and information space, it poses a particular problem that the construction of a management system for the national information space involves a number of different actors. At the same time, private operators are trying to slow down or water down administrative measures, because the construction of a national segment of the internet will increase their costs.[300] Corruption, coupled with the efforts to circumvent mandatory state regulation, leads to a weak culture of cyber security.[301] The interaction between the public and private sector is also eroded by the culture of secrecy.[302] To summarise the above, *the key characteristics of the Russian state include increasingly authoritarian governance; the centralisation of power; the strong position of the state in the economy; the influence of the security system; competition between and stove-piping of public administration organisations; informal networks; corruption; and state-led militarism and nationalism*.

3.3 Concepts and background of the national segment of the internet

To understand the Russian national segment, we need to define the key concepts related to it, such as a closed national network, national segment of the internet, unified information space, and information security and defence system. A closed na-

---

[295] Pynnöniemi, K. (ed.): *Nexus of Patriotism and Militarism in Russia: A Quest for Internal Cohesion*. Helsinki University Press, Helsinki, 2021.
[296] Freedom House: *Freedom in the World – 2022: Russia.* [https://freedomhouse.org/country/russia/freedom-world/2022], visited 22.9.2022.
[297] Porfiriev, Boris & Simons, Greg (Eds.): *Crisis in Russia: Contemporary Management Policy and Practice From a Historical Perspective. Routledge*, New York, 2016 (org. 2012).
[298] Buckley, Noah: *Corruption and Power in Russia*. FPRI, Philadelphia, PA, 2018.
[299] Vendil Pallin, Carolina: Internet Control Through Ownership: The Case of Russia. *Post-Soviet Affairs*, Vol. 33, No. 1 (2017), pp. 16–33.
[299] Mikoyan, Sergo A.: Eroding the Soviet "Culture of Secrecy". *Studies in Intelligence*, Vol. 45, No. 5 (2001), pp. 45–56.
[300] Kukkola (2020a).
[301] Simovits, Mikael: Axiom För Cybersäkerhet: Ett Ryskt Perspektiv. 19 February 2021. [https://simovits.com/axiom-for-cybersakerhet-ett-ryskt-perspektiv/], visited 22.9.2022.
[302] Mikoyan (2001).

tional network is a theoretical concept, describing a state-controlled part of the cyberspace, which can be technically disconnected from the global internet but still remain capable of functioning normally with regard to services of critical importance to the nation. Its opposite is an open national network, which is not directly controlled by the state. As a rule, an open network cannot be disconnected from the global cyberspace without special preparations or serious disruptions in the critical functions of society and the economy. The national segment of the internet is a manifestation of the national information security and defence system in cyberspace and an applied representation of a closed national network. It consists of the internet infrastructure, services and management systems, the necessary technological foundations and other information networks and systems which reside on a state's territory and under its sovereign jurisdiction. A national information security and defence system is a system of systems that provides information security. It is a unified collection of government tools and means for delineating, building, managing and securing the national information space in the information environment. The system produces power from the information society and the economy for state use. The relationships between the concepts are described in Appendix 1.

I have described the historical development of the national network in detail in my doctoral dissertation.[303] It should be noted that, in the 2020s, the internet has become an object of Russian national security. The Russian state aims to acquire centralised control of the national segment of the internet and to safeguard its functioning against external and internal threats –above all, to ensure that the segment does not become a source of threat. By means of doctrines, strategies, national programmes and numerous laws, Russia aims to establish top-to-bottom control on a national network that has developed from the bottom-to-top. The objective is a unified, nationwide, centrally controlled information space, the target state of which resembles the Soviet plans for a national cybernetic information and management network.

At present, Russia's national segment of the internet is based on a highly disruption-tolerant data network with good internal and external connections. The content of information on the internet is restricted under the pretext of eradicating extremism and protecting children. Information disseminators are regulated by means of registers and holding them responsible for the content of services and websites. Anonymity and the use of VPN are restricted by law. Internet service providers are obliged to retain all data traffic for six months and the data of Russian users on servers located on Russian territory. The targeted surveillance system SORM, which was already used by the security authorities during the Soviet Union, was updated in 2015 to make it capable of monitoring the internet and mobile traffic.[304]

In 2017 was enacted the Act on Critical Information Infrastructure, which, in practice, placed the telecommunications infrastructure under government regulation. Most of the services critical to the functioning of the internet were transferred under the management of state institutions or corporations by 2021, and private operators have been ordered to classify and protect the systems that remained in their possession under the threat of punishment. The 2017 Act also finalised the concept of the GOSSOPKA

[303] Kukkola (2020a).
[304] Ibid.

system, i.e., the Government System for Detecting, Preventing and Eliminating the Effects of Computer Attacks. It is a national *Security information and Event Management* (SIEM) system managed by the security services. At least the central government and companies considered to be of strategic importance will be connected to the system. By 2020, the attempts to limit the foreign ownership of certain online services and critical information infrastructure had not succeeded.[305] However, the law adopted in July 2021 makes it possible to restrict the activities of foreign operators on the "internet located on Russian territory".[306]

In 2019, a law was passed to disconnect the national segment of the internet from the global internet, and national exercises on responding to cyber threats were launched.[307] A government order also started the development of 'cyber exercise areas'. By the beginning of 2020, Russia's national cyber security came to be based on the resilience, security and integrity of the internet and public communications networks operating on the Russian territory. These are secured by a centralised supervision and control system (TSPU - *tekhnicheskie sredstva protivodeĭstviia ugrozam*). The relevant devices to be installed on operators' networks can limit traffic and, if necessary, isolate Russia's telecommunications networks from the global internet.[308]

The Digital Economy Programme was adopted in 2017 and transformed into a national programme in 2019. It is aimed at implementing the digitalisation of the Russian economy and administration and, at the same time, bringing the country's internet in terms of services and content under the control of the state by 2024. The goal is to achieve 'technological sovereignty', i.e., extensive domestic software and hardware development and production.[309] The project has been supported by ordering public administration actors to procure hardware and software produced in Russia.[310] Due to developmental and financial difficulties, the prescribed deadlines have been changed time and time again, and in 2020 the aim was to move to using domestic technology in 2023–2024.[311] Alongside the Digital Economy Programme, a so-called

---

[305] Ibid.

[306] ФЗ-236: Федеральный закон от 01.07.2021 N 236-ФЗ "*О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации*". [http://publication.pravo.gov.ru/Document/View/0001202107010014?index=1&rangeSize=1], visited 29.7.2021.

[307] Роскомсвобода: Ростелеком создаст киберполигон. *Роскомсвобода*, 06.12.2019. [https://roskomsvoboda.org/53137/], visited 12.1.2021.

[308] Kukkola (2020a).

[309] Cf. Касми, Эльяс: Минкомсвязи хочет влить миллиарды рублей в российскую мобильную ОС. *CNEWS*, 7.7.2020. [https://www.cnews.ru/news/top/2020-07-07_minkomsvyazi_hochet_vlit], visited 7.7.2020.

[310] Чернышова, Евгения & Балашова, Анна: Банки договорились с властями о постепенном переходе на российский софт Требование об импортозамещении должно вступить в силу с начала 2023 года. *РБК*, 16.7.2021. [https://www.rbc.ru/finances/16/07/2021/60f14f009a794702b097f76a?from=from_main_9], visited 28.7.2021.

[311] Скрынникова, Анастасия, Бурмистрова, Светлана, Скобелев, Владислав & Чернышова, Евгения: Банки и ТЭК обяжут перейти на российское оборудование и софт к 2025 году. *РБК*, 2.11.2020. [https://www.rbc.ru/technology_and_media/02/11/2020/5f9c0f189a7947834b411b98?from=from_main_3https://www.rbc.ru/technology_and_media/02/11/2020/5f9c0f189a7947834b411b98?from=from_main_3], visited 1.3.2022.

People's internet (*dostupnyĭ Internet*) is also being developed to ensure citizens' free access to basic internet services.[312]

Furthermore, in 2017, the Russian Government adopted the Information Society Development Programme, which formalised the concept of a national segment of the internet, while at the same time linking it to state sovereignty and military threats. In line with the Digital Economy Programme and Strategy, own data networks, systems and data centres will be created for the presidential, federal and local administrations. Similar systems have been built for the defence and energy industry. Based on these systems, the Government will build a national information collection and analysis system, with clear links to the Soviet societal and economic system of OGAS(U).[313]

To develop domestic technology and production required by the development programmes, the Russian state has relied on scientific institutes and innovation park concepts. However, there is no clear evidence of their success.[314] In addition, since 2019 Russia has been enhancing its technology cooperation with China, and Chinese companies have agreed on cooperation projects with Russian ICT companies.[315] Russia has also promoted an international norm-building project with China within the framework of the UN to bring internet governance under state control and to ban the dissemination of 'information weapons', including sharing of free information.[316]

The national segment of the internet is managed by several public administration actors. The main role is played by the Ministry of Digital Development, Communications and Mass Media, its subordinate supervisory authority Roskomnadzor, the Federal Service for Technical and Export Authority (FSTEK) and the security services. The regulation mainly targets private companies that possess most of the network infrastructure and Russian-language service provision and social media. Rostelekom, Russia's largest telecommunications operator and internet service provider, is a state-owned company. It possesses significant parts of the critical information infrastructure and its services. Leading information security companies also cooperate closely with the central government.[317]

The projects described above have faced significant challenges, and many of them are semi-completed or only partially implemented.[318] In other words, the construction of

---

[312] Гаврилюк, Анастасия & Шестоперов, Дмитрий: Отступный интернет Законопроект о бесплатном доступе к значимым сайтам предложено доработать. *Коммерсантъ* №38 от 05.03.2021. [https://www.kommersant.ru/doc/4713549], visited 28.7.2021.
[313] Kukkola (2020a). On OGAS(U) cf. Peters (2016).
[314] Dear, Keith: Will Russia Rule the World Through AI? *The RUSI Journal*, Vol. 164, No. 5-6 (2019), pp. 36–60; Schiermeier, Quirin: Russia Aims to Revive Science After Era of Stagnation. Some Researchers See Promise in Planned Reforms. *Nature*, 18 March 2020. [https://www.nature.com/articles/d41586-020-00753-7], 7.7.2020; Гордеев, Владислав: Счетная палата не увидела прорывного эффекта от особых экономических зон. *РБК*, 9.4.2020. [https://www.rbc.ru/economics/09/04/2020/5e8eb2679a79477a36b61c5f], visited 8.7.2020.
[315] Bendett, Samuel & Kania, Elsa B.: *A new Sino-Russian high-tech partnership. Authoritarian innovation in an era of great-power rivalry*. The Australian Strategic Policy Institute, Policy brief Report No. 22/2019.
[316] Tikk, Eneken & Kerttunen, Mika (Eds.): *Routledge Handbook of International Cybersecurity*. Routledge, London and New York, 2020.
[317] Kukkola (2020a).
[318] Воейков, Денис: Власти хотят признавать «железо» российским за деньги. В этой идее нашлись «коррупциогенные факторы». CNEWS, 16 July 2021. [https://cnews.ru/link/n532505], visited 28.7.2021;

the national segment of the internet is progressing, but not in keeping with the schedule, the rate of efficiency or relying on Russian competence to the extent the state would wish. However, the political will to this end does exist. In spring 2021, several politicians, under President Putin's leadership, called for further tightening of the management of the internet[319], and in autumn 2021, the system demonstrated its functioning capability by blocking the opposition's activities on the internet during the Duma elections.[320]

The networks of the Russian Armed Forces are part of the national cyberspace, and they are affected by the construction of the national segment of the internet. For example, the links between the Defence-Industrial Complex, cooperation between security authorities and international military activities form the interface between interdependent actors. Under Russian law, military networks fall under the category of 'special networks', which are subject to separate orders and are kept separate from the public telecommunications network to which the internet belongs.[321] The Russian Armed Forces have been trying to develop their own unified information network, i.e., the Integrated Automated Digital Communication System (OATsSS) since 2008. It is an information network and system, with its own data centres and services, that combines the Armed Forces and other state security actors. The purpose of the OATsSS is to provide a nationwide and, if necessary, cross-border foundations for the Armed Forces's C2 systems and connections. It is likely that OATsSS was originally supposed to be based on civil telecommunications networks, but in 2019 the Armed Forces announced that they would develop a completely separate Multiservice Transport Network (MTSS) for their own needs. In addition, they have started building disaster-resistant data centres in military districts.[322]

The Armed Forces operate their own 'military internet', which is based on Russian software services and provides encrypted services and connections to the needs of the Armed Forces. In addition to these fixed services and networks, the Armed Forces have numerous field communications systems, and the various arms and services also have their own information networks and systems, which are not necessarily mutually compatible. The Defence-Industrial Complex (OPK) has its own telecommunications network as does the Armed Forces mobilisation system. It is unlikely that the communications system of the Armed Forces could manage without the electricity produced by civilian networks or dual-use infrastructure.[323]

Гаврилюк, Анастасия: «Суверенный рунет» сочли угрозой стабильности. Операторы критикуют новые требования Роскомнадзора. Коммерсантъ №132, 29.07.2021. [https://www.kommersant.ru/doc/4919761?from=main_9], visited 29.7.2021; Президент России: Указ о национальных целях развития России до 2030 года. *Kremlin.ru* 21.7.2020. [http://kremlin.ru/events/president/news/63728], visited 31.7.2020.

[319] Роскомсвобода: Путин заявил о том, что соцсети управляют сознанием человека. *Роскомсвобода*, 2.2.2021. [https://roskomsvoboda.org/69233/], visited 1.3.2022.

[320] Freedom House: *Freedom in the World – 2022: Russia*. [https://freedomhouse.org/country/russia/freedom-world/2022], visited 22.9.2022.

[321] ФЗ-123: Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 07.04.2020) "*О связи*". [http://www.consultant.ru/document/cons_doc_LAW_43224/], visited 14.5.2020.

[322] Kukkola (2020a).

[323] Ibid.

The information networks of the Armed Forces also include the early warning system for nuclear attacks and even the C2 system for strategic nuclear weapons. The command and control system Signal is based on a diverse range of analogue and digital data networks and systems, including several radio networks, command missiles, aircraft and satellites.[324] The early warning system consists of just under 20 *Over-the-Horizon* (OTH) radars, optical sensors and 3–4 satellites.[325] The main purpose of the C2 system is to provide sufficient early warning and enable positive and negative control of strategic nuclear weapons.[326] In addition, efforts have been made to network ballistic missile defence systems with sensors and command posts at different levels.[327] Nuclear deterrence is also linked to the C2 systems of the Aerospace Forces, which are tasked with, among other things, enabling the prevention of surprise attacks by using conventional precision weapons. The objective of such an attack could be to paralyse Russia's strategic nuclear defence capability.

3.4 National information security and defence system

A national information security and defence system is a model for controlling the national information space. The most significant and comprehensive manifestation of the system (characteristic of digital territory) in cyberspace is a national segment of the internet, which is an applied version of a theoretical closed network. The internet segment does not cover all elements or manifestations of the information security and defence system that extend to the socio-cognitive, information-physical and electromagnetic space. The subject of this thesis being structural cyber asymmetry, the focus is on cyberspace, and thus, from an analytical point of view, the national segment of the internet is the same as the system of systems to be presented below, as the modelling of the system's subsystems is focused on digital territory factors. These factors are based on the Russian strategic cultural idea of a state-controlled information space and information system, the characteristics of the Russian state and the actual projects of the Russian state to control the national information space, which are presented in the previous chapters.

The model to be presented is an ideal case, in which form the Russian state's national information security and defence project or its representation in cyberspace, the national segment of the internet, will hardly be implemented in full. The system consists of eight subsystems (Figure 2), which have been classified based on their purpose, components, functions, operating principles and objectives. The systems are interrelated, but their operation and the operation of the entire system are controlled by the eighth subsystem that monitors and controls the others. The subsystems of the model

---

[324] Blair, Bruce, G.: *The Logic of Accidental Nuclear War*. The Brookings Institution, Washington, D.C., 1993; Yarynich, Valeri E.: *C3: Nuclear Command, Control, Cooperation*. Center for Defence Information, Washington, D.C., 2003.

[325] Honkova, Jana: *The Russian Federation's Approach to Military Space and Its Military Space Capabilities*. George Marshall Institute, Arlington, VA, 2013.

[326] Blair (1993).

[327] Arbatov, Alexei & Dvorkin, Vladimir (Eds.): *Missile Defense: Confrontation and Cooperation*. Carnegie Moscow Center, Moscow, 2013; Persson, Gudrun (ed.): *Russian Military Capability in a Ten-Year Perspective – 2016*. FOI, Stockholm, 2016; Defence Intelligence Agency: *Russia Military Power: Building a Military to Support Great Power Ambitions*, 2017, pp. 33. [http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf], visited 8.7.2020.

are, in principle, applicable to other similar state control systems of the information space.

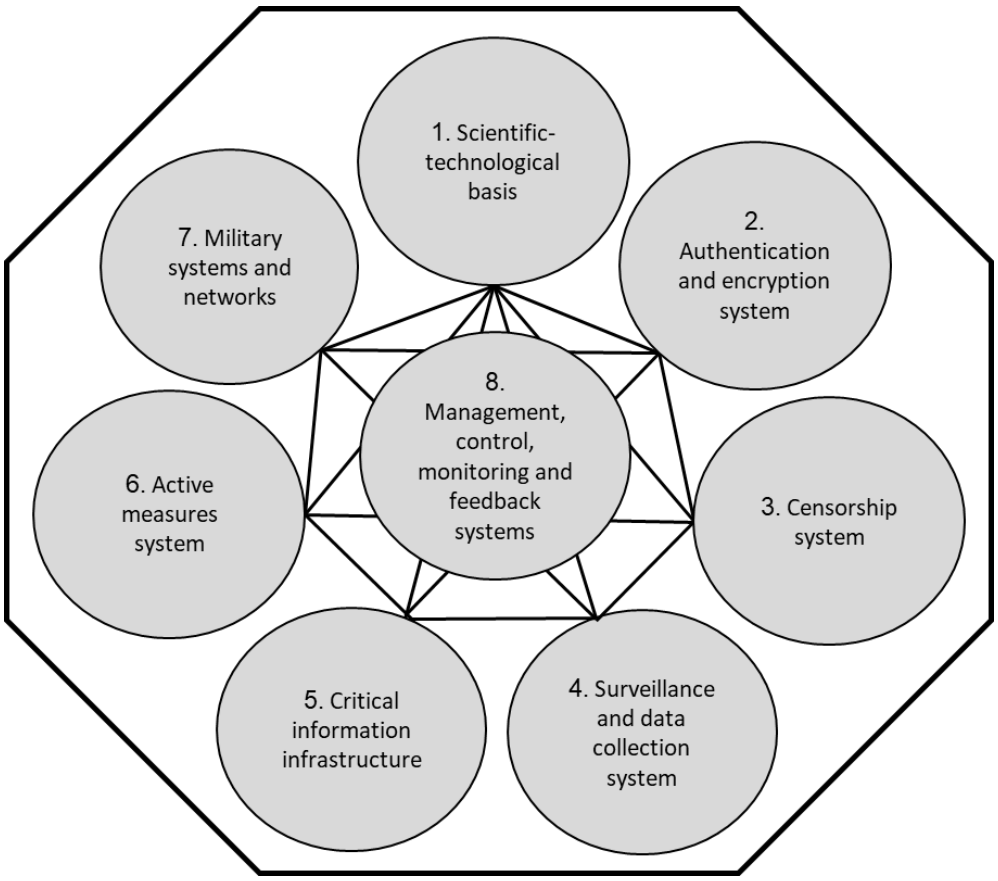

Figure 2: National information security and defence system

The first subsystem of the system of systems of information security and defence is an economic and scientific system, i.e., the scientific-technological basis of the state. It is based on autarkic economic policies, including the import substitution policies, and state investments in education and science. The subsystem's primary function is to promote the creation of a domestic digital economy, to boost the Russian economic power and to improve the stability of society by creating well-being. In addition, it indirectly shapes the national cyberspace in a direction advantageous to the regime by providing services and systems tied to the regime. It also provides national security through domestic hardware and software production by limiting the threat of supply-chain vulnerabilities and ensuring the independence of critical information infrastructure and information security systems of foreign suppliers. In principle, domestic solutions also provide *security through obscurity*. Domestic manufacturers are obliged to build backdoors for the security services to their services and products. In other words, the security services (and the Armed Forces) also have access to Russian systems used abroad.[328]

[328] Kukkola (2020a), 361–362.

The second subsystem consists of state encryption and authentication services. It is based on a central government encryption and authentication system which should replace any foreign systems. Initially, the use of the system is only mandatory for the public administration but will gradually be introduced to private enterprises and private users through voluntary adoption and 'freedom of choice'. The objective is to make all data traffic in the national segment of the internet transparent to the security services. The system may include a backbone network implemented using quantum encryption. Encrypted communications transited through the internet segment are not affected by the subsystem, but foreign operators may also be obliged to use state encryption or systems approved by it or to steer their traffic through state proxies.[329]

The third subsystem is composed of administrative and technological processes to deny and restrict access to internet content considered unwanted with a view to state security. It operates as part of the state censorship system. This includes removing content, blocking access, and closing services and user accounts. The national moral and value issues have been used as justification for restricting free expression and bringing expression of political opinions under criminal law. The system makes it possible to restrict and prohibit the operation of foreign companies. The subsystem also includes self-censorship of the users and service providers and voluntary vigilante groups who monitor the national segment for 'unlawful' content. The subsystem is primarily intended as a tool for practising political control, although it is formally a law enforcement instrument.[330]

The fourth subsystem consists of targeted surveillance systems and massive internet data traffic retention and localisation. The former is the responsibility of the security services, and the latter is the responsibility of the internet service providers, who must give security services access to their data reserves. The subsystem is based on distributed data centres and networked monitoring and analysis systems. It produces extensive intelligence data and alerts of information threats and ongoing attacks. The information produced by the system can be used for both technical and political attribution as well as for own impact operations in and outside the cyber environment. The subsystem increases the transparency of the national segment of the internet in the direction of security actors.[331]

The fifth subsystem consists of critical information infrastructure and its regulation. It designates the critical infrastructure and those responsible for protecting it. These parties are primarily private actors whose obligations are based on law and a threat of punishment. They are supervised by the security services. The system also includes the duplicated, state-governed critical internet services, such as domain name servers, routing tables and traffic exchange points. It serves as the foundation for the ability to circulate the internal network traffic within the borders of the state concerned. Thus, the subsystem enables disconnecting the internet segment from the global internet without losing critical services. In addition, the subsystem strengthens the resilience of information networks to cyberattacks.[332]

---

[329] Ibid.
[330] Kukkola (2020a), 363.
[331] Ibid.
[332] Ibid.

The sixth subsystem consists of active information-technological and information-psychological countermeasures. On the one hand, the subsystem consists of state-controlled or affiliated news services and educational, patriotic and religious institutions. On the other hand, it also includes dedicated cyber diplomacy organisations and cyber espionage and warfare units of the security services and the military. The subsystem controls the domestic information environment by producing and adapting information. In addition, it conducts espionage, influence and cyber operations to prevent threats from emerging. The subsystem improves information security by weakening potential opponents, binding them with norms and restricting the capacity of advanced adversaries by creating taboos related to the use of cyber capabilities.[333]

The seventh subsystem consists of military networks and systems. The subsystem is largely separate from other subsystems, but dependent on, among other things, critical information infrastructure in terms of its capabilities. It includes the systems of the military command, troops, institutions and institutes. The Armed Forces supervise and maintain their own systems, but rely in part on civil service providers and network operators. The subsystem secures the command and control capacity of the Armed Forces and its connections with the rest of the state administration during peace and war. It enables the military defence of the state and the maintenance of national security.

The eighth subsystem consists of management, control, monitoring and feedback systems. It includes cyberattack prevention systems, state information management systems, the network of CERTs functioning in public and private networks and the network of civilian and military situation centres. The subsystem provides the vertical control and horizontal integration of the national segment of the internet. It collects information on the national segment and the whole society and produces threat analysis of both technological and psychological information threats and enables the control of information flows. The subsystem is responsible for controlling all other subsystems and actively defending the national segment of the internet against state-level cyberattacks.[334]

The subsystems of the system are closely interconnected to secure national information security. The scientific-technological basis produces the capabilities for all other systems. Its technological weaknesses or backwardness and vulnerabilities pose a risk to other subsystems. The authentication and encryption system secures the connections and information of other systems and lays the foundation for the reliability of the systems' services, but its vulnerabilities, i.e., the construction of potential backdoors for the security services, pose a risk to all other subsystems.[335] The censorship system contributes to the implementation of the economy, information infrastructure and control by weakening social resistance and strengthening the national management of critical resources. However, the use of the subsystem may generate a counter-reaction that increases internal threats and weakens the innovation potential of the

---

[333] Kukkola (2020b), 18. The name of this subsystem is a direct reference to the Russian concept of active measures cf. DeBenedictis, Kent: *Russian 'Hybrid Warfare' and the Annexation of Crimea. The Modern Application of Soviet Political Warfare*. Bloomsbury Academic, London, 2022, pp. 52–54.
[334] Kukkola (2020a), 364.
[335] Abelson, Harold et al.: Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, Vol. 1, No. 1 (2015), pp. 69–79.

scientific-technological basis. The massive data retention and monitoring processes produce a data and information resource for national projects and the control system. However, through a threat of data leakage, it poses a risk to all other systems and the objective of the entire system. Tailored surveillance systems enable preventing information threats to other systems but placing them as part of the information infrastructure creates vulnerabilities in the very same infrastructure. The functionality and resilience of critical infrastructure is the foundation for the operation of the entire system and the national segment of the internet. On the other hand, ways of managing infrastructure can pose a risk to both the economy and national security.[336] Active measures legitimise the system of systems and reduce threats against other parts of the system. On the other hand, they may cause both internal and external counterreactions, which may lead to the materialisation of new threats.[337] The military networks and systems create demand for technologies and expertise provided by the civilian world, but are, at the same time, vulnerable to disruptions of the critical infrastructure. When functional, the control system will safeguard the functioning capacity of the administration, economy and infrastructure. However, a centralised system in itself poses a security threat, the ultimate risk of which is the national segment of the internet becoming paralysed.[338]

In other words, the information security and defence system provides security by combating information psychological and technological threats, and providing the resilience and security needed by networks, while laying the foundation for the state's digital sovereignty by delineating borders in the state's cyberspace and controlling them. In principle, the system is relatively flexible and enables the mobilisation of the whole nation's scientific and technological resources to safeguard the state's interests in the cyber environment. Despite its flexibility, the system is undoubtedly also very complex and does not reach the entire information environment, part of which remains beyond the government's reach and thus becomes a source of potential threats.

3.5 Structure and characteristics of a theoretical open national network

A theoretical open national network is based on the way the internet was governed in technologically advanced, leading European countries in the mid-2010s. The description of the network is based on contemporary sources from which the characteristics of the open network were derived through the strengths and weaknesses indicated.[339]

---

[336] Cf. e.g., Keizer, Gregg: Garden-variety DDoS attack knocks North Korea off the Internet Experts cite the fragility of North Korea's connection, note that routine DDoS attacks could have easily forced the country offline. *Computerworld*, 23.12.2014. [https://www.computerworld.com/article/2862652/garden-variety-ddos-attack-knocks-north-korea-off-the-internet.html], visited 29.7.2021.

[337] Cf. e.g., Степанова, Юлия, Занина, Анна & Гаврилюк, Анастасия: Техноложная тревога. Чем займутся российские IT-компании под санкциями США. *Коммерсантъ* №67, 16.04.2021. [https://www.kommersant.ru/doc/4773434?from=main_5], visited 29.7.2021.

[338] A good example is SolarWinds attack in December 2020 (Gatlan, Sergiu: SolarWinds Victims Revealed after Cracking the Sunburst Malware DGA. *Bleeping Computer*, December 22, 2020. [https://www.bleepingcomputer.com/news/security/solarwinds-victims-revealed-after-cracking-the-sunburst-malware-dga/], visited 28.12.2020).

[339] In addition to the sources used in Chapter 2 the concept of a national open network is based on the following sources: International Telecommunication Union (ITU): *Global Cybersecurity Index & Cyberwellness Profiles*, April 2015. [https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf], visited 15.9.2020; ENISA: *Critical Information Infrastructures Protection approaches in EU*, July 2015. [https://resili-

The sources have been supplemented with the author's own contemporary observations. Setting the scope of the study on this particular time frame and region was based on Russia having formed the basic principles for the construction programme of its national segment of the internet in relation to how the information space was managed in the West around 2014. The Russian project is a response to the strengths perceived in those management models. The change in Western cyber security policy since the mid-2010s is taken into account at the end of the chapter and in Chapter 5 when examining the strategic effects of structural cyber asymmetry.

Although, the United States is Russia's main great power competitor, the open national network model is not directly based on the United States because of its unique relationship with the development of the internet and its economic and scientific-technological power. Using the U.S. as the basis for the model would obscure the fact that the rest of the world is highly dependent on the information technology products and services provided by U.S. companies. Using the U.S. as a model would also lead to overestimating the intelligence, surveillance and information capabilities of the open national network. The ability of U.S. allies to rely on its capabilities has been taken into account in the description of the open network through international co-operation. The purpose of the comparison of closed and open national networks below is to highlight the asymmetric impacts of the Russian project.

Although an open national network is not a system of systems in the same sense as the national information security and defence system, below, it is approached through the subsystems of the Russian national system. This is done because the subsystems capture almost all technological, administrative, economic, normative, political and security aspects of a territorially delimited part of cyberspace. This approach helps to compare different types of national networks.

The scientific-technological basis of an open national network is mainly based on the product development and production of national and international private companies. While the state plays a role in scientific development through innovation subsidies and funding provided to universities and scientific institutes, the share of funding collected from private investors and donors is also significant. The ICT market is open. Only the central government and armed forces have restrictions on the use of foreign software and hardware, and they are not usually applied to products provided by allies. As a rule, open source code is seen as a positive matter, but companies generally use software produced by international companies. Private citizens may use a wider range of software. Measures used for trying to prevent vulnerabilities and protect production chains include agreements, data exchange and trusted partners.

---

ence.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf], visited 15.9.2020; European Commission: *Reports and Studies about Digital Economy and Society Index*, 2020. [https://ec.europa.eu/digital-single-market/en/reports-and-studies/76018/3650], visited 14.7.2020; NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE): *Strategy and Governance* (webpage). [https://ccdcoe.org/library/strategy-and-governance/], visited 14.7.2020; Tikk-Ringas, Eneken (ed.): *Evolution of the Cyber Domain. The Implications for National and Global Security*. IISS, London, 2015; OECD: *Digital Security Risk Management for Economic and Social Prosperity*. OECD Recommendation and Companion Document, 2015. [https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf], visited 12.1.2021; ENISA: *Supply Chain Integrity. An overview of the ICT supply chain risks and challenges, and vision for the way forward*, Version 1.1, August 2015 [https://www.enisa.europa.eu/publications/sci-2015/at_download/fullReport], visited 12.1.2021.

The interdependencies of the ICT economy are accepted, and international cooperation is seen as a positive thing. The challenge is the fragmentation of the network of public- and private-sector suppliers and service providers. With regard to component production, states lack resources or will to seek products of domestic origin except in some very narrow sectors. The ability of security services to widely penetrate the software or hardware used through production chains is limited without international public-private cooperation.

National encryption or authentication services are not widely used in open national networks. Only critical security sectors use national systems or systems produced with allies. The economic and financial sectors widely use commercial solutions, mainly of international origin. Civil society actively uses encryption services provided by international companies, at least some of which are based on open source code. According to legislation, the security services are permitted to monitor and decode encrypted traffic and to obtain information on national citizens. However, their capabilities are limited. Companies have an obligation to disclose user information to the security services, but opening encrypted information requires a transparent legal process or is technically impossible even for the company itself. An open national network is not transparent to the security services.

An open national network does not have a centralised censorship system. No state-led system has been created for the removal, filtering or blocking of material, which service or content providers would be obliged to join. Legislation may prohibit the dissemination of specific, very restricted content or criminal uses of telecommunications. It is possible to remove material from national and international services to a limited extent and in compliance with the administrative requirements of the rule of law. Voluntary actions of citizens do not play an important role in monitoring the state's own cyberspace. Political self-censorship is practised to a very limited extent.

In an open national network, intelligence services have targeted data collection systems in place for strictly limited tasks related to national security or criminal investigation. Their use requires a court or administrative decision issued on a case-by-case basis, and the operations of security services are subject to parliamentary supervision. Open networks do not collect and store mass data on the state's own citizens for the purpose of guaranteeing national security, although this is done for commercial reasons. There is no obligation to retain data on citizens in their home country, but the use of personal data and data related to an individual is increasingly regulated by contract. Much of the data necessary for the economic and financial sector and vital functions of society is located outside the state territory. The ability of security services to monitor the national network with their own systems is limited. Foreign intelligence services are capable of targeted foreign network and system reconnaissance, and they exchange information with the organisations of their allies.

The critical information infrastructure of the open national network is in the hands of the private sector. The critical information services of the central government have largely been outsourced. Some of the critical information infrastructure has been mapped, but safeguarding it is mainly regulated by the terms and conditions of service agreements. The state can support development projects of critical information infrastructure, but the duplication of systems is based on commercial factors. An open

national network may include data centres dedicated to the central government, but their capacity is limited and restricted for storing classified government data. Most of the capacity is leased from private operators. The functioning of open national networks is highly dependent on services located outside state borders, and the network cannot be disconnected from the global internet without significant and long-term service disruptions, malfunctions and degradation of service.

Democratic open network states have a free media space and pluralistic political systems. News services are privately owned, and the activities of foreign news services are not restricted to any significant extent. As a rule, states support the *multistakeholder* management model of the internet.[340] States do not have strong agendas of their own, but they practise diplomacy through different alliances. The alliances are not always united in their positions. The 'countermeasures' of open national networks are based on soft power, strategic communication and tailored information operations supported by foreign intelligence services. These operations are perceived as negative and are not generally disclosed to the public.[341] In terms of military theory, cyber and information capabilities have been tied as part of military operations, and their strategic use is perceived as a sign of backwardness or lagging behind competitors.[342] On the other hand, intelligence cooperation within the framework of multilateral and bilateral partnerships enables large-scale foreign surveillance of information networks.[343] The operations by intelligence services are based on law, and their activities are restricted by strict administrative and civil society oversight. Cyber defence is considered defensive action, and carrying out offensive operations is politically difficult. Despite this, the cyber capabilities of the armed forces are increasingly perceived as part of the normal character of war.[344] Sharing communications intelligence data between allies is normal.[345]

Military networks and systems are an integral part of open national networks. The armed forces do not have the resources to isolate all their fixed data networks and systems from those of private service providers. The isolation is therefore mainly based on service contracts and separation on a logical level. Many of the administrative connections of the armed forces have been outsourced and they are shared with other authorities. The armed forces operate the most critical connections and systems themselves and strive to duplicate their most important systems and connections.

---

[340] Broeders, Dennis & van den Berg, Bibi (eds.): *Governing Cyberspace. Behavior, Power, and Diplomacy*. Rowman & Littlefield, Lanham, Maryland, 2020.
[341] Rid, Thomas: *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux, London, 2020.
[342] Inglis, John C., Lumpkin, Michael D., Waltzman, Rand & Watts, Clint: *Cyber-enabled Information Operations*. Subcommittee on Cybersecurity, Committee on Armed Services, United States Senate, One Hundred Fifteenth Congress, First Session, April 27, 2017. [https://www.hsdl.org/?view&did=802817], visited 21.2.2021; European Parliament: *Cyber defence in the EU Preparing for cyber warfare?* Briefing, October 2014. [https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf], visited 21.2.2021.
[343] Kilcullen (2020), 76–77.
[344] NATO: *Wales Summit Declaration*. Press Release (2014) 120, Issued on 05 Sep. 2014. [https://www.nato.int/cps/en/natohq/official_texts_112964.htm], visited 19.2.2021.
[345] NATO (2014); Gold, Josh: *The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'*. NATO CCD COE, Tallinn, 2020. [https://ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf], visited 19.2.2021.

Open networks do not have a centralised management, control, monitoring and feedback system. They may have a national monitoring system for information security threats, the adoption of which is voluntary in the private sector, but it does not cover all critical sectors. At the national level, the system for monitoring and responding to information security incidents is mainly based on the cooperation and information sharing between national CSIRTs/CERTs and private actors.[346] The questions related to responsibilities and mandates are partly undefined, and the ability of public authorities to intervene in the activities of private actors is very limited. With regard to cyber security, there is no actor who would be responsible for the information security of the networks of the public administration and state-owned companies, and the supervision of the information security of private actors critical to the state. In addition, the public sector is stovepiped when it comes to its systems and information security solutions. The authorities practise some cooperation, but private parties are given limited access to training for reasons related to, for example, trade secrets and competition. National information security authorities are networked within alliances (or equivalent) and exchange information with each other.[347] In combating cyber crime, cooperation between authorities and private actors is functional, but still in the early phases of development.[348]

Since the mid-2010s, the approach of the Western states to the internet and cyberspace in general has begun to change significantly.[349] For example, threats related to the *Internet of Things (IoT)*, 5G technology and production chains have tightened market regulation. Several countries seek at least limited self-sufficiency in cryptography, hardware and software.[350] National cyber security increasingly includes blocking harmful or dangerous websites and services, and requirements for removing content assigned to supranational companies.[351] Data protection legislation is drafted by state and by alliance, which requires that the user and company data is localised. One of the measures aimed at preventing critical data from ending up outside the national borders is building national data centres.[352] CERT/CSIRTs are encouraged to engage in international cooperation, and many countries are building national cyber security

---

[346] ENISA: *CSIRTs by Country - Interactive Map.* [https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map], visited 10.7.2020.
[347] ENISA: *EU Member States incident response development status report*, November 27, 2019 [https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report], visited 10.7.2020.
[348] ENISA: *An overview on enhancing technical cooperation between CSIRTs and LE*, May 07, 2020. [https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-tools-for-enhancing-cooperation-between-csirts-and-le], visited 10.7.2020.
[349] On the events of past couple of years cf. Kaplan (2016); Sanger, David, E.: *The Perfect Weapon. War, Sabotage, and Fear in the Cyber Age*. Scribe, London, 2019; Greenberg, Andy: *Sandworm. A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday, New York, 2019.
[350] The strategies of EU member states are available at: ENISA: *National Cyber Security Strategies - Interactive Map* [https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map], visited 12.1.2021.
[351] Scott, Mark: Welcome to New Era of Global Digital Censorship. It's Dangerous to Ask Tech Companies to Decide What's Legitimate Free Speech. *Politico*, January 14, 2018. [https://www.politico.eu/article/google-facebook-twitter-censorship-europe-commission-hate-speech-propaganda-terrorist/], visited 12.1.2021.
[352] European Commission: *A European strategy for data*. COM(2020) 66 final, 19.2.2020. [https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066], visited 12.1.2021.

management systems.[353] States increasingly want to use the cyber capabilities of the armed forces and intelligence services for 'active deterrence' rather than for defensive tasks, and to develop better and more comprehensive capabilities for intelligence services to engage in foreign information network and system surveillance.[354] Instead of cyber warfare, countries are increasingly talking about the need to develop cyber-enabled information operations.[355]

Many of the above-mentioned projects are voluntary and based on cooperation between the private sector and public administration. However, they are clearly based on national security interests. Protection of interests would also seem to drive Western countries to adopt some kind of a version of cyber sovereignty.[356] At the same time, cyber threats and, in a broader sense, information threats are increasingly considered 'national emergency situations', the management of which requires cross-administrative resilience that mobilises the resources of the whole society or even 'civil defence'.[357] Therefore, the nature of open national networks seems to be changing, and it is possible that the analysis of the structural cyber asymmetry presented in the next chapter will no longer be accurate as such in the 2030s.

---

[353] ENISA: *Study on CSIRT landscape and IR capabilities in Europe 2025*, February 2019 [https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025/at_download/fullReport], visited 12.1.2021.
[354] Pernik, Piret: National Cyber Commands. In *Routledge Handbook of International Cybersecurity*. Tikk, Eneken & Kerttunen, Mika (eds.) Routledge, London, 2020; Lubin, Asaf: A New Era of Mass Surveillance is Emerging Across Europe. *Just Security*, January 9, 2017 [https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe/], visited 12.1.2021.
[355] Congressional Research Service: *Defense Primer: Information Operations, Updated December 15, 2020*. [https://fas.org/sgp/crs/natsec/IF10771.pdf], visited 21.2.2021.
[356] Tikk & Kerttunen (2020); Hobbs, Carla (ed.): *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry*. European Council on Foreign Relations, July 2020. [https://www.ecfr.eu/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf], visited 17.10.2020.
[357] Austin, Greg & Sharma, Munish: From Cyber Resilience to Civil Defence. In *National Cyber Emergencies*. Austin, Greg (ed.) Routledge, London & Newy York, 2020, pp. 10–30, pp. 26–27.

4. Analysis of structural cyber asymmetry

This chapter analyses the structural cyber asymmetry deriving from the relationship between the Russian national segment of the internet (in short: internet segment) and a theoretical open national network. The first part of the chapter complements the earlier analysis based on attack vectors with new and further developed concepts.[358] The second part examines the internet segment and open national networks through the subsystems of the national information security and defence system model, using the concepts of freedom of action, common situation picture, command and control, and resilience for comparing the networks. In the third part, the internet segment and open national networks are compared at different phases of the development of interstate relations. The fourth part summarises and reflects on the observations made on structural cyber asymmetry, which are used in Chapter 5 to assess the strategic effects of asymmetry.

4.1 Attack vectors

Kukkola, Ristolainen and Nikkarila summarise the results of the attack vector analysis carried out in their earlier study as follows: "In our analysis we have shown that the frontlines of a closed network; the possibility to completely disconnect a closed network from other networks; and, the relative freedom of action in open-society networks create a 'cyber asymmetry' that favors a closed-network nation. It has greater situation awareness, a faster decision-making cycle, and more freedom to maneuver than states with an open-network society. It can attack wherever and whenever it wants."[359] This chapter complements the previous analysis by adding the concept of resilience to the examination and further developing the analysis through the concepts of freedom of action, common situation picture, and command and control specified in Chapter 2.5.

The original attack vector analysis examined the freedom of action as the ability to penetrate through national network interfaces and internal interfaces. The complemented definition of freedom of action presented in Chapter 2.4.1 extends the analysis to examining the shaping and management of the space. At the national level, the defender of the internet segment can, by shaping the network flexibly and adapting to the opponent's behaviour, deny the attacker's freedom of action. Parts of the national network can be closed, connections changed, and traffic intervened in more easily than in open networks. The aggressor's freedom of action can also be denied by patching vulnerabilities centrally and relatively quickly. In open national networks, features described above are only found in separate intranets managed by various parties. However, when alliances or public-private partnerships work effectively, the performance of an open network improves. The internet segment also has significantly fewer internal administrative or commercial interfaces than open networks that would not be accessible to those responsible for the security of the national network. In other words, open network defenders lack freedom of action, as they only have access to a fraction of the important subnetworks and interfaces of the open network.

[358] Kukkola, Ristolainen & Nikkarila (2017).
[359] Kukkola, Ristolainen & Nikkarila (2017), 103.

Internet segment defenders, on the other hand, can move around fairly freely in their own network and establish pre-emptive presence in potential targeted systems, instead of needing to start defensive action by responding to an enemy attack that has caused some impact. In addition, the software and hardware used in the internet segment are likely to differ from those of the aggressor. The aggressor is forced to operate in an environment deviating from its own and to spend a significant amount of time and resources on reverse engineering. Furthermore, the internet segment features security systems all the way from the national level to the targeted level, which makes it difficult to carry out offensive action. Aggressors must also try to achieve impacts as fast as possible, as with every passing minute it becomes more and more difficult to hide inside the internet segment and easier for enemy reconnaissance to detect the operation.

However, the internet segment is not watertight. From the aggressor's point of view, the opportunity to affect the target is more emphasised than the freedom of manoeuvre. The target systems can be affected in various ways, and it does not necessarily require a direct, continuously maintained access to the target and its manipulation. Some of the closed-network defence systems can be circumvented or bypassed. The ability of an open aggressor to manipulate users and use insider attacks becomes further emphasised. The aggressor can also shape cyberspace or make the defender shape it according to its preferences. The management systems of the internet segment, closed ecosystems and network interdependencies can create useful spillover and multiplier effects for the aggressor, thus opening up new attack vectors. Another weakness is related to how the external connections of the internet segment have been implemented. If they are based on only a few connections, they constitute a critical vulnerability if someone wants to prevent the state's access to the global internet from the outside. However, if there are several connections, it is challenging to monitor them centrally without involving the private sector. Private sector participation, on the other hand, increases the uncertainty related to the functioning of the system, especially in a crisis situation. As such, the weaknesses identified above do not affect the results of the previous analysis. However, they highlight the importance of controlling the space internally alongside controlling its borders and the requirements for successfully controlling the internet segment's external connections.

On the other hand, using the common situation picture as a tool of attack vector analysis instead of situational awareness does not significantly affect the earlier research results, since, in fact, the original analysis examined the situation picture, not situation awareness. The common situation picture of the internet segment defender is undoubtedly better than that of the open network defender. The former has access to the organisation, processes, data models and data flows to create a national cyber situation picture[360]. In an open national network, the defender cannot merge data in a similar manner. In addition, the internet segment defender can collect data from several levels throughout the depth of the network. It has sensors in all parts of the

[360] Cyber situational picture consists of systems and network architecture, threats, recognized attacks, countermeasures, and current and future actions affecting the organisation's cyber operating environment. (Cf. Conti, Gregory, Nelson, John & Raymond, David: Towards a Cyber Common Operating Picture. In *2013 5th International Conference on Cyber Conflict*. Podins, K., Stinissen, J. & Maybaum, M. (Eds.) NATO CCD COE Publications, Tallinn, 2013, pp. 179–295).

national network and can use automated systems to analyse the data provided by them. The open network defender may have similar systems, but they do not exchange information with each other or exchange it only to a limited extent, so no common situation picture can be created. Due to the common situation picture, the connections and interfaces of a closed network are significantly better monitored than those of an open network.

In principle, anyone attacking the internet segment must pay particular attention to hiding their tracks, modifying their tactics, and exploiting unique vulnerabilities or using totally new types of attack. This is because the defender builds and analyses a situation picture of the entire system in a centralised manner. In addition, the aggressor's common situation picture is limited by the changing nature of the space, national hardware and software solutions, and the defender's active deception and counter operations. In an open network, the same features appear in a fragmented and independent form, guided by private interests. In other words, the internet segment defender has a more complete and up-to-date situation picture of its own and the adversary's activities than the open network defender.

Although sharing a situation picture in a closed national network is one of the main benefits provided by the system, it is not entirely certain that the sharing will take place. The stovepiped administrative structures may weaken the functioning of technical solutions. Furthermore, technical systems cannot fully guarantee that decision-makers share an accurate understanding of the situation. The understanding of the vulnerabilities of nationally produced systems may be limited. Automated and AI-based systems can be deceived. Furthermore, open networks do not entirely lack useful features either. For example, the diversity of data protection practices used in subnetworks and subsystems makes reconnaissance of an open network difficult. Despite the limitations, the situation picture of someone attacking an open national network is relatively better than that of someone attacking a closed network.

In the attack vector analysis, replacing decision-making with the concept of command and control does not change the results of the previous research. This is because the previous analysis focused on examining the access to information available for decision-making and the speed and efficiency of execution, and they are, in fact, characteristics of a command and control system, not decision-making. However, the concept of command and control draws the attention to technology, organisation and operating methods. The defence of the internet segment is based on a centralised C2 system, made possible by a high-quality common situation picture and C2 connections built at lower levels. The system has a hierarchical structure in which the C2 levels of various systems meet at the same points – in practice, in the network control centres of security authorities. The centralised management system is essentially linked with organised information management based on machine learning, which prevents challenges posed by an excessive amount of information. The C2 system enables efficient and rapid control of external and internal interfaces of the internet segment. Therefore, the challenge for the aggressor is that it is more difficult for the aggressor to exploit technological and organisational interfaces, since, in practice, there is only one defender. In addition, the defender can respond to attacks from different vectors very quickly. The aggressor must also continuously protect its own

C2 connections, which requires a more complex operation when the internet segment connections are controlled.

In practice, critical vulnerabilities may occur in the command and control of the internet segment. The C2 system may be fragmented for bureaucratic or technological reasons, in which case the C2 system may in practice be stovepiped and converge only at the top of the hierarchy. In this case, much of the benefits its command and control offers will be lost. In addition, the aggressor may gain access to the internet segment's C2 system, which enables sabotaging the entire network or concealing the aggressor's actions.

The defender of an open national network lacks a national C2 system. Its command and control are based on separate systems that exchange information to a limited extent. Attacks are responded to in a stovepiped manner and with significant delay, especially when attacks cross the borders of different C2 systems. Parties involved may hold back threat information from authorities or partners for financial or political reasons. Furthermore, an open network system as a whole cannot adapt itself as the attacks would require. On the other hand, its C2 system is not particularly vulnerable to attacks against it due to diverse technological solutions and segmented networks. All in all, the internet segment's C2 system makes it possible to close connections and interfaces in a manner that is not available for the open network defender.

Adding resilience as a category of the analysis of attack vectors strengthens the argument concerning the existence of structural cyber asymmetry. Regardless of the attack vector, the internet segment defender has a clear advantage because duplicated and controlled interfaces and critical services can withstand attacks and enable mitigation of their impacts. Attacks from within the network are, of course, still dangerous, but their impacts can also be restricted. The critical infrastructure is known, protected, partially duplicated and continuously monitored. The internet segment can be divided into separate sections to avoid an attack, and recovery has been practised at a national level. Therefore, the opportunities of the aggressor to cause any significant long-term impacts are limited. The ability to regulate the number of external connections significantly contributes to the resilience of a closed network.

The resilience of open networks depends on the particular part of the network and the system targeted by an attacked. The resilience of the network is fragmented and of varying quality, as the subnetworks of the open network are managed by private and public bodies independent of each other. An aggressor may use different connections to simultaneously strike a single target from multiple directions or multiple targets through various connections. This makes it possible to cause an extensive state of disruption in services based on an open national network due to the various interdependencies. Since cooperation and recovery have not been practised at the national level, it is difficult to manage the spillover effects. On the other hand, a mere random attack on an open national network is unlikely to cause critical damage, since the heterogeneity of the network also serves as a source of resilience. Both the internet segment and the open network have their strengths when it comes to resilience. When examining resilience through attack vectors, control of the interfaces on the one hand and identification of their interdependencies on the other become a significant factor.

4.2 Internal structural differences

The attack vector analysis presented in the previous chapter can be complemented by comparing the features of the internet segment and open national networks categorised under their subsystems in terms of freedom of action, common situation picture, command and control, and resilience. Table 1 presents the characteristics of the internet segment and open national networks side by side examined through the subsystems of the national information security and defence. The characteristics listed in the table are based on the descriptions of the characteristics of the Russian state, the target state of the national segment of the internet project and the theoretical open network presented in Chapters 3.2 to 3.5. In this approach, an open national network is defined through the information security and defence system. This is a pragmatic approach, since the work studies the characteristics of the Russian national segment of the internet and its relationship with structural cyber asymmetry.

Table 1: Comparison between the internet segment and open national networks through subsystems.[361]

Network type: Internet segment	**Network type: Open national network**
Subsystems: 1. Scientific-technological basis	
- State-led - Seeks wide-ranging self-sufficiency and avoidance of international interdependencies - The use of foreign products highly regulated - State ownership of strategic assets - foreign ownership well controlled - National SW/HW ecosystem - Primarily proprietary source code - Limited international cooperation in cyber security	- State involvement varies - Self-sufficiency sought in very narrow sectors only - Science and technology developed in a market-driven manner - Significant foreign interdependencies (supply-chains in particular) - Privatisation of strategic assets - foreign ownership regulated - Few domestic SW/HW - Fractured field of suppliers
Subsystems: 2. Authentication and encryption system	
- Domestic solutions - State certification required for all cryptography - State able to decrypt all traffic without judicial or administrative process	- Limited domestic solutions - State provides certification for official use and recommends good practices - Slow decryption because of political and legal issues
Subsystems: 3. Censorship system	
- State-led centralised system - Widespread state censorship and self-censorship of the media - Removing politically undesired material from the information space or blocking access - Excluding foreign actors from the information space - Removing user anonymity - Significant amount of voluntary activity	- No centralised system - No political censorship - Free media that may practise self-censorship on limited national issues - Grounds for removing material or restricting access other than political - Protection of identity and communication secrecy as principles of communication - Little voluntary action

[361] The table and analysis are based on Kukkola, Juha: The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry. In *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Ertan, A., Floyd, K., Pernik, P. & Stevens, T. (Eds.) CCD COE, Tallinn, 2020b, pp. 9–30.

Subsystems: 4. Surveillance and massive data collection systems	
- The security services monitor national data traffic in a centralised manner and without parliamentary supervision - Massive data collection from data traffic in the national network - Localisation of critical data of companies and citizens based on national security	- Restricted and under parliamentary supervision - No massive data retention on own citizens for security purposes - Data protection and localisation based on privacy issues - A portion of critical company and state data abroad
Subsystems: 5. Critical information infrastructure	
- Owned by the state and private sector - Legal obligation to categorise, maintain and protect - Critical services mostly state-controlled and duplicated - Ability to disconnect from the global internet in a controlled manner	- Owned by the private sector - Protection guided by market economy factors - Some government regulation and certification - No duplication of critical services by the state - No ability to disconnect from the global internet in a controlled manner
Subsystems: 6. Active measures system	
- State-controlled media - Strict regulation of foreign media and foreign ownership of media assets - Religious and patriotic institutions supporting the state leadership and led by the state, and guidance on how to interpret history - Dedicated cyber diplomacy organisation with clear national objectives - Overt propaganda, covert and disruptive information operations - Obfuscation of cyber warfare capabilities, several operators, using a wide range of substitute operators - Cyber and information warfare capabilities as part of deterrence and wartime escalation control - Limited international cooperation	- State-owned and commercial media - Few restrictions for foreign media companies - Civic education by a politically independent early childhood education and school system - Cyber diplomacy has no particular role as part of foreign policy, diverging interests among allies - Soft power, overt strategic communications and targeted cyber information operations - Cyber warfare forces established openly, with controlled and defensive operations - Active international cooperation in foreign communications intelligence
Subsystems: 7. Military networks and systems	
- Armed forces defend their own networks under normal conditions and the critical infrastructure under emergency conditions - Separate and own operational networks, systems and information security solutions - Limited interfaces with other security actors - Duplicated and geographically decentralised infrastructure	- Armed forces defend their own networks at most - Military networks operate in parallel and overlap with civil networks and the networks of other security actors - Cooperation with private telecommunications operators and cyber security companies - Separate field messaging and most critical systems
Subsystems: 8. Management, control, monitoring and feedback system	
- Led by the security services - Multiple centralised information management and security systems - Nationally controlled response to technological and psychological security threats - Limited international cooperation and information exchange	- No clear national leadership - Only a limited and narrow national cyber security system - Concentrates on crime prevention - National computer incident response team (nCSIRT) coordinates, and an array of sector-specific CSIRTs execute cyber security - Developing international cooperation and information exchange

Table 1 makes it possible to examine the characteristics of the internet segment and an open national networks from the defender's point of view, since the national network itself does not 'attack' in the actual sense of the word. In other words, in the analysis, the aggressor is represented by a generic actor. The active measures system, to which we will return further below, constitutes an exception to the rule.

The scientific-technological basis of the internet segment provides a definite advantage in defence, as the attacker must engage in reverse engineering regarding the national hardware and software solutions. This slows down the attacker and limits its freedom of action. Conversely, the defender knows the systems it needs to protect and is able to modify them and move around freely in them. Domestically produced technologies and integrated systems provide the internet segment defender an advantage in unified situation picture, and command and control. Resilience is further enhanced by a domestic and state-controlled cyber ecosystem where observed vulnerabilities can be repaired quickly, even by coercive measures. The fragmented nature of open networks hinders the freedom of action of their defender. The common situation picture is limited due to administrative and legal mandate issues and incompatible systems, while command and control lacks integrated C2 support systems. The resilience of open national networks is highly dependent on the risk calculations of independent service providers, but international cooperation may offer tools for enhancing resilience.

The national authentication and encryption system of a closed network guarantees a definite advantage in freedom of action and common situation picture to the defender. All traffic is in principle transparent, and there are no connections, spaces or networks that are closed to the defender. Its weakness lies in potential critical vulnerabilities in the encryption system. Conversely, the defender of an open national network is limited in its ability to decrypt traffic. As a rule, the private sector and citizens use solutions closed to the defender. Decrypting them takes time and often requires an administrative decision. In addition, domestic encryption solutions are used only in some systems and their quality is mixed, although the use of multiple encryption and authentication systems might increase resilience through redundancy. The vulnerability in a single solution does not threaten the entire network.

The censorship system used in the internet segment provides a definite advantage for the internet segment defender in freedom of action. The freedom of action of an attacker using information-psychological and technological attacks can be denied by removing the necessary resources and platforms from the national cyberspace. The removal of anonymity enhances the defender's situation picture, making it possible to identify the devices and actors in the cyber environment. In addition, vigilante groups can support the formation of a common situation picture by reporting their observations to the authorities. A centralised censorship system enhances the speed and effectiveness of the command and control of defence measures. The resilience of a closed network is improved as the censorship system is tested and operated constantly even under normal conditions. Defenders of open networks are disadvantaged in all these categories. They are not totally impotent, but the use of a censorship system – should such a system exist in the first place – is slow and has legal, political and economic limitations.

The targeted surveillance and data retention system of the internet segment provides the defender a significant advantage in its common situation picture. Furthermore, these systems provide the defender a direct access to all public and open networks and their content, which further enhances the common situation picture and freedom of action. As the content-monitoring systems are connected to the national centralised monitoring and management systems, they also support command and control by providing timely and exact data on cyber and information threats. Large data reserves can be screened for indications of threats without need for any separate administrative decisions. In addition, the localisation of data to national data centres enhances network resilience. In principle, open networks lack systems for monitoring network content and collecting data. Resilience is weakened by critical data being located abroad or in data centres of foreign service providers. However, once there is enough evidence of hostile action in the network, open network defenders usually have the ability and mandate to start network surveillance.

The critical information infrastructure of the internet segment provides the defender an advantage in all the categories included in the analysis. The freedom of action is guaranteed by the fact that critical systems are state-owned or controlled, and access to private systems is guaranteed by law. The critical information infrastructure is connected to centralised monitoring and control systems, which gives an advantage in common situation picture, and command and control. Resilience of the whole network is high as the infrastructure is constantly monitored, duplicated and protected. The whole internet segment or parts of it can be disconnected from the global data network to manage threats and enable system recovery. However, how high resilience actually depends on the way external connections are managed and restricted. Although open national network defenders are somewhat disadvantaged, much depends on the actions of those – usually private actors – responsible for the infrastructure. Resilience may be quite good due to duplicate and parallel systems of private service providers. Diversity may increase resilience, but only if private operators follow the best possible practices and competition does not lead to the centralisation of services to the same physical and logical systems. On the other hand, the freedom of action, situation picture, and command and control are restricted by the boundaries between the networks of the aforementioned service providers. Many of the existing systems are administratively stovepiped or designed to maintain the information security of private companies.

The active measures system of the internet segment provides the closed network defender with a definite advantage in freedom of action. This is based on manipulating information, destabilising opponents and eroding their unity on a continuous basis and under any circumstances through cyberspace without any significant internal restrictions. Constant aggressive domestic monitoring and intelligence (espionage) operations provide an advantage in common situation picture. Similar data collection can also be extended to foreign networks. Coordinated actions of the authorities and C2 systems provide an advantage in the command and control of countermeasures. When targeting external networks, the command and control countermeasures enables multi-vector, multidisciplinary and high-impact attacks and provides a clear advantage. The control of the media space and patriotic education provide an advantage in information-psychological resilience. Since the system cannot cover the entire national information space, psychological resilience always remains vulnerable. In an

open network, on the other hand, democracy and transparency enhance the information-psychological resilience. With regard to other factors, the open network defender is somewhat handicapped because of the decentralisation of C2 functions to various administrative sectors, the need to coordinate actions with allies, the restrictions posed by legislation and agreements, and the unclear division of responsibilities between public and private actors. However, this does not mean that the defender would not have relatively quick access to sufficient response capabilities, including offensive ones, if necessary.

As regards military networks and systems, there is no clear advantage/disadvantage division between the internet segment and open national networks. This is due to the fact that in both network types the armed forces aim to separate their own connections and services from public networks, to share the situation picture mainly with only those who need it, and to implement command and control through hierarchical, regionally distributed command echelons, the objective being maximum resilience. The differences arise mainly from technological solutions, not from structural differences in principle. The armed forces of open network states have relied on cooperation with civil operators, while the armed forces of the internet segment state have sought to keep the C2 system infrastructure in their own hands. The first model restricts the defender's freedom of action, but has enhanced resilience, while the latter model, in principle, ensures the defender's freedom of action and improves the common situation picture and command and control. In practice, however, it can lead to stove piping of the branches of service and, at worst, technological backwardness. For both networks, the development of the cyber environment is leading to broadening the mandate of the armed forces for defensive operations outside their own networks.

The management, control, monitoring and feedback systems of the internet segment provide the defender with an advantage in all categories under analysis. Interconnected state-controlled systems enable freedom of action and provide national-level common situation picture. Management and support systems, and centralised and hierarchical C2 systems provide superior C2 capability. It enhances resilience that the critical information infrastructure is continuously monitored, threats are countered, personnel operating the infrastructure is trained, and national training exercises are arranged. On the other hand, as stated earlier, centralised systems are also a risk factor when it comes to resilience. The open national network defender, on the other hand, is disadvantaged because of administrative stove piping. The defender might gain an advantage in common situation picture through international cooperation and mandatory voluntary public-private cooperation, but only if the acquired information can be collected, analysed and shared in a manner that suits all parties involved.

Although the comparison of characteristics presented above seems to favour the internet segment, this is not necessarily so in all respects. Internet segments are highly dependent on state participation and, thus, on state resources, revenues and administrative efficiency. Unfair competition positions in the domestic market may disincentivise innovation, as may the close relationship between science institutes and the state. Bureaucracy and corruption undermine the efficiency of projects and organisations. Domestic encryption solutions and the use of *proprietary* code or hardware does not automatically provide better security than, for example, an open code that is being

tested continuously. Politically motivated censorship breeds political apathy and resistance which may, at worst, increase the risk of insider attacks. Massive retention of information creates troves of data that offer an attractive target for both criminals and state actors. Databases created based on the mapping of critical information infrastructure also constitute potential targets. Furthermore, significant parts of a closed national network can be paralysed by jamming national network monitoring and management systems.

The authoritarian and superpower-centric policies underlying the closed networks are hard to mask in cyber diplomacy, which reduces the international appeal of the model. Active measures are not always as 'holistic' or centrally commanded as they may appear. The information security and defence system is operated by a large number of national actors who may have conflicting interests.[362] This may impair the development and functioning of the internet segment. Administrative or technological stove piping may be much more significant than public information suggests. For example, the resilience of critical information infrastructure may remain illusory if instructions are not followed and supervision is weak, or politically or economically motivated. Furthermore, it is impossible to completely close the information space, so a section of uncontrolled space always remains outside the internet segment or, in a broader sense, outside the information security and defence system. This space serves as a potential platform for an attack.

Despite the critical reservations presented above, it is clear that structural cyber asymmetry is also present at the level of internal properties of the networks. The observations made and the addition of resilience as a category of analysis just strengthen the attack-sector analysis. However, the reservations presented should be taken into account when considering the strategic effects of structural cyber asymmetry, as they constitute framework conditions for whether states decide to use force in the cyber environment or not and affect the impacts of the use of force.

4.3 The continuum of interstate relations

In my doctoral dissertation, I described how Russia's national information security and defence system could function as interstate relations change and in the context of different threat scenarios.[363] This thesis adds the concept of theoretical open national network alongside that description to allow examining structural cyber asymmetry in time. In general, it can be stated that the operating logic of the internet segment is based on flexible regulation of cyberspace through the subsystems of the information security and defence system. Open national networks, on the other hand, operate in a considerably more decentralised manner, often based on consultation and contracts. The results of the analysis below are summarised in Figure 3.

---

[362] On these actors cf. Radin, Andrew, Demus, Alyssa & Marcinek, Krystyna: *Understanding Russian Subversion Patterns, Threats, and Responses*. RAND, Santa Monica CA, 2020, pp. 16.
[363] Kukkola (2020a), 366–367.

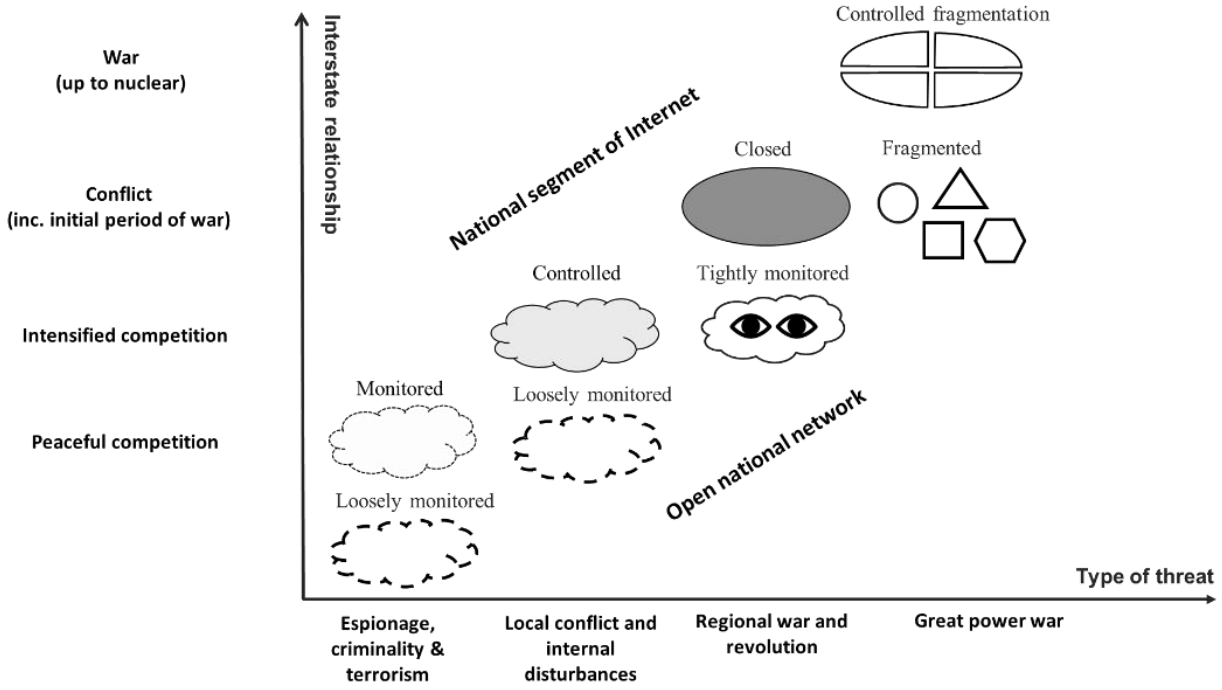

Figure 3: The relationship between closed and open national networks on the continuum of interstate relations and threats

In Figure 3, the vertical axis shows the phases of interstate relations and the horizontal axis the types of potential threats. The axes of the figure do not represent independent variables but describe the strategic environment of national networks from different perspectives. As described in Chapter 2.2, the interstate relations include peaceful competition; intensified competition; conflict, including the initial period of war; and war. Threats placed on the horizontal axis are based on the manifestations of indirect and direct military threats to state security, the type of actors involved and the intensity of actions.[364] During peaceful competition, states primarily use non-violent and non-military means of struggle. Espionage, crime and non-state terrorism are threats faced by states on an everyday basis, but they may also be relevant with a view to national security. They may originate from state or non-state sources. During the phase of intensified competition, the means used by states are still non-military, covert and indirect, and their objectives are limited. The local conflicts related to the phase are operations with limited objectives conducted using conventional armed forces or short-term military operations against another state. Other threats include internal, limited disturbances and terrorism, which may be supported from outside the state. The disturbances are spontaneous and, as a rule, not aimed at seizing political power.

[364] This delineation of interstate relations and threats is based on Russia's military doctrine, the views of Russian military theorists and the United States' Armed Forces doctrine (Указ-2976: Указ Президента РФ 25 декабря 2014 г., № Пр-2976. *Военная доктрина Российской Федерации.* [http://base.garant.ru/70830556/], visited: 21.3.2019; 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, с. 35–43; Mulgund & Kelly (2020)).

During conflict and the initial period of war, the means used by the state still remain limited. However, the situation may escalate very quickly into the initial period of war, involving the use of open, direct military force. In both cases, the state considers its existence to be threatened by either state or non-state entities. The prevailing threat scenarios include insurgencies or getting into a regional war. Regional wars involve several states or alliances and are solved by conventional armed forces in one geographical direction. The duration of regional wars varies and may require declaring a full state of war in society. Operations are conducted in the whole depth of the parties involved and in all operational domains. Insurgency refers to a violent, armed revolution that is aimed at seizing political power. It probably receives support from outside the national borders and may lead to a military intervention from outside the borders.

War is a state of affairs between nations in which they use open military force to pursue their political objectives. The predominant threat in case of great powers is a war between the great powers, which may escalate into a total nuclear war. When the war involves smaller states, the threat is a large-scale conventional war. A major war involves several states or alliances and is conducted by all means available, including nuclear weapons. The goal of all parties involved is survival. A major war can last a long time, although the use of nuclear weapons makes it difficult and probably inappropriate to continue hostilities.

All subsystems of the internet segment (national information security and defence system) are operational at all stages of interstate relations and when facing various threats, but the quality of operations and level of activity varies. The subsystems of a theoretical open national network are also in operation, but fewer changes take place in their functioning as interstate relations or threats change. During peaceful competition, the advantage the internet segment has over open networks is that its monitoring of the cyberspace is more effective and it has a higher capacity to respond centrally to individual cyber operations at a national level. In addition, active measures maintain psychological resilience and constantly challenge and destabilise potential enemies. Open national networks are capable of monitoring only part of their networks and systems. Open national networks benefit from the openness of the cyber and information environment in their countermeasures, the possibility of international sharing of information related to cyber threats and the global supply chains and markets. At this phase of interstate relations, the internet segment can be called 'controlled', while open networks can be described as 'controlled to a limited extent' at most. The most significant difference is that a state with an internet segment can signal that it will be capable of tightening its control of the network quickly, while open network nations have more limited freedom of action because, in reality, they do not govern their own national cyber environment.

During intensified competition, at least one of the parties identifies the situation as a national crisis of a certain degree. In the case of the internet segment, the national encryption system, censorship system and targeted surveillance systems as well as massive data collection make the national cyberspace transparent to the entities responsible for cyber and information defence. This enables enhanced protection of the critical information infrastructure and centralised command and control of the national cyber security. A good situation picture allows quick attribution of attackers and the use of the attribution data for supporting the pursuit of political goals. At the

very least, it can help restrict the suspected attacker's freedom of action. Active measures make it possible to manage and defend one's own information space, while making it more difficult to challenge the opponents as they raise their readiness. While both the internet segment and open national network states can call different alliances to action, open network alliances may be more efficient in establishing a common situation picture and possibly in combating threats. In open network states, the challenge lies in identifying a national crisis situation and making a decision to enhance resilience or to initiate active measures. The private companies, government agencies and administrative sectors of open national networks have to combat threats using their own, separated resources. The open network states do not have access to a similar national situation picture as the internet segment operators. At this phase of interstate relations, the internet segment can be describes as being 'controlled' and open networks still as being 'controlled to a limited extent'.

During a conflict or the initial period of war, at some point not determined in advance, the interstate struggle crosses the threshold of an open, declared war. At this point, the internet segment operates using its full capabilities. The national cyber environment and thus the information space can be disconnected from the global cyber and information space and managed internally. Society can be taken under control and internal revolutionary actors can be isolated from their external supporters. As the disconnection has been planned in advance, the functions critical for the state's defence and essential operations (e.g., water supply, electricity, food supply) can be secured. Command and control are centralised, and both technological and psychological resilience are maximised. Active measures can be directed against the adversary in the conflict through allies or other networks. All of the above measures can be implemented flexibly, and the internet segment can be restored to its normal state when the political situation permits.

During a conflict, open network states lack the possibility of acting in a similar manner as states with an internet segment. The powers of security actors and the monitoring of the national network can be increased, but, for legislative and commercial reasons, the process of enhancing the capabilities is slow. Establishing cooperation with cyber security actors requires crossing sectoral boundaries, coordination and negotiations. The freedom of action of the armed forces or security actors of open network states may be negatively impacted by social, commercial or normative factors as they are defending national networks. A conflict and the initial period of war may disrupt the scientific-technological basis in a way that degrades the resilience of open national networks. The negative impacts on the international interdependencies may be deliberate or unintentional. The primary factors affecting the balance of power between the networks are the speed and timing of measures and the sharing of situational information and thus forming an understanding of the situation during the initial period of war. At this phase of interstate relations, the internet segment can be referred to as 'closed' and open networks as 'controlled to a limited extent'.

In an open major war, some of the subsystems of the internet segment and open national network are likely to lose their functioning capacity. The advantage of the internet segment is its ability to internally fragment into territorial parts in a controlled manner. This is possible because its critical infrastructure has been built under state

leadership and is controlled by the state. If a centralised management system is destroyed or paralysed, territorial civilian and military echelons will be able to continue their operations. The armed forces are capable of continuing their operations even if the highest command is separated from the forces or destroyed. Until the network begins to break down into parts, it is easier to produce remedying updates to the internet segment's systems based on domestic production. During active military operations, national software and hardware systems can help win time as the attacker must engage in reverse engineering and look for weaknesses in them. On the other hand, centralised systems can also prove to be critical weaknesses in open warfare.

During war, it is not possible to disconnect open national networks from the global cyberspace. Their defenders do not have the ability to control how networks break down into separate parts. They lose the freedom of action, and the common situation picture becomes fragmented. The governance of civilian administration becomes paralysed. In open network states, the armed forces may have the ability to continue their operations in isolated entities but their earlier close cooperation with civil operators to build capabilities may have created critical interdependencies and lead to paralysing spillover effects. Redundant connections based on commercial agreements may prove unsuitable for their purpose or they have not been implemented at all. At this phase of interstate relations, the internet segment can in extreme cases be described as 'fractured in a controlled manner' and the open networks as 'fragmented'.

The internet segment and open national networks differ from each other on the continuum of interstate relations also in terms of which entity is responsible for their operation and security and which principles are applied to managing the networks. During peaceful competition, the security services or other designated authorities are responsible for the security of the internet segment. Private operators are obligated by law to protect the critical information infrastructure in their possession. They bear the costs of the obligations. In theory, the national nCERT/CSIRTs are responsible for the security of open national networks. In the real world, the network and information security control rooms of service providers and operators are responsible for security, and private companies provide the information security services to their customers. Cooperation between the public and private sectors is voluntary and is only loosely based on legislation or recommendations. Although international cooperation and contracts provide more tools for managing cyberspace in open networks, in networks left open the level of cyber security is determined by the markets and risks.

During intensified competition, the security of the internet segment is transferred exclusively to the state. Security operations are managed centrally by cross-administrative bodies of state administration. The implementation is led by the security services and the national network management authority. The private sector becomes the tool of implementation. In open networks, very few changes happen in terms of the principles applied to organisational management of security and network governance. On the other hand, different contractual arrangements may enter into force, in which case the public-private cooperation may intensify, and national and international cooperation mechanisms may be activated.

During conflict and the initial period of war, the management and security of the internet segment are in the government's hands and they are executed by the security

services, network management authorities and, to a limited extent, the Armed Forces. In the early stages of war, friction may occur between different actors as the control of the cyber environment is increasingly transferred to the Armed Forces. As regards the open network, national legislation or lack thereof, the existing systems and earlier training largely determine how the responsibility for management is allocated and how successfully it is implemented. The field of actors may be strongly divided by administrative sectors and into areas of responsibility of regional and local actors. The private sector is responsible for its own networks, while the central government mainly provides consultancy, synchronisation, integration and data transmission services. In time-critical situations, it is challenging to reach objectives set for cooperation.

In the event of war, the Armed Forces are responsible for the internet segment in cooperation with the regional government. The government has assumed its wartime composition. If necessary, network management and security can be controlled in a decentralised manner by territorial units and regional and local government measures. When getting fragmented, an open national network may find itself in a situation where it is impossible to coordinate management and security measures at the national level. Cooperation between regional actors takes places on an *ad hoc* basis. Communication and exchange of information between the fragmented parts of the network is difficult. If the central government becomes paralysed, an open network will not be able to switch to operating in isolated entities with their own command.

The analysis carried out through the continuum of interstate relations deepens the analysis of the structural cyber asymmetry between the internet segment and open national networks. It shows that the advantage the internet segment has in freedom of action is even greater than previously analysed. It has the initiative and can shape its own battlespace as the crisis progresses. It is faster and more agile. Instead, when it comes to a common situation picture, during peaceful and intensified competition international cooperation and an open scientific-industrial basis provide an advantage to the open national network. In conflict and war, the cooperation mechanisms become less important, but they do not disappear. The strength of the internet segment lies in centralised command and control in all phases of interstate relations, although it may also become a vulnerability. As state relations become more strained, resilience tends to turn in the favour of the internet segment. In the early phases, the open network benefits from global production chains and services, but during a conflict or war, they constitute a risk. Much depends on the actions and preparations made by private service providers. The internet segment, on the other hand, will start enjoying the investments made in protecting the national scientific-technological basis and critical information infrastructure from the conflict phase onwards.

4.4 Summary of the analysis

When examined through the continuum of attack vectors, national network structures and interstate relations, the relationship between the internet segment and open national networks creates structural cyber asymmetry through differences in the freedom of action, common situation picture, command and control, and resilience. However, asymmetry has significant framework conditions related to the practical implementation and functioning of the networks.

An essential addition complementing the attack vector analysis made in the previous study is the conclusion that internet segment defenders are far more efficient in shaping their network and repairing its vulnerabilities than open network defenders and thus denying the attacker's freedom of action in cyber battlefield. On the other hand, should the attacker be able to manipulate the space, this ability may also prove to be a vulnerability. The common situation picture of internet segment defenders is considerably better than that of open network defenders and, in addition, there are many factors limiting the situation picture obtained by the party attacking the internet segment. The management and implementation system of the internet segment provides the defender with fast and flexible decision-making, effective implementation and the possibility to evaluate results achieved almost in real time. Open network defenders lack a similar system. However, an attacker to the internet segment can target the attack against the closed network management system, which is an essential vulnerability. The internet segment defender has an advantage in resilience due to domestic production and control of the critical infrastructure. Resilience of the open network is potentially fragmented due to varying risk assessments made by subnet administrators. On the other hand, the heterogeneity of the open national network may also serve as a source of resilience.

The examination of the internal structures of the internet segment and open national networks strengthens the observation of the existence of structural cyber asymmetry. However, the analysis highlights some noteworthy issues in the properties of open networks. International cooperation and global supply chains may promote shared situational awareness and resilience. The segmentation of networks and the heterogeneity of technological solutions can turn into strength from the perspective of an open network. In open networks, the properties related to the freedom of action, common situation picture, command and control, and resilience are strongly connected to how the cooperation between the central government and the private sector has been arranged and how successfully it has been implemented. It is also worth noting that even if the comparison of networks would seem to favour the internet segment, this may not always be the case in practice. Many of the internet segment's strengths can contain conflicting elements and turn into weaknesses under certain circumstances.

The analysis carried out through the continuum of interstate relations also offers a more complex picture than could have been deduced from the initial design of the thesis. First of all, the internet segment is not the same as the *'internet shutdown* processes', in which national connections to the global internet are simply disconnected by service providers when so ordered by the state. Disconnection from the global internet is an extreme form of controlling the national cyberspace. Secondly, the advantage of a national information security and defence system lies, above all, in its ability to shape the information environment as the crisis evolves and to keep the systems functioning with the help of technological self-sufficiency in the event of global supply chains breaking down. The further the crisis in interstate relations advances, the greater the advantage of the internet segment in offensive and defensive freedom of action, and command and control. With regard to common situation picture, the situation is not as clear, since international cooperation between open network states makes it possible to exchange information with partners and allies. As concerns resilience, the situation depends on how capable the public and private parties involved in the open network are to cooperate with each other. If an open national

network can be successfully disconnected from the outside world, it will lose all potential advantages and suffer all possible disadvantages, while the internet segment has basically been built precisely for such an event.

In addition to proving the existence of structural cyber asymmetry, the analysis made in this chapter also shows the complex nature of asymmetry. Firstly, it must be understood that structural cyber asymmetry is a strategic-level phenomenon. The above analysis does not dispute the fact that individual cyber vulnerabilities could have a significant impact on the functioning of the internet segment. However, as a whole and in the long term, the internet segment is better equipped to defend itself, to recover and to support an attack than open national networks. Secondly, it must be stated that there are significant interdependencies within the internet segment, as highlighted in Chapter 3.4. The spread of harmful consequences within it is potentially devastating. At the same time, however, it should be noted that the subsystems of the information security and defence system support each other. In other words, the internet segment has internal strengths and weaknesses that compensate for each other. Thirdly, it must be stated that the strengths of the closed national network are largely based on an authoritarian political system and a state-led economy. Implementing an internet segment based on a different political system would probably face almost insurmountable resistance from the economy and civil society. In fact, constructing a national segment of the internet could permanently change the character of a state in an authoritarian direction.

5. Structural cyber asymmetry and use of force

This chapter answers the question of how structural cyber asymmetry affects the threat or use of force to achieve political objectives at different phases of interstate relations – i.e., analyses the strategic effects of structural cyber asymmetry. The chapter consists of four subchapters, analysing the strategic effects by setting the observations made in Chapter 4 on the relationship between the internet segment and open national networks into the context of strategic forms of use of force. The different forms of use of force are tied to the different phases of interstate conflict by examining how threats are prevented, how functional deterrence is, how the escalating conflict is managed and how structural cyber asymmetry is exploited militarily. The categorisation of use of force is based on the Western *bargaining model of war* presented in Chapter 2.2. In the analysis, this rationalistic and mechanistic perspective is complemented by social and cultural factors. The analysis is tied to the Russian information security and defence system and its representation in cyberspace, the national segment of the internet, and their relationship with the theoretical open national network.

5.1 Conflict prevention

Conflict prevention refers to the neutralisation of potential threats through any means available, without needing to resort to the threat or use of direct armed force. With regard to cyber activities, conflict prevention is related to intelligence, achieving early warning, persuasion by supporting information operations, building international norms and alliances, and shaping the domain to prevent potential threats. The aim of threat prevention is to safeguard national interests by preventing the emergence of acute and real threats arising from potential challenges in the operating environment. Prevention is sought because it is more cost-effective than combating threats, while maintaining the state's freedom of action in international politics to promote its own interests.

Structural cyber asymmetry is not at its strongest in a situation where conflicts can still be prevented. At that point, the differences between the internet segment and open national networks are at their smallest. On the other hand, the subsystems of the information security and defence system are operational and offer means for managing threats and shaping the operating environment. The system serves as a tool for external and internal communication; promotes the building of norms, rules and sovereign boundaries in cyberspace; produces technological independence and self-sufficiency; builds a nationally unified media environment; collects a national cyber and information situation picture; and implements a state-led, centralised, comprehensive information security model. Reciprocally, in line with their definition, open national networks are open to influencing. They have fewer opportunities than the internet segment to combat the means of non-military and limited use of force. Their effective functioning is tied to the balance of the international order, supply chains and diverse cooperation mechanisms.

Reconnaissance constitutes an important part of the ongoing low intensity 'cyber conflict' during the phases of peaceful and intensified competition.[365] It provides an economic, political and military advantage and prevents surprises. Information gathering applies to both foreign and domestic actors. At the same time, the aim is to prevent the adversary from gathering information or to feed desired information to the adversary.[366] As a rule, gathering intelligence is easier in open national networks than in the internet segment, but the encryption included in the latter also generates suspicion and uncertainty among potential opponents and increases their surveillance efforts. The increase in the intensity of surveillance can be interpreted as provocation. Intense monitoring and control of one's own information environment may lead to the observations and interpretations made of it becoming distorted. The fears of authoritarian state leaders and mirror imaging may lead to false assessments.[367] False and erroneous interpretations may lead to early warning failures or to other erroneous actions.

Diverse information operations[368] are part of conflict prevention, and cyberspace serves as a tool and platform for them. The information security and defence system prevents threats by monitoring its own state, intervening in its free use and supporting counter operations. The emergence of internal unrest is prevented when groups arising from civil society and/or their external supporters cannot communicate, network and mobilise themselves freely. No information that would justify external intervention in the internal affairs of the state is transmitted to the outside. The integrity and resilience of one's own nation is strengthened by promoting patriotism and nationalism and by denying any alternative value systems. Divergent opinions are pushed to the margins and, in extreme situations, suppressed by violence. The use of free information environment is denied from potential threats. However, the national information environment is not completely closed. The system must have a 'pressure valve'[369] so that dissidence would not lead to a revolution. From the point of view of surveillance, some freedom must be allowed in the information space to make it possible to track the 'enemies of the state'.

Active measures are aimed at shaping the global cyber and information space and turning it from a hostile space to even a favourable one. The methods are based on diplomacy, espionage, manipulation, dissemination of false information and deception.[370] However, the means employed cannot be merely hostile or concealed, but they have several directions, audiences and lines of approach.[371] For example, the Russian national segment of the internet can be offered as an example of a positive development option. The information security and defence system may become a symbol of superpower status and attract certain groups of people and states.

---

[365] Rid (2017); Valeriano & Maness (2015).
[366] Johnson, Loch K.: *Handbook of Intelligence Studies*. Routledge, London & New York, 2007.
[367] Bar-Joseph, Uri & Levy, Jack S.: Conscious Action and Intelligence Failure. *Political Science Quarterly*, Vol. 124, No. 3 (Fall 2009), pp. 461–488.
[368] On this concept cf. Sanastokeskus TSK (2018), 29.
[369] The idea of pressure valve is from Whyte & Mazanec (2019), 178–179.
[370] Cf. Rid (2020).
[371] Gioe, David V., Lovering, Richard & Pachesny, Tyler: The Soviet Legacy of Russian Active Measures: New Vodka from Old Stills? *International Journal of Intelligence and CounterIntelligence*, Vol. 33, No. 3 (2020), pp. 514–539.

In other words, the national segment of the internet is not just a means of isolation. It may strengthen a state's influence and thus prevent threats and conflicts through the force of attraction. A potential 'cyber blockade', i.e., disconnecting all internet connections from the outside, is difficult to implement or its impact will be reduced if the great power succeeds in creating its own cyber sphere of interest or even a network of trusted allies. The reverse side of creating attraction is that, due to interdependencies, the security logic of a closed network begins to erode. For example, increased technological cooperation between Russia and China may create interdependencies that may be difficult for Russia to break if it so wishes.[372] On the other hand, Russia and China challenge the control of the open global cyber and information space based on Western values and economic interests.[373] Alternative standards and technologies may change the balance of power in how the global information space is controlled, creating demand and pressure to renegotiate the rules of the cyber and information space or to form blocks with own rules.

In fact, cyber diplomacy plays at least as important a role as covert and indirect information operations. It may be used for shaping the actions, interests and values of states in a direction preferred by the party in question. Promoting information and cyber sovereignty and the norms to ban information and cyber weapons support the building of internet segments. Russia, along with China, is strongly advocating both.[374] Norms also have a preventive effect. If the world accepts the norm of cyber sovereignty in the form driven by Russia and China, and national segments of internet as a sovereign space, it will give technologically weaker states additional protection against information operations and global market forces, and allow authoritarian states to undermine human rights. At the same time, alliances based on a liberal democratic set of universal values would have to rethink their values and interests.

Cyber diplomacy is not only based on creating shared values and interests or dependencies that control the use of force. The combined effects of diplomacy and cyber and information operations that remain below the threshold of offensive, armed actions may change the approach of potential adversaries to the cyber and information space.[375] For example, Russia's cyberattacks have been responded to by developing special active cyber deterrence in which cyberattacks are responded to immediately and the perpetrators are attributed down to individuals involved.[376] To put it simply, this logic of measures and countermeasures may lead to three outcomes: deterrence works and forms a set of informal rules for accepted behaviour; deterrence acts as a mitigating factor at most and a continuous cyber conflict becomes a normalised part of great power relations; deterrence does not work, and the latent global cyber conflict

---

[372] Bendett & Kania (2019).
[373] Shahbaz, Adrian: *Freedom on the Net 2018. The Rise of Digital Authoritarianism*. Freedom House, 2019. [https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism], visited 29.12.2020.
[374] Boeders, Dennis & van den Berg, Bibi: *Governing Cyberspace: Behavior, Power, and Diplomacy*. Rowman & Littlefield, New York & London, 2020.
[375] Cf. e.g., Mazarr, Michael J.: Virtual Territorial Integrity: The Next International Norm. *Survival*, Vol. 62, No. 4 (2020), pp. 101–118; Whyte, Christopher: Beyond Tit-for-tat in Cyberspace: Political Warfare and Lateral Sources of Escalation Online. *European Journal of International Security*, Vol. 5, No. 2 (2020), pp. 195–214; Brantly, Aaron F.: Entanglement in Cyberspace: Minding the Deterrence Gap. *Democracy and Security*, Vol. 16, No. 3 (2020), pp. 210–233.
[376] Braw & Brown (2020).

escalates so that an international set of norms based on sovereignty is ultimately considered necessary.

From the perspective of the information security and defence system, conflict prevention is largely based on shaping the global cyber environment. Strategic impacts can be achieved by controlling one's own information space, building potential cyber power to maintain balance, and shaping the global cyberspace and the interests of the actors therein by using technological, economic and normative means. The national segment of the internet produces cyber power by supporting the strengthening of domestic expertise, production and infrastructure. Through such measures, the internet segment can affect the strategic balance, which is theoretically a guarantee of global stability.[377]
On the other hand, the U.S., Chinese and Russian leadership have all designated information technology capabilities as their state's source of power.[378] These capabilities cannot be any weaker than those of the rivals. It follows from this that one's own backwardness or the lead of a competing superpower is seen as a threat to peace and an existential threat to the state. When the information security and defence system functions too well, it can be perceived as a threat to the balance of power between great powers and thus lead to unintentional escalation.

It is perfectly justified to ask whether the internet segment is a disproportionate solution to the security threat stemming from the information environment? Using it for threat prevention may cause resistance and fear in potential adversaries, creating new threats.[379] On the other hand, the national segment of the internet provides a better situation picture and understanding of potential threats, which makes it possible to make efforts to influence them in advance. Whatever the case, the national segment of the internet is not a perfect cyber strategy tool for preventing threats. It is of such a nature that it requires from its builders the resources of a superpower and a certain political system to gain the advantages enabled by it.

5.2 Effectiveness of deterrence

Deterrence is in operation at the same time as conflict prevention but is based on a risk of pain instead of persuasion. Once the target has decided to openly use armed force to achieve its goals, deterrence has failed. Cyber deterrence is linked to the phases of peaceful competition, intensified competition and conflict in interstate relations, which means that the threats of espionage, terrorism, local conflicts, internal unrest, regional war and insurgency become emphasised. The means of cyber deterrence range from non-military to military but remain below the threshold of the use of open, violent, military armed force.

---

[377] Schörnig, Niklas: Neorealism. In *Theories of International Relations*. Schieder, Siegfried & Spindler, Manuela (ed.) Routledge, New York, 2015, pp. 37–55.
[378] Chekov, Alexander D., Makarycheva, Anna V., Solomentseva, Anastasia M., Suchkov, Maxim A. & Sushentsov, Andrey A.: War of the Future: A View from Russia. *Survival*, Vol. 61, No. 6 (2019), pp. 25–48; Kania, Elsa B & Costello, John: Seizing the Commanding Heights: The PLA Strategic Support Force in Chinese Military Power. *Journal of Strategic Studies*, Vol. 44, No. 2 (2021), pp. 218–264; Raska, Michael: The sixth RMA wave: Disruption in Military Affairs? *Journal of Strategic Studies*, Vol. 44, No. 4 (2020), pp. 456–479.
[379] Assuming that the theory of security dilemma is correct. (Glaser, Charles L.: The Security Dilemma Revisited. World Politics, Vol. 50, No. 1 (1997), pp. 171–201).

Structural cyber asymmetry has a significant impact on deterrence by denial, but its strength varies depending on the state of the internet segment. During peaceful competition, intensified competition and conflict, it is possible to monitor and shape the state of the internet segment and to respond to threats in a centralised and quick manner. The information security and defence system binds civilian and military actors to a cross-administrative cooperation model tasked with protecting the state from, inter alia, cyber and information threats. The model develops capabilities and engages the whole nation in combating threats. A high-quality and up-to-date cyber and information situation picture enables the attribution of attacks not crossing the threshold of military operations. The system promotes strong psychological crisis resilience as well as the will to defend the nation, and secures the control of the national information environment and its borders. All these factors increase the costs of the attackers and the uncertainty of achieving the intended objectives.

The resilience of the internet segment makes the preparation of attacks more difficult, which raises the attacker's costs and increases the uncertainty of success. Resilience may make the cost of compelling the target too high and the outcome too uncertain. The conflict becoming prolonged due to resilience may mean that the attacker's position in international politics becomes more difficult. Before an attack, the attacker must assess its own ability and willingness to prolong or escalate the conflict if the target state does not yield because of the attack. To accelerate the rate at which objectives are achieved, it may be necessary to extend the use of force to other operational domains. The attacker may not have the will or resources to do so, and it could lead to a negative reaction from the international community.

To function perfectly as part of deterrence by denial, the national information security and defence system must also extend to the other spheres of the information environment in cyberspace. The state must be able to monitor and prevent the flow of information everywhere. However, complete isolation is not a prerequisite for deterrence. It suffices that attacking becomes too costly and uncertain in relation to the objectives. Besides, there always remains some space outside the system that can be used for threatening the rulers. However, full isolation may be sought because of the uncertainties and fears decision-makers have.

Alongside controlling the information space, one of the basic arguments for building a Russian national segment of the internet is the idea of denying the technological superiority of the United States. The internet segment must prevent disconnecting the state from the internet from the outside or at least mitigate the adverse effects of it being disconnected. It must prevent hostile cyber operations and attacks on critical information infrastructure. It must protect the state from external pressure, blackmail and paralysing the leadership. The challenge is that the internet segment has value as deterrence only if potential attackers feel this way.[380] Consequently, the funds sacrificed by Russia to the national segment of the internet should in principle increase the credibility of deterrence by denial, as the major costs related to constructing a 'sovereign internet' constitute a part of communicating the level of national engagement.

[380] Mazarr, Michael J.: *Understanding Deterrence*. RAND, Santa Monica, 2018.

The implementation of deterrence by denial through the means provided by the information security and defence system requires continuous maintenance and development. The information security solutions of the internet segment must be based on the latest technology. The average age of modern operating systems in terms of major updates is a few years.[381] On the other hand, new technologies bring new vulnerabilities. The dependence of national segments of the internet on technology significantly increases the risks of cyber arms race. The arms race highlights the fact that once the system has been created, it will be difficult to give it up without exposure to significant vulnerabilities during the transition period.[382]

An attacker's chances of success on a modern battlefield are questionable if it cannot gain information superiority. Without being certain of its superiority, it may decide not to attack. Therefore, denying the use of the information sphere also affects the preconditions for using force in other operational domains. In other words, the national information security and defence system and the internet segment are tools for cross-domain deterrence.

The construction of the internet segment also affects cyber deterrence by punishment. The impacts may be such that they do not necessarily maintain a strategic balance. A closed national network only exacerbates many of the problems of deterrence by punishment. The most important factor is the increasing level of concealment. The lack of information on the properties of the internet segment reduces the credibility and predictability of the deterrence by punishment targeted against a country with such capability. This may lead to the security dilemma and a cyber arms race. In addition, the internet segment can be interpreted as a disproportionate investment in civil defence. According to the logic followed during the Cold War, civil defence lowers the threshold of the first strike when own population is relatively well protected from retaliation.[383] It is difficult to achieve a balance in deterrence if the parties are making efforts to protect themselves completely while developing ways of penetrating the other party's defences.

The national information security and defence system can provide protection, in the same way as missile defence, from behind which it is possible to make the first strike or retaliate. The system enables aggressive surveillance of open national networks through the countermeasures subsystem to achieve early warning, while it is more difficult for open network states to obtain similar information on a closed network. An open national network cannot protect its critical infrastructure in the same way as a closed one, and, in itself, it does not act as a tool of deterrence or support its implementation.[384] Since it is practically impossible to destroy the target state's retaliatory

---

[381] Camino, Alex: *The never-ending software lifecycle*. The Softtek Blog, 31.1.2014. [https://blog.softtek.com/en/the-never-ending-software-lifecycle], visited 21.2.2021.

[382] For example, Microsoft has faced significant difficulties in trying to convince users to transfer from Windows XP and 7 to newer versions even though technical support for XP and 7 has been discontinued. (Warren, Tom: Microsoft Bids Farewell to Windows 7 and the Millions of PCs That Still Run It: An End of the Traditional Windows Era. *The Verge*, 14.1.2020. [https://www.theverge.com/2020/1/14/21065122/microsoft-windows-7-end-of-support-lifecycle-millions-pcs], visited 5.1.2021).

[383] Geist, Edward M.: *Armageddon Insurance. Civil Defense in the United States and Soviet Union, 1945-1991*. University of Northern Carolina Press, Chapel Hill, 2019.

[384] This has been understood by the U.S. and the EU cf. Cyberspace Solarium Commission (2020); European Commission: *Joint Communication to The European Parliament and the Council: The EU's Cybersecurity Strategy for the*

capacity with a first strike in cyberspace, the open network remains vulnerable to retaliation. On the other hand, the protection provided by the closed network, combined with the suitability of cyber weapons for the first strike, lowers the threshold of a closed network state to use surprise tactics.

In addition to increasing the attractiveness of a surprise attack, the internet segment may lower the threshold of using cyber weapons alongside other military capabilities as part of deterrence by punishment. Cyber weapons can be used to compensate for weaknesses in other operational domains when it is assumed that own significant targets are protected from similar impacts. The emphasised importance of information superiority in modern warfare may reinforce this kind of thinking. Closing the internet segment may protect the networks and C2 systems of the state's own armed forces, in which case the kinetic forms of deterrence by punishment are better protected and the credibility of their capabilities is higher.

To reduce the risk of first strike and horizontal escalation, deterrence by punishment may be reinforced by sending a message that any attacks against critical information infrastructure or the whole information security and defence system will be defined as crossing the threshold warranting a response with conventional or nuclear weapons.[385] However, it is highly questionable whether the great powers engaged in a mutual conflict that threatens to escalate into a war would refrain from using the opportunity to paralyse the adversary's C2 systems. Therefore, in Russia, cyber weapons have often been compared to strategic nuclear weapons, and the arguments used in cyber diplomacy are similar to those used in nuclear disarmament negotiations.[386] The objective of the Russian cyber diplomacy aimed at limiting cyberattack capabilities is therefore to shift the strategic balance in favour of Russia.

The ability to threaten the data traffic of rivals, for example, by disconnecting the global internet connections in undersea cables, destroying telecommunications satellites or carrying out massive denial of service attacks, can also be considered part of deterrence by punishment. The deterrence calculations may be affected by the fact that these attacks have a short-term impact and can also cause harm to the party using such means. Furthermore, a country that closes its internet segment can produce malware from which its own systems are protected. It may make it known that it has permanently deployed offensive cyber forces outside its borders. Structural cyber asymmetry thus increases the credibility of deterrence by punishment, as the country closing its network has an undeniable ability to strike back while its own valuable targets are, in relative terms, better protected than those of open network states.

Digital Decade. Brussels, 16.12.2020 JOIN(2020) 18 final. [https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade], visited 18.12.2020.

[385] This policy has been already partly implemented cf. Указ-355: Указ Президента РФ от 2.6.2019 N 355 "Об основах государственной политика Российской Федерации в области ядерного сдерживания". [http://www.kremlin.ru/acts/bank/45562], visited 30.12.2020; The United States Department of Defense (U.S. DoD): *Cyber Strategy – Summary, 2018*. [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF], visited 5.5.2020.

[386] Compare for example Arbatov & Dvorkin (2013); 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, с. 11–17; Комов, С.А. (под общ. редакцией). *Международная информационная безопасность: дипломатия мира*. Сборник статей. Военинформ, Москва, 2009.

In theory, the balance of deterrence should be based on mutual vulnerability to retaliation, i.e. *'Mutually Assured Destruction'* (MAD), but, in practice, no one believed in this set-up even during the Cold War.[387] In other words, when updated to the cyber environment, the *Mutually Assured Disruption* may not work. This would require that all countries keep their networks relatively open and vulnerable. If implemented, the Russian national segment of the internet would break this logic. If one party is able to limit or prevent even normal, i.e., acceptable, cyber espionage and preparation of operations, the other parties should extend their operations to other operational domains. In other words, horizontal escalation would take place. However, espionage and preparations made in other operational domains may be more prone to escalation than cyber operations, which may lead to unintentional vertical escalation. The balance of deterrence by punishment could only be achieved if all countries were to build a national segment of the internet.

Deterrence by punishment is considered to require firm attribution.[388] The national information security and defence system can contribute to attribution up to a certain point. However, it does not facilitate the attribution of attacks from outside the national segment of the internet and, in fact, hampers international information gathering and sharing.[389] It should also be noted that the technological ability for attribution alone is not sufficient for implementing deterrence by punishment, as it may be impossible to determine who actually commissioned the cyberattack. In authoritarian states, the lack of parliamentary or judicial supervision makes it easier to implement deterrence by punishment.[390] The speed of the process does not, of course, guarantee its accuracy and correctness, as authoritarian regimes are at least as prone to distorted thinking in intelligence services and among decision-makers as democratic administrations.[391] It would facilitate attribution if the whole internet were changed to support the protocol standards driven by China by which packet traffic could be made traceable. This would obliterate anonymity in all internet traffic.[392] On the other hand, attribution as a means of communicating deterrence is not necessarily as important to actors operating in the authoritarian grey zone as it has been to the West.[393] This has caused frustration in the West, and David Blagden, among others, has suggested that instead of attributing the actor, we should only identify the interests behind the attack and thus threaten these interests with retaliation.[394]

---

[387] Green, Brendan R. & Long, Austin: The MAD Who Wasn't There: Soviet Reactions to the Late Cold War Nuclear Balance. *Security Studies*, Vol. 26, No. 4 (2017), pp. 606–641.
[388] Brantly (2020).
[389] Goel, Sanjay: How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race. *Connections*, Vol. 19, No. 1 (Winter 2020), pp. 87–95.
[390] Kilcullen (2020), 152–153.
[391] Honig, Or Arthur & Zimskind, Sarah: Not Completely Blind: What Dictators Do to Improve Their Reading of the World. *Comparative Strategy*, Vol. 36, No. 3 (2017), pp. 241–256.
[392] Durand, Alain: *New IP. ICANN Office of the Chief Technology Officer, 27 October 2020.* [https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf], visited 6.1.2021.
[393] The United States Department of Justice: *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, May 19, 2014. [https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor], visited 30.12.2020.
[394] Blagden, David: Deterring Cyber Coercion: The Exaggerated Problem of Attribution. *Survival*, Vol. 62, No. 1 (2020), pp. 131–148.

From a Western perspective, the main reason for the failure of cyber deterrence is considered to lie in the difficulty of attribution: since the risk of getting caught is small, the temptation to use the capabilities is too high. In other words, deterrence in cyberspace cannot be based solely on the threat of the use of weapons, but it also requires active defensive action.[395] In recent years, the United States and the United Kingdom have been building their cyber deterrence basing it on pre-emptive defence, cross-domain deterrence and continuous reciprocity (Chapter 2.2).[396] The idea is that active measures modify how the target behaves and, over time, create thresholds that, if crossed, justify retaliation.[397] So far, 'active deterrence' has generated only limited impacts.[398] In addition, to the target, it may appear as a violation of state sovereignty. In fact, the information security and defence system prevents effects of 'active deterrence'. It reduces the number of relevant targets that may be affected by low-intensity counterattacks and increases the resilience of the remaining targets. The system prevents 'active deterrence' from influencing the public opinion and thus strengthens the nation's psychological resilience. The system also collects information about the attacks to assess the adversary's capabilities and, at its most effective level, the system can use its own countermeasures to steer the attackers' 'active deterrence' in the desired direction. In addition, 'active deterrence' happens to legitimise the closed national network model.

Martin Libicki has argued that by signalling the superiority of its cyber capabilities during peace, the U.S. can force its adversaries to intensify their national networks up to a point where the adversary loses the advantages provided by networking.[399] The case of the Russian national segment of the internet would appear to partially support Libicki's claim. On the other hand, if 'active deterrence' contributes to the fragmentation of the global internet, leads to a cyber arms race and maintains a latent cyber conflict and an atmosphere of fear, we could ask whether the advantage is worth the consequences? Behind the Western cyber deterrence thinking, we may even distinguish the unspoken hope of finding a new cheap instrument of deterrence by punishment.[400] However, to the opponent cyber weapons may appear as a technological threat of such a magnitude that it makes sense to build an internet segment to deny the use of force from the adversary. The Russian internet segment may well be a manifestation of the conception of deterrence by denial intended as a response to the perceived Western deterrence by punishment.

The national information security and defence system also prevents impacts of deterrence by engagement. In the case of Russia, engagement functions poorly to begin with, because its foreign policy relies on the idea of zero-sum game and the opposed

---

[395] Cf. Brantly (2020).
[396] Blagden (2020).
[397] Fischerkell, Michael P. & Harknett, Richard J.: Deterrence Is Not a Credible Strategy for Cyberspace (and What Is). *Orbis,* Vol. 61, No. 3 (2017), pp. 381–393.
[398] Valeriano, Jensen & Maness (2018), 203.
[399] Libicki (2016), 169–170.
[400] For example, nuclear deterrence was perceived in the United States and in Great Britain in the 1950s as cheaper and politically more feasible than maintaining large conventional forces against the Soviet threat. (Wheeler, N. J.: British Nuclear Weapons and Anglo-American Relations 1945-54. *International Affairs*, Vol. 62, No. 1 (Winter, 1985-1986), pp. 71–86; House, Jonathan M.: *A Military History of the Cold War 1944-1962*. University of Oklahoma Press, Norman, 2012, pp. 128, 224).

interests of the superpowers.[401] Basically, the purpose of the existence of a national information security and defence system is to break the kind of dependencies a state with a great power status cannot have. For this reason, deterrence directed against individuals (i.e., punishment) functions poorly. The objective of the national segment of the internet is to create such a parallel space and reality that the items residing within cannot be affected by external sanctions. Russia and China can recruit cyber warriors by appealing to patriotism, status in a closed community and economic benefits.[402] In fact, the information security and defence system is in some cases even more effective internal deterrent against individuals than the techniques of personal sanctions, and naming and shaming. With the help of some suitably selected examples, it is possible to make dissidents, revolutionaries and terrorists reassess the risks of their actions.

The national information security and defence system shapes cyberspace and cyber environment and affects deterrence by denial or punishment. For this reason, in Western military thinking, consideration should be given to disconnecting the concept of *shaping* the battlespace from studying the operative level alone.[403] The use of cyber power shapes the preconditions for the use of force on a strategic level, which can be seen when examining the cost/benefit and probability calculations of the deterrence theory through the relationship between the internet segment and open national networks. It can, therefore, be argued that closing the national segment of the internet is part of a cyber strategy in which punishment, denial and defence are integrated. The national segment of the internet is an instrument of deterrence by its very existence. Disconnecting it from the global internet can strengthen the credibility of communicating deterrence by punishment, as it can make it possible for a part of the nation to survive a total war while the information society of an open network state is destroyed. However, the Western deterrence theory does not fully explain the nature of the national segment. According to Joss Meakins, the Russians are critical of the effectiveness of cyber deterrence by punishment. The Russians perceive cyber weapons as offensive fist-strike weapons and fear that their development will undermine nuclear stability, which is the basis of their great power status.[404] A special Russian element of deterrence is that cyber means are considered a part of broader strategic deterrence.[405] In fact, the national segment of the internet is intended not only for the purposes of prevention and deterrence, but also for controlling the information space and winning conflicts. By its nature, it is active and engages the whole state administration and security system. Despite the different perspectives, Russian and Western cyber security thinking approach each other in the sense that cyber deterrence is considered the business of the whole public administration and nation.[406]

---

[401] Brantly (2020), 228–229.
[402] Cf. Braw & Brown (2020).
[403] U.S. DoD JP 3-0 (2018), II-7.
[404] Meakins, Joss: *Living in (Digital) Denial: Russia's Approach to Cyber Deterrence*. Euro-Atlantic Security Report. European Leadership Network, 2018. [https://www.europeanleadershipnetwork.org/report/living-in-digital-denial-russias-approach-to-cyber-deterrence/], visited 29.4.2020.
[405] Forsström, Pentti: *Venäjän sotilasstrategia muutoksessa: tulkintoja Venäjän sotilasstrategian perusteiden kehityksestä Neuvostoliiton hajoamisen jälkeen*. Doctoral thesis, Maanpuolustuskorkeakoulu, Julkaisusarja 1 Nro 32, Helsinki, 2019; Kukkola (2020a); Bruusgaard (2022).
[406] Kukkola (2020a); Wilner (2020).

An open national network has effects deriving from its own properties on the deterrence relationship between closed and open national network states. From the perspective of an open national network state, when a crisis becomes more tense, it makes cyber deterrence less likely to succeed, as the costs of protecting an open network and attacking a closed one increase and the chances of success decrease when the conflict progresses. It is therefore difficult for an open network state to maintain a credible deterrence in relation to a state with an internet segment. Since structural cyber asymmetry increases when an internet segment is closed down, to an open network state making a pre-emptive or first strike appears as a more rational solution from the perspective of costs and probability than waiting. How sensible it is to make the first strike depends on whether the open network state believes that it is threatened and on how it evaluates its own objectives.

In interstate relations, the logic of the first cyber strike is linked to other operational domains and forms of use of force. Due to the temporary nature and uncertainty of the impacts of a cyberattack, the first strike must be combined with other forms of compellence if there are any suspicions that the cyber use of force will not cause the desired impact. In other words, the deterrence provided by the national information security and defence system can have an unintended vertical and horizontal escalating effect. An open network state may find it necessary to make the first strike in several operational domains solely based on the observed disconnection of the national segment of the internet. The disconnection could be interpreted as preparing for a surprise first strike. On the other hand, if interpreted wrongly, it could also be seen as a signal of preparing a first strike. Protecting one's important targets or first-strike capacity could be considered preparing for a surprise attack.

The fears of open national network states are not the only source of potential unintentional escalation. An internet segment state may trust the capabilities of its information security and defence system too much. In such a case, the defender may end up taking excessive risks in other operational domains, believing in the deterrent impact of the internet segment. It will complicate matters even more if neither of the parties believes in the other party's capabilities, and disbelief is combined with uncertainty.

Based on the above, it can be concluded that if the Russian national segment of the internet fails to build an instrument of deterrence by denial that is credible in the eyes of a potential opponent, it is a futile and potentially harmful project. Firstly, the internet segment is very bad at communicating who is the designated potential opponent. Secondly, it can increase the fears on the opponent's side without providing real protection. Thirdly, defence being perceived as strong may lead to false sense of security, a desire or a 'need' to use military force before a potential opponent does so. The factors listed above increase the instability of the global cyber environment.

Finally, when assessing the effectiveness of deterrence, we need to take account of the subjectivity of considering the cost it threatens to cause. The party building an internet segment cannot determine how a potential attacker evaluates the benefits and costs caused by the attack. On the other hand, the attacker may not be able to assess what kind of damage to, say, critical information systems cross the threshold that the leaders of the target country consider a sign of failure of the deterrence constituted

by the internet segment. This may lead to executing a retaliatory strike in such a way and in such an operational domain that the attacker could not have expected.

5.3 Conflict escalation control

Managing the escalation of a conflict in a cyber environment means regulating the intensity of a conflict that has started by threat or use of cyber force in or through cyberspace. In interstate relations, escalation control is related to the phases of conflict, the initial period of war and war, in which case the prevailing threat scenarios are a regional war, uprising and a great power war. The initial period of war and war proper can significantly change all dimensions of a state's strategic operating environment. With regard to the internet segment and open national networks, it should be noted that the various operational domains are intertwined in ways that can cause unpredictable spillover effects and repercussions. In other words, in the cyber environment escalation control is related not only to the use of coercive force but also to controlling unintentional and accidental escalation.

Escalation management has been considered to be difficult in the cyber domain due to its properties. The risk of escalation is increased by differences in the balance of power between operational domains, poor situational awareness and understanding among decision-makers, and new technologies affecting the order of the rungs on the escalation ladder.[407] According to Ben Buchanan, the security dilemma requires states to penetrate into each other's networks to assure their own defence, making it difficult to separate efforts to reconnoitre from preparing a counterattack, which creates pressure to take countermeasures.[408] On the other hand, Fischerkeller and Harknett have argued that due to the nature of the cyber environment, competition using cyber operations, the rules of which are known to the parties involved, can help avoid escalation.[409] The decisive factor in escalation in the cyber environment, as in any other domain, is ultimately the interpretations decision-makers make on the opponent's intentions.

During war, structural cyber asymmetry reaches its full extent as the internet segment is disconnected and, in an extreme case, divided into parts in a controlled manner, while an open national network turns from a supervised system into a fragmented one. An open network may largely lose its functional capacity and external connections, while a closed network can provide critical services at least regionally. The resilience and defence systems of the internet segment prevent attacks and mitigate their consequences, and the target is punished with counterattacks executed from outside the closed network. During conflict and war, the national information security and defence system secures flexible regulation of the national information space and its

---

[407] Fitzsimmons, Michael: The False Allure of Escalation Dominance. *War on the Rocks*, November 16, 2017 [https://warontherocks.com/2017/11/false-allure-escalation-dominance/], visited 27.11.2020; Healey, Jason & Jervis, Robert: The Escalation Inversion and Other Oddities of Situational Cyber Stability. *Texas National Security Review*, Vol. 3, No. 4 (Fall 2020), pp. 30–53.
[408] Nye, Joseph S. Jr.: *ISSF Roundtable 10-6 on The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Discussion published by George Fujii on Friday, January 19, 2018. [https://networks.h-net.org/node/1252924/pdf], visited 23.11.2020.
[409] Fischerkell & Harknett (2017); Fischerkeller & Harknett (2019).

borders, neutralisation of internal information threats, restriction of external information threats, technological and mental resilience, protection of strategic capabilities and influencing the opponent's information domain with first-strike and secondary-strike capabilities. Escalation control is implemented in a situation where the national information security and defence system provides maximum freedom of action and the widest range of optional actions.

When examining the impact of structural cyber asymmetry on escalation control, we should first distinguish between long-term and short-term impacts. Secondly, we must make a distinction between the pursuit of escalation dominance and controlling the unintended consequences. Here, the long term means several years during which parties to a potential conflict seek to maintain a strategic balance or to gain an advantage by developing new offensive and defensive instruments and methods. When examined from this point of view, Russia's national segment of the internet can be seen as a response to the creation of U.S. cyber forces and cyber operations, which have been further accelerated by the adoption of the *persistent engagement* doctrine.[410] Similarly, the *Clean Network* programme introduced by the United States in summer 2020 is a response to the cyberattacks and espionage by China and Russia.[411] In other words, the long time span of escalation control is linked to the great power competition and its most prominent manifestation is the arms race, which, due to a momentarily perceived advantage or existential threat, may unintentionally and accidentally escalate into a conflict. In the context of cyber environment, technological development plays an emphasised role in the balance of power assessments of great powers. A new technology may enable escalation dominance for one party, which in turn creates insecurity in potential adversaries and increases the possibility of unintentional escalation.

The short-term effects of structural cyber asymmetry are related to changes in networks in the context of a conflict over months, weeks and days. In certain cases, it may be a question of minutes, seconds or even less than a second if the systems are automated to an adequate level. The use of the internet segment as a tool of escalation dominance is based on the ability to threaten the opponent from behind a shield, already detected when examining deterrence above. This shield and the attacks made from behind and outside the shield can be activated gradually, in part or at once, quickly and extensively. On the other hand, automation and the short time span can serve as a source of unintentional escalation.

Regulating the borders of the national segment of the internet has the most immediate and visible impact on the nature of the conflict. The regulation is of cross-domain nature, since, through cyberspace, it is reflected in all operational domains dependent on the services provided in the sphere. It can be used for trying to prevent a threat or to avoid loss in an acute situation. Closing the network will have spillover effects on global network traffic and all foreign companies operating within the state borders. If the closure extends into the electromagnetic sphere and space, the impacts are one

---

[410] Klimburg (2020).

[411] The United States Department of State: *Announcing the Expansion of the Clean Network to Safeguard America's Assets*. A Press Statement Michael R. Pompeo, Secretary of State August 5, 2020. [https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/], visited 1.1.2021.

order of magnitude bigger. It should be noted that these impacts are of a short duration. Data traffic is rerouted, and, after the initial chaos, the impacts may turn against the state that closed its network or lead to accidental escalation due to spillover effects.

Closing the internet segment changes the nature of the conflict and serves as a means of communication. A country that has closed its national segment demonstrates its ability and readiness to suffer financial and other consequences, or even to blackmail foreign actors dependent on its own information domain. It forces the adversary to make the next move either by protecting itself, by demonstrating the weaknesses of the closed network, that is, by attacking, or by mitigating the conflict. It is totally possible that the next step of the conflict is taken in another operational domain. Shaping cyberspace cannot be distinguished from a wider interstate conflict, since, with a view to successfully gaining escalation dominance, it is of great importance what the balance of power is like between the opponents in other operational domains.

The technological and mental resilience reinforced by the national information security and defence system also contributes to escalation dominance. Resilience constitutes the threshold for the use of force already during peace. It shapes the national critical information infrastructure and the will of citizens and state leadership in a more resilient direction compared to open national network states and their inhabitants. The attacker must use greater force, new methods or morally questionable means to be able to attack the state operating an information security and defence system. This means that it must be prepared to escalate the conflict to a higher level.

The monitoring and control systems of the information security and defence system are also a tool of escalation dominance. They can intervene in the development of internal threats and prevent them and collect information on cyber and information attacks made from the outside and on external support received by internal actors. The attacker is forced to increase and expand its support to the internal actors as control systems help to weaken the internal threat. In other words, the attacker must escalate if it wants to achieve its objectives. A state operating an information security and defence system can use the accumulated evidence for attribution and on its basis, in turn, escalate the conflict into other operational domains, and in a manner that appears justified in the eyes of the international community. The attacker will have to consider at what stage it will renounce its support to the insurgents or whether it wants to continue escalating the conflict into a direct interstate struggle.

Once the internet segment is disconnected, the countermeasures system enables the first strike and secondary strike. A closed network state may attack against the adversary's critical information infrastructure or more limited targets using cyber operations during the initial period of war. Cyberattacks can be used for gaining an advantage of surprise or to show force and raise the threshold of escalation. In the first case, the intention is to exploit structural cyber asymmetry to win a war, and it will be discussed in the next chapter. In the latter case, the target of the first strike must decide whether it escalates the conflict, in which operational domain and by what means. The adversary may need to escalate by using conventional forces or nuclear weapons, which would significantly increase the intensity of the conflict. It can also, naturally, respond

with non-military measures, such as sanctions, or détente. If the target of the first strike is an open network state, non-military reactions do not eliminate the vulnerabilities of the state network and the threat of a new attack.

Disconnecting the internet segment does not necessarily mean increasing the intensity or extent of the conflict. The ability to refrain from escalation or tolerate escalating actions by the opponent is also part of escalation dominance. The internet segment can deny the attacker access to the cyber environment, which means that it must decide whether to continue escalating the situation in another operational domain. The adversary's actions in the cyber environment not crossing the threshold of deterrence by punishment during the grey zone phase, i.e., '*salami tactics*'[412], become more difficult as the operating space narrows. On the other hand, it is also possible for the attacker to persuade the target to disconnect its network by gradually increasing the intensity of its attacks. Disconnecting the internet segment may cause costs that force the closed network state to change its behaviour.

Disconnecting the internet segment is not an ambiguous measure in itself. In addition, defensive actions in cyberspace are not as ambiguous as the adversary's cyber operations targeted against the networks, the purpose of which may be espionage, reconnaissance, preparing an attack or an actual attack.[413] However, ambiguity and uncertainty may be linked to the reasons why the national network is disconnected. It may be unclear to the potential adversary whether the network is disconnected with an intention to prepare for war or to secure internal security. Disconnecting the network can be considered as preparing for a first strike using some kind of a cyber weapon with global impact. Disconnecting the internet segment and closing the information space may deteriorate communication between the parties and increase the possibility of misunderstandings. In addition, disconnecting the national network may affect third parties, such as multinational companies, which may take measures to protect their own interests. In the worst case, their interests and actions may lead to unintentional escalation.

As the norm of cyber sovereignty develops and is more firmly integrated into the critical information infrastructure, the threshold of escalation of cyberattacks changes. At present, it is difficult to know in advance what kind of a cyberattack Russia, for example, would consider state-to-state armed use of force.[414] The internet segment links many systems and services run by private operators to the government in a manner that differs from that of open networks states. For example, an espionage operation targeting an energy or military complex may lead to unintentional escalation. What could be interpreted as a private sector cybersecurity issue in the West may be interpreted as a national security issue in Russia.

---

[412] Schelling (2008), 67–69; Wirtz, J. J.: Life in the "Gray Zone": Observations for contemporary strategists. *Defense & Security Analysis*, Vol. 33, No. 2 (2017), pp. 106–114, 107.
[413] Valeriano, Jensen & Maness (2018), 31.
[414] Some information can be gained from a list of critical information infrastructure published by the Russian government (ПП-127a: Постановление Правительства РФ от 8 февраля 2018 г. N. 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.) [http://pravo.gov.ru/proxy/ips/?docbody=&nd=102460750], visited 22.2.2021).

For the internet segment, the risk of accidental escalation is increased by the interdependencies between the subsystems of the information security and defence system. For example, malware can spread uncontrollably in centralised management systems and networks. Hacking attempts made with intention of spying may end up having an impact on systems critical to national security. If the management of the internet segment is subordinated to artificial intelligence, decision-making will move to machine speed. How to avoid accidental escalation when people rely on opaque decisions made by machines that can be manipulated?[415] In the worst-case scenario, an attack in the cyber environment causes an automatic response in another domain. In other words, centralised decision-making and speed, which appear as strengths of a closed networks, can turn into a risk factor.

In the case of military networks and systems, the relationship between the national segment of the internet and unintentional or accidental escalation depends on the level of integration between civilian and military networks. Since, as a rule, the C2 systems of the Armed Forces are separated from civilian networks, attacks on the national segment of the internet do not automatically threaten the cyber or nuclear capabilities of the state. In reality, any efforts to integrate the security sectors of both internet segment states and open network states create connections between the armed forces and the networks of civilian actors. As the dual use of technologies increases, more and more connections will open between the armed forces and the civilian industry. Risk factors of unintentional or accidental escalation include cyber vulnerabilities in the great powers' strategic air and missile defence systems; transport systems affecting the transfer of troops; and, in particular, the C2 systems of strategic early warning systems and strategic nuclear weapons.[416]

On the other hand, if the internet segment is disconnected, military systems may suffer unexpected harm. Even controlled fragmentation of the internet segment hampers the transfer of updates, configuration changes, encryption keys and certificates from industry to the Armed Forces; the sharing of the cyber situation picture; cooperation with civil authorities; and the command of troops deployed abroad. The escalation risk increases as the Armed Forces have to rely on poor C2 connections and unclear situation picture. Russia has tried to reduce the risk by setting up a national defensive C2 centre, but what will happen if this centre suddenly disappears from the network, even for a little while?

Escalation control is a challenging part of cyber strategy when used as a means for gaining an advantage or for risk management. The internet segment shapes the cyber environment and affects other operational domains, but the factors causing friction may be unpredictable. If many different weapon systems (cyber, conventional, special ops, nuclear weapons) are used to achieve the same effect while the operating environments keep changing, the escalation ladders or thresholds related to the use of technology become blurred. The attacker may not understand how important some targets are for the defender or how harmful the defender considers the various attacks to be. For example, certain parts of the critical information infrastructure may have

---

[415] Johnson, James: Delegating Strategic Decision-making to Machines: Dr. Strangelove Redux? *Journal of Strategic Studies*, Vol. 45, No. 3, pp. 439–477.
[416] Cimbala (2017); Acton (2018).

unpredictable but significant value for the defender, and thus the conflict may escalate unintentionally.[417]

Finally, we can conclude that the functioning of the information security and defence system requires cooperation, coordination and synchronisation between several national actors. Due to the centralised management, an individual entity can make decisions concerning the information space of the whole state, which may have unknown consequences. This does not remove the fact that the internet segment is an effective tool for seeking information superiority and thus escalation dominance. It is a fortress from behind which one can either threaten the adversary on its own territory or force the adversary to expand and accelerate the conflict if it wants to take over the fortress.

5.4 Military exploitation of asymmetry

In interstate relations, military exploitation of structural cyber asymmetry is related to the phases of conflict, initial period of war and war, in which the prevailing threat scenarios include a regional war, uprising and a great power war. In conflict and war, all non-military and military open and covert means and methods are in use. All dimensions of the state's strategic operating environment interact with each other and can change rapidly. The national information security and defence system secures the control of the national information environment, the defender's freedom of action and the denial of the adversary's freedom of action. In addition, it supports cyberattacks against the adversary's systems, military action in other operational domains and contributes to the nation's survival if the war escalates into a total war.

The military exploitation of the structural cyber asymmetry is based on the scientific-technological basis previously created by the information security and defence system; technological and mental resilience; situational awareness, monitoring and management systems; and active measures capabilities. The national cyber battlefield can be shaped by the defender, and the internet segment can be disconnected from the global internet and divided into parts in a controlled manner. Even if disconnected from the outside, the internet segment can continue its operation. Control of the information environment maintains psychological resilience even if critical services in society suffer damage.

Disconnecting the internet segment is a necessary condition for structural cyber asymmetry, but not sufficient in itself. Military exploitation requires the ability to use force for compelling the adversary. Disconnecting the internet segment will only act as a means of compelling the adversary if the adversary is unable to protect itself in the same or adequate manner. Compared to the internet segment, open networks are likely to be stovepiped and fragmented in a state of war. Coordinated national defence measures are slow, if even possible in the first place. Technological and mental resilience are dependent on the commercial factors of the private sector, and the strength and value base of the political system. For example, if networks and systems are not

---

[417] On the problems of the concept of escalation ladder cf. Paret (1990), 764–766; McDermott, Basil W.: Thinking about Herman Kahn. *The Journal of Conflict Resolution*, Vol. 15, No. 1 (Mar., 1971), pp. 55–70.

duplicated according to good practices or services are centralised into the same physical and logical systems for competitive reasons, resilience is poor. An open national network can be temporarily paralysed, broken to parts and possibly isolated by means of extensive cyber and kinetic attacks on pre-localised critical points. The network can also become fragmented by itself as various actors try to protect their own systems. On the other hand, parts of the open network can continue to operate relatively normally.

The balance of power between the internet segment and open national networks is primarily affected by how the situation picture is shared and, thus, how the understanding of the situation is formed during the initial period of war; the ability to operate in one's own and the adversary's networks; the unity of command and control; the speed and timing of measures; and the ability of the networks (and the nation) to withstand and recover from attacks. Centralised control, collecting information to a single point and restricting connections are the foundation of the information security and defence system, but also its vulnerability. A determined attacker may target its attack against the control system, and once it is inside the system, its cost for further action drop, and the credibility of information security and defence collapses.[418] It further intensifies the threat when, at the time war is declared at the latest, open network states lift the legal and political restrictions on the countermeasures system and engage in closer international cooperation that provides a better situation picture and technological support. It is likely that the restrictions are lifted for some time before any formal and public decisions are taken.

Disconnecting the national segment of the internet is used for shaping the cyber battlefield. This will not change the vulnerabilities of individual systems or networks, but modifications made at the national level may contribute to deceiving, slowing down and repelling the attacker. At best, the internet segment may prevent making of unprepared attacks, make it difficult to execute some prepared attacks, and reduce the attack surface and targets for strikes. It increases the amount of resources the attacker needs for reconnaissance and preparation, and generates uncertainty about how the prepared attacks will work. Denying the use of the cyber environment makes it difficult to assess the impact of attacks carried out in all operational domains, especially if the use of space and the free electromagnetic spectrum is also denied.

Tightening the control and disconnecting the internet segment can be conducted territorially and flexibly. This is an essential feature when controlling an armed uprising or a local conflict. Internal security threats require more sensitive control from the perspective of the legitimacy of state leadership. Full closure of the internet segment can be an effective response to the measures of state actors using indirect and non-military means when a conflict is becoming more tense, but, if the situation gets prolonged, there is a risk of financial difficulties. During the initial period of war and war, full closure of the internet segment and the entire information environment offers a defensive advantage against both internal and external cyber and information attacks. Once the attacker's opportunities to influence targets valued by the defender deteriorate, it becomes significantly more difficult to affect the cost-benefit calculations of a state with an internet segment by coercive use of force. In fact, the internet segment

[418] The idea of the falling costs for the attacker is from Aaron Brantly (Brantly (2020)).

serves as a kind of an element of 'information-age civil defence', denying the attacker the possibility of influencing social targets.

The nature of war has an impact on how the national information security and defence system is used. In a war against a substantially weaker adversary, it is not necessary to disconnect the internet segment unless there is fear of third parties getting involved in the war. The network may be partially closed regarding the kind of targets that might be exposed to a weaker state's attempts to strike. In addition, control can be tightened, and the focus of countermeasures placed on shaping international opinion and paralysing and isolating a weaker adversary from the rest of the world through extensive measures against localised weaknesses. In a war against a peer adversary, it makes sense to fully close the national network as early as possible. This denies an opponent with extensive capabilities the possibility of conducting information operations, preparing cyberattacks and seeking surprise.

The effects of structural cyber asymmetry differ in terms of defensive and offensive action. In defensive action, the internet segment supports the use of conventional and nuclear weapons in other operational domains. It provides indirect protection to the C2 systems of the Armed Forces and provides backup connections in the event the Armed Forces' own systems are paralysed. The more flexibly the national network structures can be shaped and its systems updated and replaced, the more difficult it is for an attacker to reconnoitre the targets of attacks or the impacts of its attacks. The more tightly the national network is closed, including space[419] and the free electromagnetic sphere, the harder it is for an outside attacker to penetrate the Armed Forces' networks. The more resilient the national information infrastructure is, the better it will recover from the impacts of, for example, a strategic strike made by using long-range precision weapons and be able to help mobilise the state's military forces to a counterattack.

An essential factor for effectively using the national information security and defence system for defensive action is that the whole entity is being trained and its interdependencies mapped and managed already during peace. The critical infrastructure and its networks must be able to operate when connections to the global internet are broken. Otherwise, disconnecting the national network would lead to a chaos and significantly deteriorate the operating conditions of the Armed Forces. The national cyber exercises launched by Russia in 2020, and the five cyber exercise areas built in 2021 partly respond to this challenge.[420]

From the point of view of defensive action, the internet segment can be seen as an enabler of attrition warfare, which gives the defender time to secure its rear and to

[419] The ability to disrupt communication and intelligence satellites over a large land mass is possible for great powers probably by the end of the 2030s. (Harrison, Todd, Johnson, Kaitlyn, Roberts, Thomas G., Way, Tyler & Young, Makena: *Space Threat Assessment 2020*. Center for Strategic & International Studies, Washington, D.C., 2020).

[420] Правительство России: Дмитрий Чернышенко: На пяти киберполигонах пройдут учения в 2021 году. *Правительство России* -webpage, 14.5.2021 [http://government.ru/news/42174/], visited 31.7.2021.

increase its strength in relation to the adversary.[421] The national segment of the internet builds the depth needed in the cyber environment, depending on which the state can establish and position its military forces. It will support the military operations throughout their duration. In other words, the control of the information environment supports the building and leveraging of the various components of the national power of the information society. This also applies to the nation's psychological strength and readiness for war. When the defender's internet segment is protected, the defender can wear down the attacker and its support area by means of, for example, cyberattacks, until it has assembled enough force for a counterattack.

In a war between the internet segment state and open national network states, offensive cyber operations may support and enable operations in other operational domains or achieve strategic objectives by themselves. According to the criticism presented in Chapter 2, the strategic effect of cyberattacks is limited because they are of limited duration and do not cause permanent damage. However, this argument should always be examined within the framework of the balance of power in any given conflict. If the parties are equally strong in all operational domains, the strategic effect of cyberattacks requires that the defender has credible deterrence in other operational domains. Otherwise, the target of the attack will retaliate or escalate in other operational domains, and the strategic effect of the cyberattack will remain partial, if it exists at all. On the other hand, if the attacking party is stronger in all operational domains, cyber operations can be used independently for compellence, since the weaker party's ability to respond by retaliation or escalation is limited. In the third case, when the strengths and the credibility of deterrence between the parties differ in terms of quality and quantity in different operational domains, the strategic effect of cyberattacks depends on factors outside the cyber balance of power. Achieving a strategic effect may require influencing other domains through cyberspace. In all cases, geography, social structure, unity and resilience, differences in technological know-how, strategic culture and systems of alliance significantly affect the impact of attacks and their interpretation. The cases described above are shown in Figure 4.

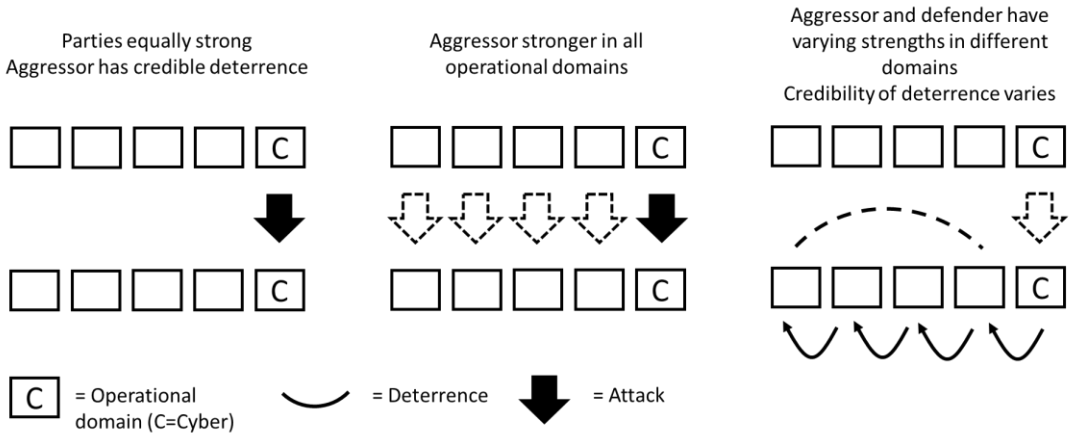

Figure 4: Strategic impact of cyberattacks on the adversary

[421] Svechin (1992), 298. Based on the views of a contemporary of Svechin A. E. Snesarev, it can be argued that the system of information security and defence prepares the state for a war the tool of which the state itself is. (Снесарев, А. Е. & Керсновский, А. А.: *Философия войны*. Вече, Москва, 2018, pp. 291–292).

The offensive advantage provided by structural cyber asymmetry can be used as a tool of deterrence or escalation control. As a means of compellence or brute force, the advantage can be used for a surprise first strike or for supporting a second strike. A surprise first strike may paralyse some of the critical information infrastructure and C2 capabilities of an open network state and prevent it from positioning or mobilising its combat forces or receiving international assistance. The foundations of the cooperation between the authorities can be paralysed and the target country can be practically broken to pieces and isolated from the rest of the world. The will of society to defend itself can be defeated by paralysing the foundations of the information society. The cyber first strike can be targeted at an open network state from anywhere in the cyber environment, which slows down the attribution and countermeasures. The attack and its preparation can be initiated before the actual declaration of war, in which case the way in which decisions are made in open network states may lead to a slow and uncertain response to the situation.

Structural cyber asymmetry makes the idea of a first strike or even a pre-emptive strike attractive. It minimizes the attacker's own costs, as it may have developed the cyber weapons in advance to exploit the weaknesses of open networks, and its own targets are at least partially protected once the internet segment has been disconnected. Asymmetry maximises the likelihood of success, since open network states will only start protecting their systems more effectively once the war has begun or under an immediate threat. The internet segment, on the other hand, minimizes the possibility of an open network state succeeding in its countermeasures. Even if cyberattacks were not used, disconnecting the internet segment supports the denial of information operations. The information environment of open networks can be employed to support the use of coercive and brute force in other operational domains while keeping own space under control. If the idea that cyberattacks are at their most dangerous as a means of either first strike or information operations is correct, then, from a military strategic perspective, it makes sense to disconnect the internet segment early on.

Structural cyber asymmetry also gives significance for depth as part of an attack. When attacking an open national network, the depth of the battlefield starts at the border of the internet segment. Attacks can be targeted to critical communication nodes and connections located outside the target state. In the same way, attacks can be targeted against financial, logistical and energy production systems in the whole depth of the battlefield, in the depth of all the interdependencies of the open network. The attacker can try to isolate the target country from the outside world by means of combined cyber, space, kinetic and electronic warfare operations. This is possible particularly if the target is geographically near the attacker, has a relatively small surface area, is bordered by bodies of water and poorly networked. The attacks can be targeted against an open network state's ability to project force beyond its borders. Strikes against its armed forces can be made anywhere in the world, including space. Cyberattacks can be used to support information operations against target audiences outside the open network state. Information operations can be echoed across the internet and reinforced, as open networks do not prevent the spread of information.

Structural cyber asymmetry affects not only the depth but also the nature of attacks. The internet segment's domestic software and hardware technology that differs from that of the adversary enables cyberattacks against open networks using malicious code

that is highly contagious and exploits general vulnerabilities. This is kind of a 'biological weapon' in cyberspace against which the internet segment' own software and hardware have been vaccinated. On the other hand, the national segment of the internet may be highly vulnerable to a similar attack. It may happen that if the global internet fragments into national sections, weapons targeted against ecosystems will be developed, and the threshold of using them will become lower as interdependence decreases.

Based on the above, it is clear that successful targeting of cyberattacks is of great importance for the impact of the attacks. Cyberattacks can therefore follow the *Single Integrated Operation Plan* (SIOP)[422], derived from nuclear weapons, which makes it easier to integrate the attacks into various conflict and war scenarios and their objectives. The SIOP can serve as a tool of deterrence during peace or as a tool of compellence and brute force during war.[423] In the context of structural cyber asymmetry, SIOPs can support compellence when attacking open networks in a first-strike style, but their benefits in attacking internet segments are limited. The defender can change the structure of its networks, patch up vulnerabilities and limit target and impact reconnaissance to such an extent that SIOPs can only be of a very general nature.

The military networks and systems of the information security and defence system are a special case of military exploitation of structural cyber asymmetry. Strategic weapon and C2 systems are vulnerable to anti-satellite weapons, long-range precision weapons and cyberattacks. Systems are often dispersed across a wide geographical area. For this reason, they offer a large number of targets and attack vectors for cyberattacks. The C2 systems of conventional and nuclear weapons becoming digitalised and intertwined, and the dual use of civilian and military infrastructure increase vulnerabilities.[424] In the case of Russia, for example, the size of the country means that strategic C2 systems have been dispersed across a wide area. Satellite communications are critical for certain regions. Other regions, on the other hand, rely on long fixed connections following the railway lines, along which there are unprotected link stations and other connection points. Sea cables play an important role, especially in the Far East. There are several attack vectors, and closing the internet segment does not disconnect them all. In addition, closing the national networks may have an impact on the missile and air defence systems of the Russian Armed Forces deployed abroad. During war, even strategic joint command echelons may run into difficulties if the networks of local government, security authorities and the federation get fragmented in a way that does not respect the joint command's spheres of responsibility or concept of operations. Here, the purpose of observations made on Russia is to show that the armed forces must be integrated into the national information security

---

[422] On the concept of SIOP cf. Kristensen, Hans M.: *Obama and the Nuclear War Plan. Federation of the American Scientists Issue Brief, February, 2010.* [https://fas.org/programs/ssp/nukes/publications1/WarPlanIssueBrief2010.pdf], visited 4.1.2021.

[423] On the application of SIOP to cyber weapons cf. Long, Austin: A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning. *Journal of Cybersecurity*, Vol. 3, No. 1 (2017), pp. 19–28.

[424] Cimbala (2017), 501; Futter, Andrew: War Games Redux? Cyberthreats, US–Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control. *European Security*, Vol. 25, No. 2 (2016), pp. 163–180; Аксенов, С.В.: Обеспечение устойчивости группировки стратегических ядерных сил в условиях информационного противоборства. *Вестник академии военных наук*, № 2 (67) (2019), с. 66–68.

and defence system if the country does not want to build a system that is a critical weakness instead of a source of power.

Technological advances have a decisive impact on the development of internet segments and thus on the military exploitation of structural cyber asymmetry. The development of artificial intelligence combined with an event database gathered from the internet segment speeds up decision-making and provides better protection against cyber threats.[425] By integrating artificial intelligence, big data and psychology, it is possible to predict events in the cyber battlefield with a certain likelihood and to help steer the societal information environment.[426] The use of AI and advanced simulations when calculating the correlation of forces makes it possible to integrate the characteristics of the national segment of the internet into cyber power calculations, which may provide a significant advantage.[427] If a state with an internet segment succeeds in developing a generic AI (AGI), it will have a completely new kind of an advantage in both attack and defence.[428] Furthermore, the closed and self-sufficient nature of the internet segment may make it difficult to obtain the data needed for developing an offensive AI against it. There are risks involved in developing AI for strategic purposes. AI may regulate the internet segment in a way that interferes with military operations in other operational domains, or it can be manipulated, or people may rely too much on it.[429]

Since AI is a new technology, the ways in which it is used by states are likely to differ in the early stages of development. Still, the argument of Thorton and Miron, suggesting that the Russians in particular see AI as providing a momentary advantage in the great power competition and are inclined to exploit this advantage, is questionable.[430] The U.S. Government's National Security Commission on Artificial Intelligence has already recommended the introduction of offensive AI.[431] It is quite likely that all great powers and regionally leading countries are developing offensive AI applications for a wide range of purposes. Due to the heritage of cybernetics, Russia will probably try to develop AI not only in the field of attack methods, but for using it on the military side for decision-making support and on the economic and social side for optimising the functioning of the economic system and society, including supporting the control of the information domain.[432]

Quantum communication and encryption is another technology that affects structural cyber asymmetry. The benefits of quantum technology are related to reconnaissance

---

[425] Stevens, Tim: Knowledge in the Grey Zone: AI and Cybersecurity. *Digital War,* Vol. 1 (2020) pp. 164–170.
[426] Dear (2019).
[427] Reach, Kilambi & Cozad (2020), pp. 133; Payne, Kenneth: Artificial Intelligence: A Revolution in Strategic Affairs? *Survival*, Vol. 60, No. 5 (2018), pp. 7–32; Geist, Edward & Lohn, J. Andrew: *How Might Artificial Intelligence Affects the Risk of Nuclear War*. RAND, Santa Monica, 2019.
[428] Ayoub, Kareem & Payne, Kenneth: Strategy in the Age of Artificial Intelligence, *Journal of Strategic Studies*, Vol. 39, No. 5-6 (2016), pp. 793–819.
[429] Fitzpatrick, Mark: Artificial Intelligence and Nuclear Command and Control. *Survival*, Vol.61, No.3 (2019), pp. 81–92; Johnson (2020).
[430] The ideas of Thorton and Miron display a tendency to mirror-imagining more than a genuine understanding of Russian strategic culture which emphasises cunningness, creativity, and surprise (Thornton & Miron (2020)).
[431] National Security Commission on Artificial Intelligence: *Final Report*, 2021. [https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf], visited 6.3.2021.
[432] Cf. Thomas (2019); Kari (2019); Kukkola (2020a).

and threat prevention rather than compellence and the use of brute force. Encrypting information or decrypting the adversary's messages provides an opportunity for surprise and an advantage on the battlefield.[433] For example, in the case of the national segment of the internet, the QKD technology already in use would enable the protection of data in circulation. However, actual quantum communications are still far too expensive to be implemented on a national scale.[434] In due course, however, it will probably become an integral part of national segments of the internet, as will mini-satellites providing broadband connections.

In order for the relationship between a closed network and an open network to create structural cyber asymmetry that can be exploited in military terms, the closed network must integrate all existing and future communications technologies into itself. Jon Lindsay has aptly stated that strategic outcomes are not determined by technology itself but by policies and social practices, such as organisational culture. They determine how new technologies are adopted and what they are used for. Moreover, state-of-the-art technology requires significant resources, and not everyone can afford the best.[435]

The military exploitation of cyber asymmetry may also have wider impacts than those concerning the belligerents. For example, relations with allies may suffer from the closure of the national segment of the internet. Defence alliances will probably be able to operate partly through connections between the armed forces, but civil society and businesses will lose their connections. The impact of the disruption will, of course, depend on the allied relationship concerned. In the case of Russia, many of its neighbouring countries depend to some extent on the Russian energy, financial and economic system, and would be in trouble if telecommunications connections were disrupted.[436] In other words, defending oneself against the use of coercive and brutal force in the cyber environment can lead to losses in other sectors. On the other hand, allies may also be of help if some of them are selected to maintain the internet segment's limited connections to the outside world. It may lead to emergence of 'transit' states or entire 'cyberblocs'. Since data networks are not the only path for transmitting data, the building of blocs should extend to space and the free electromagnetic sphere as well. In fact, the national information security and defence system can lead to formation of blocs in the information environment for essential market economic, political and military reasons. Alliance-specific and mutually exclusive divisions of resources may appear in international sets of norms and standards as regards the electromagnetic spectrum and data traffic. Efficiency requirements, incompatibility and monitoring may reduce the connections between blocs to a minimum.

---

[433] Lindsay, Jon R.: Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage. *Security Studies*, Vol. 29, No. 2 (2020), pp. 335–361.
[434] Ananthaswamy, Anil: The Quantum Internet Is Emerging, One Experiment at a Time. *Scientific American*, June 19, 2019. [https://www.scientificamerican.com/article/the-quantum-internet-is-emerging-one-experiment-at-a-time/], visited 4.1.2021.
[435] Lindsay (2020).
[436] Центральный банк российской федерации: *Внешняя торговля Российской Федерации услугами - 2019*. Статистический сборник. Банк России, Москва, 2020. [https://www.cbr.ru/statistics/macro_itm/svs/], visited 12.1.2021; Liuhto, Kari: Motivations of Russian Firms to Invest Abroad: How Do Sanctions Affect Russia's Outward Foreign Direct Investment? *Baltic Region*, Vol. 26, No. 4 (2015), pp. 4–19.

Considering all the above, it can be argued that structural cyber asymmetry supports cross-domain compellence and the use of brute force. Cyberattacks made from behind the protection provided by the internet segment and the borders secured by the armed forces, combined with the use of conventional and nuclear long-range weapons, provide the best opportunities for impact. In addition, as long as the networks of open network states are in operation, it is more advantageous for the attacker to strike against societal targets, since military targets are much more difficult to reach and paralysing them does not necessarily reduce the target's capacity to strike back in other operational domains, or lower its morale. When the adversary is an internal enemy, cyber capabilities help other security authorities destroy the enemy while it is being isolated from external support.

However, the impact of structural cyber asymmetry on defence against compellence and the use of brute force is undeniably greater than that of an attack. The internet segment can prevent both long-term efforts to destabilise a state through information and some of the effects of a strategic surprise. The national information infrastructure and its governance as well as the mental sustainability of society have been prepared for a major war. At best, the internet segment denies the adversary the opportunity of gaining information superiority, whether psychological or technological. Denial is based not only on the closure of networks, but on the operation of the whole information security and defence system. From the perspective of defence, during war, the internet segment protects the critical infrastructure and services of society; logistics systems required for economic security and security of supply; national systems intended for internal and external communications; systems needed by state leadership for decision-making and leadership; and systems needed by security authorities for the prevention of crimes, terrorism and subversive activity; and Armed Forces' systems in part.

The use of the internet segment for supporting or defending against an attack must always be set in its context. In the case of limited war, when a stronger state attacks a weaker one, a full closure of the internet segment makes no economic or military sense. The stronger party should retain its freedom of action in all domains. The exception is a situation in which a weaker state has a disproportionate cyberattack capability or is able to quickly receive external assistance from an alliance or another superpower. In all cases, the duration of the conflict becomes an essential factor. The longer the closure of the national networks continues, the greater the societal impact and the greater the likelihood of the attacker getting through the defence systems, even when reinforced.[437] A prolonged closure of the national segment of the internet only makes sense when fighting against an internal enemy. Even then, foreign connections can be kept open to a limited extent. Although the closure of the internet segment is unlikely to be economically viable, financial losses must always be compared to the expected losses and profits caused by war. In modern warfare, damage will occur in any case, but the party that has protected itself the best will be better equipped to restore the foundations of the economy and society.

---

[437] Clarke & Knake (2019), 96–97; Abdou, AbdelRahman, van Oorschot, Paul C. & Wan, Tao: Comparative Analysis of Control Plane Security of SDN and Conventional Networks. *IEEE Communications Surveys & Tutorials*, Vol. 20, No. 4, Fourth Quarter 2018, pp. 3542–3559.

Finally, we can conclude that the closure of an internet segment is not necessarily directly linked to aggression against the state closing its network. For example, in the event of a future major war between the United States and China, Russia may be a bystander or an indirect ally of one the superpowers. Even then, it must be able to protect itself against acts of war in the cyber environment. Wars tend to spread in and between operational domains. A closed and autonomous network would help Russia maintain and restore its national capacity to act faster than the rest of the world affected by war.

6. Conclusions

This thesis sought an answer to the problem whether the Russian national segment of the internet creates structural cyber asymmetry, how it manifests itself and what strategic effects does it have? The first subquestion was what is structural cyber asymmetry, how its existence can be examined and what is meant by strategic effects? The question was answered by building the concepts of cyberspace, cyber domain, cyber power and cyber strategy based on previous International Relations, strategy and cyber security research. On this basis, four forms of use of strategic cyber power were formed: conflict prevention, deterrence, conflict escalation control, and military exploitation of structural cyber asymmetry, i.e., the use of compellence and brute force. After processing the question of cyber power, previous views of asymmetry within the framework of military activities were examined and a definition of structural cyber asymmetry was formulated based on them. Finally, the concepts of freedom of action, common situation picture, command and control, and resilience used in the analysis of structural cyber asymmetry were presented.

The definition of cyberspace was intended to emphasise the nature of cyberspace as a changing and malleable environment. The purpose of the definition of cyber power, on the other hand, was to emphasise the adaptability and variability of cyberspace as a result of human activity. In the definition of cyber strategy, the aim was to emphasise how it is being built continuously and the external factors affecting it, such as other actors in the cyber domain. The guiding model for formulating the strategic-level concepts for the forms of use force was the *bargaining model of war*, which is based on the U.S. deterrence theory on nuclear weapons and operational analysis applied during the Cold War. Conflict prevention, deterrence, escalation control and military exploitation of cyber asymmetry gained their content in relation to the cyber domain and the continuum of interstate relations. In this thesis, the strategic effect was defined through changes in the operating environment and the target. The aim of the formulation was to focus specific attention not only to achieving objectives but also to shaping the strategic operating environment. Finally, structural cyber asymmetry was defined as a characteristic of cyberspace, which may occur when states shape their operating environment by means of cyber power. The perspective was deliberately state-centric, but not intended to dispute the impact of non-state actors on the changes in cyberspace.

After defining the main theoretical concepts, the work answered the second subquestions of the research, i.e., what is the Russian national segment of the internet and its relationship with the concepts of information security and defence system and closed national network? A soft system theoretical approach was adopted to understand the national segment of the internet. On this basis, the concept of digital terrain was created, which enabled presenting the control of the information environment as a system-of-systems model. This resulted in the system-of-systems model of national information security and defence. The national segment of the internet was defined as a manifestation of the system in cyberspace on the one hand, and an applied representation of a theoretical closed national network on the other. The subsystems of the system were formed by examining projects aimed at managing the Russian state's

national information environment, mainly the cyberspace, the thinking of Russian information theoreticians and the characteristics of the Russian state. The information security and defence system was defined as comprising of eight subsystems: the state's scientific-technological basis, the authentication and encryption system, the censorship system, the surveillance and data collection systems, the critical information infrastructure, the active measures system, the armed forces' networks and systems, and the management, control, monitoring and feedback system. The information security and defence system is a model of a control system for the information environment, which is applicable to other similar cases to a limited extent. Open national networks were defined as being loosely based on the way the internet was managed in technologically advanced Western countries in the mid-2010s. In the thesis, the open national network found its character in relation to the structure of the closed national network.

After defining the key concepts for the analysis, the thesis answered the third subquestion, i.e., how does the Russian national segment of the internet compare with open national networks in terms of freedom of action, common situation picture, command and control, and resilience, and does the relationship contribute to structural cyber asymmetry? Three different analyses were made to find answers.

The attack vector analysis examined the ability of an attacker and defender of a state with an internet segment and an open national network state to penetrate each other's networks and protect their own. The analysis confirmed previous findings on the existence of structural cyber asymmetry giving an advantage to the internet segment state. The internet segment defenders are far more efficient in shaping their network and repairing its vulnerabilities than open network defenders and thus denying the attacker's freedom of action in cyber battlefield. The internet segment defenders have better freedom of action in their own networks, a common situation picture provided by the organisation and technology, centralised command and control capability, and stronger resilience based on the control of the critical information infrastructure than open network defenders.

The internal structural differences between the internet segment and open national networks were compared through the subsystems of the national information security and defence systems. This analysis also confirmed the existence of structural cyber asymmetry between the internet segment and open national networks. However, the analysis showed that there are also significant strengths in the structure of open national networks. In addition, many of the strengths of the internet segment contain contradictory elements that may turn into weaknesses in certain situations. As regards the results, it should be noted that the properties of the Russian state affect the analysis and, had the internet segment model been based on another state, the results could have been different.

The third analysis examined the relationship between national networks on the continuum of interstate relations. Like the two analyses above, this analysis also confirmed the existence of structural cyber asymmetry in relation to conflict development and the change in threats. It showed how the internet segment is based on flexible regulation of the national information environment rather than on the practice of '*internet shutdown*'. The information security and defence system enables control of the

space temporally, locally and functionally in proportion to threats. Disconnecting the internet segment from the global internet is an extreme form of control.

The fourth subquestion of the work was how does structural cyber asymmetry affect the threat or use of force to achieve political objectives in different phases of interstate relations? The question was answered by examining the answers to the third question in the context of the forms of cyber use of force and strategic environment. The functions and factors supported or enabled by the information security and defence system in relation to each form of the use of force are summarised in Figure 5.

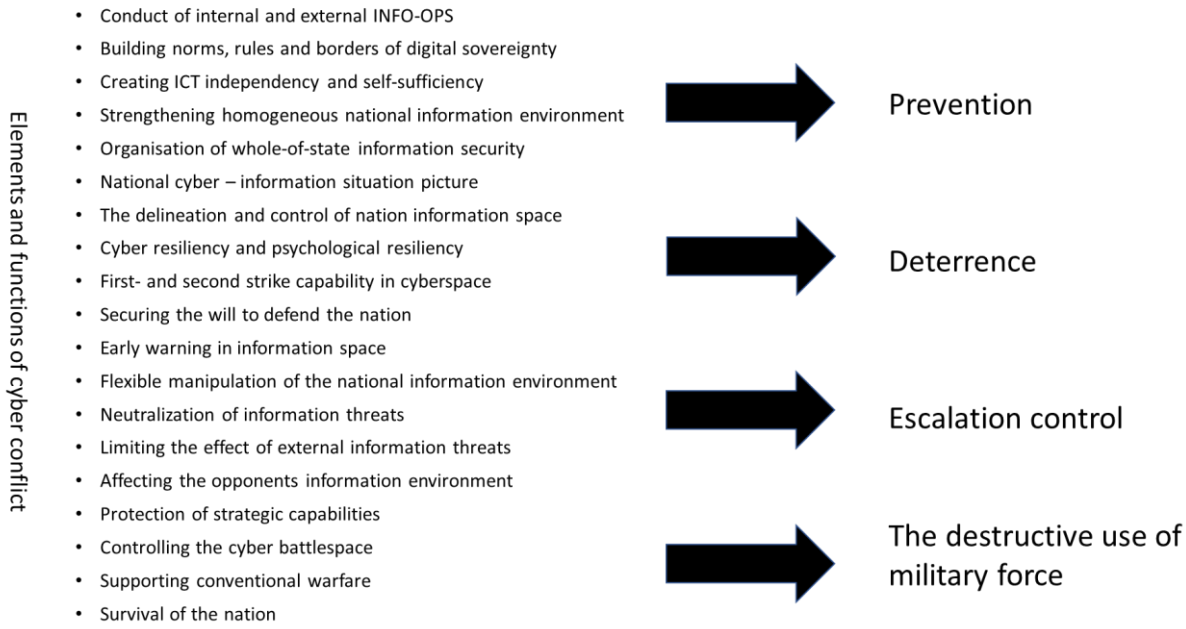

Figure 5: The functions, factors and forms of use of force of the national information security and defence system

As regards conflict prevention, it was noted that the internet segment contributes to internal and external reconnaissance and thus to obtaining an early warning. The system denies the freedom of action from potential internal threats and prevents threats through self-sufficient and independent technological development. The national segment of the internet is not only a means of isolation but can serve as a tool for spreading the state's influence and thus prevent threats and conflicts through the force of attraction. From the perspective of the information security and defence system, conflict prevention is largely based on shaping the global cyber environment, i.e., the state's strategic environment. Strategic impacts can be achieved by controlling one's own information environment, building potential cyber power to maintain balance and shaping the global cyber environment.

When examining cyber deterrence, it was found that the closed national network is based, above all, on deterrence by denial. The system significantly strengthens the state's technological and psychological resilience. Denying the use of the information sphere also affects the preconditions for using force in other operational domains.

The deterrence is of cross-domain nature. To function perfectly, the national information security and defence system must extend not only to the internet but also to space and the entire free-space electromagnetic spectrum. Structural cyber asymmetry affects deterrence as a function of time. As structural cyber asymmetry increases, to an open network state making a pre-emptive or first strike appears as a more rational solution from the perspective of costs and probability than waiting. Since, in cyberspace, it is practically impossible to destroy the target state's retaliation capacity with a first strike, the open network remains vulnerable to retaliation.

Structural cyber asymmetry increases the credibility of deterrence by punishment, as the country disconnecting its network has an undeniable ability to strike back while its own valuable targets are, in relative terms, better protected than those of open network states. As a result, the internet segment can lower the threshold of using cyber weapons alongside other military capabilities as part of deterrence by punishment. If interpreted wrongly, it could also be seen as a signal of preparing a first strike. The problem of internet segment deterrence is that the construction of a closed network can be interpreted as a disproportionate investment in 'civil defence', which in turn can be interpreted as preparing a first strike or pre-emptive strike. It is also clear that building cyber deterrence cannot be distinguished from other operational domains. Building a closed national network also affects the operating logic of other operational domains. Furthermore, it is likely that if the efforts to build the national segment of the internet into a credible deterrence by denial instrument fail in the eyes of a potential opponent, it is a needless and potentially even harmful project.

When examining escalation control, it was noted that escalation control should distinguish between the long-term and short-term impacts of structural cyber asymmetry on the one hand, and control of the unintentional consequences of escalation dominance on the other. The long time span of escalation control is related to great power competition and the balance of power. In the long term, technological development plays an emphasised role in the balance of power assessments of great powers. Norms are also related to the long time span. The threshold of escalation for cyberattacks may change as the norms of cyber sovereignty – and possibly a ban on cyber weapons – develop and become more closely connected to critical information infrastructure. What could be interpreted as a private sector cybersecurity issue in the West, may be interpreted as a national security issue, for example, in Russia.

In escalation control, the short-term effects of structural cyber asymmetry are related to changes in the internet segment and open networks within the context of a conflict in terms of months, weeks, days, or even seconds. The closure of the national network is not only a defensive measure, but it can be used to affect the functioning of the global internet as a whole. Disconnecting the national segment of the internet will only act as a means of compelling the adversary if the adversary is unable to protect itself in the same or adequate manner. The closure forces the adversary to make the next move either by protecting itself, by demonstrating the weaknesses of the closed network, that is, by attacking, or by mitigating the conflict. It is totally possible that the next step of the conflict is taken in another operational domain.

From the perspective of escalation dominance, a cyberattack can be used to gain an advantage of surprise or to show force, to cause limited destruction or paralysis, or to

raise the threshold of escalation. However, if the internet segment functions effectively, the adversary would have to escalate with conventional force or nuclear weapons, which would significantly increase the intensity of the conflict. Escalation dominance also works in the case of internal threats. An external attacker will have to consider at what stage it will renounce its support to internal insurgent movements or whether it wants to continue escalating the conflict into a direct interstate struggle. For the insurgents themselves, the narrowed information space means reduced freedom of action and weaker support from the citizens. This may force them to operate in other environments.

Disconnecting the internet segment is not necessarily aimed at increasing the intensity or extent of the conflict. It may be unclear to the potential adversary whether the network is disconnected due to preparing for war or for internal security – and they may react in a surprising way. In addition, for the internet segment, the risk of accidental escalation is also increased by the interdependencies between the subsystems of the information security and defence system. It is also possible, of course, that the internet segment defender can trust its system too much and fall into using excessive blackmail or threatening tactics.

When examining the military exploitation of structural cyber asymmetry, it was noted that disconnecting the national segment of the internet is a necessary condition for asymmetry, but not sufficient in itself. The use of asymmetry for the purposes of compellence and the use of brute force requires attack capability. In order for the structural cyber asymmetry provided by the internet segment to support the achievement of strategic objectives in the greatest possible way, cyber warfare must be accompanied by cross-domain compellence and the use of brute force. However, the impact of structural cyber asymmetry on defence against compellence and the use of brute force is undeniably greater than against an attack. The national internet segment can prevent both long-term efforts to destabilise the state through information and lower the chances of success of a strategic surprise by means of cyber weapons. A closed national segment of the internet can be seen as an enabler of attrition warfare, which gives the defender time to secure its rear and to increase its strength in relation to the adversary.

Disconnecting the national segment of the internet can be used for shaping the cyber battlefield. This will not change the vulnerabilities of individual systems or networks, but modifications made at the national level may contribute to deceiving, slowing down and repelling the attacker. In defensive action, the national segment of the internet supports the use of conventional and nuclear weapons in other operational domains. Controlling, restricting the freedom and disconnecting the internet segment can be conducted territorially and flexibly. It should be borne in mind that in order for the relationship between an internet segment and an open network to create structural cyber asymmetry that can be exploited militarily, the former must integrate into itself all existing and future ICT technologies, and their use must be practised at a national level.

The use of the internet segment as a means of compellence and brute force or as a means of defending against it must always be set in its context. In the case of limited war, when a stronger state attacks a weaker one, a full closure of national networks

makes no economic or military sense from the perspective of the stronger state. The exception is a situation in which a weaker state has a disproportionate cyberattack capability or is able to quickly receive external assistance from an alliance or another superpower. Prolonged closure of the national segment of the internet only makes sense when fighting against an internal enemy, in which case foreign connections can be kept open to a limited extent. It should also be noted that the advantage of structural cyber asymmetry can be used for a surprise first strike or for supporting a second strike. Therefore, a fist strike or even a pre-emptive strike becomes an attractive option for an open network state. When using the internet segment, the interpretations the adversary may make on its use must be taken into account.

Based on the four analyses made in the thesis, it can be argued that examining cyber power as a tool for shaping cyberspace, alongside other forms of use of force, provides a new perspective for studying the national and global impacts of national cyber strategies. The concept of structural cyber asymmetry describes the phenomenon that arises when individual states build closed national networks while their potential adversaries keep their networks open. It helps to better understand asymmetric power relationships between states in an increasingly digitalised world, albeit this viewpoint may lose its meaning if all countries of the world start to disconnect their networks.

The manifestations and strategic effects of structural cyber asymmetry are diverse. The construction of an internet segment can be compared to strategically shaping and preparing a battlefield. It forces the adversaries to respond. In the long term, cyber sovereignty may, for essential military reasons, expand into an international standard. It is possible that, in the future, cyber borders will no longer be crossed freely. New norms and standards related to the use of cyber force and cyber espionage can set significant marginal conditions for the use of force and shape their impacts. This would result in efforts to build national technological self-sufficiency and technology-based alliances. Critical information infrastructure will become an important, if not the most important, object of state security, and states will begin to monitor the borders of and objects in the cyber environment. The militarisation of the cyberspace and cyber environment seems inevitable. The aim is to control the national information environment, which can be used for gaining local and temporal information superiority already during peacetime.

7. Discussion

It would be possible to implement a closed national network in small or medium-sized democratic constitutional states. However, the question of whether to exploit this opportunity must be considered carefully, since the roots of a national segment of the internet lie in the political traditions and interests of authoritarian states. The pursuit of complete security and effectiveness is a constant threat to democracy. Seeking self-sufficiency in the ICT sector may lead to national economic problems. In addition, the control and management systems required by a closed national network may create new and unforeseen vulnerabilities. It is also possible that the feeling of security created by the information security and defence system may lead to pursuit of aggressive policies and risk-taking.

This thesis examined the Russian project of a national segment of the internet from the perspective of implementation. Criticism against how likely it is that it will be implemented is presented in several sections of the thesis. There are reasons for scepticism. A well-functioning and secure national segment of the internet can ultimately be too costly even for an authoritarian, energy-rich state to complete. Full success would require the creation of an internationally competitive ICT ecosystem, including circuit and component production, and own operating systems and services.

It is, of course, possible that the national segment of the internet can be implemented without jeopardising the foundations of a democratic rule of law and, at the same time, avoiding the problems related to the Russian implementation of the system. Even at this moment, many countries find themselves somewhere in between closed and open networks, and examining how they have succeeded or failed in their projects for managing the information environment could provide examples for finding a 'third way'. From the perspective of research in the management of the cyber and information environment, it is essential to define a model for an ideal closed network, one that is in no way linked with Russia's national segment of the internet. This requires comparative research and a universal model. The information security and defence model provided by this thesis is just the beginning. The model of open networks also needs to be specified further. In many undemocratic countries, national networks are even more open than the open networks defined in this work. How do their properties and weaknesses affect the balance of power of the cyber environment?

In my doctoral dissertation, I argued that strategic cultural ideas give a reason, i.e., make it reasonable, for Russia to construct a national segment of the internet in a specific strategic environment. The strategic effect analysis conducted in this thesis shows that structural cyber asymmetry supports the rationality of building an information security and defence system, provided that the use of force is understood in accordance with the *bargaining model of war*. During this thesis, however, I have started to doubt the suitability of the *bargaining model of war* for analysing cyber phenomena. It contextualises cyber activities as warfare or war between states, which does not necessarily contribute to understanding the phenomenon in the best possible way. It is also based on a set of concepts originally built around the use of strategic nuclear weapons – a phenomenon which has not taken place, which cannot be observed, and

which almost completely deviates from phenomena in the cyber world.[438] The model is also intended for examining the actions of great powers, and its assumptions of cyber or other power may not smoothly scale into examining the strategic actions of small states.

This thesis provides a new perspective on the claim that the coercive use of cyber power suffers from inherent weaknesses. A timely closure of a national internet segment, coupled with a specific balance of power in other operational domains, may provide an opportunity to achieve strategic effects through a cyber first strike or a pre-emptive strike. The compelling force of cyberattacks is the greater, the more societies are based on information technology and the less capacity they have to protect themselves. At the level of the international system, for example, the 'biological' tailoring of cyber weapons may become a problem. If the global internet fragments into national sections, weapons targeted against national ecosystems will emerge, and the threshold of using them will become lower as interdependence decreases. If we intend to protect ourselves against these weapons, we need to consider what will happen if all the world's states close their networks? Are we faced with the end of so-called liberal international order?[439]

Despite all the observations presented in this thesis, my personal view is that the information security and defence system, or the national segment of the internet, will not be realised in such a way some Russian theoreticians would like to see it. In other words, in the form of a unified national information space, which is a system of systems by its nature and which is used for information struggle against similar systems, and which is also a centralised national information, command, control and administration system.[440] Nor do I believe that the 'sovereign internet' will be implemented as ordered by laws and regulations. Technological challenges, vulnerabilities created by centralisation, corruption and the struggle for resources, a weak cyber security culture and the opposition from the civil society and trade and industry are too strong, even if the political will to implement the project existed. The friction encountered by the project is high, and not all vulnerabilities can ever be addressed.

On the other hand, the nature of open national networks is changing and will change even more radically as we approach the 2030s. The introduction of this thesis argued that the model of theoretical open networks is based on an outdated view of the way Western states manage their national telecommunications networks. The U.S. Cyber Solarium Commission's proposal for U.S. cyber deterrence contains similar elements as the Russian view of digital sovereignty.[441] Even in Europe, the idea of isolationist cyber sovereignty is becoming stronger.[442] As a result, structural cyber asymmetry in

---

[438] On similar thoughts cf. Whyte, Christopher A., Thrall, Trevor & Mazanec, Brian M.: *Information Warfare in the Age of Cyber Conflict*. Routledge, London, 2020; Harknett, Richard J. & Smeets, Max: Cyber Campaigns and Strategic Outcomes. *Journal of Strategic Studies*, Vol. 45, No. 4 (2022), pp. 534–567.
[439] Ikenberry, John: The End of Liberal International Order? *Foreign Affairs*, Vol. 94, No. 1 (2018), pp. 7–23.
[440] Kukkola (2020a), 360.
[441] Cyberspace Solarium Commission (2020).
[442] Burwell, Frances G. & Propp, Kenneth: *The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?* Atlantic Council, 2020. [https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf], visited 21.10.2020.

the form examined in this thesis may not emerge at all or may slowly fade away. Instead, a new world order may arise, based on power and geography, in which the differences between closed and open networks will disappear. This world order is not necessarily any better than the one we had at the beginning of the 21st century or have now.

Post Scriptum

Russian troops invaded Ukraine on 24 February 2022, when Russia failed to achieve its desired objectives with the military, economic and diplomatic pressure it had been exerting since April of the previous year. When writing this, the war has lasted seven months, and Russia has just announced that, to complete its 'special operation', it needs to declare 'a partial mobilisation'.

The use of these concepts suggests that the Russian regime sees the battle as a local conflict at most, which does not pose an existential threat to the state. Consequently, Russia has not considered it necessary to fully activate the national information security and defence system and has not disconnected the national segment of the internet. This continues to be the case despite the fact that the FSB announced that disconnection is possible and under consideration due to the unprecedented number of cyberattacks against Russia in the early months of the war.[443] Of course, censorship has been significantly tightened, the operation of foreign social and conventional media has been restricted, and efforts have been made to reduce the use of foreign software, encryption systems and hardware. Russia has tried to develop its national cyber security measures by extending the responsibility for IT security to all levels of public administration. However, the measures have shown that, despite the FSB's statement, the national segment of the internet is still far from complete, and the digital sovereignty pursued by Russia is still years away. The impact of Western sanctions will be significant, and, on the other hand, the West did not even try to cut off Russia's connections with the rest of the world.

However, the Russian information security and defence system has worked and secured internal information superiority within Russia – the West has not been able to influence the Russian elite or citizens. At the same time, the efforts to isolate the country diplomatically have failed. Internal information superiority means that threatening Russia with more stringent measures than sanctions is likely to lead to Russians joining together in support of the Kremlin to defend the Mother Russia. This is what the West has been trying to avoid. Russia has combined a potentially strong will to defend the country (deterrence by denial) with poorly masked threats to use cyber and nuclear weapons (deterrence by punishment) against the West, thereby seeking to restrict the Western aid measures and to limit the conflict to Ukraine. The same threats have served as a tool of escalation control in relations between Russia and Ukraine, as Ukraine must take into account Russia's potential for mobilisation.

Offensive cyber operations against Russia have shown that cyber security has been quite weak in some parts of the internet segment. At the same time, the impact of information leaks, denial of service attacks, sabotage of websites and news broadcasts has been relatively limited. The operations carried out by activists have apparently not affected the course of war, with the exception of perhaps the early actions against Belarussian train connections. Ukraine has also been very resilient to Russian offensive action, a significant share of which has been intended to cause strategic effects comparable to an armed attack. It seems that, in this conflict, cyber operations have

---

[443] Исакова, Татьяна: Непробиваемая интернет-изоляция. *Коммерсантъ*, 21.09.2022. [https://www.kommersant.ru/doc/5571153], visited 26.9.2022.

played a role as a tool of attrition warfare, and their most significant impacts are related to reconnaissance and intelligence gathering.

The war has also shown that states benefit significantly from cooperation with international companies and the support of allies. Ukraine has received significant support for fending off cyberattacks, and the efforts to isolate Russia with regard to software and hardware deliveries and connections have not yet succeeded. As long as a state has allies due to its geopolitical or economic position, it is quite impossible to implement cyber blockades. In fact, an unintentional consequence of the isolation policy would seem to be a greater fragmentation of cyberspace into cyber ecosystems. The conclusions drawn from sanctions against Russia cannot but strengthen the ambition of great powers and alliances to have independent software and circuit production.

The war in Ukraine is also likely to impact the development of cyber norms. Because of Russia's offensive actions, the cyber diplomacy projects of Russia and China have lost their credibility. In fact, one of the consequences of the war may be that cyberattacks become normalised as part of the approved image of war and the moral constraints related to their use become even weaker than before.

SOURCES

1 FINNISH AND ENGLISH MATERIAL

1.1 Studies and theses

Forsström, Pentti: *Venäjän sotilasstrategia muutoksessa: tulkintoja Venäjän sotilasstrategian perusteiden kehityksestä Neuvostoliiton hajoamisen jälkeen*. Doctroal thesis, Maanpuolustuskorkeakoulu, Julkaisusarja 1 Nro 32, Helsinki, 2019.

Hanska, Jan: *Times of war and war over time: the roles time and timing play in operational art and its development according to the texts of renowned theorists and practitioners*. Doctoral Dissertation. National Defence University Series 1: Research Publications No. 12, Helsinki, National Defence University, 2017.

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.

Koskinen-Kannisto, Anne: *Situational Awareness Concept in A Multinational Collaboration Environment Challenges in the Information Sharing Framework*. Doctoral Dissertation. National Defence University Department of Military Technology Series 1, n:o 31, Helsinki, 2013.

Kukkola, Juha: *Digital Soviet Union. The Russian national segment of Internet as a closed national network shaped by strategic cultural ideas*. Doctoral Dissertation. National Defence University Series 1: Research Publications No. 40. National Defence University, Helsinki, 2020a.

Kukkola, Juha: Oveluuden lupaus. *Asymmetria, epäsuoruus ja ei-sotilaalliset toimenpiteet uuden venäläisen sotataidon kiintopisteinä*. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 2: Tutkimusselosteita nro 22, Helsinki, 2022.

Kuusisto, Rauno: *Aspects On Availability: A Teleological Adventure Of Information In The Lifeworld*. Doctoral Dissertation. Series / National Defence College, Department of Tactics and Operations Art. 1, 2004.

Puranen, Matti: *Informaatioherruus. Kiinan sotilasstrategia ja sodan kuva kylmän sodan jälkeen*. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 2: Tutkimusselosteita nro 21, Helsinki, 2022.

Rindzeviciuté, Eglé: *Constructing Soviet Cultural Policy: Cybernetics and Governance in Lithuania after World War II*. Doctoral Dissertation. Linköping University, Linköping, 2008.

Siukonen, Veikko: *APT-Operaation inhimilliset tekijät: Operaation tarkastelu päätöksenteon näkökulmasta*. Jyväskylän yliopisto, Tietojenkäsittelytiede, Master's thesis, 2019.

Timonen, Jussi: *A Common Operating Picture for Dismounted Operations and Situation Room Environments*. Doctoral Dissertation. National Defence University Series 1: Research Publications No. 19, Helsinki, 2018.

1.2 Literature

Ackoff, Russell L.: *Ackoff's Best. His Classic Writings on Management*. John Wiley & Sons, Inc., New York, 1999.

Alberts, David S. & Papp, Daniel S. (eds.): *The Information Age Anthology – Volume I-III*. CCRP Publication Series, 1997–2000.

Alberts, David S., Gartska, John J. & Stein, Frederick P.: *Network Centric Warfare: Developing and Leveraging Information Superiority* (2nd ed.). CCRP Publications, 2000.

Alstyne, Marshall Van & Brynjolfsson, Erik: *Electronic Communities: Global Village or Cyberbalkans?* [https://web.mit.edu/marshall/www/papers/CyberBalkans.pdf], luettu 14.9.2022.

Andress, Jason & Winterfeld, Steve: *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners. (*2nd ed.*)* Syngress, Waltham. 2014.

Arbatov, Alexei & Dvorkin, Vladimir (Eds.): *Missile Defense: Confrontation and Cooperation*. Carnegie Moscow Center, Moscow, 2013.

Barkin, Samuel J.: *Realist constructivism: Rethinking International Relations Theory*. Cambridge University Press, Cambridge, 2010.

Bartles, C.: Sixth-generation War and Russia's Global Theatres of Military Activity. In *Russian Grand Strategy in the Era of Global Power Competition*. Monaghan, A. (ed.): Manchester University Press, Oxford, 2022, pp. 71–97.

Baylis, J., Wirtz, J. J. & Gray, C. S.: *Strategy in the Contemporary World* (4th ed.) Oxford University Press, New York, 2013.

Bendett, Samuel & Kania, Elsa B.: *A new Sino-Russian high-tech partnership. Authoritarian innovation in an era of great-power rivalry*. The Australian Strategic Policy Institute, Policy brief Report No. 22/2019.

Blair, Bruce, G.: *The Logic of Accidental Nuclear War*. The Brookings Institution, Washington, D.C., 1993.

Boeders, Dennis & van den Berg, Bibi: *Governing Cyberspace: Behavior, Power, and Diplomacy*. Rowman & Littlefield, New York & London, 2020.

Brantly, Aaron Franklin: *The Decision to Attack. Military and Intelligence Cyber Decision-Making*. University of Georgia Press, Athens, Georgia, 2016.

Broeders, Dennis & van den Berg, Bibi (eds.): *Governing Cyberspace. Behavior, Power, and Diplomacy*. Rowman & Littlefield, Lanham, Maryland, 2020.

Buchanan, Ben: *The Hacker and The State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press, Cambridge, 2020.

Buckley, Noah: *Corruption and Power in Russia*. FPRI, Philadelphia, PA, 2018.

Cadier, David & Light, Margot (Eds.): *Russia's Foreign Policy. Ideas, Domestic Politics and External Relations*. Palgrave Macmillan, Basingstoke, 2015.

Chase, Michael S. & Chan, Arthur: *China's Evolving Approach to "Integrated Strategic Deterrence"* RAND Corporation, Santa Monica, 2016.

Checkland, Peter: *Systems thinking, Systems Practice*. John Wiley & Sons ltd., New York, 1993.

Choucri, Nazli: *Cyberpolitics in International Relations*. The MIT Press, Cambridge, 2012.

Clarke, R. A. & Knake, R. K.: *Cyber War: The Next Threat to National Security and What to Do About It*. Harper Collins, New York, 2010.

Clarke, Richard A. & Knake, Robert K.: *The Fifth Domain. Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Press, New York, 2019.

Creveld Van, M.: *The Transformation of War*. The Free Press, New York, 1991.

DeBenedictis, Kent: *Russian 'Hybrid Warfare' and the Annexation of Crimea. The Modern Application of Soviet Political Warfare*. Bloomsbury Academic, London, 2022.

Deibert, Ronald, Palfrey, John, Rohozinski, Rafal & Zittrain, Jonathan (eds.): *Access Controlled the Shaping of Power, Rights, and Rule in Cyberspace*. The MIT Press, Cambridge, Massachusetts, 2010.

Donaldson, Robert H. & Nadkarni, Vidya: *The Foreign Policy of Russia. Changing Systems, Enduring Interests* (6th ed.) Routledge, New York & London, 2019.

Dunne, T., Kurki, M. & Smith, S.: *International Relations Theories: Discipline and Diversity* (4th ed.) Oxford University Press, Oxford, 2013.

Ertan, A., Floyd, K., Pernik, P. & Stevens, T. (Eds.): *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. CCD COE, Tallinn, 2020.

Freedman, Lawrence: *Strategy: A History*. Oxford University Press, New York, 2013.

Freedman, Lawrence: *The Evolution of Nuclear Strategy* (3rd ed.) Palgrave Macmillan, New York, 2003.

Friis, Karsten & Ringsmose, Jens: *Conflict in Cyber Space. Theoretical, strategic and legal perspectives*. Routledge, New York, 2016.

Fuller, J. F. C.: *The Foundations of the Science of War*. A Military Classic Reprint (org. 1925). U.S. Army Command and General Staff College Press, Fort Leavenworth, Kansas, 1993.

Gartzke, Eric & Lindsay, Jon R.: *Cross-Domain Deterrence: Strategy in an Era of Complexity*. Oxford University Press, New York, 2019.

Gat, Azar: *War in Human Civilization*. Oxford University Press, Oxford, 2006.

Geers, Kenneth: *Strategic Cyber Security*. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2011.

Geist, Edward & Lohn, J. Andrew: *How Might Artificial Intelligence Affects the Risk of Nuclear War*. RAND, Santa Monica, 2019.

Geist, Edward M.: *Armageddon Insurance. Civil Defense in the United States and Soviet Union, 1945-1991*. University of Northern Carolina Press, Chapel Hill, 2019.

Gerovitch, Slava: *From Newspeak to Cyberspeak: A History of Soviet Cybernetics*. The MIT Press, Cambridge, 2002.

Giles, Keir: *Handbook of Russian Information Warfare*. Fellowship monograph 9. Rome: NATO Defence College, 2016.

Godwin III, J. B., Kulpim, A., Rauscher, K. F. & 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, 2014.

Gray, Colin S.: *Modern Strategy*. Oxford University Press, Oxford, 1999.

Gray, Colin S.: *Strategy and Politics*. Routledge, New York, 2016.

Gray, Colin S.: *War, Peace and International Relations: An Introduction to Strategic History*. Routledge, New York, 2007.

Greenberg, Andy: *Sandworm. A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday, New York, 2019.

Guzzini, Stefano: *Power, Realism and Constructivism*. Routledge, London and New York, 2013.

Gvosdev, Nikolas K. & Marsh, Christopher: *Russian Foreign Policy: Interests, Vectors, and Sectors*. SAGE Publications, Inc., Los Angeles, 2014.

Hammes, T. X.: *The Sling and the Stone: On War in the 21st Century*. Zenith Press, St Paul, 2006.

Hammond, Grant T.: *The Mind of War. John Boyd and American Security*. Smithsonian Books, Washington, D.C., 2001.

Harrison, Todd, Johnson, Kaitlyn, Roberts, Thomas G., Way, Tyler & Young, Makena: *Space Threat Assessment 2020*. Center for Strategic & International Studies, Washington, D.C., 2020.

Hayes, Richard E. & Alberts, David S.: *Power to the Edge. Command… Control… in the Information Age*. CCRP, 2005.

Honkova, Jana: *The Russian Federation's Approach to Military Space and Its Military Space Capabilities*. George Marshall Institute, Arlington, VA, 2013.

Howard, Ronald & Abbas, Ali E.: *Foundations of Decision Analysis*. Pearson, London, 2015.

House, Jonathan M.: *A Military History of the Cold War 1944-1962*. University of Oklahoma Press, Norman, 2012.

Isserson, G. S.: G. S. *Isserson and the War of the Future: Key Writings of a Soviet Military Theorist*. Richard W. Harrison (trans., ed.). McFarland & Company, Jefferson, NC, 2016.

Johnson, Loch K.: *Handbook of Intelligence Studies*. Routledge, London & New York, 2007.

Jonsson, Oscar: *The Understanding of War. Blurring the Lines between War and Peace*. Georgetown University Press, Washington, D.C., 2019.

Jordan, D., Kiras, James D. Lonsdale, David J., Speller, Ian, Tuck, Christopher & Dale, Walton: *Understanding Modern War*. Cambridge University Press, Cambridge, 2008.

Kaldor, Mary: *New and Old Wars: Organized Violence in a Global Era* (3rd edition). Stanford University Press, Stanford, 2012.

Kane, Thomas M. & Lonsdale, David J.: *Understanding Contemporary Strategy*. Routledge, New York, 2012.

Kanet, Roger E. & Piet, Rémi (Eds.): *Shifting Priorities in Russia's Foreign and Security Policy*. Ashgate Publishing Limited, Surrey, 2014.

Kaplan, Fred: *The Wizards of Armageddon*. Stanford University Press, Stanford, California, 1991.

Kaplan, Fred: *Dark Territory. The Secret History of Cyber War*. Simon & Schuster, New York, 2016.

Keegan, J. A.: *History of Warfare* (2nd ed.) Pimlico, London, 2004.

Kello, Lucas: *The Virtual Weapon and International Order*. Yale University Press, New Haven, 2017.

Kilcullen, David: *The Dragons and the Snakes: How the Rest Learned to Fight the West*. Oxford University Press, Oxford, 2020.

Klinger, Janeen M.: *Social Science and National Security Policy. Deterrence, Coercion, and Modernization Theories*. Palgrave Macmillan, Cham, Switzerland, 2019.

Kofman, Michael, Fink, Anya & Edmonds, Jeffrey: *Russian Strategy for Escalation Management: Evolution of Key Concepts*. CNA, Washington, D. C., 2020.

Kott, Alexander, Wang, Cliff, Erbacher, Robert F. (Eds.): *Cyber Defense and Situational Awareness*. Springer International Publishing, London, 2014.

Kott, Alexander: *Information Warfare and Organizational Decision-Making*. Artech House, London, 2007.

Krygiel, Annette J.: *Behind the Wizard's Curtain: An Integration Environment for a System of Systems*. CCRP Publication Series, 1999.

Kukkola, Juha, Ristolainen, Mari & Nikkarila, Juha-Pekka: *Game Changer: Structural Transformation of Cyberspace*. Finnish Defence Research Agency, Riihimäki, 2017.

Kukkola, Juha, Ristolainen, Mari & Nikkarila, Juha-Pekka: *Game Player: Facing the structural transformation of cyberspace*. Finnish Defence Research Agency Publications 11. Finnish Defence Research Agency, Riihimäki, 2019.

Kuusisto, Rauno: *Tilannekuvasta täsmäjohtamiseen. Johtamisen tietovirrat kriisin hallinnan verkostossa*. Liikenne- ja viestintäministeriön julkaisuja 81/2005, Helsinki, 2005.

Kuusisto, Tuija (toim.): *Kybertaistelu 2020*. Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2 No. 1/2014, Juvenes, Tampere, 2014.

Laari, Tommi (toim.): *#kyberpuolustus. Kyberkäsikirja Puolustusvoimien henkilöstölle*. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 3: Työpapereita nro. 12, Helsinki 2019.

Ledeneva, Alena V.: *Can Russia Modernise?* Cambridge University Press, Cambridge, 2013.

Lewis, James Andrew: *Rethinking Cybersecurity*. A Report of the CSIS Technology Policy Program. Rowman & Littlefield, New York, London, 2018.

Libicki, M. C.: *Conquest in Cyberspace. National Security and Information Warfare*. Cambridge University Press, Cambridge, 2007.

Libicki, Martin C.: *Cyberdeterrence and Cyberwar*. RAND, Santa Monica, 2009.

Libicki, Martin C.: *Cyberspace in Peace and War*. Naval Institute Press, Annapolis, Maryland, 2016.

Liddell Hart, B. H.: *Strategy* (2nd rev. ed.) Meridian, New York, 1991.

Luhmann, Niklas: *Social Systems*. Stanford University Press, Stanford, Cal., 1995.

Luttwak, Edward N. Strategy: *The Logic of War and Peace*. The Belknap Press of Harvard University Press, Cambridge, Massachusetts, 2001.

Mankoff, Jeffrey: *Russian Foreign Policy: The Return of Great Power Politics* (2nd ed.) Rowman & Littlefield Publishers, Inc., Lanham, 2012.

Maurer, Tim: *Cyber Mercenaries. The State, Hackers, and Power*. Cambridge University Press, Cambridge, 2018.

Mazarr, Michael J.: *Understanding Deterrence*. RAND, Santa Monica, 2018.

McReynolds, J: China's Military Strategy for Network Warfare. In *China's Evolving Military Strategy*. McReynolds, J. (ed.) The Jamestown Foundation, Washington DC, 2016, pp. 195–240.

Metz, S. & Johnson, D. I.: *Asymmetry and U.S. Military Strategy L Definition, Background, and Strategic Concepts*. U. S. Army Strategic Studies Institute: Carlisle, 2001.

Milevski, Lucas: *The Evolution of Modern Grand Strategic Thought*. Oxford University Press, Oxford, 2016.

Morgan, Forrest E., Mueller, Karl P., Medeiros, Evan S., Pollpeter, Kevin L. & Cliff, Roger: *Dangerous Thresholds: Managing Escalation in the 21st Century*. RAND, Santa Monica, 2008.

Mueller, Karl P., Castillo, Jasen J. & Morgan, Forrest E. (et al.): *Striking First: Preemptive and Preventive Attack in U.S. National Security Policy*. RAND, Santa Monica, 2006.

Mueller, Milton: *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace.* Polity, Cambridge, UK, 2017.

Musiani, Francesca, Cogburn, Derrick L., DeNardis, Laura & Levinson, Nanette S. (Eds.): *The Turn to Infrastructure in Internet Governance*. Palgrave Macmillan, New York, 2016.

Nye, Joseph S. Jr.: *The Future of Power*. PublicAffairs, New York, 2011.

O'Hagan, Jacinta: *Conceptualizing the West in International Relations: From Spengler to Said*. Palgrace, New York, 2002.

Olsen, John Andreas: *Routledge Handbook of Air Power*. Routledge, Abingdon, Oxon, 2018.

Paret, Peter (ed.): *Makers of Modern Strategy from Machiavelli to the Nuclear Age*. Clarendon Press, Oxford, 1990.

Parsons, Talcott: *Social Systems and the Evolution of Action Theory*. Free Press, New York, 1977.

Perrow, Charles: *Normal Accidents: Living with High Risk Technologies (*updated edition*)*. Princeton University Press, Princeton, 1999.

Persson, Gudrun (ed.): *Russian Military Capability in a Ten-Year Perspective – 2016*. FOI, Stockholm, 2016.

Peters, Benjamin: *How Not to Network a Nation: The Uneasy History of the Soviet Internet*. The MIT Press, Cambridge, 2016.

Pomeranz, William E.: *Law and the Russian State: Russia's Legal Evolution from Peter the Great to Vladimir Putin*. Bloomsbury, London & New York, 2019.

Porfiriev, Boris & Simons, Greg (Eds.): *Crisis in Russia: Contemporary Management Policy and Practice from a Historical Perspective*. Routledge, New York, 2016 (org. 2012).

Pynnöniemi, K. (ed.): *Nexus of Patriotism and Militarism in Russia: A Quest for Internal Cohesion*. Helsinki University Press, Helsinki, 2021.

Radin, Andrew, Demus, Alyssa & Marcinek, Krystyna: *Understanding Russian Subversion Patterns, Threats, and Responses*. RAND, Santa Monica CA, 2020.

Raitasalo, Jyri: *Constructing War and Military Power After the Cold War: The Role of the United States in the Shared Western Understandings of War and Military Power in the Post-Cold War Era*. National Defence College, Series 1, Strategic Research No. 21, Helsinki, 2005.

Rantanen, Hannu: *Tilannekuvan tuottaminen, hyödyntäminen ja jakaminen - Kriittinen nykytilan tarkastelu*. Aluehallintovirastojen julkaisuja 42/2018, Vaasa, 2018.

Rattray, Gregory J.: *Strategic Warfare in Cyberspace*. MIT Press, Cambridge, 2001.

Rautava, Jori-Pekka & Ristolainen, Mari: Cyberterritory: An Exploration of the Concept *Proceedings of the 21st European Conference on Cyber Warfare and Security A Conference hosted by the University of Chester UK 16-17 June 2022*. Eze, Thaddeus, Khanand, Nabeel & Onwubiko, Cyril (eds.), pp. 239–246.

Reach, Clint, Kilambi, Vikram & Cozad, Mark: *Russian Assessments and Applications of the Correlation of Forces and Means*. RAND, Santa Monica, 2020.

Renz, Bettina & Smith, Hanna: *Russia and Hybrid Warfare: Going Beyond the Label*. Aleksanteri Papers 1/2016. Aleksanteri Institute, Helsinki, 2016.

Rid, Thomas: *Cyber War Will Not Take Place*. Oxford University Press, Oxford, 2017.

Rid, Thomas: *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux, London, 2020.

Ripsman, Norrin M., Taliaferro, Jeffrey W. & Lobell, Steven E.: *Neoclassical Realist Theory of International Relations*. Oxford University Press, New York, 2016.

Russell, A. L.: *Cyber Blockades*. Georgetown University Press, Washington DC, 2014.

Sakwa, Richard: *The Putin Paradox*. I. B. Taurus, London, 2020.

Sanastokeskus TSK: *Kyberturvallisuuden sanasto TSK 52*. Sanastokeskus TSK, Helsinki, 2018.

Sanger, David, E.: *The Perfect Weapon. War, Sabotage, and Fear in the Cyber Age*. Scribe, London, 2019.

Schelling, T. C.: *Arms and Influence*. Yale University Press, New Haven, 2008.

Schmitt, Michael N. (ed.): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, Cambridge, 2013.

Sloan, Elinor C.: *Modern Military Strategy: An introduction.* Routledge, New York, 2012.

Smith, Rupert: *The Utility of Force: The Art of War I the Modern World*. Vintage Books, New York, 2008.

Soldatov, Andrei & Borogan, Irina: *The Red Web. The Struggle Between Russia's Digital Dictators and The New Online Revolutionaries*. Public Affairs, New York, 2015.

Strachan, Hew: *The Direction of War: Contemporary Strategy in Historical Perspective*. Cambridge University Press, New York, 2013.

Susiluoto, Ilmari: *Suuruuden laskuoppi: Venäläisen tietoyhteiskunnan synty ja kehitys*. WSOY, Juva, 2006.

Svechin, Aleksandr A.: *Strategy*. East View Information Services, Minneapolis, Minnesota, 1992.

The Finnish Ministry of Defence: *Russia of Power*. Punamusta, Helsinki, 2019.

Thomas, Timothy: Russian Military Thought: Concepts and Elements. MITRE Corporation, McLean VA, 2019.

Thurner, Stefan, Hanel, Rudolf & Klimek, Peter: *Introduction to the Theory of Complex Systems*. Oxford, Oxford University Press, 2018.

Tikk, Eneken & Kerttunen, Mika (Eds.): *Routledge Handbook of International Cybersecurity*. Routledge, London and New York, 2020.

Tikk-Ringas, Eneken (ed.): *Evolution of the Cyber Domain. The Implications for National and Global Security*. IISS, London, 2015.

Treisman, Daniel (ed.): *The New Autocracy: Information, Politics, and Policy in Putin's Russia*. Brookings Institution Press, Washington, D.C., 2018.

Valeriano, Brandon & Maness, Ryan C.: *Cyber War versus Cyber Realities Cyber Conflict in the International System*. Oxford University Press, New York, 2015.

Valeriano, Brandon, Jensen, Benjamin & Maness, Ryan C.: *Cyber Strategy: The Evolving Chracter of Power and Coercion*. Oxford University Press, New York, 2018.

Vasara, Antti: *Theory of Reflexive Control: Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy*. Finnish Defence Studies 22. National Defence University, Helsinki, 2020.

Waldrop, Mitchell M.: *The Emerging Science at the Edge of Order and Chaos*. Touchstone, New York, 1992.

Weinberg, Gerald M.: *An Introduction to General Systems Thinking*. Dorset House Publishing, New York, 2001.

Whyte, Christopher & Mazanec, Brian: *Understanding Cyber Warfare. Politics, Policy and Strategy*. Routledge, London and New York, 2019.

Whyte, Christopher A., Thrall, Trevor & Mazanec, Brian M.: *Information Warfare in the Age of Cyber Conflict*. Routledge, London, 2020.

Williams, Paul D. (ed.): *Security Studies: an Introduction*. Routledge, London, 2008.

Wortzel, Larry M.: *The Chinese People's Liberation Army And Information Warfare*. Strategic Studies Institute and U.S. Army War College Press, Carlisle Barracks, PA, 2014.

Wylie, J. C.: *Military Strategy: A General Theory of Power Control*. Naval Institute Press, Annapolis Maryland, 2014.

Yarger, Harry R.: *Strategic Theory for the 21st Century: The Little Book on Big Strategy*. Strategic Studies Institute, U.S. Army War College, Carlisle, PA, 2006.

Yarynich, Valeri E.: *C3: Nuclear Command, Control, Cooperation*. Center for Defence Information, Washington, D.C., 2003.

1.3 Articles and online sources

Abdou, AbdelRahman, van Oorschot, Paul C. & Wan, Tao: Comparative Analysis of Control Plane Security of SDN and Conventional Networks. *IEEE Communications Surveys & Tutorials*, Vol. 20, No. 4, Fourth Quarter 2018, pp. 3542–3559.

Abelson, Harold, Anderson, Ross, Bellovin, Steven M., Benaloh, Josh, Blaze, Matt, Diffie, Whitfield, Gilmore, John, Green, Matthew, Landau, Susan, Neumann, Peter G., Rivest, Ronald L., Schiller, Jeffrey I., Schneier, Bruce, Specter, Michael A., Weitzner, Daniel J.: Keys under doormats: mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity*, Vol. 1, No. 1 (2015), pp. 69–79.

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), pp. 56–99.

Adamsky, Dmitry (Dima): From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture. *Journal of Strategic Studies*, Vol. 41, No. 1-2 (2018), pp. 33–60.

Alberts, David: The Future of Command and Control with DBK. In *Dominant Battlespace knowledge*. Libicki, Martin & Johnson, Stuart E. (eds.) NDU Press Book, Washington, D.C., 1995, pp. 28–38.

Ananthaswamy, Anil: The Quantum Internet Is Emerging, One Experiment at a Time. *Scientific American*, June 19, 2019. [https://www.scientificamerican.com/article/the-quantum-internet-is-emerging-one-experiment-at-a-time/], luettu 4.1.2021.

Arreguín-Toft, Ivan: Contemporary Asymmetric Conflict Theory in Historical Perspective. *Terrorism and Political Violence*, Vol. 24, No. 4 (2012), pp. 635–657.

Arreguin-Toft, Ivan: How the Weak Win Wars: A Theory of Asymmetric Conflict. *International Security*, Vol. 26, No. 1 (2001), pp. 93–128.

Article 19: Iran: *Tightening the Net 2020: After Blood and Shutdowns*. Article 19, London, 2020. [https://www.article19.org/wp-content/uploads/2020/09/TTN-report-2020.pdf], luettu 28.1.2021.

Ashraf, Cameran: Defining Cyberwar: Towards a Definitional Framework. *Defense & Security Analysis*, Vol. 37, No. 3 (2021), pp. 274–294.

Athans, Michael: Command and Control (C2) Theory: A Challenge to Control Science. *IEEE Transactions on Automatic Control*, Vol. AC-32, No. 4 (April 1987), pp. 286–293.

Austin, Greg & Sharma, Munish: From Cyber Resilience to Civil Defence. In *National Cyber Emergencies*. Austin, Greg (ed.) Routledge, London & New York, 2020, pp. 10–30.

Ayoub, Kareem & Payne, Kenneth: Strategy in the Age of Artificial Intelligence, *Journal of Strategic Studies*, Vol. 39, No. 5-6 (2016), pp. 793–819.

Banerjee, Sanjoy: Rules, Agency, and International Structuration. *International Studies Review*, Vol. 17, No. 2 (June 2015), pp. 274–297.

Bar-Joseph, Uri & Levy, Jack S.: Conscious Action and Intelligence Failure. *Political Science Quarterly*, Vol. 124, No. 3 (Fall 2009), pp. 461–488.

Barnett, M. & Duvall, R.: Power in International Politics. *International Organization*, Vol. 59, No. 1 (2005), pp. 39–75.

Biddle, Stephen & Oelrich, Ivan: Future Warfare in the Western Pacific: Chinese Antiaccess / Area Denial, U.S. AirSea Battle, and Command of the Commons in East Asia. *International Security*, Vol. 41, No. 1 (2016), pp. 7–48.

Blagden, David: Deterring Cyber Coercion: The Exaggerated Problem of Attribution. *Survival*, Vol. 62, No. 1 (2020), pp. 131–148.

Blank, Stephen: Rethinking the Concept of Asymmetric Threats in U.S. Strategy. *Comparative Strategy*, Vol. 23, No. 4-5 (2004), pp. 343–367.

Boardman, John & Sauser, Brian: System of Systems – the meaning of. *IEEE/SMC International Conference on System of Systems Engineering, Los Angeles, CA, USA, 2006*.

Borghard, Erica D. & Lonergan, Shawn W.: Cyber Operations as Imperfect Tools of Escalation. *Strategic Studies Quarterly*, Vol. 13, No. 3 (Fall 2019), pp. 122–145.

Brantly, Aaron F.: Entanglement in Cyberspace: Minding the Deterrence Gap. *Democracy and Security*, Vol. 16, No. 3 (2020), pp. 210–233.

Brantly, Aaron F.: The Cyber Deterrence Problem. In *10th International Conference on Cyber Conflict CyCon X: Maximising Effects*. Minárik, T., Jakschis, R. & Lindström, L. (eds.) NATO CCD COE, Tallinn, 2018, pp. 31–53.

Braw, Elisabeth & Brown, Gary: Personalised Deterrence of Cyber Aggression. *The RUSI Journal*, Vol.165, No.2 (2020), pp. 48–54.

Bruusgaard, Kristin Ven: Russian Concept of Deterrence. In *Russian Concept of Deterrence in Contemporary and Classic Perspective*. Pentti Forsström (ed.) National Defence University, Department Of Warfare, Series 2: Research Reports No. 11, Helsinki, 2022, pp. 9–20.

Bryant, David J.: Rethinking OODA: Toward a Modern Cognitive Framework of Command Decision Making. *Military Psychology*, Vol. 18, No. 3 (2006), pp. 183–206.

Burwell, Frances G. & Propp, Kenneth: *The European Union and the Search for Digital Sovereignty: Building "Fortress Europe" or Preparing for a New World?* Atlantic Council, 2020. [https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf], luettu 21.10.2020.

Byman, Daniel L. & Waxman, Matthew C.: Kosovo and the Great Air Power Debate. *International Security*, Vol. 24, No. 4 (Spring 2000), pp. 145–171.

Camino, Alex: *The never-ending software lifecycle*. The Softtek Blog, 31.1.2014. [https://blog.softtek.com/en/the-never-ending-software-lifecycle], luettu 21.2.2021.

Carvalho, M., Eskridge, T. C., Ferguson-Walter, K. & Paltzer, N.: MIRA: A Support Infrastructure for Cyber Command and Control Operations. *2015 Resilience Week (RWS), Philadelphia, PA, 18-20 Aug. 2015*.

Chase, Jesse: Defining Asymmetric Warfare: A Losing Proposition. *Joint Forces Quarterly*, Volume 61 (2nd Quarter 2011), pp. 115–120.

Checkland, Peter: Soft Systems Methodology: A Thirty-Year Retrospective. *Systems Research and Behavioral Science Syst. Res.* 17 (2000), pp. 11–58.

Chekov, Alexander D., Makarycheva, Anna V., Solomentseva, Anastasia M., Suchkov, Maxim A. & Sushentsov, Andrey A.: War of the Future: A View from Russia. *Survival*, Vol. 61, No. 6 (2019), pp. 25–48.

Chen, Jim Q.: A Strategic Decision-Making Framework in Cyberspace. In *Developments in information security and cybernetic wars*. Sarfraz, Muhammad (ed.) IGI Global, Hershey, PA, 2019, pp. 64–75.

Chen, Jim: Cyberdeterrence by Engagement and Surprise. *PRIMS*, Vol. 7, No. 2 (2017), pp. 100–107.

Cimbala, S. J.: Accidental/Inadvertent Nuclear War and Information Warfare. *Armed Forces & Society*, Vol. 25, No.4 (1999), pp. 653–675.

Cimbala, Stephen J.: Nuclear Deterrence and Cyber Warfare: Coexistence or Competition? *Defense & Security Analysis*, Vol. 33, No. 3 (2017), pp. 193–208.

Conti, Gregory, Nelson, John & Raymond, David: Towards a Cyber Common Operating Picture. In *2013 5th International Conference on Cyber Conflict*. Podins, K., Stinissen, J. & Maybaum, M. (Eds.) NATO CCD COE Publications, Tallinn, 2013, pp. 179–295.

Correll, John T.: The Assault on EBO. The Cardinal Sin of Effects-Based Operations Was That It Threatened the Traditional Way of War. *Air Force Magazine*, Vol. 96, No. 1 (January 2013), pp. 50–53.

Dear, Keith: Will Russia Rule the World Through AI? *The RUSI Journal*, Vol. 164, No. 5-6 (2019), pp. 36–60.

Demchak, Chris & Dombrowski, Peter: Rise of the Cybered Westphalian Age. *Strategic Studies Quarterly*, Vol. 5, No. 1 (Spring 2011), pp. 32–61.

Demchak, Chris: Cybered Conflict, Cyber Power, and Security Resilience as Strategy. In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Reveron, Derek (ed.) Georgetown University Press, Washington, D.C., 2012, pp. 121–136.

Drake, William J., Cerf, Vinton G. & Kleinwächter, Wolfgang: *Future of the Internet Initiative White Paper. Internet Fragmentation: An Overview*. World Economic Forum, January 2016. [https://www.itu.int/net4/wsis/forum/2016/Agenda/Session/169], luettu 9.2.2018.

Dunn Cavelty, Myriam & Wenger, Andreas: Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science. *Contemporary Security Policy*, Vol. 41, No. 1 (2020), pp. 5–32.

Durand, Alain: *New IP. ICANN Office of the Chief Technology Officer, 27 October 2020*. [https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf], luettu 6.1.2021.

Echevarria, Antulio J.: Deconstructing the Theory of Fourth-Generation War. *Contemporary Security Policy*, Vol. 26, No. 2 (2005), pp. 233–241.

Elbanna, Said: Strategic Decision-Making: Process Perspectives. *International Journal of Management Reviews*, Vol. 8 No. 1 (2006), pp. 1–20.

Endresen, R. S.: Hard Power in Cyberspace: CNA as a Political Means. In *Cyber Power*. Pissanidis, N., Rõigas, H., Veenendaal, M. (Eds.) NATO CCD COE, Tallinn, 2016.

Endsley, M. R.: Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, Vol. 37, No. 1 (1995), pp. 32–64.

Eriksson, Johan & Rhinard, Mark: The Internal–External Security Nexus: Notes on an Emerging Research Agenda. *Cooperation and Conflict*, Special Issue on The Internal-External Nexus, Vol. 44, No. 3 (September 2009), pp. 243–267.

Esmark, Anders: The Functional Differentiation of Governance: Public Governance Beyond Hierarchy, Market and Networks. *Public Administration*, Vol. 87, No. 2 (2009), pp. 351–370.

Evans, M.: Elegant Irrelevance Revisited: A Critique of Fourth-Generation Warfare. *Contemporary Security Policy*, Vol. 26, No. 2 (2005), pp. 242–249.

Fischerkell, Michael P. & Harknett, Richard J.: Deterrence Is Not a Credible Strategy for Cyberspace (and What Is). *Orbis,* Vol. 61, No. 3 (2017), pp. 381–393.

Fischerkeller, Michael P. & Harknett, Richard J.: Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation. *The Cyber Defense Review*, Special Edition: International Conference on Cyber Conflict (CYCON U.S.), November 14-15, 2019, pp. 267–287.

Fitzgerald, Mary: Russian Views on IW, EW, and Command and Control: Implications for the 21st Century. *Command & Control Research & Technology Symposium, 1999. U.S. Naval War College, Rhode Island. June 29 - July 1, 1999.*
[http://www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/089fitzg.pdf], luettu 5.8.2018.

Fitzpatrick, Mark: Artificial Intelligence and Nuclear Command and Control. *Survival*, Vol.61, No.3 (2019), pp. 81–92.

Fitzsimmons, Michael: The False Allure of Escalation Dominance. *War on the Rocks*, November 16, 2017. [https://warontherocks.com/2017/11/false-allure-escalation-dominance/], luettu 27.11.2020.

Fjäder, Christian: The Nation-state, National Security and Resilience in the Age of Globalisation. *Resilience*, Vol.2, No.2 (2014), pp. 114–129.

Freedman, Lawrence: Asymmetric Wars. *Adelphi Papers*, Vol. 38, No. 318 (1998), pp. 33–48.

Freedom House: *Freedom on the Net 2017: Russia, 2017*. [https://freedomhouse.org/report/freedom-net/2017/russia], luettu 11.1.2018.

Freedom House: *Freedom in the World – 2022: Russia*. [https://freedomhouse.org/country/russia/freedom-world/2022], luettu 22.9.2022.

Futter, Andrew: War Games Redux? Cyberthreats, US–Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control. *European Security*, Vol. 25, No. 2 (2016), pp. 163–180.

Gartzke, Erik J. & Lindsay, Jon R.: Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies*, Vol. 24, No. 2 (2015), pp. 316–348.

Gartzke, Erik: Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth. *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 41–73.

Gatlan, Sergiu: SolarWinds Victims Revealed after Cracking the Sunburst Malware DGA. *Bleeping Computer*, December 22, 2020. [https://www.bleepingcomputer.com/news/security/solarwinds-victims-revealed-after-cracking-the-sunburst-malware-dga/], luettu 28.12.2020.

Geers, Kenneth: The Cyber Threat to National Critical Infrastructures: Beyond Theory. *Information Security Journal*: A Global Perspective, Vol. 18, No. 1 (2009), pp. 1–7.

Geist, Edward: Deterrence Stability in the Cyber Age. *Strategic Studies Quarterly*, Vol. 9, No. 4 (Winter 2015), pp. 44–61.

Gerring, John: What Is a Case Study and What Is It Good for? *The American Political Science Review*, Vol. 98, No. 2 (May, 2004), pp. 341–354.

Gibson, Irving M.: The Maginot Line. *The Journal of Modern History*, Vol. 17, No. 2 (June, 1945), pp. 130–146.

Gioe, David V., Lovering, Richard & Pachesny, Tyler: The Soviet Legacy of Russian Active Measures: New Vodka from Old Stills? *International Journal of Intelligence and CounterIntelligence*, Vol. 33, No. 3 (2020), pp. 514–539.

Glaser, Charles L.: The Security Dilemma Revisited. *World Politics*, Vol. 50, No. 1 (1997), pp. 171–201.

Glaser, Charles L.: Why do Strategists Disagree about the Requirements of Strategic Deterrence? In *Nuclear Arguments: Understanding the Strategic Nuclear Arms and Arms Control Debates*. Eden, Lynn & Miller, Steven E. (Eds.) Cornell University Press, Ithica, NY, 1989, pp. 109–171.

Goel, Sanjay: How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race. *Connections*, Vol. 19, No. 1 (Winter 2020), pp. 87–95.

Gold, Josh: *The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'*. NATO CCD COE, Tallinn, 2020. [https://ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf], luettu 19.2.2021.

Goldman, Emily O. & Ross, Andrew, L.: Conclusion: The Diffusion of Military Technology and Ideas – Theory and Practice. In *The Diffusion of Military Technology and Ideas*. Goldman, Emily O. & Eliason, Leslie C. (eds.) Stanford University Press, Stanford, CA, 2003, pp. 371–403.

Green, Brendan R. & Long, Austin: The MAD Who Wasn't There: Soviet Reactions to the Late Cold War Nuclear Balance. *Security Studies*, Vol. 26, No. 4 (2017), pp. 606–641.

Guerlac, H.: Vauban: The Impact of Science of War. In *Makers of Modern Strategy from Machiavelli to the Nuclear Age*. Paret, Peter (ed.) Clarendon Press, Oxford, 1990, pp. 64–90.

Habermas, Jürgen: Talcott Parsons: Problems of Theory Construction. *Social Inq*. Vol 51, No. ¾ (1981), pp. 173–196.

Harknett, Richard J. & Nye, Joseph S. Jr.: Correspondence – Is Deterrence Possible in Cyberspace. *International Security*, Vol. 42, No. 2 (2017), pp. 196–199.

Harknett, Richard J. & Smeets, Max: Cyber Campaigns and Strategic Outcomes. *Journal of Strategic Studies*, Vol. 45, No. 4 (2022), pp. 534–567.

Hartmann, Kim & Steup, Christoph: Hacking the AI – the Next Generation of Hijacked Systems. In *2020 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade*. Jančárkova, Lindström, L., Signoretti, M., Tolga, I. & Visky, G. (eds.). CCD COE Publications, Tallinn, 2020, pp. 327–349.

Healey, Jason & Jervis, Robert: The Escalation Inversion and Other Oddities of Situational Cyber Stability. *Texas National Security Review*, Vol. 3, No. 4 (Fall 2020), pp. 30–53.

Heylighen, Francis, Joslyn Cliff & Turchin Valentin: What are Cybernetics and Systems Science? *Principia Cybernetica Web (Principia Cybernetica, Brussels), 1999*. [http://pespmc1.vub.ac.be/CYBSWHAT.html], luettu 7.7.2020.

Heylighen, Francis: *Web Dictionary of Cybernetics and Systems*. [http://pespmc1.vub.ac.be/ASC/INDEXASC.html], luettu 23.9.2019.

Hitchins, D. K.: A General Theory of Command and Control. *1989 Third International Conference on Command, Control, Communications and Management Information Systems, Bournemouth, UK, 1989*, pp. 111–126.

Hobbs, Carla (ed.): *Europe's Digital Sovereignty: From Rulemaker to Superpower in the Age of US-China Rivalry*. European Council on Foreign Relations, July 2020. [https://www.ecfr.eu/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf], luettu 17.10.2020.

Honig, Or Arthur & Zimskind, Sarah: Not Completely Blind: What Dictators Do to Improve Their Reading of the World. *Comparative Strategy*, Vol. 36, No. 3 (2017), pp. 241–256.

Humbert, Clemence & Joseph, Jonathan: Introduction: The Politics of Resilience: Problematising Current Approaches. *Resilience*, Vol. 7, No. 3 (2019), pp. 215–223.

Hutchins, Eric M., Cloppert, Michael J. & Amin, Rohan M.: *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*. [https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf], luettu 29.6.2020.

Ikenberry, John: The End of Liberal International Order? *Foreign Affairs*, Vol. 94, No. 1 (2018), pp. 7–23.

Inglis, John C., Lumpkin, Michael D., Waltzman, Rand & Watts, Clint: *Cyber-enabled Information Operations*. Subcommittee on Cybersecurity, Committee on Armed Services, United States Senate, One Hundred Fifteenth Congress, First Session, April 27, 2017.
[https://www.hsdl.org/?view&did=802817], luettu 21.2.2021.

International Telecommunication Union (ITU): *Global Cybersecurity Index & Cyberwellness Profiles*, April 2015. [https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf], luettu 15.9.2020.

Jensen, Benjamin, Valeriano, Brandon & Maness, Ryan: Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies*, Vol. 42, No. 2 (2019), pp. 212–234.

Jervis, R.: Dilemmas About Security Dilemmas. *Security Studies*, Vol. 20, No. 3 (2011), pp. 416–423.

Jervis, Robert: Review: Deterrence Theory Revisited. *World Politics*, Vol. 31, No. 2 (January 1979), pp. 289–324.

Johnson, James: Delegating Strategic Decision-making to Machines: Dr. Strangelove Redux? *Journal of Strategic Studies*, Vol. 45, No. 3, pp. 439–477.

Joseph, Jonathan: Resilience as Embedded Neoliberalism: A Governmentality Approach. *Resilience*, Vol. 1, No. 1 (2013), pp. 38–52.

Kallberg, Jan & Cook, Thomas S.: The Unfitness of Traditional Military Thinking in Cyber. Four Cyber Tenets That Undermine Conventional Strategies. *IEEE Access*, Vol. 5, 2017, pp. 8126–8130.

Kania, Elsa B & Costello, John: Seizing the Commanding Heights: The PLA Strategic Support Force in Chinese Military Power. *Journal of Strategic Studies*, Vol. 44, No. 2 (2021), pp. 218–264.

Kantola, Harry, Huttunen, Mika & Kiviharju, Mikko: Taistelun elementit kybertoimintaympäristössä. In *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, pp. 142–152.

Keizer, Gregg: Garden-variety DDoS Attack Knocks North Korea Off the Internet. Experts Cite the Fragility of North Korea's Connection, Note That Routine DDoS Attacks Could Have Easily Forced the Country Offline. *Computerworld*, 23.12.2014. [https://www.computerworld.com/article/2862652/garden-variety-ddos-attack-knocks-north-korea-off-the-internet.html], luettu 29.7.2021.

Kello, Lucas: The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 7–40.

Kim, Hyeob, Kwon, HyukJun & Kim, Kyung Kyu: Modified Cyber Kill Chain Model for Multimedia Service Environments. *Multimedia Tools and Applications*, Vol. 78 (2019), pp. 3153–3170.

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), pp. 36–62.

Kiviharju, Mikko & Huttunen, Mika: Kybertaktiikkaa – Yleisten periaatteiden soveltuvuudesta kybertoimintaympäristössä. In *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, pp. 161–180.

Klare, Michael T.: Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation. *Arms Control Today*, November 2019. [https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation], luettu 30.4.2020.

Klimburg, Alexander: Mixed Signals: A Flawed Approach to Cyber Deterrence. *Survival*, Vol.62, No.1 (2020), pp. 107–130.

Klimburg, Alexander: Mobilising Cyber Power. *Survival*, Vol. 53, No. 1 (2011), pp. 41–60.

Knopf, Jeffrey W.: The Fourth Wave in Deterrence Research. *Contemporary Security Policy*, Vol. 31, No. 1 (2010), pp. 1–33.

Konyshev, Valery & Sergunin, Alexander: Military. In *Tsyganov, Andrei P. (ed.) Routledge Handbook of Russian Foreign Policy*. Routledge, London and New York, 2018, pp. 168–181.

Kramer, Franklin D. & Teplinsky, Melanie J.: *Cybersecurity and Tailored Deterrence*. Atlantic Council, Washington DC., 2013.

Kristensen, Hans M.: *Obama and the Nuclear War Plan. Federation of the American Scientists Issue Brief, February, 2010*. [https://fas.org/programs/ssp/nukes/publications1/WarPlanIssueBrief2010.pdf], luettu 4.1.2021.

Kuehl, Daniel T.: *From Cyberspace to Cyberpower - Defining the Problem*. In *Cyberpower and National Security*. Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K., National Defence University Press, Washington, D.C., 2009, pp. 24–42.

Kukkola, Juha: Civilian and Military Information Infrastructure and the Control of the Russian Segment of Internet. *Presented at The International Conference on Military Communications and Information Systems (ICMCIS) Varsova, Puola, Toukokuu 22.-23., 2018*.

Kukkola, Juha: The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry. In *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Ertan, A., Floyd, K., Pernik, P. & Stevens, T. (Eds.) CCD COE, Tallinn, 2020b, pp. 9–30.

Kuusisto, Tuija: Tiedonhallinta päätöksenteossa kybertoimintaympäristössä. In *Kybertaistelu 2020*. Kuusisto, Tuija (toim.), Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2, No. 1/2014, Juvenes Print, Helsinki 2014, pp. 33–61.

Kärkkäinen, Anssi: Kyberpuolustuksen taistelukenttä nyt ja tulevaisuudessa. In *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, pp. 72–83.

Lee, Tony S., Ghosh, Sumit & Nerode, Anil: Asynchronous, Distributed, Decision-Making Systems with Semi-Autonomous Entities: A Mathematical Framework. *IEEE Transactions On Systems, Man, And Cybernetics—Part B: Cybernetics*, Vol. 30, No. 1, February 2000, pp. 206–212.

Lehto, Martti & Limnéll, Jarno: Kybersodankäynnin kehityksestä ja tulevaisuudesta. *Tiede- ja Ase*, Vol. 75 (2017), pp. 179–212.

Lehto, Martti: Kybertaistelun toimintaympäristön teoreettinen tarkastelu. In *Kybertaistelu 2020*. Kuusisto, Tuija (toim.) Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2, No. 1/2014, Juvenes Print, Helsinki, 2014, pp. 67–89.

Leuprecht, Christian, Szeman, Joseph & Skillicorn, David B.: The Damoclean Sword of Offensive Cyber: Policy Uncertainty and Collective Insecurity. *Contemporary Security Policy*, Vol. 40, No. 3 (2019), pp. 382–407.

Lewis, James A.: National Perceptions of Cyber Threats. *Strategic Analysis*, Vol. 38, No. 4 (2014), pp. 566–578.

Libicki, Martin C.: *What Is Information Warfare?* National Defense University, Institute for National Strategic Studies, Washington, D.C., 1995.

Libicki, Martin C.: The Conversion of Information Warfare. *Strategic Studies Quarterly*, Vol. 11, No. 1, (Spring 2017), pp. 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) pp. 401–428.

Lilly, Bilyana & Cheravitch, Joe: The Past, Present, and Future of Russia's Cyber Strategy and Forces. In 2020 *12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade*. T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, G. Visky (Eds.) NATO CCDCOE Publications, Tallinn, 2020, pp. 129–155.

Lin, Herbert: Attribution of Malicious Cyber Incidents: From Soup to Nuts. *Journal of International Affairs*, Vol. 70, No. 1 (Winter 2016), pp. 75–137.

Lind, William S.: *Maneuver Warfare Handbook*. Westview Press, Boulder, Colorado, 1985, pp. 6–7.

Lindsay, Jon R. & Gartzke, Erik: Politics by Many Other Means: The Comparative Strategic Advantages of Operational Domains. *Journal of Strategic Studies*, 2020 DOI: 10.1080/01402390.2020.1768372.

Lindsay, Jon R.: Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage. *Security Studies*, Vol. 29, No. 2 (2020), pp. 335–361.

Liuhto, Kari: Motivations of Russian Firms to Invest Abroad: How Do Sanctions Affect Russia's Outward Foreign Direct Investment? *Baltic Region*, Vol. 26, No. 4 (2015), pp. 4–19.

Long, Austin: A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning. *Journal of Cybersecurity*, Vol. 3, No. 1 (2017), pp. 19–28.

Lubin, Asaf: A New Era of Mass Surveillance is Emerging Across Europe. *Just Security*, January 9, 2017 [https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe/], luettu 12.1.2021.

Ma, Lin & Wang, Chaowei: Study of Decision-making Progress and Its Emergence in System of Systems. *2012 Prognostics & System Health Management Conference (PHM-2012 Beijing) 23-25 May 2012, Beijing, China.*

Mazarr, Michael J.: *Understanding Competition. Great Power Rivalry in a Changing International Order – Concepts and Theories*. RAND, Santa Monica, 2022.

Magd, Noora: Kybertaistelutila kybertoimintaympäristön sotilaallisena ulottuvuutena. In *Kyberajan viestitaktiikkaa.* Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, s.84–93.

Mahnken, Thomas G.: Cyber war and Cyber warfare. In *America's Cyber Future Security and Prosperity in the Information Age volume II*. Lord, Kristin M. and Sharp, Travis (ed.) Center for New American Security, 2011, pp. 57–64.

Mahnken, Thomas G.: The Future of Strategic Studies. *The Journal of Strategic Studies*, Vol. 26, No. 1 (2003), pp. x–xviii.

Manantan, Mark Bryan F.: Advancing Cyber Diplomacy in the Asia Pacific: Japan and Australia. *Australian Journal of International Affairs,* Vol.75, No.4 (2021), pp. 432–459.

Maness, R. C. & Valeriano, B.: Cyber spillover conflicts: Transition from cyber conflict to conventional foreign policy disputes. In *Conflict in Cyber Space: Theoretical, strategic and legal perspectives*. Routledge, New York, 2016, pp. 45–64.

Matthews, Earl D., Arata, Harold J. III & Hale, Brian L.: Cyber Situational Awareness. *The Cyber Defense Review*, Vol. 1, No. 1 (Spring 2016), pp. 35–46.

Mazarr, Michael J.: Virtual Territorial Integrity: The Next International Norm. *Survival*, Vol. 62, No. 4 (2020), pp. 101–118.

McDermott, Basil W.: Thinking about Herman Kahn. *The Journal of Conflict Resolution*, 1971, Vol. 15, No. 1 (Mar., 1971), pp. 55–70.

McDermott, Roger N.: *Russian Perspective on Network-Centric Warfare: The Key Aim of Serdyukov's Reform*. FMSO, Fort Leavenworth, Kansas, 2011.

Meakins, Joss: *Living in (Digital) Denial: Russia's Approach to Cyber Deterrence*. Euro-Atlantic Security Report. European Leadership Network, 2018. [https://www.europeanleadershipnetwork.org/report/living-in-digital-denial-russias-approach-to-cyber-deterrence/], luettu 29.4.2020.

Mikoyan, Sergo A.: Eroding the Soviet "Culture of Secrecy". *Studies in Intelligence*, Vol. 45, No. 5 (2001), pp. 45–56.

Milevski, Lucas: Asymmetry is Strategy, Strategy is Asymmetry. *JFQ*, Vol. 75, No. 4 (2014), pp. 77–83.

Miller, Benjamin: The Concept of Security: Should it be Redefined? *The Journal of Strategic Studies*, Vol. 24, No. 2 (2001), pp. 13–42.

Mingers, John & Standing, Craig: What is Information? Toward a Theory of Information as Objective and Veridical. *Journal of Information Technology*, Vol. 33 (2018), pp. 85–104.

MITRE: *ATT&CK Matrix for Enterprise.* [https://attack.mitre.org/matrices/enterprise/], luettu 29.6.2020.

Molloy, Steve & Schwenk, Charles R.: The Effects of Information Technology on Strategic Decision Making. *Journal of Management Studies*, Vol. 32, No. 3 (1995), pp. 283–311.

Morgan, Forrest E., Mueller, Karl P., Medeiros, Evan S., Pollpeter, Kevin L. & Cliff, Roger: *Dangerous Thresholds: Managing Escalation in the 21st Century*. RAND, Santa Monica, 2008.

Mulgund, Sandeep S. & Kelly, Mark D.: Command and Control of Operations in the Information Environment. Leading with Information in Operational Planning, Execution, and Assessment. *Air & Space Power Journal*, Vol. 34 No. 4 (Winter 2020), pp. 15–26.

Mälkki, Juha: Vaikutusperusteisen operatiivisen ajattelun (EBAO) sotataidolliset lähtökohdat. *Tiede ja Ase*, Vol 69 (2010), pp. 7–31.

Nagelhus Schia, Niels & Gjesvik, Lars: The Chinese Cyber Sovereignty Concept (Part 1). *The University of Nottingham's Asia Research Institute*, September 7, 2018. [https://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-1/], luettu 28.1.2021.

Nikkarila, Juha-Pekka & 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.*

Noble, Ben & Schulmann, Ekaterina: Not Just a Rubber Stamp. Parliament and Lawmaking. In *The New Autocracy: Information, Politics, and Policy in Putin's Russia*. Treisman, Daniel (ed.) Brookings Institution Press, Washington, D.C., 2018, pp. 47–78.

Nocetti, Julian: Contest and Conquest: Russia and Global Internet Governance. *International Affairs*, Vol. 91, No. 1 (2015), pp. 111–130.

Nye, Joseph S. Jr.: *ISSF Roundtable 10-6 on The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Discussion published by George Fujii on Friday, January 19, 2018. [https://networks.h-net.org/node/1252924/pdf], luettu 23.11.2020.

Nye, Joseph: Deterrence and Dissuasion in Cyberspace. *International Security*, Vol. 41, No. 3 (2016/2017), pp. 44–71.

Oehmen, Christopher & Multari, Nicholas: *AiR: Asymmetry in Resilience: Report on the First Meeting on Asymmetry in Resilience for Complex Cyber Systems*, U.S. Department of Energy, 2014. [https://cybersecurity.pnnl.gov/documents/AiR_1.0_Final_Report.pdf], luettu 15.4.2020.

Oliker, Oleg: Putinism, Populism and the Defence of Liberal Democrazy. *Survival*, Vol.59, No. 1 (February – March 2017), pp. 7–24.

Osinga, Frans: 'Getting' A Discourse on Winning and Losing: A Primer on Boyd's 'Theory of Intellectual Evolution'. *Contemporary Security Policy*, Vol. 34, No. 3 (2013), pp. 603–624.

Payne, Kenneth: Artificial Intelligence: A Revolution in Strategic Affairs? *Survival*, Vol. 60, No. 5 (2018), pp. 7–32.

Pernik, Piret: National Cyber Commands. In *Routledge Handbook of International Cybersecurity*. Tikk, Eneken & Kerttunen, Mika (eds.) Routledge, London, 2020.

Pigeau, Ross, & McCann, Carol: Re-conceptualizing Command and Control. *Canadian Military Journal*, Vol. 3, No 1. (Spring 2002), pp. 53–63.

Popescu, Ionut C: Grand Strategy vs. Emergent Strategy in the Conduct of Foreign Policy. *The Journal of Strategic Studies*, Vol. 41, No. 3, (2018), pp. 438–460.

Pynnöniemi, Katri & Busygina, Irina: Critical Infrastructure Protection and Russia's Hybrid Regime. *European Security*, Vol.22, No.4 (2013), pp. 559–575.

Raska, Michael: The sixth RMA wave: Disruption in Military Affairs? *Journal of Strategic Studies*, Vol. 44, No. 4 (2020), pp. 456–479.

Rathbun, Brian: A Rose by Any Other Name: Neoclassical Realism as the Logical and Necessary Extension of Structural Realism. *Security Studies*, Vol. 17, No. 2 (2008), pp. 294–321.

Rattray, Gregory J.: An Environmental Approach to Understanding Cyberpower. In *Cyberpower and National Security*. Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K. (Eds.) National Defence University Press, Washington, D.C., 2009, pp. 253–274.

Raymond, Mark: Puncturing the Myth of the Internet as a Commons. *Georgetown Journal of International Affairs, International Engagement on Cyber III: State Building on a New Frontier*, 2013, pp. 57–68.

Rid, T. & Buchanan, B.: Attributing Cyber Attacks. *Journal of Strategic Studies*, Vol. 35, No. 1 (2015), pp. 4–37.

Robinson, Neil & Milne, Sarah: Populism and Political Development in Hybrid Regimes: Russia and the Development of Official Populism. *International Political Science Review*, Vol. 38, No. 4, pp. 412–425.

Rose, Gideon: Neoclassical Realism and Theories of Foreign Policy. *World Politics*, Vol. 51, No. 1 (1998), pp. 144–172.

Rosnay, Joël de: *The Macroscope A new world scientific system*. Harper & Row, Publishers, New York, 1975. [http://pespmc1.vub.ac.be/macroscope/], luettu 23.9.2019.

Rowley, Jennifer: The Wisdom Hierarchy: Representations of the DIKW Hierarchy. *Journal of Information Science*, Vol. 33, No. 2 (2007), pp. 163–180.

Schiermeier, Quirin: Russia Aims to Revive Science After Era of Stagnation. Some Researchers See Promise in Planned Reforms. *Nature*, 18 March 2020. [https://www.nature.com/articles/d41586-020-00753-7], 7.7.2020.

Schörnig, Niklas: Neorealism. In *Theories of International Relations*. Schieder, Siegfried & Spindler, Manuela (ed.) Routledge, New York, 2015, pp. 37–55.

Schreier, Fred: *On Cyberwarfare*. DCAF Horizon 2015 Working Paper No. 7. [https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf], luettu 27.4.2020.

Scott, Mark: Welcome to New Era of Global Digital Censorship. It's Dangerous to Ask Tech Companies to Decide What's Legitimate Free Speech. *Politico*, January 14, 2018. [https://www.politico.eu/article/google-facebook-twitter-censorship-europe-commission-hate-speech-propaganda-terrorist/], luettu 12.1.2021.

Sengupta, Sailik, Chowdhary, Ankur, Sabur, Abdulhakim, Alshamrani, Adel, Huang, Dijiang & Kambhampati, Subbarao: A Survey of Moving Target Defenses for Network Security. *IEEE Communications Surveys & Tutorials 2020*, [https://arxiv.org/abs/1905.00964v2], luettu 11.1.2021.

Shahbaz, Adrian: *Freedom on the Net 2018. The Rise of Digital Authoritarianism*. Freedom House, 2019. [https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism], luettu 29.12.2020.

Sharp, Travis: Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony. *The Journal of Strategic Studies*, Vol. 40, No. 7 (2017), pp. 898–926.

Sheldon, John B.: The Rise of Cyberpower. In *Strategy in the Contemporary World* (4th ed.) Baylis, John, Wirtz, James J. & Gray, Colin S. (Eds.) Oxford University Press, Oxford, 2013, pp. 301–319.

Simovits, Mikael: Axiom För Cybersäkerhet: Ett Ryskt Perspektiv. 19 February 2021. [https://simovits.com/axiom-for-cybersakerhet-ett-ryskt-perspektiv/], luettu 22.9.2022.

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

Smeets, Max & Work, J.D.: Operational Decision-Making for Cyber Operations: In Search of a Model. *The Cyber Defense Review*, Vol. 5, No. 1 (2020), pp. 95–112.

Smith, Steve: The Increasing Insecurity of Security Studies: Conceptualizing Security in the Last Twenty Years. *Contemporary Security Policy*, Vol. 20, No. 3 (1999), pp. 72–101.

Snyder, Glenn H.: Deterrence and Power. *The Journal of Conflict Resolution*, Vol. 4, No. 2 (1960), pp. 163–178.

Sokhey, Sarah Wilson: What Does Putin Promise Russians? Russia's Authoritarian Social Policy. *Orbis*, Vol. 64, No. 3 (2020), pp. 390–402.

Soldatov, Andrei: From the "New Nobility" to the KGB. *Russian Politics and Law*, Vol. 55, No. 2 (2017), pp. 133–146.

Stevens, Tim: A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy*, Vol. 33, No. 1 (2012), pp. 148–170.

Stevens, Tim: Knowledge in the Grey Zone: AI and Cybersecurity. *Digital War,* Vol. 1 (2020) pp. 164–170.

Strachan, Hew: Strategy in Theory, Strategy in Practice. *Journal of Strategic Studies*, Vol. 42, No. 2 (2019), pp. 171–190.

Taillat, Stéphane: Disrupt and Restraint: The Evolution of Cyber Conflict and the Implications for Collective Security. *Contemporary Security Policy*, Vol. 40, No. 3 (2019), pp. 368–381.

Thomas, Timothy L.: Russian Views on Information-Based Warfare. *Airpower Journal* – Special Edition 1996, pp. 26–35.

Thomas, Timothy: Nation-state Cyber Strategies: Examples from China and Russia. In *Cyberpower and National Security*. Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K. (Eds.) National Defence University Press, Washington, D.C., 2009, pp. 465–488.

Thomas, Timothy: 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), pp. 554–575.

Thornton, Rod & Miron, Marina: Towards the 'Third Revolution in Military Affairs'. *The RUSI Journal*, Vol. 165, No. 3 (2020), pp. 12–21.

Tor, Uri: 'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence. *The Journal of Strategic Studies*, Vol. 40, No. 1-2 (2017), pp. 92–117.

Turunen, Maija & Kari, Martti J.: Cyber Deterrence and Russia's Active Cyber Defense. In *Proceedings of the 19th European Conference on Cyber Warfare and Security. A Virtual Conference hosted by University of Chester UK 25-26 June 2020*. Thaddeus Exe, Lee Speakman & Cyril Onwubiko (Eds.), pp. 526–532.

Van Bezooijen, B. J. A., Essens, P. J. M. D. & Vogelaar, A. L. W.: Military Self-synchronization: An Exploration of the Concept. *11TH ICCRTS, Coalition Command and Control in The Networked Era 27 September 2006*.

Vego, Milan: Effects-Based Operations: A Critique. *Joint Forces Quarterly,* Vol. 41, No. 2 (2006), pp. 51–57.

Vendil Pallin, Carolina: Internet Control Through Ownership: The Case of Russia. *Post-Soviet Affairs*, Vol. 33, No. 1 (2017), pp. 16–33.

Vendil, Carolina: The Russian Security Council. *European Security*, Vol.10, No.2 (Summer 2001), pp. 67–94.

Warren, Tom: Microsoft Bids Farewell to Windows 7 and the Millions of PCs That Still Run It: An End of the Traditional Windows Era. *The Verge*, 14.1.2020. [https://www.theverge.com/2020/1/14/21065122/microsoft-windows-7-end-of-support-lifecycle-millions-pcs], luettu 5.1.2021.

Wheeler, N. J.: British Nuclear Weapons and Anglo-American Relations 1945-54. *International Affairs*, Vol. 62, No. 1 (Winter, 1985-1986), pp. 71–86.

Whyte, Christopher: Beyond Tit-for-tat in Cyberspace: Political Warfare and Lateral Sources of Escalation Online. *European Journal of International Security*, Vol. 5, No. 2 (2020), pp. 195–214.

Willett, Marcus: Assessing Cyber Power. *Survival*, Vol.61, No.1 (2019), pp. 85–90.

Williams, Martyn: How the Internet Works in North Korea. *Slate*, November 28, 2016. [https://slate.com/technology/2016/11/how-the-internet-works-in-north-korea.html], luettu 28.1.2021.

Wilner, Alex S.: US Cyber Deterrence: Practice Guiding Theory. *Journal of Strategic Studies*, Vol.43, No.2 (2020), pp. 245–280.

Wirtz, J. J.: Life in the "Gray Zone": Observations for contemporary strategists. *Defense & Security Analysis*, Vol. 33, No. 2 (2017), pp. 106–114.

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), pp. 479–493.

1.4 Official English-language documents

Congressional Research Service: *Defense Primer: Information Operations, Updated December 15, 2020*. [https://fas.org/sgp/crs/natsec/IF10771.pdf], luettu 21.2.2021.

Congressional Research Service: *Defense Primer: Cyberspace Operations, December 1, 2021*. [https://sgp.fas.org/crs/natsec/IF10537.pdf], luettu 18.9.2022.

Cyberspace Solarium Commission: *End Report,* March 2020. [https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view], luettu 1.7.2020.

Defence Intelligence Agency: *Russia Military Power: Building a Military to Support Great Power Ambitions*, 2017. [http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf], luettu 8.7.2020.

ENISA: *An overview on enhancing technical cooperation between CSIRTs and LE*, May 07, 2020. [https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-tools-for-enhancing-cooperation-between-csirts-and-le], luettu 10.7.2020.

ENISA: *Critical Information Infrastructures Protection approaches in EU*, July 2015. [https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf], luettu 15.9.2020.

ENISA: *CSIRTs by Country - Interactive Map.* [https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map], luettu 10.7.2020.

ENISA: *EU Member States incident response development status report*, November 27, 2019 [https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report], luettu 10.7.2020.

ENISA: *National Cyber Security Strategies - Interactive Map* [https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map], luettu 12.1.2021.

ENISA: *Study on CSIRT landscape and IR capabilities in Europe 2025*, February 2019 [https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025/at_download/fullReport], luettu 12.1.2021.

ENISA: *Supply Chain Integrity. An overview of the ICT supply chain risks and challenges, and vision for the way forward*, Version 1.1, August 2015 [https://www.enisa.europa.eu/publications/sci-2015/at_download/fullReport], luettu 12.1.2021.

European Commission: *A European strategy for data*. COM(2020) 66 final, 19.2.2020. [https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066], luettu 12.1.2021.

European Commission: *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade*. Brussels, 16.12.2020 JOIN(2020) 18 final. [https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade], luettu 18.12.2020.

European Commission: *Reports and Studies about Digital Economy and Society Index*, 2020. [https://ec.europa.eu/digital-single-market/en/reports-and-studies/76018/3650], luettu 14.7.2020.

European Parliament: *Cyber defence in the EU Preparing for cyber warfare?* Briefing, October 2014. [https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf], luettu 21.2.2021.

Multinational Experiment 7: *Outcome 3 – Cyber Domain Objective 3.4 Cyber Situational Awareness Standard Operating Procedure. Version 1.0, 1 December 2012.* [https://www.hsdl.org/?view&did=760553], luettu 6.7.2020.

National Institute of Standards and Technology (NIST): *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, February 12, 2014*. [https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf], luettu 29.6.2020.

National Security Commission on Artificial Intelligence: *Final Report*, 2021. [https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf], luettu 6.3.2021.

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE): *Strategy and Governance* (webpage). [https://ccdcoe.org/library/strategy-and-governance/], luettu 14.7.2020.

NATO: *Allied Joint Doctrine for Cyberspace Operations, AJP-3.20, Edition A Version 1, January 2020*. NATO Standardization Office (NSO), 2020a. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf], luettu 13.7.2020.

NATO: *Military Strategic Level Decision Making within a (Future) Framework of Cyber Resilience*. STO-TR-SAS-116, 24.8.2020. NATO Unclassified Rel To PFP, 2020b. DOI: 10.14339/STO-TR-SAS-116.

NATO: *Wales Summit Declaration*. Press Release (2014) 120, Issued on 05 Sep. 2014. [https://www.nato.int/cps/en/natohq/official_texts_112964.htm], luettu 19.2.2021.

OECD: *Digital Security Risk Management for Economic and Social Prosperity*. OECD Recommendation and Companion Document, 2015. [https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf], luettu 12.1.2021.

Ross, Ron, Graubart, Richard, Bodeau, Deborah & Rosalie McQuaid: *Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems*. Draft NIST Special Publication 800-160 Volume 2, 2018. [https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf], luettu 1.5.2020.

The Department of the Army of the United States of America: *ADP 6-0 31 July 2019. Mission Command: Command and Control of Army Forces*. Headquarters Department of the Army, Washington D.C., 2019.

The United States Department of Defense (U.S. DoD): *Cyber Strategy – Summary, 2018*. [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF], luettu 5.5.2020.

The United States Department of Defense (U.S. DoD), Joint Staff Force Development (J7): *Cross-Domain Synergy in Joint Operations: Planner's Guide*, 14 January 2016. [http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cross_domain_planning_guide.pdf?ver=2017-12-28-161956-230], luettu 14.4.2020.

The United States Department of Defense (U.S. DoD): *DOD Dictionary of Military and Associated Terms, December, 2020*. [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2020-06-18-073638-727], luettu 11.1.2021.

The United States Department of Defense (U.S. DoD): *Joint Publication 3-13: Information Operations*; 27 November 2012 Incorporating Change 1 20 November 2014. [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf], luettu 11.1.2021.

The United States Department of Defense (U.S. DoD): *Joint Publication 3-0: Joint Operations* 2017, Incorporating Change 1 22 October 2018. [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27-160457-910], luettu 27.4.2020.

The United States Department of Defense (U.S. DoD): *Joint Publications 3-12: Cyberspace Operations, 8th June 2018*. [https://fas.org/irp/doddir/dod/jp3_12.pdf], luettu 17.10.2019.

The United States Department of Defence (U.S. DoD): *Fact Sheet: 2022 National Defense Strategy*. [https://media.defense.gov/2022/Mar/28/2002964702/-1/-1/1/NDS-FACT-SHEET.PDF], luettu 19.9.2022.

The United States Department of Justice: *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, May 19, 2014. [https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor], luettu 30.12.2020.

The United States Department of State: *Announcing the Expansion of the Clean Network to Safeguard America's Assets*. A Press Statement Michael R. Pompeo, Secretary of State August 5, 2020. [https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/], luettu 1.1.2021.

Vlacheas, Panagiotis T., Stavroulaki, Vera, Demestichas, Panagiotis, Cadzow, Scott & Slawomir Gorniak: *Ontology and taxonomies of resilience*. ENISA, 2011. [https://www.enisa.europa.eu/publications/ontology_taxonomies/at_download/fullReport], luettu 1.5.2020.

2 RUSSIAN MATERIAL

2.1 Literature

Вепринцев, В.Б., Манойло, А.В., Петренко, А.И. & Фролов, Д.Б.; *Операции информационно-психологической войны: краткий энциклопедический словарь-справочник*. Горячая линия – Телеком, Москва, 2011.

Комов, С.А. (под общ. редакцией). *Международная информационная безопасность: дипломатия мира*. Сборник статей. Военинформ, Москва, 2009.

Коцыняк М.А., Кулешов И.А., Кудрявцев А.М. & Лаута О.С.: *Киберустойчивость I Информационно-телекоммуникационной Сети*. Бостон-спектр, Санкт-Петербург, 2015.

Снесарев, А. Е. & Керсновский, А. А.: *Философия войны*. Вече, Москва, 2018.

Тюшкевич, С. А.: *О законах войны вопросы военной теории и методологии*. Проспект, Москва, 2017.

2.2 Articles and online sources

Агора: *Свобода интернета 2019: план «Крепость»*. [https://2019.runet.report/assets/files/Internet_Freedom%202019_The_Fortress.pdf], luettu 17.3.2020.

Аксенов, С.В.: Обеспечение устойчивости группировки стратегических ядерных сил в условиях информационного противоборства. *Вестник академии военных наук*, № 2 (67) (2019), с. 66–68.

Воейков, Денис: Власти хотят признавать «железо» российским за деньги. В этой идее нашлись «коррупциогенные факторы». *CNEWS*, 16.7.2021. [https://cnews.ru/link/n532505], luettu 28.7.2021.

Военный энциклопедический словарь *(ВЭС)*. Воениздат, Москва, 2007. [https://encyclopedia.mil.ru/encyclopedia/dictionary/list.htm], luettu 11.1.2021.

Гаврилюк, Анастасия & Шестоперов, Дмитрий: Отступный интернет Законопроект о бесплатном доступе к значимым сайтам предложено доработать. *Коммерсантъ* №38 от 05.03.2021. [https://www.kommersant.ru/doc/4713549], luettu 28.7.2021.

Гаврилюк, Анастасия: «Суверенный рунет» сочли угрозой стабильности. Операторы критикуют новые требования Роскомнадзора. *Коммерсантъ* №132, 29.07.2021. [https://www.kommersant.ru/doc/4919761?from=main_9], luettu 29.7.2021.

Гордеев, Владислав: Счетная палата не увидела прорывного эффекта от особых экономических зон. *РБК*, 9.4.2020.
[https://www.rbc.ru/economics/09/04/2020/5e8eb2679a79477a36b61c5f], luettu 8.7.2020.

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, с. 11–17.

Исакова, Татьяна: Непробиваемая интернет-изоляция. *Коммерсантъ*, 21.09.2022.
[https://www.kommersant.ru/doc/5571153], luettu 26.9.2022.

Касми, Эльяс: Минкомсвязи хочет влить миллиарды рублей в российскую мобильную ОС. *CNEWS*, 7.7.2020. [https://www.cnews.ru/news/top/2020-07-07_minkomsvyazi_hochet_vlit], luettu 7.7.2020.

Правительство России: Дмитрий Чернышенко: На пяти киберполигонах пройдут учения в 2021 году. *Правительство России* -webpage, 14.5.2021 [http://government.ru/news/42174/], luettu 31.7.2021.

РИА новости: Шойгу рассказал, как прозападная оппозиция "лезет" на военные объекты. *РИА новости*, 25.3.2020. [https://ria.ru/20200325/1569119235.html], luettu 6.5.2020.

Роскомсвобода: Ростелеком создаст киберполигон. *Роскомсвобода*, 06.12.2019.
[https://roskomsvoboda.org/53137/], luettu 12.1.2021.

Роскомсвобода: Путин заявил о том, что соцсети управляют сознанием человека. *Роскомсвобода*, 2.2.2021. [https://roskomsvoboda.org/69233/], luettu 1.3.2022.

Скрынникова, Анастасия, Бурмистрова, Светлана, Скобелев, Владислав & Чернышова, Евгения: Банки и ТЭК обяжут перейти на российское оборудование и софт к 2025 году. *РБК*, 2.11.2020. [https://www.rbc.ru/technology_and_media/02/11/2020/5f9c0f189a7947834b411b98?from=from_main_3https://www.rbc.ru/technology_and_media/02/11/2020/5f9c0f189a7947834b411b98?from=from_main_3], luettu 1.3.2022.

Степанова, Юлия, Занина, Анна & Гаврилюк, Анастасия: Техноложная тревога. Чем займутся российские IT-компании под санкциями США. *Коммерсантъ* №67, 16.04.2021.
[https://www.kommersant.ru/doc/4773434?from=main_5], luettu 29.7.2021.

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, с. 35–43.

Чернышова, Евгения & Балашова, Анна: Банки договорились с властями о постепенном переходе на российский софт Требование об импортозамещении должно вступить в силу с начала 2023 года. *РБК*, 16.7.2021. [https://www.rbc.ru/finances/16/07/2021/60f14f009a794702b097f76a?from=from_main_9], luettu 28.7.2021.

2.3 Official Russian documents

ПП-127a: Постановление Правительства РФ от 8 февраля 2018 г. N. 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.)
[http://pravo.gov.ru/proxy/ips/?docbody=&nd=102460750], luettu 22.2.2021.

Президент России: Указ о национальных целях развития России до 2030 года. *Kremlin.ru* 21.7.2020. [http://kremlin.ru/events/president/news/63728], luettu 31.7.2020.

РП-1632: Распоряжение Правительства РФ от 28.07.2017 N 1632-р *“Об утверждении программы "Цифровая экономика Российской Федерации"*.

[http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf], luettu 23.01.2018.

Указ-203: Указ Президента РФ от 09.05.2017 N 203 "*О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы*".
[https://www.garant.ru/products/ipo/prime/doc/71570570/], luettu 15.5.2019.

Указ-2976: Указ Президента РФ 25 декабря 2014 г., № Пр-2976. *Военная доктрина Российской Федерации.* [http://base.garant.ru/70830556/], luettu: 21 March 2019

Указ-355: Указ Президента РФ от 2.6.2019 N 355 "Об основах государственной политика Российской Федерации в области ядерного сдерживания".
[http://www.kremlin.ru/acts/bank/45562], luettu 30.12.2020.

Указ-646: Указ Президента РФ от 05.12.2016 N 646 *"Об утверждении Доктрины информационной безопасности Российской Федерации*".
[http://www.consultant.ru/document/cons_doc_LAW_208191/], luettu 5.5.2020.

ФЗ-123: Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 07.04.2020) "*О связи*". [http://www.consultant.ru/document/cons_doc_LAW_43224/], luettu 14.5.2020.

ФЗ-236: Федеральный закон от 01.07.2021 N 236-ФЗ "*О деятельности иностранных лиц в информационно-телекоммуникационной сети "Интернет" на территории Российской Федерации*". [http://publication.pravo.gov.ru/Document/View/0001202107010014?index=1&rangeSize=1], luettu 29.7.2021.

ФЗ-90: 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"*.
[http://www.consultant.ru/document/cons_doc_LAW_323815/], luettu 8.5.2019.

Центральный банк российской федерации: *Внешняя торговля Российской Федерации услугами - 2019*. Статистический сборник. Банк России, Москва, 2020.
[https://www.cbr.ru/statistics/macro_itm/svs/], luettu 12.1.2021.

APPENDIX 1

Information environment
Cyberspace
Socio-
Cognitive
space
Information-
physical space
Electro-
magnetic
space
Delineation
Construction
Control
Defence
Mobilisation
The National System of Systems of
Information Security and Defence
A map of a digital terrain
1. Scientific-
technological
industry
2.
Authentication
and
cryptography
system
3. Censorship
system
4. Monitoring
and data
collection
system
5. Critical
information
infrastructure
6. Active
measures
system
7. Military
systems and
networks
8.
Administration,
control,
monitoring and
feedback
systems
The model of the National System of Systems
of Information Security and Defence is
constructed by observing policies etc. related
to the national Internet segment and the
control of information space at large.
The national segment of the Internet is a
manifestation of a system of systems and an
applied version of a theoretical closed national
network