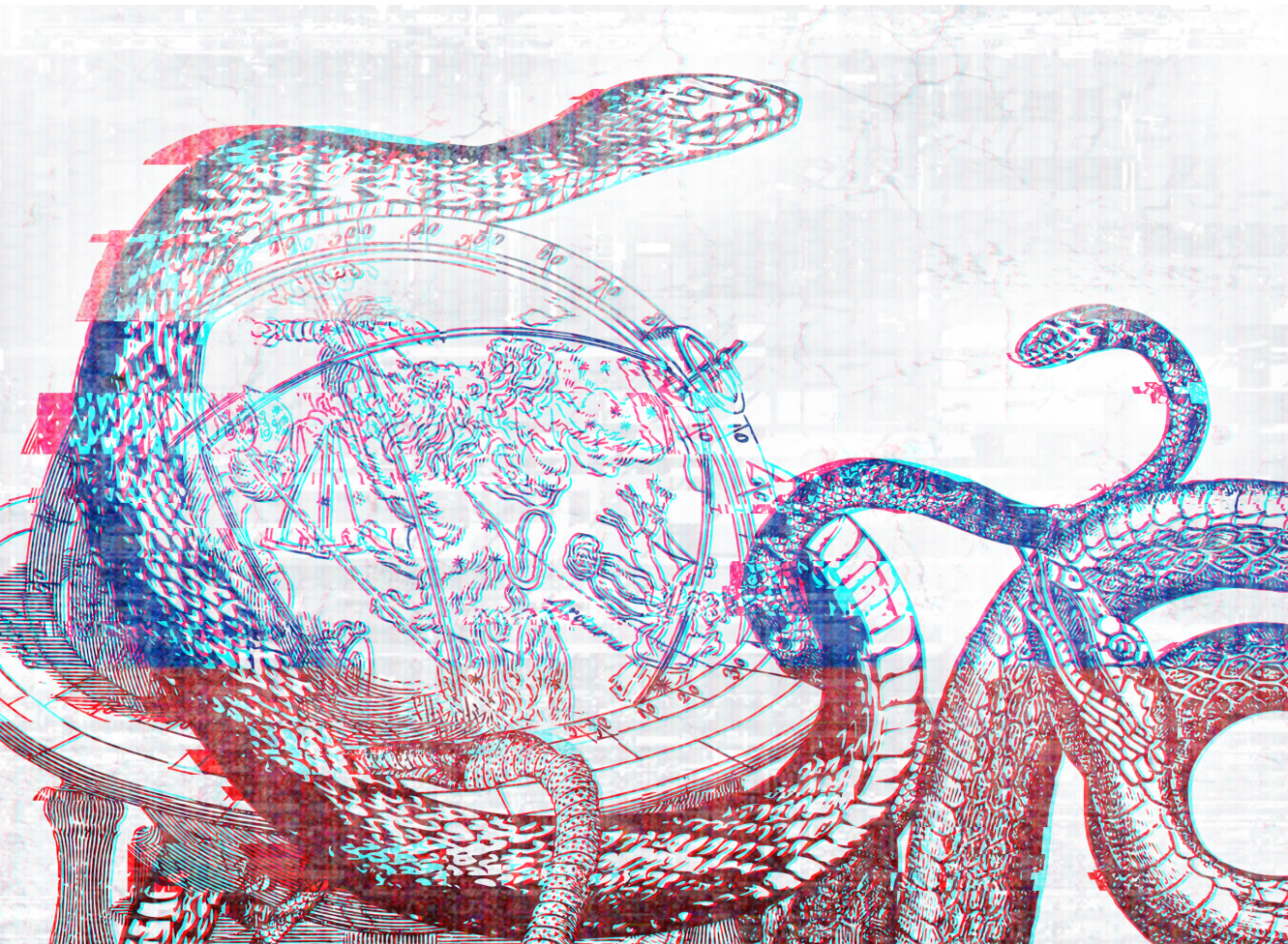
Maanpuolustuskorkeakoulu
Sotataidon laitos
Julkaisusarja 2: Tutkimusselosteita nro 31

Suvereenit hiekkamadot

Venäjän kybertoiminta osana valtioiden välistä kamppailua 2000-luvulla

Juha Kukkola



MAANPUOLUSTUSKORKEAKOULU
SOTATAIDON LAITOS
JULKAISUSARJA 2: TUTKIMUSSELOSTEITA NRO 31

NATIONAL DEFENCE UNIVERSITY
DEPARTMENT OF WARFARE
SERIES 2: RESEARCH REPORTS NO. 31

SUVEREENIT HIEKKAMADOT

Venäjän kybertoiminta osana valtioiden välistä kamppailua 2000-luvulla

Juha Kukkola

MAANPUOLUSTUSKORKEAKOULU
SOTATAIDON LAITOS
HELSINKI 2024

Juha Kukkola: *Suvereenit hiekkamadot – Venäjän kybertoiminta osana valtioiden välistä kamppailua 2000-luvulla*

Maanpuolustuskorkeakoulu
Sotataidon laitos
Julkaisusarja 2: Tutkimusselosteita nro 31
National Defence University
Department of Warfare
Series 2: Research Reports No. 31

Uusimmat julkaisut pdf-muodossa: *https://www.doria.fi/handle/10024/73990*

Kannen kuvateksti: *Suvereenit hiekkamadot ahdistavat maailmanlaajuista informaatiotilaa.*

Kannen kuva: Leevi Miettinen / MPKK

ISBN 978-951-25-3436-4 (nid.)
ISBN 978-951-25-3437-1 (PDF)
ISSN 2343-5275 (painettu)
ISSN 2343-5283 (verkkojulkaisu)

Maanpuolustuskorkeakoulu – Sotataidon laitos
National Defence University – Department of Warfare

PunaMusta Oy
Joensuu 2024

SISÄLTÖ

1. Johdanto 1
2. Strategisen kulttuurin ideat, informaatio ja kyber 5
3. Venäjän kyberpuolustus 2000–2021 19
   3.1. Kansallisen informaatiotilan turvallisuus ja puolustus 21
   3.2. Venäjän kyberpuolustajat 30
4. Venäjän hyökkäykselliset kyberoperaatiot 2000–2021 36
   4.1. Alkutaival: Vakoojat ja patriootit 37
   4.2. Maidanista eteenpäin: Informaatiokamppailu kiihtyy 41
5. Kybersodankäyntiä Ukrainassa 2022 52
   5.1. Valmistelu 2021–2022 53
   5.2. Hyökkäyksen alkuvaihe: Helmikuun loppu 2022 59
   5.3. Kaappaushyökkäys vaakalaudalla: Maaliskuun 2022 alku 63
   5.4. Kaappaushyökkäys epäonnistuu: Maaliskuu 2022 loppu 66
   5.5. Painopisteen siirto ja uudelleen ryhmittyminen: Huhtikuu 2022 68
   5.6. Taistelut kaakossa: Touko-kesäkuu 2022 70
   5.7. Pitkä sota alkaa: Heinä-elokuu 2022 73
   5.8. Harkovan vastahyökkäys ja ohjusiskut: Syys-lokakuu 2022 77
   5.9. Voimien kerääminen ohjusten varjossa: Marras-joulukuu 2022 79
   5.10. Yhteenveto vuodesta 2022 82
6. Kybersodankäyntiä Ukrainassa 2023 87
   6.1. Aloite kääntyy Ukrainalle: Tammi-huhtikuu 2023 87
   6.2. Vastahyökkäys epäonnistuu: Touko-elokuu 2023 92
   6.3. Kulutussotaa: Syys-joulukuu 2023 98
   6.4. Yhteenveto vuodesta 2023 103
7. Venäjän kyberturvallisuus ja -puolustus Ukrainan sodassa 2022–2023 110
8. Johtopäätökset 126

1. JOHDANTO

Tässä tutkimuksessa tarkastellaan Venäjän toimintaa kybertilassa[1] 2000-luvulla venäläisen, kybertoimintaan liittyvän strategiskulttuurisen[2] ajattelun kautta. Tutkimuksen päämääränä on lisätä ymmärrystä Venäjän kybertoiminnasta ja -strategiasta, jota on usein tulkittu vain Länteen kohdistuvien hyökkäyksellisten operaatioiden tai niiltä puolustautumisen näkökulmasta tai pelkästään Venäjän kansallisen informaatiotilan hallintaan liittyvänä kysymyksenä.[3] Tässä tutkimuksessa Venäjää tarkastellaan kybertilan aktiivisena valtiotoimijana, joka turvaa kansalliset intressinsä niin hyökkäyksellisin kuin puolustuksellisin keinoin. Tutkimuksen näkökulma ulottuu valtion politiikan tasolta aina yksittäisten operaatioiden toteuttamiseen. Tavoitteena on ymmärtää Venäjän valtiollisen kyberstrategian[4] lähtökohtia ja toimeenpanoa ja esittää venäläiseen sotataidolliseen ajatteluun[5] sidottu tulkinta Venäjän puolustuksellisen ja hyökkäyksellisen kybertoiminnan[6] kehityksestä. Erityisen tarkastelun kohteena on

[1] Kybertila on ihmisen luoma ja hallinnoima globaali tila informaatiotoimintaympäristön sisällä, jonka erityinen luonne perustuu elektroniikan ja elektromagneettisen spektrin käyttämiseen informaation luomiseksi, muokkaamiseksi, vaihtamiseksi ja hyödyntämiseksi toisiinsa liitettyjen informaatioteknologiaa käyttävien verkkojen kautta (Kukkola, Juha: *The Military Strategic Effects of the Russian National Segment of the Internet*. Finnish Defence Studies 23. National Defence University, Helsinki, 2023a, s. 10).

[2] Strategisen kulttuurin käsitteestä ks. Sondhaus, Lawrence: *Strategic Culture and Ways of War*. Routledge, New York, 2006; Uz Zaman, Rashid: Strategic Culture: A "Cultural" Understanding of War. *Comparative Strategy*, 28(1) 2009, s. 68–88.

[3] Aikaisemmista tutkimuksista Ks. esim. 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. Jyväskylän yliopisto, Jyväskylä, 2019; 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; Nocetti, Julian: Contest and conquest: Russia and Global Internet Governance. *International Affairs*, 91(1) 2015, s. 111–130; Vendil Pallin, Carolina: Russian information security and warfare. *Routledge Handbook of Russian Security*. Kanet, Roger E. (toim.) Routledge, London, 2019, s. 203–213; Connell, Michael & Vogler, Sarah: Russia's Approach to Cyber Warfare. CNA, Washington, DC, 2017; Sherman, Justin: Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behavior. Atlantic Council, 19.9.2022. [https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/], luettu 5.1.2024; Giles, Keir & Seaboyer, Anthony: The Russian Information Warfare Construct. DRDC, Kingston, 2019; Lilly, Bilyana & Cheravitch, Joe: The Past, Present, and Future of Russia's Cyber Strategy and Forces. *2020 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade*. T. Jančárková, L. Lindström, M. Signoretti, I. Tolga & G. Visky (Toim.) CCDCOE, Tallinn, 2020; Jensen, Benjamin, Valeriano, Brandon & Maness, Ryan: Fancy Bears and Digital Trolls: Cyber Strategy with a Russian Twist. *Journal of Strategic Studies*, 42(2), 2019, s. 212–234; Thomas, Timothy: Information Weapons: Russia's Nonnuclear Strategic Weapons of Choice. *The Cyber Defense Review*, 5(2), 2020, s. 125–144; Kantola, Harry: Categorizing Cyber Activity Through an Information-Psychological and Information-technological Perspective, Case Ukraine. *Proceedings of the 18th International Conference on Cyber Warfare and Security, 2023*. Wilson, Richard L. & Curran, Brendan (toim.) Towson University, Maryland, 2023, s. 480–488; Juutilainen, Jari: *Cyber Warfare: A Part of the Russo-Ukrainian War in 2022*. Pro gradu -tutkielma. Jyväskylän yliopisto, Jyväskylä, 2023; Giles, Keir: *Russian Cyber and Information Warfare in Practice Lessons Observed from the War on Ukraine*. Research paper. Chatham House, London, 2023; Kerr, Jaclyn A.: *Assessing Russian Cyber and Information Warfare in Ukraine: Expectations, Realities, and Lessons*. CNA, Washington D.C., 2023; Nilsson, Per-Erik: Unravelling the Myth of Cyberwar. FOI, Stockholm, 2023.

[4] Tässä tutkimuksessa strategia ymmärretään toimintana ja kyberstrategia kybertilaan liittyvänä toimintana. Strategisella toiminnalla tarkoitetaan valtion voimavarojen käyttöä ja käytön suunnittelua valtion turvallisuuspoliittisten päämäärien saavuttamiseksi rauhan ja sodan aikana. (ks. Kajanmaa, Petteri: *Sotilasstrategia. Yksinkertainen, vaikea sota*. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 2, Nro. 12, Helsinki, 2021, s. 6 & 19).

[5] Sotataito jaetaan venäläisittäin sotilasstrategiaan, operaatiotaitoon ja taktiikkaan. Se sisältää sekä sotatoimiin valmistautumisen että toimeenpanon. Mil.ru: Военный энциклопедический словарь, 'Военное искусство'. [https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=4366@morfDictionary], luettu 1.2.2024.

[6] Teoreettisesti puolustuksellisella kybertoiminnalla tarkoitetaan tässä tutkimuksessa kyberturvallisuuden ja -puolustuksen suunnittelua, rakentamista, järjestelmien operointia ja ylläpitoa sekä puolustuksellisia

Venäjän helmikuussa 2022 aloittama hyökkäysoperaatio Ukrainaan.[7] Lisäksi tutkimuksen tavoitteena on hankkia ja koota tietoa kybersodankäynnin[8] menetelmien kehittymisen ymmärtämiseksi ja kybertoiminnan merkityksen arvioimiseksi suurvaltojen kamppailun välineenä tulevaisuudessa.

Tämä tutkimus on Venäjän kyberstrategiaan kohdistuva laadullinen tapaustutkimus, jolla on vahva aikaleikkaava luonne. Tutkimus aloitetaan tarkastelemalla eräitä venäläisiä sotataidollisia käsitteitä koskien informaatiotilaa[9] ja valtion toimintaa siinä sekä informaatiosodankäyntiä[10]. Tarkasteluun valittujen käsitteiden katsotaan heijastavan Venäjän strategisen kulttuurin sisältämiä ideoita[11], jotka tekevät määrätyn toiminnan kybertilassa järkeenkäyväksi (reasonable) Venäjän valtiojohdon näkökulmasta.[12] Tutkimuksessa keskitytään informaatiotilan teknologiseen puoleen eli tietojärjestelmiin ja -verkkoihin ja niissä suoritettuihin operaatioihin, joista englanninkielisessä kirjallisuudessa tyypillisesti käytetään kyber-termistä johdettuja käsitteitä. Venäjän virallisissa asiakirjoissa kyber-termiä ei käytetä, mutta termi on muuten Venäjällä yleisesti käytetty ja ymmärretty läntisiä näkemyksiä vastaavalla tavalla.[13] Valittujen käsitteiden tarkastelu tehdään tutkimuksen toisessa luvussa käyttäen lähteinä venäläisten sotilasaikakausilehtien kirjoituksia ja aikaisempaa tutkimusta. Käsitteitä käytetään tutkimuksen seuraavissa luvuissa Venäjän kybertoimintaan liittyvien ilmiöiden ja tapahtumien tarkasteluun strategisessa, eli valtion voimavarojen käyttöön liittyvässä, ja sotataidollisessa kehyksessä.[14] Venäjän toimintaa ei selitetä strategisen kulttuurin kautta, vaan lähesty-

---

operaatioita omissa tai liittolaisen verkoissa. Hyökkäyksellisillä kyberoperaatioilla tarkoitetaan toisten verkoissa toteutettavia vihamielisiä operaatioita, joiden tavoitteena on hankkia tietoa tai tuhota tai estää sen käyttö tai manipuloida sitä. (Joint Chiefs of Staff, the U.S. Department of Defence. *Cyberspace operations* (Joint Publication 3-12), June 8th 2018. [https://fas.org/irp/doddir/dod/jp3_12.pdf], luettu 1.2.2024.

[7] Venäjän valtiojohto käyttää nimitys ”sotilaallinen erikoisoperaatio” (Специаальная военная операция). Tässä tutkimuksessa operaatio nähdään osana vuonna 2014 alkanutta Ukrainan ja Venäjän välistä sotaa.

[8] Kybersodankäynti on tarkoituksellisten ja vahinkoa tuottavien tietoverkkohyökkäyksien käyttämistä vastustajan siviili- tai sotilasinfrastruktuuria ja joukkoja vastaan voimapolitiikan osana. (Liff, Adam: Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, 35(3) 2012, s. 401–428.) Kybersota määritellään, eittämättä teoreettiseksi, sodan muodoksi, joka käydään vain kybertilassa tai sen kautta. (Mahnken, Thomas G.: Cyber war and Cyber warfare. *America's Cyber Future Security and Prosperity in the Information Age volume II*. Lord, Kristin M. and Sharp, Travis (Toim.) Center for New American Security, Washington, D.C., 2011, s. 57–64).

[9] Teoreettisena ilmiönä informaatiotilalla tarkoitetaan Naton käsitteistöä mukaillen informaatioympäristöä (information environment), joka on ”pääasiallinen päätöksentekoympäristö; jossa ihmiset ja automatisoidut järjestelmät tarkkailevat, hahmottavat, käsittelevät, suuntaavat, päättävät ja toimivat datan, informaation ja tiedon perusteella.” (NATO: *Allied Joint Publication-10.1: Allied Joint Doctrine for Information Operations*. NATO Standardization Office, Brussels, 2023, s. 15).

[10] Teoreettisena ilmiönä informaatiosodankäynnillä tarkoitetaan vihamielistä vaikuttamista valitun kohteen päätöksentekoon, toimintakykyyn ja mielipiteisiin informaatioympäristön kautta sekä suojautuminen toisten vastaavilta vaikuttamisyrityksiltä (Sanastokeskus TSK: *Kyberturvallisuuden sanasto*. Huoltovarmuuskeskus, Helsinki, 2018).

[11] Strategisen kulttuurin ideat ovat: “Episteemisiä yhteisöjä edustavien ihmisten, ja tämän seurauksena puolustus- ja turvallisuuseliittien, kausaalisia ja joskus periaatteellisia uskomuksia voimankäytöstä ja sillä uhkaamisesta, ja siitä kuinka keinot ja päämäärät sopivat yhteen valtion turvallisuusintressejä koskevissa asioissa.” (Kukkola (2020), s. ix)

[12] “Ideat vaikuttavat tapoihin, joilla valtio käyttää voimaa ajaakseen intressejään ja näin ideat muokkaavat todellisuutta voiman kautta. Toisin sanoen, ideat muokkaavat ymmärrystä ympäristöstä, antavat merkityksiä materiaaliselle voimalle, osoittavat hyväksyttävät ja ei-hyväksyttävät strategiset valinnat ja vaikuttavat omasta ja toisten voimasta tehtyihin tulkintoihin.” (Kukkola (2020), s. 389).

[13] Positive Technologies: Кибербезопасность - что это такое простыми словами, обеспечение компьютерной безопасности сети, 1.2.2024, [https://www.ptsecurity.com/ru-ru/research/knowledge-base/chto-takoe-kiberbezopasnost/], luettu 1.2.2024; Kaspersky: Что такое кибербезопасность? n.d. [https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security], luettu 1.2.2024.

[14] Strategialla tarkoitetaan tässä tutkimuksessa valtioiden välistä voimapolitiikkaa, mihin liittyvät mm. taivuttelu, pakottaminen, tuhoaminen ja pelote kaikilla valtioiden käytössä olevilla keinoilla. Sotataidolla tarkoitetaan

mistapa on pikemminkin ideoita ja toimintaa vertaileva eli yhtäläisyyksiä ja eroavaisuuksia, jatkuvuuksia ja katkoksia etsivä.

Venäläisen strategisen kulttuurin käsittelyn jälkeen tutkimuksen kolmannessa luvussa analysoidaan läntisten ja venäläisten uutislähteiden, virallisten asiakirjojen ja aikaisemman tutkimuksen kautta, miten Venäjän federaatio presidentti Vladimir Putinin kahdella jälkimmäisellä presidenttikaudella (2012–2024) rakensi kansallista informaatioturvallisuutta ja -puolustusta ja pyrki kohti digitaalista ja teknologista suvereniteettia. Analyysi tarkastelee, miten strategisen kulttuurin ideat kuten teknologinen suvereenisuus, informaatiokamppailu ja informaatioturvallisuuden järjestelmä auttavat ymmärtämään tapaa, jolla Venäjä on rakentanut kansallisen informaatiotilansa teknologista perustaa. Luvussa esitellään myös Venäjällä informaatioturvallisuudesta vastaavat organisaatiot. Tutkimuksen neljännessä luvussa analysoidaan aikaisemman tutkimuksen ja pääasiassa läntisten uutisten kautta Venäjän hyökkäyksellistä kybertoimintaa ajallisena jatkumona ennen Ukrainan hyökkäysoperaatiota 2000-luvun alusta vuoteen 2022. Analyysi erottelee Venäjän eri toiminnan muodot, toimijat, päämäärät ja kehityksen ja sitoo ne kansainvälispoliittiseen kehykseen. Analyysi tarkastelee, miten venäläiset ideat strategisesta deterrenssistä, informaatiosodankäynnistä ja -ylivoimasta ja informaatioteknologisista toimista auttavat ymmärtämään Venäjän toimintaa.

Tutkimuksen painopiste on Venäjän Ukrainaa vastaan helmikuussa 2022 aloittamaan strategiseen hyökkäysoperaatioon[15] liittyvien hyökkäyksellisten ja puolustuksellisten kybertoimien tarkastelussa. Tutkimuksen viidennessä ja kuudennessa luvussa esitetään läntisiin, venäläisiin ja ukrainalaisiin uutislähteisiin, virallisiin lausuntoihin ja asiakirjoihin sekä tietoturvayhtiöiden raportteihin ja aikaisempaan tutkimukseen[16] perustuen ja sodan tapahtumiin sitoen kronologinen kuvaus Venäjän hyökkäysoperaatioon liittyvistä kybertoimista Ukrainassa, Venäjällä ja Ukrainan liittolaismaissa aina joulukuuhun 2023 asti. Kronologinen lähestyminen mahdollistaa paremmin kuin kokoava ja tyypittelevä lähestyminen eri toimintojen ja toimijoiden suhteiden ja niiden muutoksen tarkastelun. Tarkastelutaso on operatiivinen eli hyökkäyksellisiä kybertoimia tarkastellaan niiden tekijöiden, tyyppien, kohteiden ja vaikutusten perusteella. Luvut sisältävät analyysin ja yhteenvedot vuosien 2022 ja 2023 tapahtumista, joissa huomio on venäläisen strategisen kulttuurin ideoiden ja havaitun toiminnan suhteessa ja laajemmin kybertoimintaan liittyvissä sotataidollisissa ilmiöissä. Tutkimuksen seitsemäs luku tarkastelee, miten Venäjä on järjestänyt kyberturvallisuutensa ja -puolustuksensa vuosina 2022–2023 ja analysoi sodan vaikutusta Venäjän toimintaan strategisen kulttuurin ideoiden näkökulmasta. Tarkastelutaso on strategispoliittinen, sillä puolustustoimien toteutustavoista ja vaikuttavuudesta on lähteiden puutteessa vaikea saada havaintoja. Tarkastelun lähteenä ovat pääsääntöisesti venäläiset uutiset ja viralliset asiakirjat sekä lausunnot. Kahdeksas ja viimeinen luku muodostaa synteesin tutkimuksen

---

sodan päämäärien tavoitteluun liittyviä sotavoimien käyttöön ja käyttöön valmistautumiseen liittyviä tekijöitä. Sotataitoon kuuluvat sotilasstrategia, operaatiotaito ja taktiikka. (ks. Kajanmaa (2021); Rantapelkonen, Jori & Koistinen, Lotta: *Pohdintoja sotatieteellisistä käsitteistä.* Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 2, Nro. 1, Helsinki, 2016).

[15] Käsitteestä ks. Viitaniemi, Jukka & Kytöneva, Santeri: *Venäjän hyökkäys Ukrainaan vuonna 2022. Käsiteanalyyttinen tapaustutkimus maaoperaatioiden toteutuksesta.* Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 3, Nro. 29, Helsinki, 2023, s. 9–10.

[16] Esim. Juutilainen (2023); Giles (2023); Kerr (2023); Nilsson (2023); Bateman, Jon: Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications. Carnegie Endowment for International Peace, 16.12.2022. [https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657], luettu 1.2.2024.

havainnoista. Luvussa pohditaan venäläisen kybersodankäyntiin liittyvän ajattelun tulevaisuuden suuntauksia ja kybertoiminnan sotilaallista luonnetta yleensäkin suurvaltojen välisen sotataidollisen vuorovaikutuksen näkökulmasta.

Koska Ukrainan ja Venäjän välinen sota on edelleen käynnissä, lähteisiin kohdistuu monenlaisia haasteita: tietoja kybertoiminnasta julkaistaan yksipuolisesti, rajoitetusti ja tarkoituksenmukaisesti, aikaisempi tutkimus on osiltaan poliittisesti motivoitunutta ja jotkin tapahtuvat saavat toisia enemmän julkisuutta uutuutensa tai mielenkiintoisuutensa takia toisten ilmiöiden jäädessä raportoimatta. Monet aikaisemmat tutkimukset ovat todenneet etenkin tapahtumien syiden ja kyberhyökkäysten vaikutusten olevan vaikeaa todentaa.[17] Tutkimuksessa on käytetty runsaasti lähteitä, jotta havainnot eivät jäisi yhden raportin, sivuston tai ajatuspajan katsausten varaan. Tapahtumat joiden todenperäisyyttä ei ole voitu varmistaa luotettavasta lähteestä on jätetty huomiotta. Tällaisia ovat mm. sosiaalisessa mediassa ilman todisteita esitetyt väitteet erityyppisistä kyberoperaatioista. Läntisten tiedustelupalveluiden ja tietoturvayhtiöiden raportteja on pidetty lähtökohtaisesti luotettavina, samoin kyberturvallisuuteen keskittyviä uutissivustoja. Venäläisiin uutis- ja virallisiin lähteisiin on siellä vallitsevan sotasensuurin takia ollut pakko suhtautua kriittisemmin. Venäläisten lähteiden todistusvoimaa on pyritty täydentämään läntisen median julkaisemilla tutkivilla uutisartikkeleilla sekä ulkovenäläisten kirjoittamilla artikkeleilla ja uutisilla. Tavoitteena on ollut muodostaa mahdollisimman kattava tapahtumien ja toimijoiden kuvaus, jotta yksittäiset ilmiöt eivät ohjaisi liikaa analyysiä. Kaikki venäjän kielestä tehdyt käännökset ovat kirjoittajan tekemiä. Keskeiset alkuperäiskieliset käsitteet on annettu suluissa käännöksen jälkeen.

[17] Giles (2023); Kerr (2023); Nilsson (2023).

2. STRATEGISEN KULTTUURIN IDEAT, INFORMAATIO JA KYBER

Venäjällä informaatiotilan (информационное пространство) katsotaan tarkoittavan toimintaympäristöä, joka liittyy informaation muodostamiseen, luomiseen, muuttamiseen, siirtoon, käyttöön ja säilyttämiseen liittyvään toimintaan, joilla on vaikutusta yksilön ja ihmisyhteisöjen tietoisuuteen, informaatioinfrastruktuuriin ja informaatioon. Tilan subjektien ja toisaalta fyysisen infrastruktuurin katsotaan olevan sen erottamaton osa, joten tilalla on korostuneesti sekä informaatiopsykologinen että -teknologinen luonne.[18] Teknologinen luonne on viime aikaisissa asiakirjoissa sidottu informaatiokommunikaatioteknologian (ICT) (информационно-коммуникационная технология) käsitteeseen, millä tarkoitetaan informaation etsinnän, keräämisen, tallentamisen, työstämisen, välittämisen, vastaanottamisen ja levittämisen prosesseja, menetelmiä ja välineitä.[19] Toinen keskeinen käsite on kriittinen informaatioinfrastruktuuri (критическая информационная инфраструктура). Sillä tarkoitetaan valtion ja yhteiskunnan toiminalle, turvallisuudelle ja puolustukselle kriittisten alojen informaatiojärjestelmiä, informaatiotelekommunikaatioverkkoja ja automatisoituja järjestelmiä.[20] Informaatiokommunikaatioteknologia ja -infrastruktuuri siis muodostavat laajemman informaatiotilan perustan. Käsitteenä ne korvaavat kyberin virallisissa venäläisissä asiakirjoissa, mutta valtionhallinnon ulkopuolella kyberkäsite on yleisesti käytössä ja merkitykseltään läntistä vastaava.

Venäjällä on perinteisesti tarkoitettu informaatioturvallisuudella henkilöiden, yhteiskunnan ja valtion turvaa sisäisiltä ja ulkoisilta informaatiouhilta.[21] Tämä näkemys mahdollistaa informaation sisällön esittämisen uhkana ja tukee Venäjän pyrkimyksiä rajata kansallinen informaatiotila osaksi valtion suvereenia aluetta.[22] Teknologiset uhat ovat kuitenkin erotettavissa psykologisista. Venäjän kansallisen informaatioteknologisen turvallisuuden perustana on strategisten asiakirjojen mukaan valtion kiistaton suvereenisuus informaatiotilassa ja siihen liittyvä teknologinen suvereniteetti (технологи-

[18] Министерство обороны Российской Федерации (MoD): Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. 2011. [http://ens.mil.ru/files/morf/Strategy.doc], luettu 5.1.2024; 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; Министерство обороны Российской Федерации (MoD): Основы военной политики Союзного государства в области международной информационной безопасности. 2021. [https://документы.минобороны.рф/documents/quick_search/more.htm?id=12422292@egNPA], luettu 1.2.2024.

[19] Käsite liittyy Venäjän asevoimien vastuulla olevaan informaatioaseiden käytön rajoittamiseen tähtäävään sopimushankkeeseen (MoD (2021); Указ Президента РФ (2021a) 12.4.2021, № 213 Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности. [http://www.scrf.gov.ru/security/information/document114/], luettu 5.1.2024; Дылевский, И. Н., Базылев, С. И., Запивахин, В. О., Юниченко, С. П., Шевченко, А. Л., Филиппов, В. В. & Комов, С. А.: О военной политике союзного государства в области международной информационной безопасности. *Военная мысль*, 9/2022, s. 6–11.

[20] Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации". [http://www.consultant.ru/document/cons_doc_LAW_220885/], luettu 1.2.2024.

[21] Указ Президента РФ 5.12.2016, № 646 Об утверждении Доктрины информационной безопасности Российской Федерации. [http://www.consultant.ru/document/cons_doc_LAW_208191/], luettu 5.1.2024.

[22] Ristolainen, Mari & Kukkola, Juha: Closed, safe and secure – the Russian sense of information security. *Emerging cyber threats and cognitive vulnerabilities*. V. Benson & J. McAlaney (Toim.), Elsevier Academic Press, Washington, D.C., 2019, s. 53–71; Указ Президента РФ (2021a).

ческий суверенитет)[23] eli tulevaisuuden läpileikkaavien teknologioiden (сквозная технология), laitteistojen ja ohjelmistojen kehityksen ja tuotannon omavaraisuus. Lisäksi kriittisen informaatioinfrastruktuurin, etenkin kansallisten viestiverkkojen, eheyden, turvallisuuden ja resilienssin sekä kriittisen tiedon tulee olla turvattu kansallisin keinoin.[24] Informaatioturvallisuuden teknologinen luonne liittyy siis ICT:n hallintaan ja käyttöön.

Informaatiokommunikaatioteknologian tärkeys johtuu siitä, että Venäjän johdon mukaan sitä voidaan käyttää suurvaltojen välisen strategisen tasapainon horjuttamiseen.[25] Venäjän vuoden 2015 sotilasdoktriinin mukaan informaatiota ja informaatiokommunikaatioteknologiaa voidaan käyttää sotilaspoliittisten tavoitteiden saavuttamiseen.[26] Vuoden 2021 Kansallisen turvallisuuden strategia toteaa, että informaatiokommunikaatioteknologiaa voidaan käyttää valtioiden sisäisiin asioihin sekaantumiseksi ja niiden suvereniteetin ja alueellisen eheyden horjuttamiseksi ja vuoden 2023 Ulkopoliittinen konsepti kutsuu informaatiotilaa sotatoimien ympäristöksi (сфер военных действии).[27] Venäjän puolustusministeri Sergei Šoigu totesi vuonna 2020, että Venäjä asevoimien informaatioinfrastruktuuri oli tuhansien tietokonehyökkäysten kohteena ja että informaatiotila on muuttunut sotatoimien näyttämöksi (театр военных действий).[28] Tämä käsite tarkoittaa, että tilassa käytetään asevoimien joukkoja ja välineitä taistelutehtävien toteuttamiseen.[29] ICT on siis jatkuvan valtioiden välisen kamppailun väline, jossa sotilaallisten ja ei-sotilaallisten keinojen rajat hämärtyvät.[30]

Venäläisten informaatioteknologista tilaa ja siellä toimimista käsittelevien strategiaasiakirjojen käsitteelliset juuret ovat neuvostoliittolaisessa ja venäläisessä strategisessa kulttuurissa.[31] Informaatioturvallisuusajattelun kehittymiseen ovat vahvasti vaikuttaneet KGB:n kouluttamat miehet, jotka ovat Neuvostoliiton romahdettua palvelleet Venäjän tiedustelupalveluissa ja informaatioturvallisuutta käsitelleissä poliittisissa eli-

---

[23] Tarkka määritelmä ks. Распоряжение Правительства Российской Федерации от 20 мая 2023 г. № 1315-р Концепция технологического развития на период до 2030 года. [http://government.ru/news/48570/], luettu 1.2.12024.

[24] Ks. Указ Президента РФ (2016); Указ Президента РФ (2021b) 2.7.2021, № 400 О Стратегии национальной безопасности Российской Федерации. [http://www.kremlin.ru/acts/bank/47046], luettu 5.1.2024; Указ Президента РФ, 31.3.2023, № 229 Об утверждении Концепции внешней политики Российской Федерации 2023. [http://www.kremlin.ru/acts/bank/490909], luettu 5.1.2024.

[25] Указ Президента РФ (2016).

[26] Указ Президента РФ 25.12.2014, № Пр-2976. Военная доктрина Российской Федерации. [http://base.garant.ru/70830556/], luettu 5.1.2024.
PR-2976 Military Doctrine 2015

[27] Указ Президента РФ (2021b); Указ Президента РФ (2023).

[28] 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;

[29] Тютюнников, Н. Н.: *Военная мысль в терминах и определениях, в трех томах, Том 1*. «Перо», Москва, s. 235–236. Tämä näkemys vastaa Naton tulkintaa kybertilasta sodankäynnin toimintaympäristönä tai operaatiotilana (domain of operations). NATO: *Warsaw Summit Communiqué, Warsaw 8-9 July 2016* [https://www.nato.int/cps/en/natohq/official_texts_133169.htm], luettu 1.2.2024.

[30] Указ Президента РФ (2023).

[31] Jonsson, Oscar: *The Understanding of War. Blurring the Lines between War and Peace*. Georgetown University Press, Washington, DC., 2019; Kukkola, Juha: *Digital Soviet Union. The Russian national segment of Internet as a closed national network shaped by strategic cultural ideas* (diss.) National Defence University Series 1: Research Publications No. 40. National Defence University, Helsinki, 2020; Adamsky, Dmitry (Dima). From Moscow with coercion: Russian deterrence theory and strategic culture. *Journal of Strategic Studies*, 41(1-2) 2018, s. 33–60; Pynnöniemi, Katri: The Asymmetric Approach in Russian Security Strategy: Implications for the Nordic Countries. *Terrorism and Political Violence*, 31(1), 2019, s. 154–167. Valtioilla on eri lähestymistapoja kybervoiman käyttöön ja strateginen kulttuuri voi olla yksi selittävä tekijä ympäristön, teknologian, resurssien ja intressien rinnalla (Jensen, Valeriano & Maness (2019).

missä.[32] Ajatus informaatiotilassa käytävästä jatkuvasta kamppailusta ulottuu vähintään 1920-luvun bolsevikkien ajatteluun jatkuvasta luokkataistelusta. Tätä poliittista kamppailua käytiin sodan sijasta silloin, kun Neuvosto-Venäjä oli heikko tai myöhemmin, kun ydinaseet tekivät ajatuksen kapitalismin vastaisesta suursodasta lähes mahdottomaksi.[33] Kylmän sodan loputtua jatkuvasta kamppailusta on tullut Venäjälle osa suurvaltojen reaalipoliittista arkea ja nollasummapeliä, jossa aktiivinen ”tasapainottaminen” Lännen suuntaan nähdään oleellisena osana Venäjän suurvaltana selviytymistä ja suvereniteetin säilyttämistä.[34] Viime aikaisissa tulkinnoissa tämä kamppailu on saanut nationalistisia ja sivilisationaalisia piirteitä ja perustuu entistä voimakkaammin näkemykseen vihamielisestä Lännestä, joka pyrkii murentamaan venäläiset arvot ja yhteiskuntajärjestyksen tuhotakseen ja ”kolonialisoidakseen” Venäjän.[35] Tällaisessa taistelussa valtion suvereniteetti ja teknologiset menetelmät sen turvaamiseksi ovat keskiössä.

Suvereenisuus on venäläisen strategisen ajattelun kulmakivi. Sen perusta on valtion, tarkemmin suurvallan, riippumattomuus liittokunnista, poliittisista ja kulttuurisista vaikutteista, ulkomaisesta teknologiasta ja taloussuhteista.[36] Suurvaltastatus edellyttää suvereenisuutta, mikä tarkoittaa valtion alueen (territorion) ja laajemmin ymmärrettynä tilan hallintaa.[37] Suvereenisuus on myös liitetty vahvasti modernin Venäjän kansalliseen ideaan.[38] Nyky-Venäjällä valtion rajojen katsotaan ulottuvan myös informaatio- sekä kybertilaan.[39] Tämä tarkoittaa yhtäältä sitä, että valtion tulee voida kontrolloida tuossa tilassa olevaa ja sen läpi kulkevaa informaatiota, kuin että sen tulee hallita ja kyetä suojaamaan tilan perustana olevaa teknologiaa. Teknologian hallitseminen tarkoittaa kehittämisen, tuotannon ja hankinnan koko ketjua. Mikäli informaation kontrolli ja teknologian hallinta ei toteudu, valtio ei voi olla täysin suvereeni.[40] Tästä syystä venäläiset strategia-asiakirjat painottavat digitaalisen tai teknologisen suvereniteetin tärkeyttä.

---

[32] Soldatov, Andrei & Borogan, Irina. *The Red Web. The Struggle Between Russia's Digital Dictators and The New Online Revolutionaries*. Public Affairs, New York, 2015; Borogan, Andrei & Soldatov, Irina: Russian Cyberwarfare: Unpacking the Kremlin's Capabilities, CEPA 8.9.2022. [https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/], luettu 1.2.2024.

[33] Kukkola (2020), 109.

[34] Tsygankov, Andrei P: At War with the West: Russian Realism and the Conflict in Ukraine. *Journal of Military and Strategic Studies*, 22(2) 2022, s. 110–128.

[35] Pynnöniemi, Katri: *Nexus of Patriotism and Militarism in Russia. A Quest for Internal Cohesion*. Helsinki University Press, Helsinki, 2021, s. 4–6; Pynnöniemi, Katri & Jokela, Minna: Perceptions of hybrid war in Russia: Means, targets and objectives identified in the Russian debate. *Cambridge Review of International Affairs*, 2020, DOI: 10.1080/09557571.2020.1787949.

[36] Pynnöniemi, Katri: Russia's National Security Strategy: Analysis of Conceptual Evolution. *The Journal of Slavic Military Studies*, 31(2) 2018, s. 240–256, s. 245–246.

[37] Thomas, Timothy: *Kremlin Kontrol: Russia's Political Military Reality*. Fort Leavenworth, KS: FMSO, 2017, s. 87.

[38] Lo, Bobo: *Russia and the New World Disorder*. Chatham House, London, 2015, s. 30–32, s. 40–42; Tsygankov, Andrei P.: *Russia's Foreign Policy: Change and Continuity in National Identity* (3rd ed.) Rowman & Littlefield, Lanham, 2016.

[39] Ristolainen, Mari: Should "RuNet 2020" be taken seriously? Contradictory views about cybersecurity between Russia and the West. *Journal of Information Warfare*, 16(4) 2017, s. 113–131; Nocetti (2015), s. 112; Soldatov, Andrei & Borogan, Irina: Russia's Surveillance State. *World Policy Journal*, 30(3) 2013, s. 23–30, s. 29; Soldatov, Andrei: The Taming of the Internet. *Russian Social Science Review*, 58(1) 2017, s. 39–59; Vendil Pallin, Carolina: Internet Control Through Ownership: The Case of Russia. *Post-Soviet Affairs*, 33(1) 2017, s. 16–33, s. 17; Jaitner, Margarita & Rantapelkonen, Jari: Russian Struggle for Sovereignty in Cyberspace. *Tiede ja Ase*, 71 2013, s. 64–89, s. 83; Kukkola (2020).

[40] Kukkola (2020); Kukkola, Juha & Ristolainen, Mari: Projected Territoriality: A Case Study of the Infrastructure of Russian 'Digital Borders.' *Journal of Information Warfare*, 17(2), 2018, s. 83–100.

Venäläiseen strategiseen ajatteluun kehittyi 2000-luvulla idea informaatiokamppailun (информационное противоборство) ja -sodankäynnin (информационная борьба) keskeisyydestä valtioiden välisessä kanssakäymisessä. Sen juuret olivat yhtäältä Venäjän tiedemaailman kyberneettisessä perinnössä, 1980-luvun neuvostoliittolaisessa sotilasteknologisessa vallankumouksessa ja venäläisten kokemassa Yhdysvaltojen 1990-luvun sotilasteknologisessa ylivoimassa. Toisaalta se kehittyi Neuvostoliiton romahtamisen traumasta sekä KGB:n psykologisten operaatioiden perinteestä, ja kolmanneksi Venäjän kokemuksista Tšetšenian ja Georgian sodissa ja havaitusta sodan luonteen (характер / содержание войны) muutoksesta.[41] Olennainen muutos on ollut usko epäsuorien, ei-sotilaallisten, jopa ei-aseellisten väkivallan keinojen ja menetelmien, etenkin informaation, vaikuttavuuden kasvuun poliittisstrategisten päämäärien tavoittelussa rauhan, sodan uhan ja sodan aikana.[42] Lisäksi venäläistä ajattelua uuden sukupolven sodankäynnistä on hallinnut teknologiafetisismi, määrän korvaaminen laadulla, sotilaallisten epäsuorien toimien tehokkuus, yksityisten toimijoiden lisääntynyt käytettävyys ja ajatus poliittisstrategisten päämäärien saavuttaminen halvalla.[43] Joidenkin läntisten tulkintojen mukaan sodan ja rauhan raja venäläisessä strategisessa ajattelussa on tämän kehityksen myötä hämärtynyt.[44] Tämä ei kuitenkaan venäläisten sotilaiden kirjoitusten valossa pidä täysin paikkaansa, vaan venäläiset ovat pyrkineet tarkkaan erottelemaan valtioiden välisen kamppailun eri vaiheita ja useat kirjoittajat ovat pyrkineet määrittelemään sodan erilliseksi ja erityiseksi ilmiöksi.[45] Suurvaltojen välisen kamppailun muuttuneet reunaehdot ja uudet välineet, etenkin informaatio,

---

[41] Jonsson (2019); Kukkola, Juha: *Oveluuden lupaus. Asymmetria, epäsuoruus ja ei-sotilaalliset toimenpiteet uuden venäläisen sotataidon kiintopisteinä*. Maanpuolustuskorkeakoulu, Sotataidon laitos, julkaisusarja 2: Tutkimusselosteita nro 22. Maanpuolustuskorkeakoulu, Helsinki, 2022; Thomas, Timothy L.: Dialectical versus empirical thinking: Ten key elements of the Russian understanding of information operations. *The Journal of Slavic Military Studies*, 11(1) 1998, s. 40–62; Grisé, Michelle, Demus, Alyssa, Shokh, Yuliya, Kepe, Marta, Welburn, Jonathan W. & Holynska, Khrystyna: *Rivalry in the Information Sphere Russian Conceptions of Information Confrontation*. RAND, Santa Monica, 2022; Fridman, Ofer: 'Information War' as the Russian Conceptualisation of Strategic Communications. *The RUSI Journal*, 165(1), 2020, s. 44–53, 45; Blank, Stephen: Cyber War and Information War à la Russe. *Understanding Cyber Conflict: Fourteen Analogies*. Perkovich, George & Levite, Ariel E. (Toim.) Georgetown University Press, Washington, D.C., 2017, s. 81–98; Lilly & Cheravitch (2020), s. 132; McDermott, Roger N.: *Russia's Path to the High-Tech Battlespace*. The Jamestown Foundation, Washington, D.C., 2022; Adamsky (2018).

[42] Kofman, Michael, Fink, Anya, Gorenburg, Dmitry, Chesnut, Mary, Edmonds, Jeffrey & Waller, Julian: *Russian Military Strategy: Core Tenets and Operational Concepts*. CNA, Washington, D.C., 2021; Kukkola (2022), s. 87–88; Minic, Dimitri: How the Russian army changed its concept of war, 1993–2022. *Journal of Strategic Studies*, 2023, DOI: 10.1080/01402390.2023.2199445.

[43] Kukkola (2022); McDermott (2022), s. 61; Bērziņš, Jānis: Not 'Hybrid' but New Generation Warfare *Russia's Military Strategy and Doctrine*. Howard, Glen E. & Czekaj, Matthew (toim.) The Jamestown Foundation, Washington, D.C., 2019, 2. 157–184, s. 165–166.

[44] Giles & Seaboyer (2019), s. 11–12; Blank (2017), s. 83; Thornton, Rod & Miron, Marina: Winning Future Wars: Russian Offensive Cyber and Its Vital Importance. *The Cyber Defense Review*, 7(3) 2022, s. 117–135, s. 122–123; Jonsson (2019), s. 157; Minic (2023).

[45] Kukkola (2020) & (2022); Grisé et al. (2022), s. 57; Forsström, Pentti (ed.): *Russian Concept of Deterrence in Contemporary and Classic Perspective*. National Defence University Series 2: Research Reports No. 11. National Defence University, Helsinki, 2021, s. 15; Петруня, С. Н. & Терентьев, И. А.: Подходы к сущности войны и перспективный взгляд на ее содержание. *Вестник Академии военных наук*, 80(3), 2022, s. 87–91; Малышев, А. И., Мардусин, В. Н. & Хахалев, В. Ю.: Анализ трансформации основных категорий военной конфликтологии в доктринальных основах РФ. *Военная мысль*, 8/2023, s. 7–15. Venäläinen kirjoittelu ns. hybridisodankäynnistä on eittämättä hämärtänyt vakavan sotatieteellisen keskustelun ja propagandistisen kirjoittelun rajoja vuodesta 2014 ja etenkin vuodesta 2022 eteenpäin. Киселев, В. А. & Воробьев, И. Н.: Гибридные операции как новый вид военного противоборства. *Военная мысль*, 5/2015, s. 41–48; Бартош, А. А.: Смыслы гибридной войны. *Вестник Академии военных наук*, 59(2), 2017, s. 165–173; Сайфетдинов, Х. И.: Гибридные войны, проводимые США и странами НАТО, их сущность и направленность. *Военная мысль*, 5/2022, s. 13–20.

ovat kuitenkin aiheuttaneet kiistaa sodan ja aseellisen taistelun luonteesta ja etenkin asevoimien roolista.[46]

Informaatiokamppailun, -sodan, -sodankäynnin ja -taistelun käsitteitä on käytetty venäläisissä sotilasalan kirjoituksissa varsin vaihtelevasti. Venäläisten sotilaiden ja akateemikkojen kirjoituksissa informaatiokamppailu viittaa usein geopoliittiseen, jatkuvaan informaatioperustaiseen vuorovaikutukseen suurvaltojen välillä, jossa informaatiopsykologiset uhat, vaikutukset ja kohteet korostuvat, ja tavoitteena on globaalin informaatiotilan hallinta. Länsimaisittain voitaisiin puhua strategisesta kommunikaatiosta ja poliittisesta sodankäynnistä, mutta venäläisille käsite on laajempi ja sisältää myös taloudelliset tekijät.[47] Venäjän strategisissa asiakirjoissa kamppailu kehittyy vuosien saatossa kamppailun tilasta kohti itsenäistä valtioiden välisen kamppailun muotoa.[48]

Informaatiosodallakin (информационная война) on ollut venäläisten sotilasalan kirjoittajien parissa useita määritelmiä. Käsite esiintyy vuoden 2000 informaatioturvallisuuden konseptissa, jossa sen katsotaan edustavan Venäjälle uhkaavaa, ulkomaista konseptia, mutta myöhemmin se katoaa virallisista asiakirjoista.[49] Yleisesti ottaen sillä on tarkoitettu sotilaallisia, mahdollisesti jo rauhan aikana toimeenpantuja, toimia informaatiotilassa informaatioon vaikuttamiseksi. Sodan käsitteen käyttö on usein perustunut informaatioaseiden (информационное оружие), joita on verrattu aseelliseen voimaan, käyttöön poliittisten päämäärien tavoittelussa.[50] Huomattavaa on, että informaatiosodan käsite on saanut Venäjällä osakseen samanlaista kritiikkiä kuin kybersodan käsite Lännessä.[51]

Informaatiosodankäynti tai -taistelu on venäläisissä kirjoituksissa usein viitannut eisotilaallisiin toimiin informaatiotilassa, ennen sotaa, sen alkuvaiheessa ja käynnissä ollessa, joilla pyritään saavuttamaan informaatioylivoima (информационное превосходство) eli suurempi informaation keräämisen, prosessoinnin ja päätöksenteon nopeus ja tehokkuus suhteessa vastustajaan. Suppeasti määriteltynä kyseessä on tiedonkäsittelyn ylivoima, mutta laajemmin määriteltynä käsite viittaa koko informaatiotilan hallintaan, mukaan lukien sen subjektien mieli.[52] Informaatiosodankäynnissä lopullinen vaikutus perustuu informaation hankkimiseen, kulun estämiseen, edistämiseen tai etenkin manipulaatioon.[53] Venäläiset jakavat informaatiosodankäynnin menetelmät

---

[46] Гареев, М. А.: Итоги деятельности Академии военных наук за 2012 год и задачи академии на 2013 год. *Вестник Академии военных наук*, 1(42) 2013, s. 8–21; Герасимов, Валерий: Векторы развития военной стратегии. *Красная звезда*. 4.3.2019 (a) [http://redstar.ru/vektory-razvitiya-voennoj-strategii/], luettu 4.3.2019; ТАСС: Шойгу заявил, что Россия должна выработать новую теорию ведения войн. *ТАСС*, 18 июня 2019 [https://tass.ru/armiya-i-opk/6561643], luettu 2.7.2019.

[47] Ristolainen (2017); Kukkola (2020); Jonsson (2019); Fridman (2020), s. 46; Kipp, Jacob W.: *Future War. Makhmut Gareev and Vladimir Slipchenko*. FMSO, Fort Leavenworth, KS, 2007; Thomas, Timothy: *Russian Military Thought: Concepts and Elements*. MITRE Corporation, McLean VA, 2019.

[48] Kukkola (2020).

[49] Шаклеина, Т.А. (Сост.): *Внешняя политика и безопасность современной России. 1991–2002. Хрестоматия в 4-х т. Том четвертый: Документы*. МГИМО, РАМИ, АНО "ИНО-Центр", 2002, Москва, s. 122–153.

[50] Расторгуев С. П.: *Информационная война*. 2-е изд. Moscow: Радио и связь, 1999; Федорова, А.В. & Цыгичко, В. Н. (общ. ред.): *Информационные вызовы национальной и международной безопасности*. ПИР-Центр, Москва, 2001; Панарин, И. Н.: *Информационная война и геополитика*. Поколение, Москва, 2006, s. 172–173.

[51] Орлянский, В. И.: «Военная хитрость», «информационная война» и другие понятия в свете результатов научных исследований и дискуссий. *Военная мысль,* 12/2022, s. 39–51.

[52] Федорова & Цыгичко (2001); Манойло А. В., Петренко А. И., Фролов Д. Б.: *Государственная информационная политика в условиях информационно-психологической войны*. 3-е изд., стереотип. Горячая линия – Телеком, Москва, 2012.

[53] Kukkola (2022); Thomas (2019), s. 8-15 – 8-28.

informaatioteknologisiin ja -psykologisiin menetelmiin. Ensimmäinen sisältää mm. tietoverkko- ja järjestelmäoperaatiot, ohjelmistoteknisen vaikuttamisen ja teknologisen tiedustelun – länsimaisin ymmärrettynä hyökkäykselliset kyberoperaatiot – elektronisen sodankäynnin, kineettisen vaikuttamisen johtamisjärjestelmiin ja eksoottisten asejärjestelmien käytön ja kohdistuu tietotekniikkaan tai dataan. Jälkimmäinen sisältää mm. harhauttamiseen, propagandan levittämiseen, refleksiiviseen kontrolliin ja omien joukkojen moraalispsykologiseen tukemiseen ja kohdistuu ihmismieleen tai sosiaaliseen tietoisuuteen.[54]

Venäjän asevoimien julkiset näkemykset informaatiosodankäynnistä muistuttavat 2020-luvulle tultaessa hyvin paljon jo 1990-luvulta peräisin olevia asevoimien lehdissä esitettyjä näkemyksiä. Venäjän asevoimat määritteli informaatiosodankäyntiin liittyviä käsitteitä ensimmäisen kerran vuonna 2008 Yleisesikunta-akatemian julkaisemassa sanakirjassa, mutta määritelmät perustuivat pitkälti läntisiin tai kansainvälisiin lähteisiin.[55] Vuonna 2011 julkaistussa asiakirjassa informaatiosodan määriteltiin tarkoittavan valtioiden välistä kamppailua informaatiotilassa informaatio- ja muiden kriittisten järjestelmien vahingoittamiseksi, poliittisten, taloudellisten ja sosiaalisten järjestelmien kaatamiseksi, yhteiskunnan ja valtion horjuttamiseksi ja vastapuolen pakottamiseksi hyökkääjälle edullisiin päätöksiin. Sotilaallinen konflikti informaatiotilassa taas määriteltiin vastakkainasettelun ratkomiseksi informaatioasein. Informaatioaseet määriteltiin hieman tautologisesti informaatioteknologiaksi, välineiksi ja menetelmiksi, joita käytetään informaatiosodan käymiseen.[56]

Venäjän asevoimien digitaaliseen sanakirjaan informaatiokamppailun, -sodan ja -sodankäynnin käsitteet ovat ilmestyneet 2020-luvulla eli varsin myöhään.[57] Informaatiokamppailun ja sodan käsitteet ovat varsin yhtenevät. Niitä käytetään informaatiosodankäynnin merkityksessä viittaamaan rauhan ja sodan aikana tapahtuvaan vastustajaan kohdistuvaan häiritsevään tai tuhoavaan informaatiovaikuttamiseen vastustajan informaatiotilassa, tiedon keräämiseen ja vastaavan vaikuttamisen torjuntaan (oman tiedon suojaamiseen). Informaatiokamppailun katsotaan muuttuneen omaksi taistelun muodokseen (вид борьбы) 1900-luvun puolivälistä. Sen yhteydessä informaatio on resurssi, väline ja kohde, ja tavoitteena on vastustajan lamauttaminen. Sankirjamääritelmätkin jakavat informaatiokamppailun välineet ja kohteet teknologisiin ja psykologisiin. Teknologisilla informaatioaseilla tarkoitetaan mm. tietokonehyökkäyksiä ja elektronista sodankäyntiä, joilla pyritään tuhoamaan informaatiojärjestelmiä tai pääsemään niihin laittomasti käsiksi päätöksentekoon, informaatioresursseihin tai ihmisten tietoisuuteen vaikuttamiseksi. Erään määritelmän[58] mukaan tietokonehyökkäykset ovat ei-tappavia informaatiotaistelun aseita. Kamppailua toimeenpannaan erillisillä

[54] Thomas (1998); Thomas, Timothy: *Cyber Silhouettes. Shadows Over Information Operations*. Foreign Military Studies Office, Fort Leavenworth, KS, 2005; Adamsky (2018); Thomas (2020), s. 128–130; Mil.ru: Военный энциклопедический словарь, 'Средства информационной борьбы («Информационное оружие»)'. [https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=14342@morfDictionary], luettu 1.2.2024.

[55] Тучков Ю. Н. и др.: *Словарь терминов и определений в области информационной безопасности*. 1-е изд ВАГШ ВС РФ, НИЦ информационной безопасности, Москва, 2008.

[56] MoD (2011).

[57] Venäjän asevoimien viimeisin painettu ja julkinen sanakirja on ilmestynyt vuonna 2007. Asevoimien verkkosivuilla olevan sähköisen sanakirjan sisältöä muutetaan jatkuvasti, mutta verkkosivuilla ei ole päivitysmerkintöjä. Käsitteiden päivittämistä on selvitetty Waybackwhen machine -palvelulla.

[58] Mil.ru: 'Средства информационной борьбы («Информационное оружие»)' (2024).

toimilla tai operaatioilla.[59] Kyberhyökkäykset ovat siis informaatiovaikuttamisen väline, joita voidaan käyttää niin rauhan aikana kuin sotatoimien osana poliittisten päämäärien edistämiseen.

Venäläisessä ajattelussa informaatiomenetelmien, ja yleensäkin ei-sotilaallisten menetelmien, luonne ja vaikutus riippuvat valtioiden välisten suhteiden vaiheesta. Informaatiomenetelmien sotilaallinen luonne ja väkivaltaisuus lisääntyvät sotaa lähestyttäessä, samalla kun muiden ei-sotilaallisten ja ei-väkivaltaisten menetelmien käyttöä jatketaan niiden rinnalla.[60] Rauhanaikaisen kilpailun välineenä menetelmiä käytetään Venäjän suojelemiseksi, sen etujen ja voiman edistämiseksi ja vastustajien heikentämiseksi, kiristyneessä kilpailussa deterrenssiin, konfliktin estämiseen tai edullisen voimankäytön tilanteen luomiseen ja sodan aikana informaatioylivoiman hankkimiseen, asevoiman käytön edistämiseen, vastustajan johtamisjärjestelmien heikentämiseen ja omien järjestelmiä suojelemiseen.[61] Menetelmien luonne on siis riippuvainen tilanteesta, käyttötarkoituksesta ja vaikutuksesta, ei sisäsyntyisestä ominaisuudesta.

Useat läntiset tutkijat ovat kuvanneet venäläistä informaatiosodankäyntiä holistisena, pitkälle integroituneena sekä kehittyneenä ja korostaneet informaatiopsykologisten keinojen ja vaikutusten primaarisuutta venäläisessä ajattelussa.[62] Venäläisten esittämien jaottelujen perusteella on kuitenkin selvää, että teknologisilla välineillä, keinoilla ja vaikutuksilla on oma paikkansa venäläisessä sotataidossa. Lisäksi viimeaikaisissa kansainvälisissä sopimuksissa ja strategia-asiakirjoissaan Venäjä on käyttänyt käsitettä informaatiokommunikaatioteknologinen kyberkäsitteen korvaajana.[63] On syytä olettaa, että Ukrainan sodan seurauksena ja asevoimien kybersuorituskykyjen kehittyessä informaatiokommunikaatioteknologiaan perustuvat aseet, eli läntisittäin kyberaseet, vakiinnuttavat asemansa selvemmin informaatiosodankäynnin ytimessä. Informaatio- ja psykologisten keinojen ja menetelmien suhde riippuukin siitä, kenen kirjoituksia asiasta tarkastellaan. Monet venäläiset sotilastaustaiset kirjoittajat katsovat, että informaatioteknologisilla keinoilla voi olla itsenäistä, tuhoavaa, vaikutusta ja psykologiset vaikutukset voivat olla niiden seurannaisia. Turvallisuuspalvelutaustaiset kirjoittajat taas korostavat teknologian välineellistä roolia ja psykologisia, systeemisiä vaikutuksia.[64]

---

[59] Mil.ru: Военный энциклопедический словарь, 'Информационное противоборство.' [https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5221@morfDictionary], luettu 1.2.2024; Mil.ru: Военный энциклопедический словарь, 'Информационная война.' [https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=5211@morfDictionary], luettu 1.2.2024; Остапенко, О. Н., Баушев, С. В. & Морозов, И. В.: *Информационно-космическое обеспечение группировок войск (сил) ВС РФ. Учебно-научное пособие.* Издательство «Любавич», Санкт-Петербург, 2012, s. 255–256.

[60] Näistä näkemyksistä ks. Kukkola (2022).

[61] Grisé et al. (2022).

[62] Giles, Keir: *Handbook of Russian Information Warfare*. Fellowship monograph 9. NATO Defence College, Rome, 2016; Adamsky (2018); Thomas (2019); Jonsson (2019); Vendil-Pallin (2019). Näkemys perustuu todennäköisesti siihen, että Venäjällä ei ole virallisissa yhteyksissä käytetty kyberkäsitettä Venäjän omaan toimintaan liittyen, edellä mainitut teknologiset ja psykologiset menetelmäjaottelut ovat poikenneet läntisistä, koko informaatiokamppailun käsite on ollut epäselvä venäläisille itselleenkin, ja että Venäjä ei ole perustanut varsinaisia kyberjoukkoja, ja koska Venäjän toiminta on siltä, eli kokonaisvaltaiselta ja keskitetysti johdetulta, näyttänyt.

[63] MoD (2021); Указ Президента РФ (2021); Kremlin.ru: Нью-Делийская декларация Совета глав государств – членов Шанхайской организации сотрудничества. 4 июля 2023 года. [www.kremlin.ru/supplement/5963], luettu 1.2.2024.

[64] Näkökulmaeroista ks. Kukkola (2020).

Kaikissa valtioiden välisten suhteiden vaiheissa oleellista on tiedonkeruu eli tiedustelu ja vakoilu.[65] Strategiset ohjausasiakirjat ja sotilassanakirjat tunnistavat tietokonevakoilun informaatiotilan ilmiöksi[66] ja sotilassankirja tunnistaa tietokonetiedustelun osaksi ”ulkomaista teknistä tiedustelua.”[67] Poliittinen, tieteellisteknologinen ja taloudellinen tiedustelu ja vastatiedustelu kuuluvat Venäjällä tiedustelupalveluille. Asevoimien tiedustelun piiriin kuuluvat sotilaspoliittiset ja -taloudelliset asiat sekä sotilaallisen voiman käyttöön liittyvät asiat.[68] Venäläisten sotilaiden piirissä teknologinen tiedustelu on usein liitetty elektronisen sodankäynnin osaksi, jonka kohteena ovat sotilaalliset objektit.[69] Tämä on johtanut pyrkimyksiin sulauttaa asevoimissa kybertiedustelu osaksi elektronista sodankäyntiä (ELSO), joka on Venäjällä oma aselajinsa.[70]

Yhtä kaikki kybertiedustelun ja -vakoilun mahdollisuudet ja tärkeys on tunnistettu Venäjällä jo 1990-luvulta lähtien.[71] Kybertiedustelulla hankittu tieto mahdollistaa strategispoliittiselta aina taktiselle tasolle vastustajan tuntemisen ja näin manipulaation, hämäämisen, horjuttamisen ja disorganisoinnin. Se myös mahdollistaa poliittisen, taloudellisen ja tieteellisen teknologisen etulyöntiaseman hankkimisen ja tarjoaa halvan keinon vastustajien ylivoiman neutraloimiseen (tai heikompien painostamiseen).[72] Venäjän tiedustelupalvelujen tehtäväkentässä tiedonhankinta ja sen käyttö liittyvät saumattomasti yhteen.[73]

Vaikka Venäjän asevoimien johto ja osa sotilasakateemikoista pitää nykyisellään informaatiotilaa yhtenä sotatoimien näyttämöistä[74] sotilassanakirja rajoittaa määritelmän

---

[65] Сайфетдинов, Х. И.: Информационное противоборство в военной сфере. *Военная мысль*, 7/2014, s. 38–41.

[66] Шаклеина (2002); MoD (2011).

[67] Mil.ru: Военный энциклопедический словарь, 'Иностранная техническая разведка (ИТР)'. [https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=13176@morfDictionary], luettu 1.2.2024.

[68] Soldatov, Andrei & Borogan, Irina: *The New Nobility: The Restoration of Russia's Security State and the Legacy of the KGB*. Public Affairs, New York, 2010; Меньшаков Ю.К.: *Основы защиты от технических разведок: учебное пособие*. Изд-во МГТУ им. Н. Э. Баумана, Москва, 2011; Лутовинов, В. И.: Развитие и использование невоенных мер для укрепления военной безопасности Российской Федерации. *Военная мысль*, № 5/2009, s. 2–12.

[69] Mil.ru: Военный энциклопедический словарь, 'Разведка'. [https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=10440@morfDictionary], luettu 1.2.2024; Серов, В. И.: Военная разведка: проблемы и суждения. *Военная мысль*, № 8/1991, s. 12–18; Лутовинов, В. И.: Развитие и использование невоенных мер для укрепления военной безопасности Российской Федерации. *Военная мысль*, № 5/2009, s. 2–12.

[70] Никитин, О. Г.: Направления повышения эффективности организации боевого применения войск радиоэлектронной борьбы в операциях объединений Сухопутных войск. *Военная мысль*, 5/2017, s. 23-29; Андреев, В. В., Никитин, О. Г. & Марасанов, А. В.: Особенности методического обеспечения обоснования состава органов управления разнородными силами и средствами радиоэлектронной борьбы объединений Сухопутных войск. *Военная мысль*, 6/2017, s. 51–54.

[71] Брусницын, И. А.: Глобальная техническая разведка США. *Военная мысль*, 10/1990, s. 57–65; Поздняков, А. И.: Информационная безопасность личности, общества, государства. *Военная мысль*, 10/1993, s. 13–18.

[72] Комов, С. А.: Информационная борьба в современной войне: вопросы теории. *Военная мысль*, 3/1996, s. 76–80; Пискунов, Л. В.: Технологическая безопасность как фактор укрепления оборонного потенциала России. *Военная мысль*, 6/1994, s. 54–57; Модестов, С. А.: Стратегическое сдерживание на театре информационного противоборства. *Вестник Академии военных наук*, 26(1) 1994, s. 33–36; Mil.ru: 'Иностранная техническая разведка (ИТР)' (2024); Федорова & Цигичко (2001); Панарин, И. Н. & Панарина, Л. Г.: *Информационная война и мир*. ОЛМА-ПРЕСС, Москва, 2003.

[73] Haslam, Jonathan: *Near and Distant Neighbours*. Oxford University Press, Oxford, 2015; Soldatov & Borogan (2015).

[74] ВПК: Министр обороны России выступил на заседании СФ в рамках "правительственного часа." *ВПК*, 27.03.2020. [https://vpk.name/news/387739_ministr_oborony_rossii_vystupil_na_zasedanii_sf_v_ramkah_pravitelstvennogo_chasa.html], luettu 1.2.2024; Петруня, С. Н.: О развитии теоретических основ оценки

edelleen maantieteelliseen tilaan (maa-meri-ilma-avaruus), jossa voidaan ryhmittää asevoimien strategisen kokoluokan yhtymiä ja toteuttaa strategisia sotatoimia.[75] Venäjän asevoimat eivät myöskään vielä tunnista sotataidon lajiksi informaatio- tai kyberoperaatiotaitoa, eivätkä ole virallisesti perustaneet kyberkomentoporrasta tai -aselajia.[76] Lisäksi informaatiotilan riippuvuus esimerkiksi avaruudesta ja sähkömagneettisesta spektristä on tiedostettu.[77] Täten kybertoiminnan käsitteellinen asemoiminen venäläisen sotataidon käsitejärjestelmään on jossain määrin haastavaa. Yhden näkemyksen mukaan kyberneettiset hyökkäykset (кибернетические атаки) ovat osa kuluttamis- ja tuhoamisstrategioiden rinnalle syntynyttä uusiin välineisiin ja joukkoihin perustuvaa itsenäisen lamauttavan iskun strategiaa.[78] Läntisessä tutkimuksessa onkin esitetty näkemys, jonka mukaan Venäjä valmistautuu käyttämään kaukovaikuttamista ml. informaatioaseet erillisenä strategisena operaationa, jossa uhataan ja tarvittaessa isketään vastustajan kriittistä infrastruktuuria vastaan vastustajan pakottamiseksi omaan tahtoon.[79]

Toisaalta kyberjoukkoja tai menetelmiä voitaisiin käyttää osana strategista operaatiota operatiivisina taisteluina, taisteluina tai iskuina mahdollisesti yhteistoiminnassa elektronisen ja muiden informaatiosodankäynnin joukkojen ja menetelmien kanssa.[80] Tähän liittyen sotilasalan lehdissä ja kirjallisuudessa on muotoiltu informaatioiskuoperaation (информационно-ударная операция) käsite. Se on tavoitteen, tehtävien, paikan, ajan ja keinojen suhteen yhteensovitettu ja koordinoitu informaatioiskutaisteluiden, informaatiotulitaisteluiden ja informaatioiskujen kokonaisuus vastustajan disorganisoimiseksi, informaatioresurssien tuhoamiseksi. Informaatioisku perustuu lyhytaikaiseen ja voimakkaaseen vaikutukseen, joko valikoituihin kohteisiin tai laaja-alaisesti käyttäen. Yksi informaatioiskun lajeista ovat tietokonehyökkäykset, jotka voidaan yhdistää muiden, myös fyysisten vaikutusten kanssa. Informaatioiskuoperaatiot voidaan toimeenpanna itsenäisesti tai yhdessä puolustushaarojen joukkojen strategisten ja operatiivisten operaatioiden kanssa.[81] Kyberoperaatiot voidaan myös lukea asevoimien erikoisoperaatioihin. Niitä voidaan toimeenpanna niin rauhan kuin sodan aikana ja niitä toimeenpanevat lähtökohtaisesti erikoisjoukot ja niiden luonteeseen kuuluu

---

стратегической обстановки в интересах обеспечения военной безопасности России. *Военная мысль*, 4/2023, s. 34–44, s. 35.

[75] Mil.ru: Военный энциклопедический словарь, 'Театр военных действий.' [https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=10896@morfDictionary], luettu 1.2.2024.

[76] Цилько, В. Г. & Иванов, А. А.: Тенденции развития общевойскового оперативного искусства. *Военная мысль*, 11/2022, s. 43–49.

[77] Ковалёв, А. П., Сотник, С. А. & Сотник, Д. С.: Космос как новая сфера вооруженной борьбы. *Военная мысль*, 3/2023, s. 35–52.

[78] Сержантов, А. В., Смоловый, А. В. & Терентьев, И. А.: Трансформация содержания войны: контуры военных конфликтов будущего. *Военная мысль*, 6/2022, s. 19–30, s. 28.

[79] Kofman et al. (2021); Thomas (2019), s. 8–6.

[80] Mil.ru: Военный энциклопедический словарь, 'Боевые действия'. [https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=12700@morfDictionary], luettu 1.2.2024; Mil.ru: Военный энциклопедический словарь, 'Стратегическая операция'. [https://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=14374@morfDictionary], luettu 1.2.2024; Логинов, П. К.: Информационно-психологическое воздействие в современных операциях. *Военная мысль*, 5/2022, s. 60–69; Kukkola (2022), s. 36 & 71.

[81] Остапенко, Баушев & Морозов (2012), s. 216; Воробьев, И. Н.: Информационно-ударная операция. *Военная мысль* № 6/2007, s. 14–21;

mm. tiedustelu ja sabotaasit.[82] Tiedustelu kuuluu myös Yleisesikunnan päähallinnon (GRU) eli sotilastiedustelun toimialaan.[83]

Informaatioylivoiman saavuttamisen katsotaan olevan ratkaisevaa nykyisten ja tulevien sotien voittamiselle. Se on perusta ilmaylivoimalle, mikä taas on perusta maavoimien onnistuneelle taistelulle.[84] Informaatiokamppailun ja -sodankäynnin keinoilla katsotaan olevan potentiaalisia strategisia vaikutuksia: 1) Niillä voidaan manipuloida vastustajaa poliittisstrategisten tavoitteiden saavuttamiseksi ilman suoran aseellisen voiman käyttöä (politiikan manipulointi, liittosuhteiden rapauttaminen ja uskottavuuden murentaminen),[85] 2) niillä voidaan lamauttaa vastustajan kansan puolustustahto ja poliittinen päätöksenteko,[86] 3) niillä voidaan saavuttaa yllätys sekä lamauttaa vastustajan liikekannellepano, sotatalous ja strategisten joukkoryhmien johtaminen sen strategisessa syvyydessä[87] 4) ja niillä voidaan disorganisoida[88] johtaminen taktisella ja operatiivisella tasolla.[89] Operatiivisella ja taktisella tasolla informaatioteknologiset menetelmät mahdollistavat vastaverkostokeskeisen sodankäynnin eli korkeateknologisen vastustajan johtamis- ja viestijärjestelmien häirinnän tai lamauttamisen.[90] Taistelutasolla kybervaikuttaminen[91] nähdään osana miehittämättömiin järjestelmiin vaikuttamista.[92] Informaatioteknologisilla keinoilla voidaan siis venäläisten mielestä vaikuttaa sodan kulkuun ja lopputulokseen usealla eri tasolla ja tavalla.

---

[82] Mil.ru: Военный энциклопедический словарь, 'Формы применения Вооруженных Сил Российской Федерации'. [https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=14014@morfDictionary], luettu 1.2.2024; Остапенко, Баушев & Морозов (2012), s. 101–102.

[83] Mil.ru: Главное управление Генерального штаба Вооруженных Сил Российской Федерации. [https://structure.mil.ru/structure/ministry_of_defence/details.htm?id=9711@egOrganization], luettu 1.2.2024.

[84] Thomas, Timothy L.: Russian Views on Information-Based Warfare. *Airpower Journal* – Special Edition 1996, s. 26–35, s. 26; Цымбал, В. И.: О концепции информационной войны. *Информационный сборник Безопасность*, № 9 (1995); Смолян, Г., Цыгичко, В., Черешкин, Д.: Оружие, которое может быть опаснее ядерного. *Независимая газета*, 18.11.95 г. no. 3 (18 November 1995), 1–2; Круглов, В. В.: О вооруженной борьбе будущего. *Военная мысль*, 5/1998, s. 54–58.

[85] Pynnöniemi (2019), s. 160; Jonsson (2019), s. 122–123; Fridman (2020), s. 45; Blank (2018), s. 83; Giles & Seaboyer (2019), s. 5; Панарин & Панарина (2003), s. 38–39; Панарин (2006), s. 173.

[86] Модестов, С.А.: Основополагающее понятие «война» в творческом наследии М. А. Гареева. *Вестник академии военных наук*, 83(2) 2023, s. 49–53.

[87] Сайфетдинов (2014); Baev, Pavel: *Russia's War in Ukraine. Misleading Doctrine, Misguided Strategy*. Ifri, Paris, 2022; Сержантов, Смоловый & Терентьев (2022).

[88] Disorganisaatio on neuvostoliittolaista perua oleva käsite, joka viittaa vastustajan johtamiskyvyn häiritsemiseen ja lamauttamiseen ja täten sen tavoitteiden saavuttamisen estämiseen. (Sokolovskii, V. D.: Soviet Military Strategy (with analysis and annotation by H. Dinerstein, L. Gouré, and T. Wolfe). RAND, Santa Monica, 1963; Thomas (2019), s. 6-7–6-8; Kofman et al. (2021), s. 76.

[89] Цилько & Иванов (2022), s. 47; Орлянский (2022); Thomas (2019), s. 5–3; Сайфетдинов (2014); Воробьев (2007); Цилько & Иванов (2022), s. 47.

[90] Пасичник, С. И.: К вопросу о комплексном поражении противника и способах его осуществления при дезорганизации управления. *Военная мысль,* 6/2017, s. 38–42; Холуенко, Д. В. & Анохин, В. А.: Развитие форм совместного применения группировки сил и средств при дезорганизации управления противника. *Военная мысль,* 9/2023, s. 45–51.

[91] Informaatioteknologiset vaikutukset/toimet/vaikuttaminen (воздействие) on määritelty: "Tietokoneohjelmien ja radioelektronisten keinojen järjestelmäksi, joka on tarkoitettu informaatioteknologisten objektien toiminnan manipulointiin sekä niiden toiminnan keskeyttämiseen (häirintään) tai toimintakyvyttömäksi saattamiseen määrätyksi ajaksi." Тучков Ю. Н. и др.: *Словарь терминов и определений в области информационной безопасности*. 1-е изд. ВАГШ ВС РФ, НИЦ информационной безопасности, Москва, 2008.

[92] Андрющенко, М. С. & Голик, А. М. & Сахнов, С. А.: Подходы к организации противодействия беспилотным летательным аппаратам. *Известия Российской Академии Ракетных И Артиллерийских Наук*, 1/2023, s. 15–21.

Johtuen informaatiovälineiden ja -menetelmien mahdollisista strategisista vaikutuksista ne ovat luonnollinen osa Venäjän strategisen deterrenssin konseptia[93] ja aktiivisen puolustuksen strategiaa.[94] Venäläisten mukaan informaatiokeinoilla on mahdollista tuottaa objektiivista ja subjektiivista vahinkoa ja täten niitä voidaan käyttää deterrenssi- tai ei-hyväksyttävällä vahingolla uhkaamiseen.[95] Kybertilassa tätä toimintaa voidaan nimittää kyberdeterrenssiviestinnäksi ja siihen voi kuulua esimerkiksi kohteen tietoverkkoihin tunkeutuminen tai näyttävien hyökkäysten tekeminen kolmatta osapuolta kohtaan – tarkoituksena on osoittaa kykyä, tahoa ja omia intressejä.[96] Informaatiokeinot toimivat ei-sotilaallisena ja tarvittaessa sotilaallisena keinona mahdollisten vastustajien muodostaman uhan manageroimisessa ennaltaehkäisevästi. Tällöin vaikutetaan vastustajaan tai sen liittolaisiin manipuloivasti tarvittaessa demonstraatioilla, rajoitetulla voimankäytöllä ja ylläpitämällä omaa valtiollista toimintakykyä ja tavanomaisen sekä ydinpelotteen suorituskykyä.[97] Ylläpitämällä kansallisten verkkojen ja johtamisjärjestelmien resilienssiä mahdolliselta hyökkääjältä kiistetään yllätyksellisen, lamauttavan iskun tarjoama etu. Tämän tulisi vaikuttaa hyökkääjän laskelmiin voimankäytön todennäköisyyden onnistumisesta ja kustannuksista.[98]

Sotilaallisen pidäkkeen pettäessä informaatioteknologisia keinoja voitaneen käyttää osana yllätyksellistä tai vastahyökkäyksellistä sotatoimea vastustajan kriittisten kohteiden tuhoamiseksi vastustajan pakottamiseksi lopettamaan aiottu tai alkanut hyökkäys tai omien asevoimien hyökkäysmahdollisuuksien edistämiseksi.[99] Kuten Pentti Forsström on todennut, strateginen deterrenssi on proaktiivinen konsepti, eikä toiminta perustu pelkästään reagointiin.[100] Kyberhyökkäykset osana informaatioteknologisia menetelmiä sopivat hyvin venäläisessä ajattelussa korostuvaan sodan alkua edeltävän vaiheen ja sodan alkuvaiheen ratkaisevuuteen. Ensimmäisessä vaikutetaan joukkojen käytön reunaehtoihin ja jälkimmäisessä strategisen yllätyksen saavuttamiseen ja vastustajan lamauttamiseen.[101] Huomioitava toki on, että venäläiset strategia-asiakirjat

---

[93] Калганов, В. А., Рыжов, Г. Б. & Соловьёв, И. В.: Стратегическое сдерживание как фактор обеспечения национальной безопасности Российской Федерации. Военная мысль, 8/2022, s. 6–14; Forsström (2021); Forsström, Pentti: *Venäjän sotilasstrategia muutoksessa. Tulkintoja Venäjän sotilasstrategian perusteiden kehityksestä Neuvostoliiton hajoamisen jälkeen*. Väitöskirja. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 1, Nro. 32, Helsinki, 2019.

[94] Герасимов, Валерий: Векторы развития военной стратегии. *Красная звезда* 4.3.2019. [http://redstar.ru/vektory-razvitiya-voennoj-strategii/], luettu 4.3.2019]. Tulkinnasta ks. Kofman et al. (2021).

[95] Forsström (2019); Forsström (2021), s. 84. Deterrenssivahinko liittyy vahinkoon, joka kumoaa aggressiosta saadut hyödyt. Sen yläraja on sietämätön vahinko, joka liittyy kohteen tuhoamiseen ja palautumiseen. Molemmat ovat kohteen määriteltävissä ja historiallisia. Deterrenssin käyttäjän tulee määritellä se väkivaltaisten ja täydentävien ei-väkivaltaisten keinojen taso, jolla vahingot saavutetaan. (Калганов, Рыжов & Соловьёв (2022)) Sietämätön tappio (неприемлемый ущерб) on voiton tuomat edut ylittävä vahinko, olennaisen toimintakyvyn menetys (Ковальчук, Александр & Мушков, Юрий: Сдерживание агрессии против РФ. *Арсенал отечества*, 58(2) 2022, s. 4–7).

[96] ks. Valeriano, Brandon, Jensen, Benjamin & Maness, Ryan C.: *Cyber Strategy: The Evolving Chracter of Power and Coercion*. Oxford University Press, New York, 2018, s. 140–141.

[97] Thomas (2019), s. 8-10–8-11; Kukkola (2020); Калганов, Рыжов & Соловьёв (2022); Кокошин, А. А.: Перспективы развития военной техносферы и будущее войн и небоевого применения военной силы. *Вестник Академии военных наук*, 67(2), 2019, s. 26–29. Jensen, Valeriano ja Maness ovatkin luonnehtineet rauhanajan kyberoperaatioita pakottavaksi diplomatiaksi. (Jensen, Valeriano & Maness (2019)).

[98] Kukkola (2022).

[99] Thomas (2019), s. 8-6; Cheravitch, Joe: *The Role of Russia's Military in Information Confrontation*. CNA, Washington, DC, 2021, s. 34; Kofman et al. (2021); Forsström (2021).

[100] Forsström (2021), 29–30.

[101] Thomas (2020), s. 134; Thomas, Timothy T.: The Evolving Nature of Russia's Way of War. *Military Review*, July-August 2017, s. 34-42; Сержантов, Смоловый & Терентьев (2022), s. 21.

esittävät Venäjän informaatioteknologisen toiminnan lähes poikkeuksetta puolustuksellisena tai ennaltaehkäisevänä.[102]

Venäläisten sotilaiden kirjoitusten perusteella voidaan todeta, että heidän näkemyksensä kyberaseiden (ohjelmistoase vast.) luonteesta on seurannut läntisiä näkemyksiä. Niitä pidetään helposti leviävinä, vaikutusetäisyydeltään globaaleina algoritmeina, joilla voi olla strategisia vaikutuksia. Ne ovat kontaktittomia asejärjestelmiä, halpoja ja helposti saatavavilla, yllättäviä, tarkkoja, käytettävissä rauhan aikana, vaikeasti torjuttavissa ja perustuvat haavoittuvuuksien hyödyntämiseen.[103] Yleisesti ottaen venäläiset näkevät informaation manipulaation tai sen kiistäminen altavastaajan tehokkaana ja halpana keinona saavuttaa strategisia päämääriä, minkä takia he pitävät informaatiosodankäyntiä asymmetrisenä.[104] Asymmetristen toimien avulla voidaan ylläpitää strategista tasapainoa heikkouden tilassa rauhankin aikana.[105] Uudet teknologiat ja niiden luova käyttö mahdollistavat yllätyksen hankkimisen oveluuden avulla.[106] Viimeisimpänä tällaisen teknologiana voitaneen pitää tekoälyä, joka on Venäjän valtiojohdon toimesta nostettu teknologiakehityksen prioriteetiksi.[107] Venäläisessä ajattelussa symmetrialla on ollut huono kaiku sen resurssi-intensiivisyyden takia.[108] Epäsuoria keinoja eli heikkouksiin, tahtoon, tilanneymmärrykseen ja päätöksentekoon vaikuttamista on esitetty vaihtoehdoksi.[109] Tämä on yksi syy siihen, miksi venäläiset pitävät informaatiovaikuttamista[110] tukevia kyberoperaatioita lupaavina keinoina poliittisten päämäärien saavuttamisessa niin rauhan kuin sodan aikana.[111] Informaatiopsykologinen vaikuttaminen on se informaation käytön muoto, jolla useimmat venäläiset lähteet katsovat olevan strategista potentiaalia.[112] Kyberhyökkäykset kriittistä informaatioinfra-

---

[102] Lilly & Cheravitch (2020), s. 136.
[103] Thomas (2020); Kukkola (2020).
[104] Thomas (2020); Kukkola (2020), s. 162; Kukkola (2022), s. 36.
[105] Pynnöniemi (2018), s. 252.
[106] Kukkola (2022); Орлянский (2022), s. 40; Thomas (2019), s. 5–2.
[107] Thornton, Rod & Miron, Marina: Interface between Artificial Intelligence and Cyber. Creating Revolution in Military Affairs? The Russian Military's Utilisation of Artificial Intelligence to Enhance its Cyber Operations: The Current State of Play. *Russian Concept of War, Management and Use of Military Pow*er. Forsström, Pentti (Toim.) National Defence University, Department of Warfare, Series 2, No. 19, Helsinki, 2022, s. 62–71, s. 65.
[108] Vaikuttaisi tosin siltä, että symmetria on tekemässä sotatieteellistä ja -taidollista paluuta Ukrainan operaation kokemusten seurauksena. Уланов, А. С., Завадский, В. В. & Зайченко, Я. Б.: Эффекты неоднозначности отношения превосходства при оценках сил противоборствующих сторон. *Военная мысль*, 1/2024, s. 45–58; Прокаев, А. Н. & Шабунин, А. А.: Отечественный и зарубежный опыт количественного обоснования решений в области применения сил (войск) флота. *Военная мысль*, 2/2024, s. 77–91.
[109] Сержантов, Смоловый & Терентьев (2022); Adamsky, Dmitry (Dima): Cross-Domain Coercion: The Current Russian Art of Strategy. *Proliferation Papers*, No. 54, November 2015, s. 29; Kofman et al. (2021), s. 83.
[110] "Informaatiovaikuttamisella tarkoitetaan toimintaa, jolla pyritään järjestelmällisesti vaikuttamaan yleiseen mielipiteeseen, ihmisten käyttäytymiseen ja päätöksentekijöihin sekä sitä kautta yhteiskunnan toimintakykyyn." (Valtioneuvosto kanslia: *Valtioneuvoston tehostetun viestinnän ohje. Viestintä normaalioloissa ja häiriötilanteissa*. Valtioneuvoston kanslian julkaisuja 23, Helsinki, 2019, s. 15). Englanninkielisessä kirjallisuudessa käytetään käsitettä cyber-enabled influencing, joka koostuu mm. tietomurtojen mahdollistamista tietovuodoista, disinformaatiosta ja sosiaalisen median manipulaatiosta sekä näiden vaikutuksen seurannasta data-analytiikalla. Lin, Herbert & Kerr, Jaclyn: On Cyber-Enabled Information Warfare and Information Operations. *The Oxford Handbook of Cyber Security*. Paul Cornish (Toim.) Oxford Academic. [https://doi.org/10.1093/oxfordhb/9780198800682.013.15], s. 251–272.
[111] Näitä voidaan pitää neuvostoliittolaisten ns. aktiivisten toimen moderni sovelluksena (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*, 33(3) 2020, s. 514–539; Rid, Thomas: *Active Measures. The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux, New York, 2020).
[112] Grisé et al. (2022); Grisé, Michelle, Shokh, Yuliya, Holynska, Khrystyna & Demus, Alyssa: Russian and Ukrainian Perspectives on the Concept of Information Confrontation. Translations, 2002–2020. RAND, Santa Monica, 2022.

struktuuriakin vastaan voivat aiheuttaa merkittäviä välillisiä psykologisia vaikutuksia.[113]

Informaatiomenetelmien asymmetrinen luonne vahvistaa venäläistä näkemystä informaatiosta uhkana. Tämän uhka ratkaisemiseksi venäläiset akateemikot ja sotilaat ovat esittäneet 2000-luvulta lähtien kokonaisturvallisuuden kaltaiseen konseptiin[114] perustuvaa informaatioturvallisuuden järjestelmän ja informaatiojoukkojen perustamista venäläisten suojelemiseksi ulkopuoliselta informaatioteknologiselta ja etenkin -psykologiselta vaikuttamiselta.[115] Informaatioturvallisuuden järjestelmän perustana toimisi yhtenäinen kansallinen informaatiotila (teknologinen ja sisällöllinen), joka perustuisi yhteisillä säännöille ja periaatteille, ja jonka hallinnasta vastaisi valtio. Tämä tila olisi vertikaalisti ja keskitetysti hallittu sekä horisontaalisti integroitu, eli sitä ohjattaisiin turvallisuuselinten hallinnoimilla hierarkkisilla järjestelmillä, jossa kaikki tieto kootaan huipulle ja jaetaan kontrolloidusti hierarkian eri tasojen välillä. Tilalla olisi myös selvät rajat. Informaatioturvallisuuden järjestelmällä toteutettaisiin tilan rajaaminen, rakentaminen, hallinta, puolustus ja yhteiskunnan sekä talouden informaatiovoimavarojen mobilisointi.[116] Venäjän kansallista internetsegmenttiä[117] eli Venäjän valtion hallitsemaa osaa globaaleista tietoverkoista voidaan pitää informaatioturvallisuuden järjestelmän heijasteena, vaikka itse järjestelmää ei sellaisenaan ole instituutiona perustettukaan. Ajatuksessa informaatioturvallisuuden järjestelmästä tiivistyy venäläinen käsitys valtio- ja yhteiskuntajärjestelmien välisestä, lähes kyberneettisestä taistelusta, jossa Venäjä tällä hetkellä omasta mielestään on Lännen kanssa ja jossa vastapuolen järjestelmän manipulointi voi johtaa voittoon.[118]

Venäläisen näkemyksen mukaan järjestelmien välinen informaatiokamppailu edellyttää informaatiovoimaa (информационная мощь). Informaatiovoima perustuu informaatiopotentiaaliin (информационный потенциал), joka on periaatteessa resurssipohja, inhimillinen ja materiaalinen, joka mahdollistaa informaatiovoiman, eli informaation, luomisen ja käytön määrätyllä hetkellä. Yhteiskunnan ja talouden mobilisointi sekä liittolaissuhteiden ylläpitäminen edellyttävät informaatiotilan ja -potentiaalin turvaamista. Valtion informaatiovoiman perusta on kyvyssä kontrolloida ja valjas-

---

[113] Tähän liittyy useita eri vaikutuksia kuten disorganisaatio, demoralisaatio, destabilisaatio ja disorientaatio (Дылевский, И. Н. и другие: О военной политике союзного государства в области международной информационной безопасности. *Военная мысль*, 9/2022, s. 7–11, s. 8).

[114] Esimerkiksi ks. Сержантов, А. В. & Павлов, Д. А.: Гибридный характер опасностейи угроз, их влияние на систему обеспечения военной безопасности Российской Федерации. *Военная мысль*, 5/2022, s. 7–12; Сайфетдинов, Х. И.: Гибридные войны, проводимые США и странами НАТО, их сущность и направленность. *Военная мысль*, 5/2022, s. 13–20; Коржевский, А. С. & Музяков, С. И.: Основные закономерности и принципы управления обороной государства в современных условиях. *Вестник Академии военных наук*, 80(3), 2022, s. 17–23.

[115] Kukkola (2020).

[116] Historiallisesta ja teoreettisesta näkökulmasta tarkasteltuna ks. Kukkola (2020). Viimeisimpänä visiona ks. Бартош, А. А.: Технологический суверенитет России как важный фактор победы в мировой гибридной войне. *Военная мысль*, 8/2023, s. 16–32.

[117] Kansallisen internetsegmentin käsite viittasi alun perin DNS-järjestelmän ccTLD domainien kansalliseen hallintaan, mutta on myöhemmin laajentunut tarkoittamaan valtion alueella ja sen suvereeni määräysvallan alla sijaitsevia internetin ja muiden tietoverkkojen infrastruktuuria, palveluita ja järjestelmiä sekä muuta teknologista perustaa. Ks. Seuraava luku (Kukkola, Juha: *The Military Strategic Effects of the Russian National Segment of the Internet*. Finnish Defence Studies 23. National Defence University, Helsinki, 2023, s. v). Kansallinen internetsegmentti ei ole sama asia kuin niin kutsuttu RuNet, joka viittaa suhteellisen suljettuun, online-ympäristöön, joka perustuu venäjän kielen käyttöön (Ristolainen (2017); Ristolainen & Kukkola (2019)).

[118] Ks. esim. Расторгуев (1999).

taa informaatiotila sisältöineen valtion käyttöön.[119] Seuraavassa luvussa tarkastellaankin sitä, miten venäläisten strategia-asiakirjojen[120] ja sotilasakateemikoiden kirjoitusten sisältämät strategisen kulttuurin ideat teknologisesta suvereniteetista, kriittisen informaatioinfrastruktuurin ja tiedon suojaamisesta, tietoverkkojen suojan ja resilienssin varmistamisesta, informaation ”totuusperäisyyden” varmistamisesta ja asevoimien johtamisjärjestelmien suojaamisesta ovat ohjanneet Venäjän informaatiopotentiaalin ja kansallisen kyberpuolustuksen ja -turvallisuuden rakentamista.

[119] Свиридов, Ю. В.: Информационный потенциал государства: сущность и содержание. *Военная мысль*, 7/2023, s. 125–134; Forsström (2019), s. 71–72; Расторгуев (1999), 144; Круглов, В. В.: Новый подход к анализу современного противоборства. *Военная Мысль*, 12/2006, s. 50–61.
[120] Ks. esim. Указ Президента РФ (2021b).

3. VENÄJÄN KYBERPUOLUSTUS 2000–2021

Venäjä on rakentanut kansallista kyberturvallisuutta ja -puolustustaan määrättyjä uhkakuvia vasten. Nämä ovat muuttuneet vain hieman vuosien varrella ja suurin muutos on tapahtunut informaatiopsykologisella puolella. Venäjän kansallisiin arvoihin kohdistuvien uhkien rakentamista on oikeutettu erilaisilla mentaalisen, kognitiivisen ja tietoisuussodankäynnin teorioilla.[121] 2010–2020-luvuilla informaation sisällöstä, oikeellisuudesta ja kansalaisten pääsystä siihen – ja muuhun tietoon pääsyn estämisestä – on tullut Venäjän kansallisen turvallisuuden prioriteettikysymys.[122]

Viimeaikaisia strategia-asiakirjoissa ja sotilaslehtien teksteissä esiintyviä informaatioteknologisia uhkia ovat:

- Tietoverkko- ja järjestelmätiedustelu
- Valtioiden tai terroristisen sekä ääriliikkeiden käyttämä informaatiokommunikaatioteknologinen tuhoava vaikuttaminen kriittiseen informaatioinfrastruktuuriin
- Informaatiokommunikaatioteknologian käyttö sotilaspoliittisten päämäärien ajamiseksi Venäjän suvereniteetin, alueellinen eheyden ja talouden rapauttamiseksi ja strategisen tasapainon horjuttamiseksi
- Informaatiokommunikaatioteknologian käyttö informaatiovaikuttamisen tukemiseksi venäläisen arvopohjan ja yhteiskunnan rapauttamiseksi tai kansainvälisen aseman heikentämiseksi
- Tietokonerikollisuus ja informaatioteknologinen jälkeen jääminen kilpailijoista ja Venäjän teknologisen kehityksen tahallinen heikentäminen.

Pääuhkatoimijoita ovat valtiot, etenkin Yhdysvallat ja sen liittolaiset, tai niiden sponsoroimat tahot ja itsessään informaatiotilan nykyinen luonne, joka vaikeuttaa attribuutiota ja mahdollistaa anonymiteetin, sekä antaa Yhdysvalloille ja kansainvälisille suuryrityksille mahdollisuuden käyttää johtavaa teknologista asemaansa hyväkseen.[123]

Venäläiset uhkakuvat eivät ole aivan tuulesta temmattuja ottaen toki huomioon sen, että se on itse omalla toiminnallaan ollut luomassa perustaa näiden uhkakuvien synnylle. Yhdysvallat perusti vuonna 2010 asevoimiinsa kyberjohtoportaan (U.S. Cyber Command), jonka toimintakonseptina on vuodesta 2018 ollut ns. etupainoinen puolustus (defending forward). Tämä tarkoittaa ennaltaehkäisevää toimimista vastustajan

[121] Jonsson (2019); Pynnöniemi (2019); Kukkola (2020); Fridman (2020).
[122] Interfax: Путин высказался за незыблемость цифрового суверенитета всех стран. Interfax.ru, 26.3.2021. [https://www.interfax.ru/russia/758107], luettu 2.2.2024.
[123] Указ Президента РФ (2016); Указ Президента РФ (2023); Распоряжение Правительства РФ (2023); Указ Президента РФ (2021); Российская Федерация: Обновленная концепция конвенции организации объединенных наций об обеспечении международной информационной безопасности. Предложение Российской Федерации. 16.5.2023. [http://www.scrf.gov.ru/security/information/Inf_conc/], luettu 2.2.2024; Селиванов, В. В. & Ильин, Ю. Д.: Тенденции развития средств вооруженной борьбы в современных военных конфликтах, их влияние на развитие и смену поколений вооружения, военной и специальной техники. *Военная Мысль*, 19/2022, s. 29–44; Кулаков, А. А.: Задачи информационной политики Российской Федерации в условиях «гибридной войны» с коллективным западом. *Вестник академии военных наук*, 82(1) 2023, s. 17–25; Гаврилов, А. Д., Грудинин, И. В. & Новиков, В. А.: трансформация системы угроз национальной безопасности России и специальная военная операция. *Вестник академии военных наук*, 82(1) 2023, s. 6–16; Баранов, В. П. & Болгов, Н. В.: Противодействие угрозам военной безопасности на современном этапе развития России. *Вестник академии военных наук*, 84(3) 2023, s. 16–21.

verkoissa ja deterrenssin rakentamista.[124] Komentoportaan perustamisen taustalla olivat Venäjän kybervakoiluoperaatiot.[125] Yhdysvallat liittolaisineen on käyttänyt hyökkäyksellisiä kyberoperaatiota Pohjois-Koreaa, Irania, ISIS:tä ja venäläistä Internet Research Agency -yritystä (ns. trollitehdas) vastaan.[126] Yhdysvallat asetti Venäjälle sanktioita ulkomaantiedustelupalvelun SVR:n (Служба внешней разведки Российской Федерации) SolarWinds -operaatioon liittyen.[127] Yhdysvallat on myös toimeenpannut kyberavusteisia informaatio-operaatioita mm. Lähi-idässä.[128] Se on hyvin mahdollisesti osallistunut Venäjän valtiojohdolle kiusallisten tietovuotojen toteuttamiseen[129] ja on liittolaisineen toteuttanut globaalia tietoverkko- ja järjestelmävakoilua mukaan lukien tietomurron johtavaa venäläistä ICT-alan yritystä Yandexia vastaan ja mahdollisesti tunkeutunut SORM-järjestelmään.[130] Yhdysvaltojen tiedustelupalvelut ovat myös jääneet kiinni yhdysvaltalaisten yritysten tuotteiden haavoittuvuuksien hyväksikäytöstä.[131] Nato on vuodesta 2016 lähtien pitänyt kybertilaa sodankäynnin toimintaympäristönä (domain) ja laatinut siihen liittyvän doktriinin[132] ja vuodesta 2022 se on omaksunut yhdysvaltalaisen näkemyksen ”kilpailujatkumosta” (continuum of competition) kansainvälisiä suhteita kuvaavana mallina, mikä on hyvin lähellä venäläistä näkemystä valtioiden välisestä jatkuvasta kamppailusta.[133] Myös strateginen kumppani Kiina on kohdistanut Venäjään teknologista ja talouskybervakoilua.[134] Mikään edellä esitetty ei vähennä Venäjän autoritaarisen johdon intressien merkitystä maan infor-

[124] Di Pane, James: Cyber Warfare and U.S. Cyber Command. The Heritage Foundation, 24.1.2024. [https://www.heritage.org/military-strength/assessment-us-military-power/cyber-warfare-and-us-cyber-command], luettu 2.2.2024.
[125] Healey, Jason (ed.): *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*. CCSA, Vienna, 2013.
[126] Council on Foreign Relation: Cyber Operations Tracker. [https://www.cfr.org/cyber-operations/], luettu 2.2.2024; Smeets, Max: A US history of not conducting cyber attacks. *Bulletin of the Atomic Scientists*, 11.7.2022. [https://thebulletin.org/premium/2022-07/a-us-history-of-not-conducting-cyber-attacks/], luettu 2.2.2024.
[127] Greenberg, Andy: US Sanctions on Russia Rewrite Cyberespionage's Rules. *WIRED*, 15.4.2021. [https://www.wired.com/story/us-russia-sanctions-solarwinds-svr/], luettu 2.2.2024.
[128] Faife, Corin: The Pentagon has ordered a review of US psyops on social media. *The Verge*, 19.9.2022. [https://www.theverge.com/2022/9/19/23360688/pentagon-review-military-influence-operations-social-media], luettu 2.2.2024.
[129] Jajecznyk, Stefan: The Dark Side of the Kremlin: Hacked Russian documents explained. *Al-Jazeera*, 26.2.2019. [https://www.aljazeera.com/features/2019/2/26/the-dark-side-of-the-kremlin-hacked-russian-documents-explained], luettu 2.2.2024.
[130] Zetter, Kim: Leaked Files Show How the NSA Tracks Other Countries' Hackers. *The Intercept*, 6.3.2018. [https://theintercept.com/2018/03/06/leaked-files-show-how-nsa-tracks-other-countries-hackers/], luettu 2.2.2024; Bing, Christopher, Stubbs, Jack & Menn. Joseph: Exclusive: Western intelligence hacked 'Russia's Google' Yandex to spy on accounts – sources. *Reuters*, 28.6.2019. [https://www.reuters.com/article/us-usa-cyber-yandex-exclusive/exclusive-western-intelligence-hacked-russias-google-yandex-to-spy-on-accounts-sources-idUSKCN1TS2SX], luettu 2.2.2024; Maurizi, Stefania: New revelations from the Snowden archive surface. *Computer Weekly.com*, 19.9.2023. [https://www.computerweekly.com/news/366552520/New-revelations-from-the-Snowden-archive-surface], luettu 2.2.2024.
[131] Armasu, Lucian: Backdoors Keep Appearing in Cisco's Routers. *Tom's Hardware*, 19.7.2018. [https://www.tomshardware.com/news/cisco-backdoor-hardcoded-accounts-software,37480.html], luettu 2.2.2024; Robertson, Jordan: Juniper Breach Mystery Starts to Clear with New Details on Hackers and U.S. Role. *BNN Bloomberg*, 2.9.2021. [https://www.bnnbloomberg.ca/juniper-breach-mystery-starts-to-clear-with-new-details-on-hackers-and-u-s-role-1.1647206], luettu 2.2.2024.
[132] NATO: Allied Joint Publication-3.20. Allied Joint Doctrine for Cyberspace Operations. Edition A Version 1 January 2020. [https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf], luettu 2.2.2024.
[133] NATO: Allied Joint Publication-01 Allied Joint Doctrine. Edition F Version 1 with UK national elements December 2022 [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1148298/AJP_01_EdF_with_UK_elements.pdf.pdf], luettu 2.2.2024.
[134] Bergman, Ronen & Conger, Kate: Chinese Hackers Tried to Steal Russian Defense Data, Report Says. The *New York Times*, 19.5.2022. [https://www.nytimes.com/2022/05/19/world/asia/china-hackers-russia.html], luettu 2.2.2024.

maatiotilan kontrolloimisessa ja toimia oikeuttavien uhkakuvien luomisessa, mutta asettavat ne kybertilan ja suurvaltasuhteiden kehityksen kontekstiin.[135]

3.1. Kansallisen informaatiotilan turvallisuus ja puolustus

Vaikka Venäjän johto otti jo 2000-luvun alussa hallintaansa kansallisen informaatiotilan perinteisemmät osat, TV:n ja lehdistön, internet sai Venäjällä kehittyä suhteellisen rauhassa ja markkinavetoisesti aina 2010-luvun alkuun saakka. Tämä toki tarkoitti, että lainsäädännöllinen sääntely oli vähäistä, kyberrikollisuus yleistä ja että yhteiskunnan kriittinen informaatioinfrastruktuuri palveluineen oli yksityisyritysten käsissä. Vuonna 2011 internettiä käytti 44 % väestöstä, mutta pääosa ihmisistä sai uutisensa televisiosta. Venäjälle oli kuitenkin kehittynyt vahva kotimainen, kilpailukykyinen internetpalvelutarjonta lippulaivoinaan Yandex, VKontankt, Odnoklassniki, Mail.ru ja Rambler, mikä mahdollisti venäjänkielisen, suhteellisen itseriittoisen online-yhteisön synnyn. Maan televerkot olivat pääosin viiden suuren operaattorin hallussa, joista Rostelekom oli suurin ja valtio-omisteinen. Internetpalveluntarjoajia (Internet Service Provider – ISP) oli satoja, mutta pääosa myi vain eteenpäin suurien operaattorin palveluja. Presidentti Dmitri Medvedevin (2008–2012) kauden loppuun asti valtio näki yksityissektorin valtion informaatiotalouden rakentajana ja pyrki tukemaan sitä liberaalissa ja yhteistyöhakuisessa hengessä. Informaatiotilan teknologisia pääuhkia olivat rikollisuus ja terrorismi. Venäjän turvallisuuspalvelut, asevoimat ja osa poliitikoista kuitenkin tunnistivat 1990-luvulta lähtien Yhdysvaltojen ICT-teknologisen vahvuuden kansalliseksi uhaksi. Venäjä pyrki ehkäisemään valtioiden kybersuorituskykyjen käyttöä, todellisuudessa informaatiovaikuttamista, ajamalla YK:n piirissä kansainvälistä informaatioturvallisuussopimusta siinä kuitenkaan onnistumatta.[136]

Tilanne muuttui voimakkaasti vuosina 2011–2012. Sosiaalinen media vaikutti Lähi-idässä vuosina 2009–2011 puhjenneiden levottomuuksien leviämiseen ja Venäjä tulkitsi Lännen intressien vaikuttavan niiden taustalla. Venäjällä osoitetiin mieltä 2011 duuman vaalien tulosten väärentämistä ja tämän jälkeen Vladimir Putinin presidentiksi uudelleen valintaa vastaan. Yhdysvaltojen ja Venäjän suhde heikkeni. Yhdysvaltojen perustaman kyberjohtoportaan nähtiin uhkaavan Venäjää. Venäjän talous ei kehittynyt toivotulla tavalla. Vuonna 2013 Edward Snowdenin paljastamat tiedot Yhdysvaltojen kansallisen turvallisuusviraston (NSA) harjoittamasta vakoilusta legitimoivat Venäjän valtiojohdon pelot. Se aloitti internetpolitiikan tiukentamisen säätämällä joukon lakeja, joilla rajoitettiin ilmaisunvapautta internetissä ja luotiin ensimmäiset, poliittisesti ohjatut, estolistat. Vaikka kielletyn informaation poistaminen annettiin ISP:iden ja sivustojen ylläpitäjien vastuulle, myös viranomaiset saivat oikeuden estää pääsyn verkkosivustoille ja vuosien kuluessa tätä oikeutta on laajennettu niin, ettei estoihin käytännössä tarvitse oikeudellisesti ja hallinnollisesti läpinäkyvää päätöstä. Lainsäädäntöön luotiin käsite ”informaation jakamisen organisoija”, jonka perusteella kaikkia mediayhtiöistä bloggareihin on vaadittu vastuuseen alustoillaan julkaistusta informaatiosta ja myös vaadittu luovuttamaan käyttäjiensä viestejä ja henkilötietoja turvallisuuspalveluille. Vaikka kiristynyt lainsäädäntö helpottikin opposition valvontaa ja sen toi-

[135] Digitaalisesta autoritarismista ks. Howells, Laura & Henry, Laura A.: Varieties of Digital Authoritarianism. *Communist and Post-Communist Studies*, Vol. 54, Number 4, s. 1–27; Sinkkonen, Elina & Lassila, Jussi: Digital Authoritarianism and Technological Cooperation in Sino-Russian Relations: Common Goals and Diverging Standpoints. *Russia-China Relations. Emerging Alliance or Eternal Rivals?* Kirchberger, Sarah, Sinjen, Svenja & Wörmer, Nils (Toim.) Springer, 2022, s. 165–184. [https://doi.org/10.1007/978-3-030-97012-3].
[136] Tapahtumien kuvaus perustuu Kukkola (2020).

minnan hankaloittamista, oli Venäjän liittovaltion turvallisuuspalvelu FSB:llä (Федеральная служба безопасности Российской Федерации) jo ennestään käytössään televerkkotiedusteluun käytetty SORM-järjestelmä (Система технических средств для обеспечения функций оперативно-разыскных мероприятий), joka oli vuodesta 1998 kyennyt kaappaamaan TCP/IP liikennettä.[137]

Varsinaisiin kyberuhkiin päätettiin vastata rakentamalla GosSOPKA (Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак) järjestelmä havaitsemaan ja estämään tietokonehyökkäyksiä kriittistä informaatioinfrastruktuuria vastaan. Kyseessä on käytännössä valtion laajuinen SIEM-järjestelmä, jota FSB hallinnoi ja jonka kaikki kriittistä informaatioinfrastruktuuria hallinoivat tahot on lailla velvoitettu asentamaan verkkoihinsa. Kriittisen informaatioinfrastruktuurin (KII) käsite ilmaantui Venäjällä viralliseen käyttöön 2012 ja se määritteli valtiovallan suhteen internetin infrastruktuuriin. Tässä suhteessa korostui valtion suvereeni oikeus suojella ja säädellä infrastruktuuria. GosSOPKA:n järjestelmän rakentaminen viivästyi aina vuoteen 2017, jolloin Venäjällä säädettiin laki kriittisestä informaatioinfrastruktuurista, johon sisällytettiin käytännössä hallinnon, tieteen ja talouden kriittisten sektoreiden infrastruktuuri. Viivästymisen taustalla oli Viestintä- ja teleliikenneministeriön ja FSB:n kiista toimivallasta. Laista huolimatta kriittisen informaatioinfrastruktuurin käsite on edelleen monitulkintainen ja mahdollistaa valtiovallan merkittävän puuttumisen yksityissektorin toimintaan.[138] Samaan aikaan GosSOPKA:n kanssa Venäjä alkoi rakentaa valtiollista tilannekeskusten verkostoa, jonka tuli kerätä tieto maan poliittisesta, taloudellisesta ja yhteiskunnallisesta tilanteesta ylimmän johdon päätöksenteon tueksi.[139] Kybertilan informaatiovirtojen ohjaamisen taustalla oli havaittavissa kaikuja neuvostoliittolaisista kyberneettisistä yhteiskunnan ja talouden kontrollia tavoitelleista hankkeista.[140]

Krimin miehittäminen ja Venäjän järjestämä kansannousu Itä-Ukrainassa vuonna 2014 johtivat Lännen asettamiin sanktioihin ja yleiseen kansainvälisen ilmapiirin kiristymiseen. Informaatio- ja kybertilasta tuli Venäjälle kansallisen turvallisuuden keskeinen kysymys, kun riippuvuus globaaleista tietoverkoista, etenkin niistä ulossulkemisesta, ja yhdysvaltalaisista ICT-yrityksistä turvallistettiin. Ukrainan tapahtumat haluttiin Venäjällä tulkita läntiseksi värivallankumoukseksi[141] ja omat toimet puolustuksellisiksi. Kiina oli näyttänyt jo vuodesta 2009 mallia siitä, miten internetsensuuri kyettiin toimeenpanemaan tehokkaasti ja miten läntisten yritysten vaikutusvaltaa murta-

[137] Ibid.
[138] Ibid.
[139] Cooper, Julian: Strategic Planning, Situation Centres and the Management of Defence in Russia: An Update. Changing Character of War Centre, Pembroke College, Oxford [http://www.ccw.ox.ac.uk/blog/2018/11/14/strategic-planning-situation-centres-and-the-management-of-defence-in-russia-an-update-by-julian-cooper], luettu 2.2.2024; Королев, Игорь: ФСО дадут 700 миллионов на развитие сети распредцентров органов власти. *CNews,* 18.9.2013. [https://www.cnews.ru/news/top/2023-09-18_fso_dadut_700_millionov_na] luettu 2.2.2024; Сухарев, Сергей & Ильин, Николай: «СЦ необходимы и должны быть в каждом субъекте Российской Федерации». *Jetinfo*, 5.12.2017. [https://www.jetinfo.ru/interviews/scz-neobhodimy-i-dolzhny-byt-v-kazhdom-subekte-rossijskoj-federaczii/], luettu 2.2.2024.
[140] Näistä ks. Peters, Benjamin: *How Not to Network a Nation: The Uneasy History of the Soviet Internet*. MIT Press, Cambridge, 2016.
[141] Värivallankumous on venäläinen käsite, joka viittaa ulkoa johdettuun vallankumoukseen ks. Nikitina, Yulia: The "Color Revolutions" and "Arab Spring" in Russian Official Discourse. *Connections*, Vol. 14, No. 1 (Winter 2014), s. 87–104.

maan.[142] Kesällä 2014 pidettiin valtakunnallinen kyberharjoitus, jonka on väitetty osoittaneen, että kansallinen internetsegmentti oli haavoittuvainen. Venäjän turvallisuusneuvosto todennäköisesti käski Viestintä ja teleliikenneministeriötä löytämään ratkaisun havaittuihin ongelmiin. FSB:llä ja Puolustusministeriöllä oli aiheesta omat näkemyksensä ja varsinainen ratkaisu saatiin vasta vuonna 2017.[143]

Venäjällä jatkettiin internetin uutis- ja somealustojen säätelyä tekemällä palveluntarjoajat vastuullisiksi alustoillaan levitettävän tiedon aitoudesta ja laillisuudesta. Viestintäsovellusten tarjoajia vaadittiin tunnistamaan asiakkaansa ja yleisesti pyrkimys hävittää kaikenlainen anonymiteetti tiedonjakamisen piirissä vahvistui voimakkaasti. Vuoteen 2017 mennessä säädettiin lakeja, joilla vaadittiin säilyttämään venäläisten henkilökohtainen data Venäjällä, rajoitettiin ulkomaalaisten omistusta media- ja telekommunikaatioyhtiöissä ja vaadittiin yhtiöitä ilmoittamaan, mikäli ne saivat ulkomaalaista rahoitusta. Niin kutsutut antiterrorismilait (ns. Jarovaja-laki) vuodelta 2016 edellyttivät internetpalveluntarjoajia keräämään kaiken välittämänsä datan, säilyttämään sen useiden kuukausien ajan ja luovuttamaan datan viranomaisille käskettäessä. Vaatimuksia oli käytännössä mahdoton täyttää ja yritysten vastarinta on osittain jatkunut tähän päivään saakka. Kiristynyt säätely johti yhteenottoon sosiaalisen median palveluiden kanssa. Googlea, Facebookia ja Twitteriä uhattiin useaan otteeseen sakoilla ja LinkedIn käyttö kiellettiin. Venäjän valtiovalta yritti saada Telegram-palvelun luovuttamaan viestiliikenteen salausavaimet FSB:lle, mutta epäonnistui lopulta yrityksissään estää palvelun käyttö Venäjällä.[144] Roskomnazor pyrki Revizor-järjestelmän avulla valvomaan internetpalveluntarjoajien kykyä ja halua estää käyttäjien pääsy mustalistattuihin verkkoresursseihin, mutta tämä aiheutti monenlaisia ongelmia kuten mustalistaus itsekin.[145] Valtiovallan halu lisätä venäläisen internetin kontrollia ei siis kulkenut käsikädessä kyvyn kanssa – puhumattakaan yksityissektorin tuesta.

Kiristyneen säätelyn varjolla Venäjän internetpalveluntarjoajien ja teleyhtiöiden omistus alkoi enenevässä määrin siirtyä Putinia lähellä olevien liikemiesten omistukseen. Valtionyhtiö Rostelekom hankki itselleen aikaisemmin yhdistysten hallinnoimia internetin toiminnalle kriittisiä nimi- ja reitityspalveluita ja -pisteitä (Internet eXchange Point IXP). Rostelekom ja Rosteh, toinen valtion teknologiayritys, hankkivat omistukseensa menestyviä pieniä ja keskisuuria kyberalan yrityksiä. VKontakt, Mail.ru ja Odnoklasniki päätyivät oligarki Ališer Usmanovin yhtiön omistukseen vuonna 2016 ja vuonna 2021 VK:ksi uudelleen nimettynä valtioyhtiö Gaspromin omistukseen.[146] Vuonna 2019 Yandex joutui taipumaan omistus- ja hallintojärjestelyihin, jotka varmistivat Kremlin omistaman Sberpankin hallinnan yrityksestä.[147] Käytännössä Venäjän

[142] Griffiths, James: *The Great Firewall of China: How to Build and Control an Alternative Version of the Internet*. Zed Books Ltd., London, 2019.
[143] Tapahtumien kuvaus perustuu Kukkola (2020).
[144] Ibid.
[145] Stadnik, Ilona: Control by infrastructure: Political ambitions meet technical implementations in RuNet. *First Monday*, April 2021. [DOI:10.5210/fm.v26i5.11693].
[146] Mikadze, Ana: Digital Iron Curtain: Russia's Quest for Internet Sovereignty. *Ridl.io*, 14.9.2023. [https://ridl.io/digital-iron-curtain-russia-s-quest-for-internet-sovereignty/], luettu 5.1.2024; Scott, Mark: Mail.ru Takes Full Ownership of VKontakte, Russia's Largest Social Network. *The New York Times*, 16.9.2014, [https://archive.nytimes.com/dealbook.nytimes.com/2014/09/16/mail-ru-takes-full-ownership-of-vkontakte-russias-largest-social-network/], luettu 2.2.2024.
[147] Gershkovich, Evan: The uneasy coexistence of Yandex and the Kremlin. *MIT Technology Review*, 19.8.2020. [https://www.technologyreview.com/2020/08/19/1006438/yandex-putin-arkady-volozh-kremlin/], luettu 5.1.2024.

ICT-sektori alkoi muistuttaa omistusjärjestelyiltään media- ja energiasektoreita, joissa valtio suoraan tai epäsuorasti kontrolloi merkittävimpiä toimijoita.

Venäjän asevoimat heräsivät puolustusministeri Anatoli Serdjukovin ja myöhemmin Sergei Šoigun johdolla informaatioaikakauteen (tosin puolustusministeri Sergei Ivanov oli jo 2000-luvun alussa tunnistanut asian tärkeyden)[148] ja aloittivat verkostokeskeisen sodankäynnin suorituskykyjen, ”informaatiojoukkojen” ja ”sotilasinternetin” kehittämisen osana asevoimien reformia. Työlistalle kuului Venäjän satelliittilaivaston uusiminen ja etenkin GLONASS järjestelmän saattaminen operatiiviseksi. Asevoimat kehittivät omaa koko organisaation laajuista, integroitua johtamisjärjestelmää (OATsSS tai MTSS) siihen kuuluvine viestijärjestelmineen. Sen ytimeksi rakennettiin vuonna 2014 Kansallinen puolustuksen johtamiskeskus Moskovaan, jonka tuli mahdollistaa strategisten operaatioiden johtaminen, muodostaa poliittisstrateginen tilannekuva maailmasta ja Venäjältä ja yhdistää kaikkien liittovaltion turvallisuusviranomaisten tilannekuva ja johtaminen. Keskuksen ytimenä toimi supertietokone, jonka väitettiin olevan kykenevä ennustamaan konfliktien kulkua.[149]

Vuonna 2016–2017 Venäjän hallitus hyväksyi joukon informaatioyhteiskunnan ja talouden rakentamiseen liittyviä ohjelmia ja strategioita mukaan lukien uuden informaatioturvallisuusdoktriinin.[150] Nämä strategia-asiakirjat turvallistivat kansallisen informaatiotilan, ottivat viralliseen käyttöön kansallisen internetsegmentin käsitteen ja niiden pohjalta laadittiin ensimmäinen digitaalisen talouden ohjelma, joka teki digitaalisen suvereniteetin tavoittelusta vuoteen 2024 mennessä Venäjän valtiojohdon virallisen linjan. Ohjelma yhdisti talous- ja turvallisuustekijät ja asetti tavoitteeksi riippumattomuuden ulkomaisista ohjelmistoista, ICT-järjestelmistä ja salausjärjestelmistä sekä tietoverkoista. Se asetti tavoitteeksi turvallisen ja kestävän kansallisen tiedonsiirto- ja säilytysinfrastruktuurin rakentamisen. Vuonna 2018 ohjelma sai kansallisen ohjelman statuksen. Sen alkuperäinen budjetti vuosille 2019–2024 oli 3,5 triljoonaa ruplaa (15,5 $ mrd vuoden 2019 kurssilla), mutta tämä on vuosien varrella laskenut n. 2 triljoonaan. Valtionyritykset vastaavat suurilta osin rahoituksesta ja vastaavasti pääosa valtion budjettivaroista on mennyt valtionyhtiöille.[151] Vaikka Viesti- ja teleliikenneministeriö otti ohjelmasta vetovastuun, kansallisilla turvallisuusviranomaisilla on ollut merkittävä rooli alaohjelmien ohjaamisessa ja toteuttamisessa, ja etenkin informaatioturvallisuuden alaohjelmassa korostuvat Venäjän johdon uhkakuvat. Digitaalisen talouden ohjelmaan on myöhemmin lisätty tekoälyohjelma (jonka kehittämisesti laadittiin myös erillinen strategia)[152] ja internetsatelliittiohjelma, mikä osoittaa näiden teknologioiden tärkeyden valtiojohdolle.[153] Lisäksi vuonna 2018 ohjelmaa päivitettiin ja siihen lisättiin

[148] The Defence Ministry of the Russian Federation: The priority tasks of the development of the armed forces of the Russian Federation, 2004 [http://red-stars.org/doctrine.pdf], luettu 30.3.2019.
[149] Газета.Ru: Национальный центр управления обороной Российской Федерации. Газета.Ru, n.d. [https://www.gazeta.ru/tags/organization/ntsuo_rf.shtml], luettu 2.2.2024.
[150] Liittoneuvosto laati luonnoksen Venäjän kyberturvallisuuskonseptista vuosina 2012–2013, mutta sitä ei ikinä hyväksytty.
[151] Tadviser.ru: Финансирование национального проекта Цифровая экономика. *Tadviser.ru*, 31.1.2024. [https://www.tadviser.ru/index.php/Статья:Финансирование_программы_Цифровая_экономика#], luettu 2.2.2024.
[152] Указ Президента РФ от 10 октября 2019 г. № 490 "О развитии искусственного интеллекта в Российской Федерации.” [https://www.garant.ru/products/ipo/prime/doc/72738946/], luettu 2.2.2024; Путин, Владимир: Совещание по вопросам развития технологий в области искусственного интеллекта. *Kremlin.ru*, 30.5.2019 [http://www.kremlin.ru/events/president/news/60630], luettu 2.2.2024.
[153] Russia Briefing: Russia Accelerates Its Artificial Intelligence Development Program. *Russia Briefing*, 1.2.2023. [https://www.russia-briefing.com/news/russia-accelerates-its-artificial-intelligence-development-

”tiekartat” poikkileikkaaville teknologoille tekoälylle, robotiikalle, big datalle, lohkoketjuteknologialle, kvanttiteknologialle, uusille tuotantoteknologioille, teolliselle internetille, langattomalle tiedonsiirrolle ja virtuaali- ja lisätylle todellisuudelle.[154] Listaus kuvastaa Venäjän johdon näkemystä kriittisistä tulevaisuuden teknologioista, joka ei juuri poikkea länsimaisista.

Vuonna 2019 hyväksyttiin lakimuutospaketti, joka sai epävirallisen nimen ”laki suvereenista internetistä.”[155] Se käytännössä määritteli Venäjän kansallisen kyberturvallisuuden perustaksi kansallisen segmentin resilienssin, turvallisuuden ja eheyden ja käski rakentaa valtakunnallisen uhkien torjunnan teknisen järjestelmän (технические средства противодействия угрозам – TSUP)[156], jota operoi viestinnän valvontaviraston Roskomnadzorin alle perustettu julkisten verkkojen monitorointi ja hallintakeskus (Центра мониторинга и управления сетью связи общего пользования – TsMUSSOP), ja jolla voidaan suodattaa ja estää verkkoliikenne valtakunnallisesti. Kyseessä on Deep Packet Inspect (DPI) teknologiaan perustuva standardoitu ratkaisu, jolle on useita lisensoituja toteuttajia, ja jonka jokaisen ISP:n pitää asentaa järjestelmiinsä. Käytännössä järjestelmä kykeni suodattamaan ja estämään kaiken verkkoliikenteen Venäjän internetsegmentissä. Myöhemmin vuonna 2021 TSPU:lle hahmoteltiin myös roolia palvelunestohyökkäysten torjuntajärjestelmänä.[157] Laki suvereenista internetistä vaati myös kahdentamaan kansallisen internetsegmentin kriittiset järjestelmät ja kielsi julkishallinnolta ja valtionyrityksiltä ulkomaisten datakeskusten käytön. Testit järjestelmän käyttöönottamiseksi aloitetiin 2019 samalla, kun kansallisen kyberturvallisuuden kehittämisen tueksi alettiin rakentaa kyberharjoitusympäristöjä.[158] Vuoden 2019 laki oli virstapylväs siinä mielessä, että se teki tosiksi monia venäläisten poliitikkojen, akateemikkojen ja asiantuntijoiden autoritaarisia ideoita informaatio- ja teknologisesta suvereniteetista. Samalla tietoverkkojen resilienssistä, turvallisuudesta ja eheydestä on tullut valtiollisen kyberturvallisuuden synonyymi vastaava termin puuttuessa virallisesta kielenkäytöstä.

Vuosina 2020–2021 COVID-19 pandemia ja osaltaan yksityissektorin vastustus hidastivat digitaalisen talouden hankkeita. Valko-Venäjän opposition mielenosoitukset ja vuoden 2021 syksyllä järjestetyt duuman vaalit ajoivat Venäjän valtiojohdon kuitenkin tehostamaan kyber- ja informaatioturvallisuuteen liittyviä hankkeita. Taustalla vaikuttivat myös Yhdysvaltojen teknologiasanktiot venäläisiä kyberalan yrityksiä vastaan sekä niitä edeltäneet venäläisten kyberhyökkäysten ja vaalivaikuttamisen julkiset attribuoinnit Venäjän tiedusteluorganisaatioihin.[159] Maaliskuussa 2021 Putin vaati turval-

program.html/], luettu 5.1.2024; TASS: Putin sets task to boost production of domestic satellites for various purposes. *TASS*, 12.4.2023. [https://tass.com/politics/1603343], luettu 5.1.2024.

[154] Tadviser.ru: Сквозные технологии цифровой экономики. cross-cutting technology. end-to-end technology. *Tadviser.ru*, 10.4.2023. [https://www.tadviser.ru/index.php/Статья:Сквозные_технологии_цифровой_экономики], luettu 2.2.2024.

[155] 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.

[156] Comnews: ТСПУ по правилам и без. *Comnews*, 31.3.2021. [https://www.comnews.ru/content/213851/2021-03-31/2021-w13/tspu-pravilam-i-bez], luettu 5.1.2024.

[157] Интерфакс: Центр управления сетью связи в РФ займется глобальными хакерскими атаками. *Интерфакс*, 20.10.2021. [https://www.interfax.ru/russia/798386], luettu 2.2.2024.

[158] Kukkola (2020); Comnews: На пяти киберполигонах пройдут учения в 2021 году. *Comnews*, 14.5.2021. [https://www.comnews.ru/content/214490/2021-05-14/2021-w19/pyati-kiberpoligonakh-proydut-ucheniya-2021-godu], luettu 2.2.2024.

[159] U.S. Department of the Treasury: Press Releases: Treasury Sanctions Russia with Sweeping New Sanctions Authority. April 15, 2021. [https://home.treasury.gov/news/press-releases/jy0127], luettu 2.2.2024.

lisuuspalveluita vahtimaan internettiä ja väitti sen hajottavan yhteiskuntaa.[160] Lopputuloksena median sääntelyä kiristettiin edelleen, oppositiopuolueiden online-resurssit käytännössä blokattiin ennen syksyn 2021 duuman vaaleja, Twitter-liikennettä kuristettiin, TSPU:n avulla toteutettiin tilapäinen VPN:n esto – jota oli aikaisemmin pidetty teknisesti mahdottomana – ja myöhemmin osa VPN-palveluista kiellettiin pysyvästi. Lisäksi testattiin globaalista internetistä irtautumista ja ulkomaiset internetyritykset pakotettiin rekisteröitymään Venäjälle.[161] Google ja Apple taipuivat painostukseen ja poistivat omatoimisesti oppositiopoliitikko Aleksei Navalnyin äänestyssovelluksen palveluistaan.[162] Huolimatta viivästyksistä ”suvereenin internetin” rajaus-, kontrolli- ja puolustuselementit olivat vuoden 2021 lopulla kehittymässä kohti tavoitetta.

Kansallisen informaatiotilan voimavarojen mobilisointi ja osiltaan hallinta eivät edenneet yhtä menestyksekkäästi. Venäjän johto vaati Digitaalisen kehityksen, teleliikenteen ja massaviestinnän ministeriöksi (Mintsifr) muuttuneen Viesti- ja teleliikenneministeriön suulla julkishallintoa ja valtionyrityksiä siirtymään kotimaisen ohjelmiston ja ICT-järjestelmien käyttöön vuoteen 2024–2025 mennessä, mikä oli täysin mahdoton tehtävä.[163] Venäjältä puutuivat kotimaiset yleiseen käyttöön sopivat käyttöjärjestelmät, toimisto-ohjelmistot, ja tuotannonohjaus- sekä teollisuusohjelmistot. Laitetuotanto perustui ulkomailta ostettujen komponenttien kokoamiseen ja kotimainen sirutuotanto oli olematonta.[164] Kotimainen piirituotanto perustui lisensoituun ARM-arkkitehtuuriin ja venäläiseen Elbrus-arkkitehtuuriin, jotka olivat joko vanhentuneita, erityistarkoituksiin soveltuvia tai kärsivät teknologiasanktioista.[165] Venäjän runko- ja mobiiliverkko olivat pitkälti ulkomaisten laitteiden varassa.[166] Datakeskuksia rakennettiin kiihtyvällä tahdilla, mutta ne käyttivät läntistä teknologiaa.[167] Supertietokoneiden laadussa ja määrässä Venäjä jäi selvästi jälkeen Yhdysvalloista ja Kiinasta.[168] Merkittävä

[160] Тадтаев, Георгий: Путин заявил об угрозе разрушения общества из-за интернета. *RBC*, 4.3.2021. [https://www.rbc.ru/politics/04/03/2021/6040c97c9a7947263f812b1c?from=from_main_6], luettu 5.1.2024.

[161] Шестоперов, Дмитрий & Лебедева, Валерия: Мимо замедленного действия. *Коммерсантъ*, 23.4.2021. [https://www.kommersant.ru/doc/4783593?from=main_6], luettu 5.1.2024; CNews: В России блокируют VPN. Проблема массовая, решения пока нет. *CNews*, 31.5.2023. [https://www.cnews.ru/news/top/2023-05-31_v_rossii_blokiruyut_vpnproblema], luettu 5.1.2024.

[162] Prince, Todd: Navalny App Disappearance Shows Russia's Strength in The Battle Against Big Tech. *RFE/RL*, 22.9.2021. [https://www.rferl.org/a/navalny-app-google-apple/31473261.html], luettu 2.2.2024.

[163] Филипенок, Артем: Путин выступил за личную ответственность за непереход на российский софт. Comnews, 25.11.2021. [https://www.comnews.ru/content/217624/2021-11-25/2021-w47/putin-vystupil-za-lichnuyu-otvetstvennost-za-neperekhod-rossiyskiy-soft], luettu 2.2.2024; Epifanova, Alena & Dietrich, Philipp: Russia's Quest for Digital Sovereignty Ambitions, Realities, and Its Place in the World. DGAP Analysis, 21.2.2022. [https://dgap.org/en/research/publications/russias-quest-digital-sovereignty], luettu 2.2.2024.

[164] Niskanen, Juho: *Russia's ICT-infrastructure and its development prospects in the near future*. Finnish Defence Research Agency Publications 15. Finnish Defence Research Agency, Riihimäki, 2023.

[165] Epifanova & Dietrich (2022); Nocetti, Julien & Wilde, GavinRussia's Technological Sovereignty. Russian Analytical Digest (RAD) 298. 18.7.2023. [https://doi.org/10.3929/ethz-b-000621535], luettu 2.2.2024.

[166] Королев, Никита & Гаврилюк, Анастасия: Базовые полустанки. *Коммерсантъ*, 19.11.2021. [https://www.kommersant.ru/doc/5080226?from=top_main_6], luettu 2.2.2024.

[167] Epifanova & Dietrich (2022); Холупова, Кристина: Зарубежные вендоры перестали поставлять инженерное оборудование в российские дата-центры. Как ЦОДы выкручиваются. *CNews*, 20.4.2022. [https://www.cnews.ru/news/top/2022-04-20_zarubezhnye_vendory_perestali], luettu 2.2.2024.

[168] Martin, Dylan: Russia cobbles together supercomputing platform to wean off foreign suppliers. *The Register*, 11.4.2022. [https://www.theregister.com/2022/04/11/russia_reveal_supercomputer_to_help/], luettu 2.2.2024.

osa maassa käytetyistä kyberturvallisuusohjelmistoistakin oli ulkomaalaisia.[169] Tekoälykehitystä yritettiin edistää, mutta siinäkin jäätiin jälkeen kilpailijoista.[170]

Vaikeuksista huolimatta Kreml ei luopunut haaveistaan kontrolloida venäläistä yhteiskuntaa ja taloutta ja marraskuussa 2021 Putin käski luomaan maahan strategisen suunnittelun yhtenäisen informaatiotilan (единое цифровое информационное пространство в интересах стратегического управления) maan sosiaalitaloudelliseksi ohjaamiseksi ja turvallisuuden varmistamiseksi.[171] Järjestelmän tuli perustua olemassa oleviin tilannekeskuksiin, joita oli viime vuosina rakennettu.[172] Venäjä on jatkanut pyrkimyksiään uhkia ennaltaehkäisevän ja sen intressejä palvelevan informaatioturvallisuuden sopimusjärjestelmän luomiseksi globaalilla, alueellisella, ja kahdenvälisellä tasolla.[173] Se on muun muassa yrittänyt vuodesta 2021 alkaen ajaa Kiinan tuella YK:ssa läpi uutta esitystään valtiokeskeisestä ja informaation sisältöön painottuvasta sopimuksesta.[174]

Ennen Ukrainaan hyökkäämistä Venäjän digitaalinen suvereniteetti ja kansallinen kyberturvallisuus ja -puolustus sen osana olivat kehittymässä, mutta etenkin valtiovallan ajamat hankkeet olivat jäämässä tavoitteistaan, joko täydellisen epärealismin, yksityissektorin vastustuksen ja korruption tai markkinatekijöiden johdosta.[175] Alueelliset ja talouden sektorikohtaiset erot kyberturvallisuudessa olivat suuria Moskovan, Pietarin ja muutamien muiden suurkaupunkien ja finanssialan ollessa kehityksen kärjessä. Tosin Venäjä menestyi kansainvälisissä vertailuissa hyvin, koska sen lait, strategiat ja kyberturvallisuusorganisaatio olivat päällisin puolin kunnossa.[176] Venäjän digitaalinen

---

[169] Чупров, Денис: Российский рынок кибербезопасности срывает джекпот. *Телеспутник*, 25.1.2023. [https://telesputnik.ru/materials/trends/article/rossiiskii-rynok-kiberbezopasnosti-sryvaet-dzekpot], luettu 2.2.2024.

[170] Nocetti, Julian: *The Outsider. Russia in the Race for Artificial Intelligence*. Ifri, Russie.Nei.Reports, No 34, Paris, 2020.

[171] Указ Президента РФ от 8 ноября 2021 г. N 633 "Об утверждении Основ государственной политики в сфере стратегического планирования в Российской Федерации" [https://base.garant.ru/403015816/], luettu 2.2.2024.

[172] Овчаренко, Андрей: ЦУР – это только элемент полноценного ситуационного центра. *D-Russia.Ru*, 29.4.2020. [https://d-russia.ru/cur-jeto-tolko-jelement-polnocennogo-situacionnogo-centra.html], luettu 6.2.2024.

[173] Указ Президента РФ (2021).

[174] Korzak, Elaine: *Russia's Cyber Policy Efforts in the United Nations*. Tallinn Paper No. 11. CCDCOE, Tallinn, 2021; Известия: В МИД РФ предложили заключить соглашение о международном управлении интернетом. *Известия*, 29.12.2021. [https://iz.ru/1271127/2021-12-29/v-mid-rf-predlozhili-zakliuchit-soglashenie-o-mezhdunarodnom-upravlenii-internetom], luettu 2.2.2024.

[175] Khodayar Barari Reykandeh & Shahab Alddin Shokri: Russian Digital Economy and Cybersecurity: An Overview of Recent Developments. *Journal of World Sociopolitical Studies* [https://doi.org/10.22059/wsps.2023.351976.1326]; European Commission: Report on Russia: Technological Capacities And Key Policy Measures. European Commission, Brussels, 2021. [https://monitor-industrial-ecosystems.ec.europa.eu/reports/other-reports/report-russia-technological-capacities-and-key-policy-measures]; Lowry, A.: Russia's Digital Economy Program: An Effective Strategy for Digital Transformation? *The Palgrave Handbook of Digital Russia Studies*. Gritsenko, D., Wijermars, M., Kopotev, M. (Toim.) Palgrave Macmillan, Cham., 2020 [https://doi.org/10.1007/978-3-030-42855-6]; Institute of the Information Society: *Digital economy country assessment for Russia*. Institute of the Information Society, Moscow, 2018; IMD: IMD World Digital Competitiveness Ranking 2021. [https://imd.cld.bz/Digital-Ranking-Report-2021/202/], luettu 2.2.2024; Romanyuk, Maria, Sukharnikova, Maria & Chekmareva, Natalia: Trends of the digital economy development in Russia. *IOP Conf. Ser.: Earth Environ*. Sci. 650 012017; Epifanova & Dietrich (2022).

[176] Ks. esim. NCSI: Country Profile – Russia. Archived data from 2016–2023. [https://www.ncsi.ega.ee/country/ru_2022/], luettu 3.2.2024; ITU: Global Cybersecurity Index. [https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx], luettu 3.2.2024; Сергей Сергеевичоценка, Красных: Оценка уровня цифровизациирегионов России с позиции межрегионального взаимодействия. Информационное общество, 3/2023. [http://infosoc.iis.ru/article/view/831/664], luettu 3.2.2024.

talous oli kehittynyt merkittävästi, mutta se oli selvästi BKT-osuudeltaan ja investoinneiltaan kilpailijoitaan Yhdysvaltoja, Kiinaa ja EU:ta jäljessä. Venäjän koulutusjärjestelmä tuotti ICT-alan osaajia, mutta nämä joko poistuivat maasta parempien palkkojen perässä tai heidän osaamistaan ei saatu valjastettua tiede- ja teknologiakehityksen edistämiseen. Yleisesti ottaen T&K toiminta kärsi alisuorittamisesta, jota aivovuoto ulkomaille pahensi. Valtiojohtoiset innovaatiopuistot eivät ole tuottaneet toivottuja tuloksia, vaan ovat kärsineet salailusta, rahoituksen tempoilusta, korruptiosta ja tuotetun osaamisen pakenemisesta ulkomaille. Monet ongelmista on yhdistetty Venäjän poliittisen ja taloudellisen järjestelmän erityispiirteisiin.[177] Eräänlaisena oireena voidaan pitää valtionyritysten ympärille kehittyneitä horisontaaleja yritysryhmiä, jotka tukahduttivat pienyritykset pois markkinoilta.[178]

Venäjä ei rakentanut vuosina 2011–2021 digitaalista ja teknologista suvereniteettiaan tyhjiössä. Kiinan autoritaarinen kyberpolitiikka on tarjonnut Venäjälle yhdenlaisen mallin, etenkin kun kahden suurvallan suhteet ovat vuosi vuodelta tiivistyneet. Kiinasta on jopa haettu oppia sensuurijärjestelmän rakentamiseen.[179] Digitaalisen autoritaarisuuden ja internetin ”balkanisaation” vahvistuminen on antanut Venäjän johdolle moraalista tukea.[180] EU:ssakin on hyväksytty digitaalisen suvereniteetin perusajatus ja Yhdysvallat on ryhtynyt suojelemaan teknologista riippumattomuuttaan muista suurvalloista.[181] Venäläinen digitaalisen suvereniteetin idea on siis vahvasti sidoksissa suurvaltapolitiikan vuorovaikutukseen, vaikka sillä on voimakkaat sisälähtöisetkin tekijänsä. Sama huomio koskee kyberturvallisuutta ja -puolustusta. Yhdysvallat liittolaisineen ja Kiina ovat julkaisseet sotilaallisia kyberstrategioita ja perustaneet asevoimiinsa kyberjoukkoja. Ne tunnustivat suoraan tai epäsuorasti kybertilan sotilaallisen luonteen 2020-luvun alkuun mennessä. Venäjä vältteli virallisissa kannanotoissaan kybertilan sotilaallistamista, muuta sen vuoden 2016 informaatiodoktriini tunnisti informaatioteknologian sotilaallisen käytön osaksi sotilaspolitiikkaa ja, kuten alla todetaan, perusti omatkin ”informaatiojoukkonsa” viimeistään 2017.[182]

---

[177] WIPO: Global Innovation Index 2022. What is the future of innovation driven growth? WIPO, Geneva, 2022. [https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2022-en-main-report-global-innovation-index-2022-15th-edition.pdf], luettu 3.2.2024; Lehtinen, Santtu, Saari, Sinikukka & Suominen, Arho (Toim.): Russia's technological policy and knowhow in a competitive global context. Prime Minister's Office, Helsinki, 2022.

[178] Kolesnikov, Andrei & Volkov, Denis: The Coming Deluge: Russia's Looming Lost Decade of Unpaid Bills and Economic Stagnation. Carnegie Endowment for International Peace, 24.11.2021. [https://carnegieendowment.org/2021/11/24/coming-deluge-russia-s-looming-lost-decade-of-unpaid-bills-and-economic-stagnation-pub-85852], luettu 3.2.2024.

[179] Kremlin.ru: Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development. 4.2.2022. [http://www.en.kremlin.ru/supplement/5770], luettu 3.2.2024; Kremlin.ru: Совместное заявление Российской Федерации и Китайской Народной Республики о развитии отношений всеобъемлющего партнерства и стратегического взаимодействия, вступающих в новую эпоху. 5.6.2019. [http://www.kremlin.ru/supplement/5413], luettu 3.2.2024; Belovodyev, Daniil, Soshnikov, Andrei, Standish, Reid & Systema: Exclusive: Leaked Files Show China And Russia Sharing Tactics On Internet Control, Censorship. *RFE/RL*, 5.4.2023. [https://www.rferl.org/a/russia-china-internet-censorship-collaboration/32350263.html], luettu 3.2.2024.

[180] Freedom House: Freedom on the Net 2018 - The Rise of Digital Authoritarianism. 2018. [https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism], luettu 3.2.2024; Lewis, James Andrew: Sovereignty and the Evolution of Internet Ideology. CSIS, 30.10.2020. [https://www.csis.org/analysis/sovereignty-and-evolution-internet-ideology], luettu 3.2.2024.

[181] Raman, Sujit: Two Visions of Digital Sovereignty. *Lawfare*, 1.6.2023. [https://www.lawfaremedia.org/article/two-visions-of-digital-sovereignty], luettu 3.2.2024.

[182] Pääosa maailman kehittyneemmistä valtioista ovat olleet avoimempia sotilaallisten kybersuorituskykyjensä suhteen. Ks. vertailun tueksi IISS: Cyber Capabilities and National Power: A Net Assessment. 28.6.2021.

Venäjän puolustukselliset toimet kybertilassa seuraavat venäläisen strategisen deterrenssin ja informaatiosodankäynnin perusideoita:

- Suojaa omat suorituskykysi ja potentiaali vihollisen vaikutukselta. Kansallinen internetsegmentti järjestelmineen ja teknologinen suvereniteetti ilmentävät tätä ajatusta.
- Rakenna asymmetrinen asetelma vastustajaasi nähden kustannustehokkaasti käyttäen hyväksesi vastustajan heikkouksia ja kehitä kapeita etulyöntiaseman tarjoavia suorituskykyjä. Etenkin läpimurtoteknologioiden tavoittelu ilmentää tätä ajatusta.
- Manipuloi vastustajan intressejä tai toiminnan reunaehtoja hankkiaksesi informaatioylivoima jo rauhan aikana. Vastustajien suorituskykyjä sitovan kansainvälisen informaatioturvallisuusjärjestelmän ajaminen ilmentää tätä ajatusta.
- Varmista kyky aloittaa sotatoimi riittävillä suorituskyvyillä ja yllättävästi. Todellisten kybersuorituskykyjen salaaminen ja erilaiset nk. aktiiviset toimet[183], joista enemmän alempana, vastustajan harhauttamiseksi ilmentävät tätä ajatusta.

Venäjän informaatioturvallisuuden ja -puolustuksen toimet tulee ymmärtää osana valtioiden välistä jatkuvaa kamppailua, joka voidaan tarvittaessa eskaloida sotilaallisen voimankäytön asteelle. Samat toimet palvelevat myös Venäjän johdon pyrkimystä käyttää kyberturvallisuuden mekanismeja oman valtansa jatkuvuuden turvaamiseen. Nämä motiivit saattava olla ulkoista turvallisuutta vahvempia. Sensuurin rinnalla Venäjän valtiojohtoinen media ja valtiosta riippuvat yksityiset toimijat, turvallisuuspalveluiden avustuksella, ovatkin pyrkineet hallitsemaan informaatiotilan substanssia yhä voimakkaammin. Tässä toiminnassa informaatiopsykologiset keinot ja menetelmät ovat luonnollisesti pääosassa. Informaatioteknologisia keinoja on käytetty omien kansalaisten ja Venäjällä toimivien ulkomaisten toimijoiden vakoiluun, tietovuotoihin ja sosiaalisen median manipulointiin.[184] Internetuutispalveluiden säännöstelyllä on epäsuorasti vaikutettu toivotun ja ei-toivotun materiaalin ja toimijoiden näkyvyyteen Venäjän internetsegmentissä.[185] Venäjän valtio on käytännössä käynyt informaatiosotaa

[https://www.iiss.org/research-paper//2021/06/cyber-capabilities-national-power], luettu 3.2.2024; CCD COE: Strategy and Governance. Database of National Cybersecurity Documents. [https://ccdcoe.org/library/strategy-and-governance/], luettu 3.2.2024.

[183] Gioe, Lovering & Pachesny (2020).

[184] Vázquez-Liñán, Miguel: Historical Memory and Political Propaganda in the Russian Federation. *Communist and Post-Communist Studies*, vol. 50, no. 2, 2017, s. 77–86; Alieva, Iuliia & Carley, Kathleen M.: Internet Trolls against Russian Opposition: A Case Study Analysis of Twitter Disinformation Campaigns against Alexei Navalny. *2021 IEEE International Conference on Big Data (Big Data)At: Orlando, FL, USA*; Kuznetsova, Elizaveta: Kontrpropaganda today: The roots of RT's defensive practices and countering ethic. *Journalism*, 24(4) 2021, s. 839–856; Oates, Sarah: How Russian 'kompromat' destroys political opponents, no facts required. The Washington Post, 13.1.2017. [https://www.washingtonpost.com/posteverything/wp/2017/01/13/how-russian-kompromat-destroys-political-opponents-no-facts-required/], luettu 3.2.2024; Freedom House: Freedom on the Net 2020 – Russia. 2020. [https://freedomhouse.org/country/russia/freedom-net/2020], luettu 3.2.2024; Williams, Evan M. & Carley, Kathleen M.: Search engine manipulation to spread pro-Kremlin propaganda. *Misinformation Review*, 16.2.2023. [https://misinforeview.hks.harvard.edu/article/search-engine-manipulation-to-spread-pro-kremlin-propaganda/], luettu 3.2.2024; Salikov, Alexey: Social Media in Russian Politics. *Politologija*, Vol. 99(3) 2020, s. 64–92; Kurowska Xymena & Reshetnikov, Anatoly: Russia's trolling complex at home and abroad. *Hacks, Leaks and Disruptions: Russian Cyber Strategies.* Popescu, Nicu & Secrieru, Stanislav (Toim.) EUISS, 2018, s.25–32. [https://www.jstor.org/stable/resrep21140]; Parkinson, Joe & Hinshaw, Drew: Inside the Secretive Russian Security Force That Targets Americans. *Wall Street Journal*, 7.7.2023. [https://www.wsj.com/articles/fsb-evan-gershkovich-russia-security-force-dkro-e9cf9a49], luettu 3.2.2024.

[185] Wijermars, Mariëlle: Russia's law 'On news aggregators': Control the news feed, control the news? *Journalism*, 22(12) 2021, s. 2938–2954.

tai toimeenpannut aktiivisia toimia omaa kansaansa vastaan internetissä 2010-luvulta alkaen – muilla media-alustoilla jo 2000-luvun alusta. Venäläisittäin nähtynä informaatiotilan toimijoiden ja substanssin hallinta on oleellinen osa kansallisen informaatioturvallisuuden ja -puolustuksen takaamista ja informaatiopotentiaalin rakentamista.

3.2. Venäjän kyberpuolustajat

Digitaalisen suvereniteetin rakentamisesta ja kansallisesta kyberturvallisuudesta ja -puolustuksesta vastaava useat eri toimijat, joiden intressit eivät aina ole yhtenevät. Venäjän presidentti johtaa maansa strategista suunnittelua ja Vladimir Putin on vuodesta 2011 osoittanut suurta kiinnostus Venäjän informaatiotilan suojaamiseen ja hallitsemiseen. Digitaalisen talouden kansallinen ohjelma perustuu alkujaan Putinin asettamiin kansallisiin tavoitteisiin ja hän ohjaa aktiivisesti informaatiotalouden ja -turvallisuuden kehitystä ministereiden, presidentin avustajien, johtavien virkamiesten ja oman lähipiirinsä kautta, johon kuuluu merkittäviä talousalan vaikuttajia esimerkiksi Herman Gref Sberpankin johtaja ja Aleksei Kudrin, joka istuu Yandexin hallituksessa.[186] Putin johtaa Venäjän turvallisuusneuvostoa, joka toimii presidentin neuvoaantavana elimenä ja jonka piirissä koordinoidaan kansallisen turvallisuuden asioita. Neuvoston alla toimii Informaatioturvallisuuden komissio, joka analysoi informaatioturvallisuustilannetta, tekee esityksiä ja ottaa osaa strategiseen suunnitteluun. Neuvostossa istuvat mm. ministeriöiden, turvallisuuspalveluiden, asevoimien ja valtionyritysten edustajat.[187] Venäjän hallitus antaa puolestaan tarkempaa ohjausta ja asettaa tarkempia tavoitteita digitaalisen talouden ja suvereniteetin tavoittelun osalta. Lisäksi se on vastuussa pääosasta Venäjän kansallista informaatiotilaa säätelevistä lakialoitteista ja niiden valmistelusta.[188] Duuma on Vladimir Putin jälkimmäisillä kausilla (2011–2024) ollut käytännössä pelkkä Kremlin tilaamien lakialoitteiden alullepanija ja kumileimasin valtiojohdon haluamille lakimuutoksille ainakin silloin, kun ne ovat koskeneet kansallista turvallisuutta.[189]

Venäjän informaatioinfrastruktuurin, -palveluiden ja -talouden kehittäminen sekä osaltaan informaatioturvallisuus on Digitaalisen kehityksen, teleliikenteen ja massaviestinnän ministeriön vastuulla. Ministeriö vastaa digitaalisen talouden ohjelman toimeenpanosta ja ohjaa vahvasti Venäjän ICT-sektoria tarjouskilpailujen, sääntelyn ja valtionyritysten kautta. Se on vastuussa suuresta osasta digitaalisen ja teknologisen suvereniteetin tavoitteluun liittyvistä hankkeista. Ministeriö sääntelee julkisia televerkkoja ml. internetin kansallista segmenttiä ja sen sisältöä. Digitaalisen talouden ja suvereniteetin rakentamiseen osallistuvat luonnollisesti muutkin ministeriöt ja hallinnon, yritysmaailman ja tiedeyhteisön yhteistyötä koordinoidaan usean eri komitean kautta.[190] Useat ministeriöt ja liike-elämän järjestöt ovat kritisoineet kansallisen internet-

[186] Kukkola (2020), s. 294; Gorenburg, Dmitry: The Political Elite Under Putin. *Marshall Center Security Insight*, no.53, April 2020. [https://www.marshallcenter.org/en/publications/security-insights/political-elite-under-putin-], luettu 3.2.2024; Institute of the Information Society (2018); WIPO (2022).
[187] Указ Президента РФ от 10 ноября 2018 г. N 648 "Об утверждении состава Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности по должностям" (с изменениями и дополнениями). 24.4.2023. [https://base.garant.ru/72100350/#block_1000], luettu 3.2.2024.
[188] Kukkola (2020); Institute of the Information Society (2018).
[189] Noble, Ben & Chaisty, Paul: The Federal Assembly – More than Justa a "Rubber Stamp"? *Routledge Handbook of Russian Politics and Society: Vol. Second edition*. Graeme Gill (Toim.) Routledge, London, s. 99–110.
[190] Institute of the Information Society (2018).

segmentin rakentamiseen liittyviä hankkeita liian kalliina, kunnianhimoisina tai yritysten tuottavuutta heikentävinä, mutta se ei ole heikentänyt Mintsifrin asemaa.[191]

Mintsifrin alainen Roskomnadzor virasto on viime vuosina muuttunut teleliikenteen säätelyviranomaisesta yhä enemmän sensuuri- ja valvontaviranomaiseksi. Virasto on myös vastuussa kansallisen internetsegmentin resilienssistä, turvallisuudesta ja eheydestä. Viraston alla toimii Radiotaajuuspääkeskus (Главный радиочастотный центр» (ФГУП ”ГРЧЦ”)) niminen valtionyritys, jonka julkisten verkkojen monitorointi ja hallintakeskus (TsMUSSOP) hallinnoi TSPU-järjestelmää eli valmistautuu suodattamaan valtakunnallisesti tietoliikennettä tai kytkemään Venäjän kansallisen segmentin kokonaan irti globaalista Internetistä – virallisesti suojelemaan Venäjää ulkopuolelta tapahtuvalta irtikytkennältä.[192] Roskomnadzor hallinnoi myös .ru ja .рф domaineja.[193] Vanhaa Neuvostoliiton aikaista .su domainia hallinnoi RIPN yhdistys.[194]

FSB:llä on keskeinen rooli Venäjän kansallisen internetsegmentin turvaamisessa. Se hallinnoi SORM-verkkotiedustelujärjestelmää, on kansallisen SIEM-järjestelmän (GosSOPKA) pääkäyttäjä, toimii valtiollisena kybervalvontaviranomaisena koordinoiden eri CERT/CISRT toimintaa ja hyväksyy kaikki Venäjällä käytettävät salausratkaisut. Venäjän kansallisen internetsegmentin liikenne on lähtökohtaisesti avointa FSB:lle ja se voi pyytää kaikilta Venäjälle rekisteröityneiltä toimijoilta, mikä on pakollista mm. sosiaalisen median palveluille, haluamiensa käyttäjien tiedot ml. viestiliikenteen sisältö ja salausavaimet. FSB:llä on lähes rajoittamaton ja valvomaton toimivalta toimeenpanna tiedustelu- ja vastatiedustelutehtäväänsä Venäjän informaatiotilassa.[195] FSB:n Informaatioturvallisuuskeskus (18. Keskus n/o 64829) keskittyy kyberrikollisuuden vastaiseen toimintaan ja yhteistyöhön yksityissektorin kanssa, Erityisviestipalvelu (16. Keskus n/o 71330) vastaa elektronisesta ja tietoliikennetiedustelusta ja Kommunikaatioturvallisuuskeskus (8. Keskus n/o 43753) vastaa mm. kryptografiasta ja lisensseistä.[196] FSB on osoittanut tehokkuutta toimivaltansa käytössä, mutta on myös osoittanut, että Venäjällä toimivalta on läheisessä suhteessa korruptioon.[197] Kyberrikollisuuden torjumisen osalta sisäministeriön alainen hallintoyksikkö K toimii rinnakkain FSB:n kanssa.[198] FSB tekee laajaa yhteistyötä yksityissektorin kanssa. Se on mm. hankkinut kyberturvallisuus ja -hyökkäystyökaluja Positive Technologies, SyTech,

---

[191] Ведомости: В законопроекте о «суверенном рунете» могут ограничить расширение функций Роскомнадзора. *Ведомости*, 25.2.2019. [https://www.vedomosti.ru/technology/news/2019/02/25/794980-o-suverennom-runete], luettu 3.2.2024; Посыпкина, Александра, Коломыченко, Мария & Балашова, Анна: РСПП нашел в приказе Минкомсвязи требование перевести весь Рунет на VPN. *РБК*, 23.7.2019. [https://www.rbc.ru/technology_and_media/23/07/2019/5d35b0c69a794793c972ca9c?from=from_main], luettu 3.2.2024; Касми, Эльяс: Власти: Переход на российское «железо» и ПО грозит «необоснованными расходами» бизнеса и государства. *Cnews*, 14.5.2021. [https://www.cnews.ru/news/top/2021-05-14_minekonomiki_raskritikovalo], luettu 3.2.2024; Гаврилюк, Анастасия: Минэкономики подключилось к суверенному рунету. *Коммерсантъ*, 25.8.2021. [https://www.kommersant.ru/doc/4957042], luettu 3.2.2024.

[192] О ФГУП «ГРЧЦ»: Kotisivut [https://grfc.ru/grfc/about/about-grfc/], luettu 3.2.2024; CNews: Минцифры РФ, Роскомнадзор, ГРЧЦ ФГУП Главный радиочастотный центр. Cnews, n.d. [https://www.cnews.ru/book/Роскомнадзор_-_ГРЧЦ_ФГУП_-_Главный_радиочастотный_центр], luettu 3.2.2024; Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций: Kotisivut, n.d. [https://rkn.gov.ru], luettu 3.2.2024.

[193] Координационный центр доменов .RU/.РФ. Kotisivut, n.d. [https://cctld.ru/about/], luettu 3.2.2024.

[194] RIPN: Kotisivut, n.d. [http://www.ripn.su/en/domen-su/], luettu 3.2.2024.

[195] Kukkola (2020), s. 303.

[196] Borogan & Soldatov (2022).

[197] Borogan & Soldatov (2015).

[198] SecurityLab.ru: Управление К. n.d. [https://www.securitylab.ru/news/tags/Управление+К/], luettu 3.2.2024.

MSI Soft, VAS Experts ja Protei -yrityksiltä, jotka kuuluivat vuoteen 2023 asti oligarkki Ališer Usmanovin Citadel group -yritysryhmään.[199]

Venäjän kansallinen tietoturvapoikkeamien koordinointikeskus (CERT) (Национальный координационный центр по компьютерным инцидентам – NKTsKI) on osa FSB:tä (8. Keskus).[200] Se valvoo mm. tiedonvaihtoa venäläisten CERT:ien välillä ja ulkomaisten CERT:ien kanssa ja vastaa GosSOPKA-järjestelmän hallinnoinnista. NKTsKI:n lisäksi Venäjällä ovat toimineet ainakin RU-CERT, CERT-GIB, GOV-CERT-RU, FinCERT ja Kaspersky LAB ICS CERT. Lisäksi Sberillä on BI.ZONE ja Rostelekomilla Rostelekom-Solar JSOC -kyberturvallisuuspalvelualusta, joista ainakin jälkimmäinen tekee tiivistä yhteistyötä FSB:n kanssa.[201] FSB:llä vaikuttaisi olevan merkittävä rooli kyberturvallisuuden kansallisessa ohjaamisessa ja valvonnassa, mutta etenkin pankkialalla on itsenäisiä kybervalvomo- ja tietoturvapoikkeamahallintapalveluja ja suuryrityksillä on omat verkko- ja tietoturvavalvomonsa.[202]

Liittovaltion suojelupalvelu (Федеральная служба охраны Российской Федерации – FSO) vastaa presidentinhallinnon ja hallituksen viestiliikenteen turvaamisesta sekä valtiojohdon sisäverkon (RSNet) ylläpidosta. Se vastaa mm. valtionhallinnon kriisiajan johtamisyhteyksien turvaamisesta. Lisäksi FSO kerää tietoa valtiojohdon päätöksenteon tueksi liittovaltiontason, mukaan lukien muiden turvallisuusviranomaisten, toiminnasta ja tapahtumista.[203]

Liitovaltion teknologian ja viennin valvontavirasto (Федеральная служба по техническому и экспортному контролю – FSTEK) toimii puolustusministeriön alla ja vastaa valtiollisesta tiedon suojaamisesta yhteistyössä FSB:n kanssa myöntäen lisenssit hyväksytyille salaustuotteille ja toteuttaa teknologista vastatiedustelua. FSTEK ohjaa kriittisen informaatioinfrastruktuurin suojaamista ja ylläpitää rekisteriä tästä, laissa määritellystä, infrastruktuurista.[204] FSTEK:lla on omaa tutkimustoimintaa ja Yhdysvallat onkin syyttänyt sen tutkimuskeskusta (TsNIIKhM) Triton-haittaohjelman kehittämisestä ja käytöstä.[205] Kuten seuraavassa luvussa tullaan huomaamaan, yksikään Venäjän kyberturvallisuuteen liittyvä organisaatio ei ole täysin puolustuksellinen.

---

[199] O'Neill. Patrick Howell: The $1 billion Russian cyber company that the US says hacks for Moscow. *MIT Technology Review*, 15.4.2021. [https://www.technologyreview.com/2021/04/15/1022895/us-sanctions-russia-positive-hacking/amp/], luettu 3.2.2024; Cimpanu, Catalin: Hackers breach FSB contractor, expose Tor deanonymization project and more. *ZDNet*, 20.7.2019. [https://www.zdnet.com/article/hackers-breach-fsb-contractor-expose-tor-deanonymization-project/], luettu 3.2.2024; Krolik, Aaron, Mozur, Paul & Satarino, Adam: Cracking Down on Dissent, Russia Seeds a Surveillance Supply Chain. *The New York Times*, 6.7.2023. [https://www.nytimes.com/2023/07/03/technology/russia-ukraine-surveillance-tech.html], luettu 3.2.2024; Putin's List: Usmanov Alisher. n.d. [https://www.spisok-putina.org/en/personas/usmanov-2/], luettu 3.2.2024.

[200] ВПК: Кибербезопасность страны – дело всенародное. *ВПК*, № 11 (577) 2015.

[201] Stadnik, Ilona: Sovereign Runet: What Does it Mean? Internet Governance Project, Georgia Institute of Technology, 2019. [https://www.internetgovernance.org/research/sovereign-runet-what-does-it-mean/], luettu 3.2.2024; Cnews: НКЦКИ и «Ростелеком-Солар» рассказали об атаках иностранных проправительственных кибергруппировок на российские органы власти. *Cnews,* 18.5.2021. [https://www.cnews.ru/news/line/2021-05-18_nktski_i_rostelekomsolar], luettu 3.2.2024.

[202] Stadnik (2019).

[203] Kukkola (2020), s. 343; Galeotti, Mark: In Moscow's Shadows podcast, osa 21. 11.1.2021. [https://inmoscowsshadows.buzzsprout.com/], luettu 3.2.2024.

[204] Kukkola (2020), s. 301; Borogan & Soldatov (2022); Rathkeen, L. S.: Перспективы развития российской системы защиты информации. Защита информации. *Inside*, 3/2023, s. 4–9.

[205] U.S. Department of the Treasury: Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware. 23.10.2020. [https://home.treasury.gov/news/press-releases/sm1162], luettu 3.2.2024.

Kyberpuolustus kuuluu Venäjän puolustusministeriön alaisille asevoimille, mutta ne vastaavat vain omista verkoistaan ja järjestelmistään. Venäjä asevoimat eivät ole virallisesti perustaneet kyberjohtoporrasta tai -joukkoja, mutta puolustusministeriön johdon lausuntojen perusteella voidaan päätellä, että vuoteen 2017 mennessä vastaavan suorituskyvyn eli ”informaatiojoukkojen” rakentaminen oli aloitettu. Tosin näiden joukkojen rooliin kuuluu myös vastapropaganda.[206] Vuonna 2013 puolustusministeri Sergei Šoigu ilmoitti ”tiedekomppanioiden” perustamisesta. Niiden tuli rekrytoida asevelvollisia asevoimien tiede- ja teknologiatoiminnan tueksi. Vuoteen 2018 mennessä perustettiin 16 tiedekomppaniaa, joista ainakin viiden tehtävät liittyivät kybertoimintaan.[207] Osa tiedekomppanioista osallistuu verkkojen ylläpitämiseen, puolustamiseen ja kouluttaa sekä rekrytoi osallistujia kyberjoukkojen tarpeisiin, joten asevelvollisuusarmeija on valjastettu kyberpuolustuksen käyttöön.[208] Asevoimien alla on useita tutkimusinstituutteja (ns. TsNII organisaatioita), joilla on rooli kyberpuolustuksen kehittämisessä. Asevoimat myös johtavat ”sotateknopolis” ERA:a, jonka tulisi tuottaa läpimurtoteknologioita asevoimien tarpeisiin.[209] Lisäksi asevoimilla, tai sen edustajilla, on merkittävä rooli yhdessä ulkoministeriön kanssa Venäjän informaatio (kyber)diplomatian toteuttamisessa eli kansainvälisen informaatioturvallisuussopimusjärjestelmän edistämisessä.[210] Tämä roolitus lienee perua aikaisemmista aseriisuntaneuvotteluista.

Siviilipuolella ERA:a vastaa valtion rahoittama Skolkovon teknologiapuisto, joka perustettiin vuonna 2011. Sitä ovat vaivanneet korruptioskandaalit, valtiorahoituksen tempoilu ja yksityisen pääoman keräämisen on epäonnistuminen. Lisäksi onnistuneet yritykset ja tutkijat ovat usein lähteneet Venäjältä ja ulkomaiset investoinnit ovat romahtaneet vuoden 2022 Ukrainan hyökkäysoperaation jälkeen.[211] Skolkovo on USA:n sanktiolistalla, koska sen on katsottu tukeneen Venäjän kybersuorituskykyjen ja asevoimien kehittämistä.[212] Toinen valtiojohtoinen hanke ICT-teknologiakehityksen

---

[206] Wilde, Gavin: Cyber Operations in Ukraine: Russia’s Unmet Expectations. Carnegie Endowment for International Peace, 12.12.2022. [https://carnegieendowment.org/2022/12/12/cyber-operations-in-ukraine-russia-s-unmet-expectations-pub-88607], luettu 3.2.2024.

[207] Mil.ru: 12 научных рот Вооруженных Сил РФ примут участие во II Международном военно-техническом форуме «АРМИЯ-2016». Mil.ru, 28.6.2016. [https://function.mil.ru/news_page/country/more.htm?id=12088700@egNews], luettu 3.2.2024; Thomas, Timothy: Russia’s 21st Century Information War: Working to Undermine and Destabilize Populations. *Defence Strategic Communications*, 1(1) 2015, s. 11–26; ТАСС: Минобороны РФ: научные роты пополнили 300 призывников по итогам осенней кампании 2018 года. *ТАСС*, 12.12.2018 [https://tass.ru/armiya-i-opk/5902450], luettu 18.5.2019; Boltenkov, Dmitry: Russian MoD’s “Science Companies”. *Moscow Defense Brief*, No. 6 (2017), s. 10–12.

[208] Grisé et al. (2022), s. 17–18; Cheravitch (2021), s. 20; Министерство Обороны Российской Федерации: Научные роты и взвода. n.d. [https://recrut.mil.ru/for_recruits/research_company/companies.htm], luettu 3.2.2024; Lysenko, Volodymyr & Brooks, Catherine: Russian information troops, disinformation, and democracy. *First Monday*, 23(5) 2018 [http://dx.doi.org/10.5210/fm.v23i5.8176]. Yleisesikunnan 8. hallinnon tehtävänä on asevoimien verkkojen puolustaminen (Министерство Обороны Российской Федерации: История создания и развития службы защиты государственной тайны в Вооруженных Силах Российской Федерации. n.d. [https://zgt.mil.ru/O_sluzbe/Istoriya], luettu 3.2.2024).

[209] Golts, Aleksandr: Russian Scientists in Military Uniforms. *Eurasia Daily Monitor*, Volume: 15 Issue: 108 2018. [https://jamestown.org/program/russian-scientists-in-military-uniforms/], luettu 3.2.2024.

[210] Kukkola (2020), s. 299.

[211] Klebanov, Sam: Skolkovo: The story of Russia’s failed attempt to build its own Silicon Valley. *Business to Business*, 22.4.2022. [https://www.businessofbusiness.com/articles/skolkovo-russias-failed-silicon-valley-tech-putin/], luettu 3.2.2024; Borak, Masha: How Russia killed its tech industry. *MIT Technology Review*, 4.4.2023. [https://www.technologyreview.com/2023/04/04/1070352/ukraine-war-russia-tech-industry-yandex-skolkovo/], luettu 3.2.2024.

[212] U.S. State Department: Imposing Additional Costs on Russia for Its Continued War Against Ukraine. Fact Sheet – Office of the Spokesperson, 2.8.2022. [https://www.state.gov/imposing-additional-costs-on-russia-for-its-continued-war-against-ukraine/], luettu 3.2.2024.

edistämiseksi on 2012 perustettu FPI (Фонд перспективных исследований), joka jäljittelee toimintamalliltaan Yhdysvaltojen DARPA:a. Se on keskittynyt edistämään asevoimien käyttöön tarkoitettujen läpileikkaavien ja kärkiteknologioiden tutkimusta- ja kehittämistä ja sen tutkimuskohteen on mm. kybersodankäynti.[213] ERA:n, Skolkovon ja FPI:n avulla Venäjän valtio pyrkii edistämään siviili-sotilasyhteistyöstä ja kaksoiskäyttöteknologioiden kehittämisestä.[214] Asevoimat tekevät tiivistä yhteistyötä kyberturvallisuudessa yksityissektorin ja valtioyritysten kanssa.[215]

Yliopistojen ja valtion tutkimusinstituuttien tehtävänä on rekrytoida ja kouluttaa informaatioturvallisuuden ammattilaisia. FSB:llä ja asevoimilla on omat koulunsa kyberkaadereiden kouluttamista varten. Asepalveluksen suorittaminen korkeakoulujen informaatioturvallisuuslinjoilla tai tiedekomppanioissa on edistänyt rekrytointia – samoin FSB:n ja asevoimien sponsoroimat hackathon tapahtumat.[216] Haasteena jo ennen Ukrainan hyökkäysoperaation alkua oli osaavien ja kielitaitoisten korkeakoulutettujen IT-alan ammattilaisten halukkuus suunnata Yhdysvaltoihin, Länsi-Eurooppaan tai Aasiaan parempien palkkojen ja elinolojen toivossa.[217]

Venäjän kansallisen informaatioturvallisuuden ja -puolustuksen perustan muodostavat valtionyhtiöt (mm. Rostelekom, Rosteh ja Rosatom), valtiosidonnaiset tutkimusinstituutit, joilla on sidoksia turvallisuuspalveluihin ja asevoimiin[218], sekä yliopistot sekä yksityisyritykset (mm. Sber, Yandex, Kaspersky). Merkittävä osa venäläisestä telekommunikaatioinfrastruktuurista on venäläisten yksityisyritysten hallussa samoin kuin palvelutuotanto ja sosiaalinen media.[219] ICT-sektorin kehityksen haasteena on ollut jatkuvasti lisääntyvä sääntely, valtiorahoituksen tempoilevuus ja kilpailutuksiin liittyvä korruptio.[220] Yritysten itsenäisyys suhteessa valtiovaltaan on vuosi vuodelta kaventunut maan johdon pyrkiessä yhtäältä valjastamaan niiden tuottamat hyödyt valtion palvelukseen ja toisaalta kontrolloimaan niiden tuottamia potentiaalisesti disruptiivisia innovaatioita.[221] Valtionyritykset tai Kremliä lähellä olevat liikemiehet ovat

---

[213] Uppal, Rajesh: Russia's DARPA, the Advanced Research Foundation aims breakthrough high-risk research and development. *IDST*, 2.8.2022. [https://idstch.com/geopolitics/russia-s-advanced-research-foundation-advancing-as-an-answer-to-us-darpa/], luettu 3.2.2024.

[214] Lehtinen, Saari, & Suominen (2022), s. 26–27.

[215] Lapienytė, Jurgita: Kaspersky neutral stance in doubt as it shields Kremlin. *Cybernews*, 15.11.2023. [https://cybernews.com/security/kaspersky-neutral-stance-in-doubt-as-it-shields-kremlin/], luettu 3.2.2024; Cnews: Российские разработчики квантовых технологий будут работать в интересах Минобороны. *Cnews,* 22.8.2022. [https://www.cnews.ru/news/line/2022-08-22_rossijskie_razrabotchiki], luettu 3.2.2024; Любавина, Анна: У российских госслужащих появится «военизированный» оператор связи. *Cnews*, 18.8.2023. [https://www.cnews.ru/news/top/2023-08-18_u_rossijskih_gossluzhashchih], luettu 3.2.2024; Воейков, Денис: Российский «военный Linux» допустили до использования в госорганах. *Cnews*, 24.1.2023. [https://www.cnews.ru/news/top/2023-01-24_rossijskij_voennyj_linux], luettu 3.2.2024.

[216] Borogan & Soldatov (2022).

[217] Kolesnikov & Volkov (2021); Kobza, Rober: Russia's People Problem. Georgetown Security Studies Review, 6.4.2020. [https://georgetownsecuritystudiesreview.org/2020/04/06/russias-people-problem/], luettu 3.2.2024.

[218] Borogan & Soldatov (2022).

[219] Yablokov, Ilya & Solovyeva, Olga: ICT in Putins's Russia: 1999–2021. *Routledge Handbook of Russian Politics and Society: Vol. Second edition*. Graeme Gill (Toim.) Routledge, London, 2023, s. 364–376; Lehtinen, Saari, & Suominen (2022); Bendett, Samuel, Boulègue, Mathieu, Connolly, Richard, Konaev, Margarita, Podvig, Pavel & Zysk, Katarzyna: Advanced military technology in Russia. Capabilities and implications. Chatham House, Russia and Eurasia Programme, September 2021. [https://www.chathamhouse.org/2021/09/advanced-military-technology-russia], luettu 3.2.2024.

[220] Institute of the Information Society (2018).

[221] Dear (2019); 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

ostaneet osuuksia useista menestyneistä kyber- ja ICT-alan yrityksistä tai yritysten johtoon on nostettu Kremliä lähellä olevia henkilöitä.[222] Patrimoniaaliseen kapitalismiin[223] perustuvassa talousjärjestelmässä menestyvistä ICT-alan yrityksistä on tullut eliittipolitiikan välikappaleita. Toisaalta valtio on aktiivisesti suojellut ICT-sektoria ulkomaiselta kilpailulta.[224] Venäjän markkinoille onkin syntymässä digitaalisia ekosysteemejä johtavien yritysten (Sber, Yandex) laajentaessa palveluntarjontaa yhä uusille alueille.[225] Kehitys ei kuitenkaan ole aivan näin yksiselitteistä, sillä Kiinan ja Venäjän teknologiayhteistyö oli tiivistynyt jo ennen helmikuuta 2022 ja kiinalaiset yritykset olivat sopineet yhteistyöhankkeista venäläisten ICT-alan yritysten kanssa.[226] Länsimaistenkin ICT-alan yritykset toimivat aktiivisesti Venäjällä ja osallistuivat venäläisten tytäryhtiöiden ja kumppanien tai vähintään tuotteidensa kautta Venäjän valtionhallinnon hankkeisiin.[227] Näin ollen Venäjän digitaalisen suvereniteetin ja informaatioturvallisuuden ja -puolustuksen kehitys nojasi voimakkaasti ulkomaalaisella perustalle Ukrainan hyökkäysoperaation alkaessa. Venäjän informaatiopotentiaalin teknologinen osa ei siis ollut sen kansallisessa hallinnassa Ukrainan hyökkäysoperaation alkaessa.

экономических зон. *РБК*, 9.4.2020.
[https://www.rbc.ru/economics/09/04/2020/5e8eb2679a79477a36b61c5f], luettu 8.7.2020.

[222] Vendil Pallin (2017); Связь: *Связь в Вооруженных Силах Российской Федерации 2017*. Информационный мост, Москва, 2017; Minkomzsiaz': Nikolay Nikiforov Presented Branch Plan on Import Substitution of Software. 3.4.2015. [http://minsvyaz.ru/en/events/32967/.], luettu 12.1.2018; Petrella, Stephanie: The Kremlin Has Set Its Sights on Russia's Private Tech Firms. *Foreign Policy*, 26.11.2019. [https://foreignpolicy.com/2019/11/26/kremlin-moscow-nationalize-russian-private-tech-firms-yandex-mailru/], luettu 3.2.2024; Cordell, Jake: Yandex Proposes Sweeping Restructure to Allay Government Concerns. *The Moscow Times*, 18.11.2019. [https://www.themoscowtimes.com/2019/11/18/yandex-proposes-sweeping-restructure-allay-government-concerns-a68209], luettu 3.2.2024.

[223] Robinson, Neil: Political Economy. *Routledge Handbook of Russian Politics and Society: Vol. Second edition*. Graeme Gill (Toim.) Routledge, 2023, s. 253–262; s. 257–258.

[224] Yablokov, Ilya & Solovyeva (2023).

[225] Allinger, Katharina, Barisitz, Stephan & Timel, Andreas: Russia's Large Fintechs and Digital Ecosystems – In the Face Of War And Sanctions. *Focus On European Economic Integration*, 3/2022, s. 47–65.

[226] 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.

[227] Niskanen (2023).

4. VENÄJÄN HYÖKKÄYKSELLISET KYBEROPERAATIOT 2000–2021

Venäjän hyökkäyksellinen kybertoiminta kehittyi vuosina 2000–2021 voimakkaasti ja oli useiden eri toimijoiden toteuttamaa. Venäjän tiedustelupalvelut ja asevoimien tiedustelun ja informaatiojoukkojen kyberyksiköt toteuttivat useita pidempi aikaisia kampanjoita, joiden perusteella ne on attribuution yhteydessä nimetty ns. APT (Advanced Persistent Threat) ryhmäksi tai uhkatoimijaksi. Käsite viittaa kybertoimijaan, jolla on käytössään merkittävät resurssit ja osaaminen. Se keskittyy pitkäaikaisiin operaatioihin ja kampanjoihin ja käyttää useita hyökkäystapoja ja -reittejä.[228] Lisäksi Venäjän valtiolliset toimijat ovat tukeneet kolmansien osapuolien eli patrioottisten hakkereiden[229], haktivistien[230] ja rikollisten toteuttamaa hyökkäyksellistä kybertoimintaa. Silloin kun näiden ryhmien toiminta on tukenut suoraan Venäjän valtion toimintaa tai yhteys valtiolliseen toimijaan on ollut muuten todennettavista, ryhmistä on käytetty tässä tutkimuksessa nimitystä sijaistoimija (proxy).

Venäjän hyökkäykselliset kyberoperaatiot ovat kehittyneet suurvaltasuhteiden, vastustajien toimintatapojen ja Venäjän sisäisen tilanteen sekä teknologian kehittyessä. Venäjä on 2000-luvulla toteuttanut:

- Tietojärjestelmätiedustelua ja -vakoilua koti- ja ulkomaisia kohteita vastaan
- Informaatiovaikuttamisen tukemista kybermenetelmillä
- Häiritseviä, lamauttavia ja jopa tuhoavia kyberhyökkäyksiä kriittistä infrastruktuuria vastaan
- Taistelutoimien tukemista sotatoimien osana
- Demonstratiivista deterrenssiviestintää
- Vale- ja sijaisoperaatioita yleisen ”kohinatason” nostamiseksi ja oman toimintansa peittämiseksi.[231]

Aikaisemmin esiteltyyn venäläisen strategisen ajattelun suhteen on pidettävä mielessä, että asevoimilla ja turvallisuuspalveluilla on toimilleen eri lähtökohdat ja sotaa edeltävänä aikana turvallisuus- ja tiedustelupalveluiden menetelmät ja päämäärät hallitsevat hyökkäyksellisiä kyberoperaatioita. Lisäksi Venäjän kybertoiminta on kuluneina vuosina saanut suhteettoman paljon julkisuutta, eikä sen toiminnan määrää tai laatua ole helppoa verrata muiden valtioiden toimintaan etenkin, kun Venäjällä tai Kiinalla tai niiden tietoturvayrityksillä ei ole ollut tapana attribuoida kyberoperaatioita samalla tavalla kuin esimerkiksi Yhdysvalloilla ja Iso-Britannialla.

Tässä ja seuraavassa luvussa käytetään Venäjän hyökkäyksellisistä kybertoimista käsitteitä hyökkäys, operaatio ja kampanja, jotka ovat yleisesti käytössä länsimaisessa kybertutkimuksessa. Näin siksi, että lähdeaineisto käyttää näitä käsitteitä ja venäläinen käsitteistö ei mahdollista tapahtumahistorian kirjoittamista ilman ennakko-oletusta sotatoimesta, johon luvussa 2 tarkastellut käsitteet liittyvät. Tässä tutkimuksessa kampanja viittaa sarjaan ajan kuluessa tehtyjä peräkkäisiä tai samanaikaisia ja koordinoituja

[228] NIST: Glossary – Advanced Persisten Threat. n.d. [https://csrc.nist.gov/glossary/term/advanced_persistent_threat], luettu 3.2.2024.
[229] Barrett, Barin: Don't Buy Into Putin's Latest Misdirection on Election Hacking. *WIRED*, 1.6.2017. [https://www.wired.com/2017/06/putin-russia-hackers-election/], luettu 3.2.2024.
[230] Tietokoneperustaisten tekniikoiden kuten hakkeroinnin käyttö kansalaistottelemattomuuden muoto poliittisen agendan tai sosiaalisen muutoksen ajamiseksi.” Wikipedia: Hactivism. n.d. [https://en.wikipedia.org/wiki/Hacktivism#cite_note-1], luettu 3.2.2024.
[231] Yksi tuoreimmista kuvauksista Venäjän toiminnasta ks. Kerr (2023).

kyberoperaatioita, joilla tavoitellaan operatiivisia tai strategista päämäärää. Kampanja voi kohdistua useaan eri järjestelmää ja sillä voi olla useita toimeenpanijoita. Kyberoperaatio koostuu joukosta koordinoituja toimia määrättyä järjestelmää tai verkkoa vastaan operatiivisen tai taktisen päämäärän saavuttamiseksi. Operaatiolla voidaan pyrkiä varastamaan tietoja tai estämään niiden käyttö häiritsemällä, lamauttamalla tai tuhoamalla informaatiojärjestelmiä ja niissä olevaa informaatiota. Operaatiolla on yleensä useampi vaihe ja ne pyrkivät yleensä joko nopeaan vaikutukseen tai pidempään oleskeluun kohdejärjestelmissä. Kyberhyökkäys viittaa yksittäiseen taktisen tai taisteluteknisen tason toimintaan tai hyökkäystyyppiin.[232] Huolimatta länsimaisten käsitteiden käytöstä tapahtumien kuvailussa palataan venäläisiin käsitteisiin pohdittaessa hyökkäysoperaatioiden luonnetta Venäjän sotataidollisesta näkökulmasta.

4.1. Alkutaival: Vakoojat ja patriootit

Venäjä aloitti hyökkäykselliset kyberoperaatiot jo 1990-luvulla kuuluisimpana Moonlight Maze kybervakoiluoperaatio, joka oli mahdollisesti Venäjän signaalitiedustelun FAPSI:n (Федеральное агентство правительственной связи и информации) toteuttama.[233] FAPSI:n tehtävät ja suorituskyvyt jaetiin vuonna 2003 FSB:n, FSO:n ja SVR:n kesken.[234] Venäjän turvallispalvelut käyttivät hyväkseen informaatioyhteiskuntien kehitystä ja keskittyivät 2000-luvun alussa kybervakoiluun. FSB aloitti kybervakoilun viimeistään Snake kyberhaittaohjelman avulla 2004. FSB:n kohteina ovat olleet hallitusten tietoverkot, tutkimuskeskukset ja toimittajat sekä yritykset ja kriittinen infrastruktuuri.[235] Samoihin aikoihin Venäjän sotilastiedustelupalvelu GRU (Главное управление Генерального штаба ВС РФ) aloitti Pawn Stormiksi nimetyn kybervakoilukampanjan. Sen kohteet ovat vaihdelleen läntisistä sotilasorganisaatioista siviilihallintoon, mediaan ja toisinajattelijoihin.[236] Myöhemmin Pawn Storm on liitetty GRU:n 85. Erikoispalvelukeskukseen (n/o 26165) ja APT28 uhkatoimijaan.[237] SVR:n kyberoperaatioista 2000-luvun alussa ei ole tarkempaa tietoa, mutta se onnistui värväämään entisen virolaisen tiedustelu-upseerin Herman Simmin, joka vuosi tietoja Naton kyberturvallisuusasioista aina kiinni jäämiseensä vuoteen 2008 asti.[238] Tiedustelun ohella Venäjä pyrki estämään tšetšenikapinallisten internetviestinnän Tšetšenian toisen sodan aikana (1999–2009) mm. hyökkäämällä kapinallisten verkkosivuja vastaan.[239] Venäjällä ymmärrettiin vuosituhannen vaihteessa erittäin hyvin informaatio-

[232] Harknett, Richard J. & Smeets, Max: Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, 45(4) 2022, s. 534–567; Nilsson (2023).
[233] Rid, Thomas: *Rise of the Machines*. WW Norton, New York, 2016, s. 316–322.
[234] Borogan & Soldatov (2022).
[235] CISA: Hunting Russian Intelligence "Snake" Malware. 9.5.2023. [https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a], luettu 5.1.2024; Tanriverdi, Hakan, Flade, Florian & Frey, Lea: The Elite Hackers of the FSB. *BR24*, 17.2.2024. [https://interaktiv.br.de/elite-hacker-fsb/en/index.html], luettu 5.1.2024.
[236] Trend: Operation Pawn Storm: Fast Facts and the Latest Developments. 16.1.2016. [https://www.trendmicro.com/vinfo/pl/security/news/cyber-attacks/operation-pawn-storm-fast-facts], luettu 5.1.2024.
[237] NCSC: Reckless campaign of cyber attacks by Russian military intelligence service exposed. NCSC, 3.10.2018. [https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed], luettu 5.1.2024.
[238] Kukkola (2020); Schmid, Von Fidelius & Ulrich, Andreas: New Documents Reveal Truth on NATO's 'Most Damaging' Spy. *Der Spiegel*, 6.5.2010. [https://www.spiegel.de/international/europe/betrayer-and-betrayed-new-documents-reveal-truth-on-nato-s-most-damaging-spy-a-693315.html], luettu 3.2.2024.
[239] Krushelnycky, Askold: Chechnya: Rebels Use Internet In Propaganda War With Russians. *RFE/RL*, 5.5.2000. [https://www.rferl.org/a/1093909.html], luettu 5.1.2024; Billo, Charles & Chang, Welton: Cyber

psykologisen vaikuttamisen merkitys etenkin omien sotilaiden ja kotimaisen yleisön piirissä. Venäjä ei kuitenkaan onnistunut taivuttelemaan läntistä yleisöä puolelleen, minkä seurauksen voitetun sodan kansainvälispoliittiset mahdollisuudet jäivät osin toteutumatta ja Venäjän maine heikkeni.[240]

Venäjä on 2000-luvun ajan käyttänyt sijaistoimijoita kyberoperaatioidensa tukena. 2000-luvun ensimmäisenä vuosikymmenenä Venäjän internet oli pitkälti sääntelemätön ja rikollisuuden läpäisemä tila ja se toimi alustana ulko- ja kotimaahan suuntautuvalle kyberrikollisuudelle. Kyberrikolliset ovatkin tarjonneet Venäjän tiedustelupalveluille halvan, suhteellisen riskittömän tavan hankkia tarvittaessa lisäresursseja lyhyellä aikavälillä.[241] Venäjän tiedustelupalvelut ovat käyttäneet esimerkiksi Russian Business Network -kyberrikollisryhmää sekä yksittäisiä hakkereita, jotka painostettiin tai ostettiin toteuttamaan turvallisuuspalveluiden operaatioita, operaatioidensa peitteenä. Toimintamalli on edellyttänyt rikollisryhmien suhteellisen vapaan toiminnan sallimista Venäjällä.[242] Rikollisten lisäksi nuorisojärjestöt ja patrioottiset hakkerit ovat tarjonneet tiedustelupalveluille hyödyllisiä lisäresursseja.[243] Sijaistoimijoiden käytön avulla Venäjä on voinut hämärtää rooliaan hyökkäysten taustalla ja on voinut toimeenpanna operaatioita, joiden suorasta yhdistämisestä Venäjään olisi voinut koitua liiallinen mainehaitta. Rikollisia ja haktivisteja on käytetty kotimaisen opposition ja tshetsheenikapinallisten viestinnän häirintään sekä kyberhyökkäyksillä toteutettuun poliittiseen viestintään mm. Ukrainassa 2006 ja Virossa 2007.[244] Venäjä osoitti olevansa valmis hyväksymään määrätyn riskin, sillä sijaistoimijat voivat toimia omapäisesti, tuhlata resursseja tai kääntyä isäntiään vastaan.[245] Venäjä on myös käyttänyt yksityisyrityksiä, esimerkiksi NTC Vulkan ja Positive Technologies yrityksiä, hyökkäyksellisten kyberoperaatioidensa tukena. Nämä ovat luotettavampia sijaistoimijoita, mutta yhteistoiminnan tulisi olla niille taloudellisesti kannattavaa, ja ne ovat päätyneet paljastuessaan sanktioiden kohteeksi.[246]

Venäjä kybertoiminta muuttui aggressiivisemmaksi vuodesta 2007, kun mahdollisesti valtiollisten toimijoiden ohjailemat patrioottiset hakkerit toteuttivat 22 vuorokautta kestäneen massiivisen palvelunestohyökkäyksen[247] Viron hallinnon, finanssialan ja

---

Warfare An Analysis Of The Means And Motivations Of Selected Nation States. ISTS Dartmouth College, 2004.

[240] Thomas (2005); Berger, Heidi: Venäjän informaatio-psykologinen sodankäyntitapa terrorismin torjunnassa ja viiden päivän sodassa. Maanpuolustuskorkeakoulu, Johtamisen ja sotilaspedagogiikan laitos, Julkaisusarja 1, Nro. 5, Helsinki, 2010.

[241] Connell & Vogler (2022); Cheravitch (2021).

[242] Flook, Kara: Russia and the Cyber Threat. CriticalThreats, 13.5.2009. [https://www.critical-threats.org/analysis/russia-and-the-cyber-threat], luettu 5.1.2024; U.S. Department of the Treasury (2021).

[243] Sherman (2022); Lewis, James A., Lonergan, Erica D., Voo, Julia, Garson, Melanie & Ertan, Amy: *The Implications of Cyber Proxies in the Ukraine Conflict*. Center for Strategic and International Studies, 2023; Maurer, Tim: *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge University Press, Cambridge, 2018.

[244] Jellenc, Eli & Zenz, Kimberly: Global Threat Research Report: Russia. An iDefense Security Report, VeriSign, 2007 [https://file.setav.org/Files/Pdf/global-threat-research-report-russia-idefence-2007.pdf], luettu 3.2.2024; Nazario, Jose: Politically Motivated Denial of Service Attacks. *Cryptology and Information Security Series EbookVolume 3: The Virtual Battlefield: Perspectives on Cyber Warfare*. Czosseck, Christian & Geers, Kenneth (Toim.) IOS Press Books, 2009, s. 163–181. [10.3233/978-1-60750-060-5-163].

[245] Lonergan (2023).

[246] Antoniadis, Nikolai et al.: A Look Inside Putin's Secret Plans for Cyber-Warfare. *Der Spiegel*, 30.3.2023. [https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236], 3.2.2024; O'Neill (2021).

[247] Hajautettu palvelunestohyökkäys (Distributed denial-of-service – DDoS) pyrkii lamauttamaan kohdepalvelimen, -verkon tai -palvelun liikenteen kohdistamalla siihen niin paljon liikennettä, että se ei kykene enää toimimaan normaalilla tavalla. (Clouflare: What is a DDoS attack? n.d. [https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/], luettu 3.2.2024.

median kohteita vastaan. Taustalla oli poliittinen kiista Neuvostoliiton aikaisen muistomerkin siirtämisestä ja kyberhyökkäyksellä tuettiin organisoituja mielenosoituksia ja Venäjän asettamien sanktioiden vaikutusta Viron hallitukseen.[248] Kyberhyökkäys oli aikanaan poikkeuksellinen ja herätti huomiota mediassa, mutta sen suorat vaikutukset olivat lopulta vähäisiä. Seurannaisvaikutuksena oli sen sijaan Naton kyberpuolustuksen kehittäminen.[249] Operaationa se osoitti, että Venäjä ymmärsi hyökkäyksellisten kyberoperaatioiden tarjoamat mahdollisuudet poliittisten päämäärien saavuttamisessa ja oli valmis käyttämään niitä.

Vuonna 2008 Venäjä tuki hyökkäyksellisellä kyberkampanjalla sotilasoperaatiotaan Georgiaa vastaan. Ilmiö ei ollut uusi, sillä Yhdysvallat oli hyökännyt jo vuonna 1999 Serbian ja vuonna 2003 Irakin sotilas- ja siviilitelekommunikaatio- ja satelliittiyhteyksiä vastaan osana sotatoimiaan.[250] Venäjän kampanja oli kuitenkin varsin näkyvä. Operaatio keskittyi Georgian hallinnon sisäisen ja ulkoisen viestinnän häiritsemiseen ja lamauttamiseen sekä informaatiovaikuttamisen tukemiseen, mutta myös median ja finanssialan toimintaa pyrittiin häiritsemään. Venäjän ilmaiskut vaurioittivat Georgian runkoverkkoa ja TV- ja radiolähetysasemia. Kyberoperaatioiden on väitetty olleen osittain koordinoituja kineettisen vaikuttamisen kanssa, mutta tästä on vähän näyttöä. Pääosin hyökkäykset olivat patrioottisten hakkereiden toteuttamia ja teknisesti vaatimattomia palvelunesto- ja verkkosivujen sotkemishyökkäyksiä, mutta todennäköisesti asevoimien ja turvallisuuspalveluiden tukemia ja osittain jo ennen sotatoimien alkua valmistelemia. Hyökkäysten taustalla toteutettiin kybertiedustelutoimintaa ja Venäjän kyberrikollisorganisaatioiden on väitetty kaapanneen Georgian ulkomaanliikennettä Venäjälle. Georgia vastasi Venäjän hyökkäyksiin estämällä Venäjän TV-lähetykset alueellaan ja estämällä pääsyn venäläisille sivustoille. Venäläisen median verkkosivuja vastaan tehtiin hyökkäyksiä.[251] Jälkikäteen informaatiosodankäynnin johtava tukija professori Igor Panarin oli sitä mieltä, että Venäjä oli epäonnistunut informaatiovaikuttamisessa, koska kansainvälinen yleisö piti Venäjää hyökkääjänä.[252] Näin tapahtuikin ja Georgian kokemukset vaikuttivat siihen, että Venäjän asevoimien piirissä alettiin entisestään korostaa informaatioylivoiman hankkimista jo rauhan aikana.[253] Ilman sodan oikeutusta kansainvälisen yhteisön silmissä onnistunut sotatoimi saattaisi jäädä ilman voittoa ja täten poliittiset päämäärät saavuttamatta.

Vuosina 2008–2012 Venäjän turvallisuuspalvelut jatkoivat kybervakoilua muun toiminnan ohessa. Operaatio Buckshot Yankee johti, haittaohjelmalla saastutetun USB-tikun kautta, Yhdysvaltojen puolustusministeriön turvaluokitellun verkon (SIPRNet)

---

[248] Herzog, Stephen: Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of Digital Insecurity. *Georgetown Journal of International Affairs*, 28(3) 2017, s. 67–78; Juurvee, Ivo & Mattiisen, Anna-Mariita: The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict. RKK ICDS, 21.8.2020. [https://icds.ee/en/the-bronze-soldier-crisis-of-2007/], luettu 3.2.2024.

[249] NATO StratCom COE: 2007 cyber attacks on Estonia. Report, 2018. [https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf], luettu 3.2.2024.

[250] Markoff, John & Shanker, Thom: Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk. *The New York Times*, 1.8.2009. [https://www.nytimes.com/2009/08/02/us/politics/02cyber.html], luettu 3.2.2024; Kaplan, Fred: *Dark Territory. The Secret History of Cyber War*. Simon & Schuster, New York, 2016.

[251] Deibert, Ronald J., Rohozinski, Rafal & Crete-Nishihata, Masashi: Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue*, Vol. 43, No. 1 2012, s. 3–24; Healey (2013), s. 196–198; Flook (2009); Nazario (2009).

[252] Grisé et al. (2022).

[253] Thomas, Timothy T.: The Bear Went Through the Mountain: Russia Appraises its Five-Day War in South Ossetia. *Journal of Slavic Military Studies*, 22 2009, s. 31–67; Bartles, Charles K.: Defense Reforms of Russian Defense Minister Anatolii Serdyukov. *Journal of Slavic Military Studies*, 24(1) 2011, s. 55–80; Горбунов, В. Н. & Богдановo, С. А.: О характере вооруженной борьбы в XXI веке. *Военная мысль*, 3/2009, s. 2–15.

ja globaalin tiedustelutietojen jakamisverkon (JWICS) murtamiseen vuonna 2008,[254] samaan aikaan, kun Yhdysvallat ja Israel toteuttivat operaatio Olympic Gamesia (Stuxnet) Iranin ydinohjelman viivästyttämiseksi.[255] Buckshot Yankeen taustalla oli FSB:n Snake/Turla Agent.BTZ haittaohjelmallaan.[256] Vuosikymmenen taitteessa Dukes-kampanja, joka on yhdistetty APT29 uhkatoimijaan, joka taas osiltaan on yhdistetty FSB:hen ja SVR:ään,[257] aloitti Venäjän suurvaltakilpailijoiden ja näiden liittolaisten vakoilemisen. Sen kohteena olivat maailmanlaajuisesti hallitukset, ajatushautomot ja valtioiden alihankkijat sekä Venäjän oppositio, separatistit ja rikolliset.[258] Duke-vakoiluohjelmakampanja paljastui 2013, mutta se ei estänyt FSB/SVR:ä jatkamasta haittaohjelmaperheen käyttämistä.[259] Myös Venäjän asevoimat jatkoivat tiedustelutoimintaansa. GRU:n Sandwormiksi myöhemmin nimetty ryhmä (Erikoisteknologioiden pääkeskus n/o 74455) perustettiin vuosien 2004–2007 aikana ja sen vuodesta 2009 kestänyt mm. Natoon, EU:hun ja Ukrainaan kohdistunut vakoilukampanja paljastui 2014.[260] Venäjän tiedustelupalveluille ulkomaisten kohteiden kybervakoilu ja kotimaisten kohteiden tiedustelu oli luonnollinen jatko KGB:n toiminnalle. Kerättyä tietoa käytettiin noina vuosina ensisijaisesti Putinin hallinnon vastustajia vastaan.[261]

Muutamia vuosia ennen Arabikevään tapahtumia ja Kremlin vastaisia mielenosoituksia Venäjän presidentinhallinto ja turvallisuuspalvelut käänsivät katseensa sisäänpäin ja alkoivat etsiä keinoja kontrolloida ja valvoa Venäjän sisäistä internetuutisointia ja viestintää mm. painostamalla Yandexia. Samaan aikaan Venäjän johtoa tukevat haktivistit ja nuorisojärjestö Nashin jäsenet toteuttivat palvelunestohyökkäyksiä venäjävastaisiksi katsomiaan tahoja vastaan ja yrittivät manipuloida internetin keskustelupalstoilla ja blogialustoilla käytäviä poliittisia keskusteluja.[262] Kun Kreml sitten vuoden 2011 mielenosoitusten jälkeen aloitti verkkosensuurijärjestelmän rakentamisen, Putinia tukevista ja Kremlin ohjailemista kansalaisjärjestöistä tuli sensuurijärjestelmän ja sisäisen informaatiovaikuttamisen kiinteä osa.[263] Venäjän johdon näkemykset informaatiotilan uhista ja mahdollisuuksista valtioiden välisessä kamppailussa, tiedustelupalveluiden kybersuorituskykyjen kehittyminen ja sosiaalisen median kehittyminen loivat perustan aktiivisten toimien uudelle, digitaaliselle tulemiselle. Vaikka niiden

[254] Farwell, James P.: Industry's Vital Role in National Cyber Security. *Strategic Studies Quarterly*, 6(4) 2012, s. 10–41; Healey (2013), s. 196–198, s. 207.
[255] Lindsay, Jon R.: Stuxnet and the Limits of Cyber Warfare. *Security Studies*, 22(3) 2013, s. 365–404.
[256] Faou, Matthieu: From Agent.BTZ to ComRAT v4: A ten-year journey. ESET Research, 26.5.2020. [https://www.welivesecurity.com/2020/05/26/agentbtz-comratv4-ten-year-journey/], luettu 3.2.2024.
[257] Council on Foreign Relation (2024); F-Secure: The Dukes. 7 Years of Russian Cyberespionage. September 2015. [https://blog.f-secure.com/the-dukes-7-years-of-russian-cyber-espionage/], luettu 3.2.2024; Michael, Melissa: Deconstructing the Dukes: A Researcher's Retrospective of APT29. Blogikirjoitus, 6.5.2020. [https://blog.f-secure.com/podcast-dukes-apt29/], luettu 3.2.2024; Estonian Foreign Intelligence Service: International Security and Estonia 2018. [https://www.valisluureamet.ee/doc/raport/2018-en.pdf], luettu 3.2.2024. Vaikuttaisi siltä, että jossain vaiheessa vuosina 2021–2022 APT29, The Dukes ja Nobillium on attribuoitu SVR:ään ja FSB:lle jäi Snake/Turla. Dukesin attribuution tarkentamista määrättyyn toimijaan vaikeuttaa vuonna 2003 tapahtunut KGB:n signaalitiedustelusuorituskyvyn perijän FAPSI:n jakaminen FSB:n ja SVR:n kesken. Borogan & Soldatov (2022).
[258] F-Secure (2015).
[259] Michael (2020).
[260] MITRE: MITRE ATT&CK – Sandworm Team. 6.10.2023. [https://attack.mitre.org/groups/G0034/], luettu 3.2.2024.
[261] Soldatov & Borogan (2015).
[262] Soldatov & Borogan (2015), s. 115–117; Elder, Miriam: Polishing Putin: hacked emails suggest dirty tricks by Russian youth group. *The Guardian*, 7.2.2012. [https://www.theguardian.com/world/2012/feb/07/putin-hacked-emails-russian-nashi?fb=optOut], luettu 3.2.2024; Flook (2009); Nazario (2009).
[263] Turovsky, Daniil: This is how Russian Internet censorship works A journey into the belly of the beast that is the Kremlin's media watchdog. *Meduza,* 13.8.2015. [https://meduza.io/en/feature/2015/08/13/this-is-how-russian-internet-censorship-works], luettu 5.1.2024.

käyttöä harjoiteltiin ensin kotimaisessa ja lähialueiden piirissä, Venäjän tiedustelupalveluiden kunnianhimo alkoi pian kurottaa kauemmas.

4.2. Maidanista eteenpäin: Informaatiokamppailu kiihtyy

Venäläiset toimijat aktivoituivat Ukrainassa tilanteen kiristyessä talvella ja keväällä 2014. Etenkin Kiovan Itsenäisyyden aukion mielenosoituksista seuranneen, myöhemmin Arvokkuuden vallanmumoukseksi (Революція гідності) nimetyn vallanvaihdon jälkeen, GRU:hun (APT28 Fancy Bear) liitetty haktivistiryhmä Cyber Berkut, joka pyrki alkuvaiheessa esiintymään ukrainalaisena, hyökkäsi Ukrainan uutta hallitusta ja sen läntisiä tukijoita vastaan sotkemalla verkkosivuja, tekemällä palvelunestohyökkäyksiä, vuotamalla sähköposteja ja puhelinkeskusteluita ja häiritsemällä elektronisen äänten laskentajärjestelmän ja tulospalvelun toimintaa Radan vaaleissa lokakuussa 2014.[264] Venäjä käytti lavastettuja (nk. false flag) operaatioita disinformaation levittämiseen, jota sitten kaiutettiin venäläisen median kautta kansainväliselle yleisölle.[265] Venäjä kykeni myös vaikuttamaan VKontaktin ja Odnoklasnikin hallinnan kautta ukrainalaisten laajasti käyttämiin informaatiopalveluihin.[266] Huolimatta Krimin runkoyhteyksien katkaisemisesta ja yhteyksien uudelleen reitittämisestä Venäjälle sekä mobiiliverkkojen kautta toteutetusta vakoilusta ja informaatiovaikuttamisesta uhkaavien tekstiviestien avulla kyberoperaatiot olivat sivuasemassa Krimin valtaamisen ja Donbassin kansannousun tukemisessa eikä lamauttavaa strategista informaatioiskuoperaatiota toteutettu.[267]

Venäjän ja Yhdysvaltojen suhteet olivat heikentyneet 2010-luvun alussa ja ne sopivat vuonna 2013 ”kuuman linjan” perustamisesta kybereskalaation estämiseksi.[268] Krimin laittoman miehittämisen ja Ukrainan sodan alkamisen seurauksena Venäjän kybervakoilu kuitenkin kiihtyi ja sen rinnalla kehittyi myös informaatiovaikuttamisen tukeminen – ja lopulta häiritsevät, lamauttavat ja tuhoa aiheuttavat kyberhyökkäykset. Jo ennen Ukrainan vuoden 2014 vallankumousta FSB:n 18. Keskus perusti Gamaredoniksi nimetyn APT-ryhmän Ukrainan hallituksen, asevoimien, oikeuslaitoksen ja viranomaisten vakoilemiseksi ja ryhmä on jatkanut toimintaansa tähän päivään saakka. Raporttien mukaan Gamaredonilla on poikkeuksellisen laaja infrastruktuuri ja se ei ole erityisesti pyrkinyt salaamaan toimintaansa.[269] Gamaredonin intensiivisyys vaihteli Itä-

---

[264] Bing, Chris: Russian hacker group ‘CyberBerkut’ returns to public light with allegations against Clinton. *CyberScoop*, 12.7.2017. [https://cyberscoop.com/cyberberkut-returns-hillary-clinton/], luettu 3.2.2024; Jensen, Valeriano & Maness (2019).

[265] Jensen, Valeriano & Maness (2019); Greenberg, Andy: A Brief History of Russian Hackers' Evolving False Flags. *WIRED*, 21.10.2019. [https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/], luettu 3.2.2024; Cheravitch (2021).

[266] Kofman, Michael, Migacheva, Katya, Nichiporuk, Brian, Radin, Andrew, Tkacheva, Olesya & Oberholtzer, Jenny: *Lessons from Russia's Operations in Crimea and Eastern Ukraine*. RAND, Santa Monica, 2017.

[267] Geers, Kenneth (ed.): *Cyber War in Perspective: Russian Aggression against Ukraine*. CCDCOE, Tallinn, 2015, s. 46–51.

[268] Gallagher, Sean: US, Russia to install “cyber-hotline” to prevent accidental cyberwar. *Ars Technica*, 19.6.2013. [https://arstechnica.com/information-technology/2013/06/us-russia-to-install-cyber-hotline-to-prevent-accidental-cyberwar/], luettu 3.2.2024.

[269] Prince, Brian: ‘Operation Armageddon’ Cyber Espionage Campaign Aimed at Ukraine: Lookingglass. *SecurityWeek*, 28.4.2015 [https://www.securityweek.com/operation-armageddon-cyber-espionage-campaign-aimed-ukraine-lookingglass/], luettu 5.1.2024; Toulas, Bill: Ukraine links members of Gamaredon hacker group to Russian FSB. *Bleeping Computer*, 4.11.2021. [https://www.bleepingcomputer.com/news/security/ukraine-links-members-of-gamaredon-hacker-group-to-russian-fsb/], luettu 5.1.2024; SSU Ukraine: Gamaredon / Armageddon Group. Kyiv 2021. [https://ssu.gov.ua/uploads/files/DKIB/Technical%20report%20Armagedon.pdf], luettu 3.2.2024.

Ukrainan tilanteeseen liittyneiden rauhanneuvottelujen tai konfliktin kiristymisen mukaan. Venäjä todennäköisesti käytti sitä vakoilun ohella kybersuorituskykyjensä kehittämiseen ja harjoituttamiseen.[270]

FSB:n Turlaksi nimetty uhkatoimija jatkoi 2008 alkanutta ja 2015 kiihtynyttä Venäjän johtoa kiinnostavien valtioiden kybervakoilua.[271] Etenkin Saksan valtionhallinnon tietoverkot olivat FSB:n mielenkiinnon kohteena.[272] Turla jatkoi menetelmiensä kehittämistä ottamalla käyttöön mm. satelliittilinkkien ja toisten hakkeriryhmien infrastruktuurin kaappaamisen.[273] Vuonna 2019 FSB:n väitettiin käyttäneen Iranin kybervakoiluinfrastruktuuria omien jälkiensä peittämiseen.[274] Samoin jatkui Dukes-kampanja keskittyen etenkin ulkoministeriöihin, mm. Yhdysvaltojen ulkoministeriön verkko jouduttiin sulkemaan tunkeutumisen takia, ja ajatushautomoihin. Venäjän tiedustelupalvelut ovat kohdentaneet vakoilu- ja informaatiovaikuttamisen tukemisoperaatioita, esimerkiksi tietovuotoja, myös yksityishenkilöihin ja näiden käyttämiin salattuihin sähköpostipalveluihin kuten Protonmailiin.[275] Vuosina 2015–2020 kohteet olivat globaaleja ja operaatioiden aktiivisuus vaihteli vanhojen ohjelmaversioiden poistuessa ja uusien tullessa käyttöön.[276]

Vuosina 2011–2020 FSB:n 16. Keskus tunkeutui Yhdysvalloissa ja Länsi-Euroopassa energia-alan yritysten, teollisuuden ja telekommunikaatioyritysten verkkoihin todennäköisesti selvittääkseen niiden teollisuusohjausjärjestelmien haavoittuvuuksia. Tämä kampanja tai uhkatoimija sai useita eri nimiä kuten Berserk Bear, Energetic Bear, Dragonfly ja Crouching Yeti.[277] Vuonna 2018 Yhdysvaltain kotimaan turvallisuusvirasto

---

[270] Kremez, Vitali: Pro-Russian CyberSpy Gamaredon Intensifies Ukrainian Security Targeting. Sentinel Labs, 5.2.2020. [https://www.sentinelone.com/labs/pro-russian-cyberspy-gamaredon-intensifies-ukrainian-security-targeting/], luettu 3.2.2024; Seals, Tara: Gamaredon APT Improves Toolset to Target Ukraine Government, Military. *ThreatPost*, 5.2.2020. [https://threatpost.com/gamaredon-apt-toolset-ukraine/152568/], luettu 3.2.2024.

[271] Malpedia: Turla. 31.10.2023. [https://malpedia.caad.fkie.fraunhofer.de/actor/turla], luettu 3.2.2024; Sharma, Srivathsa: Examining the Activities of the Turla APT Group. Trend Micro, 22.9.2023. [https://www.trendmicro.com/en_us/research/23/i/examining-the-activities-of-the-turla-group.html], luettu 3.2.2024.

[272] Spiegel International: The Breach from the East. *Spiegel International*, 5.3.2018. [https://www.spiegel.de/international/germany/cyber-espionage-likely-from-russia-targets-german-government-a-1196520.html], luettu 3.2.2024.

[273] Secure List: Satellite Turla: APT Command and Control in the Sky. Secure List, 9.9.2015. [https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/], luettu 3.2.2024; Greenberg, Andy: The Underground History of Russia's Most Ingenious Hacker Group. *WIRED*, 20.5.2023 (a). [https://www.wired.com/story/turla-history-russia-fsb-hackers/], luettu 3.2.2024.

[274] Stubbs, Jack & Bing, Christopher: Hacking the hackers: Russian group hijacked Iranian spying operation, officials say. *Reuters*, 21.10.2019. [https://www.reuters.com/article/us-russia-cyber-idUSKBN1X00AK], luettu 5.1.2024.

[275] Campbell, Duncan: How Russian intelligence hacked the encrypted emails of former MI6 boss Richard Dearlove. *Computer Weekly*, 26.9.2022. [https://www.computerweekly.com/news/252525366/How-Russian-intelligence-hacked-the-encrypted-emails-of-former-MI6-boss-Richard-Dearlove], luettu 4.2.2024.

[276] ESET: Operation Ghost: The Dukes aren't back – they never left. ESET Research, 17.11.2019. [https://www.welivesecurity.com/2019/10/17/operation-ghost-dukes-never-left/], luettu 4.2.2024; Malpedia: APT29. 13.12.2023. [https://malpedia.caad.fkie.fraunhofer.de/actor/apt29], luettu 4.2.2024; Mohammed, Arshad: U.S. State Department's unclassified email systems hacked. *Reuters*, 17.11.2014. [https://www.reuters.com/article/cybersecurity-statedept-idINKCN0J11GR20141117], luettu 4.2.2024.

[277] Reuters: U.S. government asks firms to check networks after 'Energetic Bear' attacks. *Reuters*, 2.7.2014. [https://www.reuters.com/article/us-cybersecurity-energeticbear-idUSKBN0F722V20140702], luettu 4.2.2024; Gov.uk: Russia's FSB malign activity: factsheet. 7.12.2023. [https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet], luettu 5.1.2024; CISA: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. 20.4.2022. [https://media.defense.gov/2022/Apr/20/2002980529/-1/-1/1/JOINT_CSA_RUSSIAN_STATE-

ilmoitti, että venäläiset olivat vuotta aikaisemmin päässeet niin syvälle sähköjärjestelmien ohjausjärjestelmiin, että olisivat voineet toteuttaa laajoja sähkökatkoja.[278] Yhdysvaltojen lisäksi myös saksalaiset energia- ja vesiyhtiöiden valvonta- ja ohjausjärjestelmät (Operational technology – OT) olivat FSB:n vakoilun kohteena 2018–2020.[279] Operaatioita voidaan pitää vakoilun ja tiedustelun sekä valmistelun lisäksi strategiseen deterrenssiin liittyvänä viestintänä tai asymmetrisen edun hankkimisena kiristyneessä tilanteessa. Lännessä operaatioiden paljastaminen ja Venäjän uhan korostaminen on palvellut kyberturvallisuuden kehittämistä uhkatietoisuuden lisäämisen kautta.

Venäjä jatkoi sijaistoimijoiden käyttöä läpi 2010-luvun. Sijaistoimijoiden käyttämisellä Venäjä on pyrkinyt etääntymään kyberoperaatioista ja laskemaan kustannuksia ja riskejä. Niiden avulla se on sekoittanut informaatiotilaa, pyrkinyt heikentämään läntisiä narratiiveja, toteuttanut eskalaatioviestintää, painostanut päätöksentekijöitä ja yrittänyt rapauttaa kansalaisten luottamusta näihin sekä heikentää liittolaissuhteita.[280] Vuodesta 2015 GRU (APT28) esiintyi ISIS-liitännäisenä CyberCaliphate ryhmänä, joka mm. lamautti ranskalaisen TV5 Monde kanavan lähetystoiminnan ja uhkaili amerikkalaisten sotilaiden vaimoja sosiaalisessa mediassa. Tavoitteena oli todennäköisesti siirtää Yhdysvaltojen huomio pois Ukrainasta ja korostaa kansainvälisen terrorismin uhkaa.[281] Vuodesta 2016 eteenpäin Venäjä on jatkanut kyberrikollisten, mm. RomComRAT/Cuba Ransomware ryhmä, käyttämistä sijaistoimijoina kyberoperaatioissaan Ukrainaa vastaan ja sen operaatioissa alkoi korostua kiristysohjelmien käyttö disinformaation levittämisen ja lavastusoperaatioiden rinnalla.[282] Kybersijaistoimijoiden käytössä oli samankaltaisuuksia KGB:n kylmän sodan aikaiseen toimintaan. Tuolloinkin turvallisuus- ja tiedustelupalvelun toimintaan saattoi liittyä väkivaltaa tai sillä uhkaamista erilaisten peiteorganisaatioiden takaa.[283]

Vuoden 2015 loppu muodostui Venäjän hyökkäyksellisen kybertoiminnan käännekohdaksi. GRU:n Sandworm hyökkäsi joulukuussa Ukrainan sähköverkkoja vastaan BlackEnergy3 ja Killdisk haittaohjelmilla ja sai katkaistua sähköt 230 000 Ivano-Frankivskin alueen asukkaalta kuudeksi tunniksi. Hyökkäykseen yhdistettiin palvelunesto-

SPONSORED_AND_CRIMINAL_CYBER_THREATS_TO_CRITICAL_INFRASTRUCTURE_20220420.PDF], luettu 5.1.2024.

[278] RFE/RL: Report: Russian Hackers Have Gained Capability to Cause U.S. Blackouts. *RFE/RL*, 24.7.2018. [https://www.rferl.org/a/russian-hackers-came-close-causing-us-blackouts-last-year-wall-street-journal-reported-department-homeland-security-briefing/29386156.html], luettu 4.2.2024.

[279] Lyngaas, Sean: German intelligence agencies warn of Russian hacking threats to critical infrastructure. Cyberscoop, 26.5.2020. [https://cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/], luettu 4.2.2024.

[280] Jensen, Valeriano & Maness (2019); Kollars, Nina A. & Petersen, Michael B.: Feed the Bears, Starve the Trolls. *The Cyber Defence Review*, Special Edition 2019, 145–160.

[281] ETDA: Threat Group Cards: A Threat Actor Encyclopedia - APT group: Sofacy, APT 28, Fancy Bear, Sednit. ETDA, 29.11.2023. [https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Sofacy%2C%20APT%2028%2C%20Fancy%20Bear%2C%20Sednit&n=1], luettu 5.1.2024; Cheravitch (2021); Satter, Raphael: Russian hackers posed as IS to threaten military wives. *AP*, 8.5.2018. [https://apnews.com/article/mi-state-wire-or-state-wire-russia-co-state-wire-north-america-4d174e45ef5843a0ba82e804f080988f], luettu 4.2.2024; Schwartz, Mathew J.: French Officials Detail 'Fancy Bear' Hack of TV5Monde. Bank Info Security, 12.6.2017. [https://www.bankinfosecurity.com/french-officials-detail-fancy-bear-hack-tv5monde-a-9983], luettu 4.2.2024.

[282] Franceschi-Bicchierai, Lorenzo: Cybercriminals who targeted Ukraine are actually Russian government hackers, researchers say. *TechCrunch*, 15.5.2023. [https://techcrunch.com/2023/05/15/cybercriminals-who-targeted-ukraine-are-actually-russian-government-hackers-researchers-say/], luettu 4.2.2024; Greenberg, Andy: A Brief History of Russian Hackers' Evolving False Flags. *WIRED*, 21.10.2019. [https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/], luettu 4.2.2024.

[283] Schoen, Fletcher & Lamb, Christopher J.: *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference.* Strategic Perspectives 11. INSS, NDU, Washington, D.C., 2012.

hyökkäys asiakaspalvelun puhelinkeskusta vastaan sekaannuksen lisäämiseksi.[284] Hyökkäyksen tavoitteena oli painostaa Ukrainan päätöksentekijöitä ja horjuttaa maan sisäistä tilannetta ja se oli mahdollisesti sidoksissa Krimin sähkönjakelun katkaisuun Ukrainan puolelta.[285] Vuoden 2016 joulukuussa Sandworm hyökkäsi uudelleen Kiovan sähköverkkoa vastaan Crashoverride/Industroyer haittaohjelmilla. Operaatio epäonnistui, mutta käytetyt haittaohjelmat osoittivat GRU:n jatkaneen ICS/SCADA[286] järjestelmien tuhoamiseen tarkoitettujen tekniikoiden kehittämistä.[287] GRU hyökkäsi myös ukrainalaisia pankkeja vastaan Killdisk haittaohjelmalla tavoitteenaan tuhota pankkien tietokoneilla olleet tiedot.[288] Vuoden 2017 kesäkuussa GRU hyökkäsi Ukrainaa vastaan EternalBlue ja Mimikatz ohjelmien pohjalle rakennetulla autonomisesti leviävällä ja kohdejärjestelmän tiedot tuhoavalla haittaohjelmalla, jonka nimeksi tuli NotPetya. Haittaohjelma levisi hallitsemattomasti ja aiheutti globaalisti 10 miljardin dollarin tappiot.[289] NotPetyaa seurasi lokakuussa vastaava BadRabbit operaatio, joka tehokkaammasta tietojen kryptausominaisuudesta huolimatta jäi vaikutuksiltaan vähäiseksi ja levisi tahallisesti tai tahattomasti mm. Venäjän media-alan yrityksiin.[290] Huhtikuussa 2020 Ukraina ilmoitti estäneensä Venäjän uuden kyberhyökkäyksen sähköverkkojaan vastaan.[291] NotPetyan aiheuttaman kaaoksen taustalle jäi FSTEK:n TsNIIKhM instituutin toteuttama hyökkäys Triton/Trisis-haittaohjelmalla saudiarabialaista petrokemian yritystä vastaan.[292] Hyökkäys olisi voinut aiheuttaa teollisuuskatastrofin ja on epäonnistuessaankin toiminut deterrenssiviestinnän välineenä. Hyökkäyksen Ukrainan sähköverkkoja vastaan olivat yhteydessä Ukrainan sisäpoliittiseen tilanteeseen ja toisaalta Ukrainan ja Venäjän suhteeseen. Niillä pyrittiin toden-

[284] Zetter, Kim: Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. *WIRED*, 3.3.2016. [https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/], luettu 5.1.2024.

[285] Jensen, Valeriano & Maness (2019); Luhn, Alec: Crimea declares state of emergency after power lines attacked. *The Guardian*, 22.11.2015. [https://www.theguardian.com/world/2015/nov/22/crimea-state-of-emergency-power-lines-attacked], luettu 4.2.2024.

[286] Industrial Control Systems ja Supervisory Control and Data Acquisition (ENISA: Communication network dependencies for ICS/SCADA Systems. December 2016. [https://www.enisa.europa.eu/publications/ics-scada-dependencies], luettu 4.2.2024.

[287] Greenberg, Andy: New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction. *WIRED*, 12.9.2019. [https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/], luettu 5.1.2024.

[288] Leyden, John: BlackEnergy power plant hackers target Ukrainian banks. *The Register*, 15.12.2016. [https://www.theregister.com/2016/12/15/ukraine_banks_apt], luettu 4.2.2024; Cherepanov, Anton: The rise of TeleBots: Analyzing disruptive KillDisk attacks. ESET, 13.12.2016. [https://www.welivesecurity.com/2016/12/13/rise-telebots-analyzing-disruptive-killdisk-attacks/], luettu 4.2.2024.

[289] Greenberg, Andy: The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *WIRED*, 22.8.2018. [https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/], luettu 5.1.2024.

[290] Polityuk, Pavel& Stubbs, Jack: New wave of cyber-attacks hits Russia, other nations. *Reuters*, 24.10.2024. [https://www.reuters.com/article/us-ukraine-cyber/new-wave-of-cyber-attacks-hits-russia-other-nations-idUSKBN1CT21F], luettu 4.2.2024; NCSC (2018).

[291] Lyngaas, Sean: Russian military-linked hackers target Ukrainian power company, investigators say. *CNN*, 14.4.2022. [https://edition.cnn.com/2022/04/12/politics/gru-russia-hackers-ukraine-power-grid/index.html], luettu 4.2.2024.

[292] Greenberg, Andy: The US Sanctions Russians for Potentially 'Fatal' Triton Malware. *WIRED*, 23.10.2020. [https://www.wired.com/story/russia-sanctions-triton-malware/], luettu 4.2.2024; Giles, Martin: Triton is the world's most murderous malware, and it's spreading. *MIT Technology Review*, 5.3.2019. [https://www.technologyreview.com/2019/03/05/103328/cybersecurity-critical-infrastructure-triton-malware/], luettu 4.2.2024.

näköisesti joko vaikuttamaan Ukrainan politiikkaan tai viestimään Venäjän suorituskyvyistä kybertilassa.[293]

Kaikista eniten huomiota herätti kuitenkin niin kutsuttu DNC Hack vuonna 2016. Kesken Yhdysvaltojen presidentinvaalikampanjan GRU:n 85. Erikoispalvelukeskukseen liitetty uhkatoimija (Fancy Bear, Pawn Storm, APT28) tunkeutui Demokraattien kansallisen komitean ja Hilary Clintonin vaalikampanjan tietoverkkoihin ja sähköposteihin. Tämän jälkeen GRU:n Erikoisteknologioiden keskus julkaisi tuhansia tiedostoja, osa mahdollisesti muokattuja, valeprofiilien (Guccifer 2.0 ja DC Leaks) ja sijaistoimijoiden (Wikileaks) kautta. Ilmeisemmin GRU:sta tietämättä myös FSB:n tai SVR:n uhkatoimija Cozy Bear oli pyrkinyt tunkeutumaan samoihin järjestelmiin vuodesta 2015 alkaen. GRU julkaisi varastamaansa materiaalia useaan otteeseen syksyn aikana ja kykeni näin horjuttamaan Demokraattien vaalikampanjaa median uutiskierron ylläpitäessä kriisiä. Lisäksi Shadow Brokers niminen ryhmä julkaisi samaan aikaan NSA:n Tailored Access Operations hakkeriryhmältä varastettuja työkaluja Githubissa. Ryhmä julkaisi lisää työkaluja 2017 keväällä. Shadow Brokersin tapauksessa on voinut olla kysymys venäläisten deterrenssiviestinnästä tai sitten varastetut työkalut olivat menettäneet arvonsa ja niillä haluttiin mustamaalata Yhdysvaltojen tiedustelupalveluita.[294] GRU:n operaation vaikutuksia lisäsivät mm. Internet Research Agencyn (IRA) eli ”trollitehtaan” informaatiovaikuttamisoperaatiot, joissa käytettiin mm. Facebook mainoksia, sosiaalisen median valetilejä ja bottiverkkoja.[295] Venäjän tavoitteena ei välttämättä ollut vaikuttaa suoraan Yhdysvaltojen presidentinvaalien tulokseen vaan korruptoida amerikkalaisten luottamus vaalijärjestelmään ja demokratiaan yleensä.[296] Venäjä pyrki informaatiovaikuttamiseen myös Yhdysvaltojen vuoden 2020 presidentinvaaleissa, mutta panostus ja vaikutukset jäivät vähäisiksi.[297] Huolimatta aikanaan saamasta julkisuudesta ja Yhdysvaltojen esittämistä protesteista Venäjän operaatio ei poikennut kylmän sodan aikaisesta vaalivaikuttamisesta kuin kenties uusien tekniikoiden ja laajuutensa puolesta.[298] Läntinen reaktio Venäjän hyökkäykseen oli kuitenkin yllättynyt ja jopa pelokas, mikä osiltaan selittää tarvetta attribuoida Venäjän operaatiot aikaisempaa selvemmin ja tarvetta asettaa sanktioita ja nostaa syytteitä operaatioiden toteuttajia vastaan.[299]

Kyberhyökkäysten lisäksi GRU vaikuttaa vuodesta 2015 alkaen lisänneen merkittävästi kybervakoiluoperaatioita tai sitten kyseessä oli edellä mainittu attribuutiokynnyksen lasku.[300] GRU:ta on syytetty vuosien 2015–2020 aikana mm.:

- Saksan Bundestagin
- Ison-Britannian ulkoministeriön

---

[293]Jasper, Scott: *Russian Cyber Operations: Coding the Boundaries of Conflict*. Washington, DC, Georgetown University Press, 2020.

[294] Rid, Thomas: How Russia Pulled Off the Biggest Election Hack in U.S. History. *Esquire*, 20.10.2016. [https://www.esquire.com/news-politics/a49791/russian-dnc-emails-hacked/], luettu 5.1.2024; Mueller, Robert S.: *Report on The Investigation Into Russian Interference In The 2016 Presidential Election*. U.S. Department of Justice, Washington, DC, 2019.

[295] Polyakova, Alina: What the Mueller report tells us about Russian influence operations. Brookings, 18.4.2019. [https://www.brookings.edu/articles/what-the-mueller-report-tells-us-about-russian-influence-operations/], luettu 4.2.2024.

[296] Jensen, Valeriano & Maness (2019).

[297] National Intelligence Council: Foreign Threats to the 2020 US Federal Elections. NIC, 10.3.2021. [https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf], luettu 4.2.2024.

[298] Connell & Vogler (2022); Rid (2020).

[299] Lännen reaktioista ks. Kerr (2023), s.6–7.

[300] NCSC (2018).

- Tšekin tasavallan ulkoministeriön
- Tanskan puolustusministeriön
- Norjan parlamentin
- Itä-Euroopan Kaukasian ja Keski-Aasian maiden lähetystöjen ja ulkoministeriöiden
- Montenegron hallituksen
- Ranskan Emmanuel Macronin presidentinvaalikampanjan
- Vuoden 2018 yhdysvaltalaissenaattoreiden ja puolueiden välivaalien ja EU:n parlamenttivaaleihin osallistuvien puolueiden kampanjoiden
- Malesian Airlines MH17 tuhoa tutkineen turvallisuuslautakunnan
- Kansalaisjournalismijärjestö Bellingcatin
- Maailman antidopingtoimiston (WADA)
- Kemiallisten aseiden kieltojärjestön (OPCW)
- Kansainvälinen yleisurheiluliiton (IAAF)
- Kansainvälisen jalkapalloliiton (FIFA)
- Euroopan puolustusviraston (EDA)
- COVID-19 rokotetutkimuskeskusten vakoilusta.[301]

Lokakuussa 2023 Yhdysvallat ilmoitti Venäjän pyrkineen vaikuttamaan yhteentoista vaaliin yhdeksässä demokraattisessa maassa vuosina 2020–2022.[302] Kaikilla tapauksilla on ollut selkeä yhteys kansainvälispoliittiseen tilanteeseen ja Venäjän tarpeeseen saada informaatiota vastustajistaan ja lähialueen valtioiden poliittisesta tilanteesta sekä toisaalta vastustajien tarpeeseen paljastaa ja attribuutioida Venäjän vakoilu. GRU:n toiminnasta kertovien lähteiden länsipainottuneisuuden sekä osittain tietoturvayhtiöiden markkinointilogiikan takia osa GRU:n vakoiluoperaatioista on varmasti jäänyt pimentoon. Yhtä kaikki vakoilulla ei pelkästään pyritty hankkimaan tietoa Venäjän valtiojohdon päätöksenteon tueksi vaan myös informaatiovaikuttamisen kautta manipuloimaan vastustajia.

Vuosina 2015–2020 Venäjän tiedustelupalvelut, usein miten väitetysti GRU, toteuttivat joukon kyberoperaatioita, joilla oli tarkoitus tukea informaatiovaikuttamista Lännen ja Venäjän suhteiden kiristyessä. Vuoden 2018 Pyeongchangin talviolympialaisten verkkosivut olivat poissa käytöstä 12 tuntia ja TV- ja viestiliikenneyhteyksissä oli häiriöitä, kun venäläiset hakkerit, mahdollisesti GRU:n Erikoisteknologioiden keskus, estivät järjestelyorganisaation toimialueen ohjauskoneiden toiminnan Olympic Destroyer kyberhyökkäyksellä. Pohjois-Korea pyrittiin lavastamaan operaation toteuttajaksi.[303] GRU:ta on syytetty myös kyberoperaation valmistelusta Tokion olympialaisia

[301] Council on Foreign Relation (2024); CSIS: Significant Cyber Incidents. December 2023. [https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents], luettu 4.2.2024; NCSC (2018); Hacquebord, Feike: Pawn Storm in 2019. A Year of Scanning and Credential Phishing on High-Profile Targets. Trend Micro Research, 2019. [https://documents.trendmicro.com/assets/white_papers/wp-pawn-storm-in-2019.pdf], luettu 4.2.2024.

[302] Landay, Jonathan & Lewis, Simon: US intelligence report alleging Russia election interference shared with 100 countries. *Reuters*, 20.10.2013. [https://www.reuters.com/world/us/us-intelligence-report-alleging-russia-election-interference-shared-with-100-2023-10-20/], luettu 4.2.2024.

[303] Mercer, Warren: Olympic Destroyer Takes Aim At Winter Olympics. Talos, 12.2.2018. [https://blog.talosintelligence.com/olympic-destroyer/], luettu 4.2.2024; Greenberg, Andy: US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit. *WIRED*, 19.10.2020. [https://www.wired.com/story/us-indicts-sandworm-hackers-russia-cyberwar-unit/], luettu 5.1.2024; Greenberg, Andy: The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History. *WIRED*, 17.10.2019. [https://www.wired.com/story/untold-story-2018-olympics-destroyer-cyberattack/], luettu 4.2.2024.

vastaan 2020.[304] Secondary Infektion kampanja levitti väärennettyjä dokumentteja sosiaalisen media alustoilla synnyttääkseen sisäpoliittista hajaannusta Virossa ja Georgiassa.[305] Lokakuussa 2019 Sandworn toteutti kyberhyökkäyskampanjan Georgiaa vastaan, jossa sotkettiin hallinnon, median ja kansalaisjärjestöjen verkkosivuja ja estettiin tilapäisesti TV-kanavien toiminta.[306] Venäjä on myös pyrkinyt vakoilemaan Baltiaan ja Puolaan sijoitettujen Naton sotilaiden kännyköitä ja pyrkinyt pelottelemaan sotilaita manipuloimalla kännyköitä.[307] Lisäksi Venäjää on syytetty 2017–2020 Ghostwriter kampanjasta, jossa pyrittiin levittämään disinformaatiota Natosta puolalaisella, latvialaiselle ja liettualaiselle yleisölle väärennettyjen sähköpostiosoitteiden ja tai verkkosivujen manipuloinnin kautta. Tämän operaation ovat kuitenkin todennäköisesti toteuttaneet valkovenäläiset.[308] Operaatioiden aiheuttaman sekaannuksen, epäluulon ja pelon oli todennäköisesti tarkoitus horjuttaa ja heikentää Venäjän vastassa ollut liittoumaa ja täten ennaltaehkäistä sen muodostamaa uhkaa strategisen deterrenssin periaatteiden mukaisesti. Niiden vaikutus kuitenkin jäi toiseksi venäläisen median ja diplomaattien perinteisemmän propaganda- ja disinformaatiokampanjan rinnalla.[309]

Kybervakoilun menetelmät kehittyivät 2010-luvun kuluessa merkittävästi. Venäjän on vakoillut Baltiaan ja Puolaan sijoitettujen Naton sotilaiden kännyköitä mobiiliverkkoja hyväksikäyttämällä ja pyrkinyt pelottelemaan sotilaita manipuloimalla kännyköitä.[310] GRU on liitetty yli 500 000 kotireitittimen saastuttamiseen VPNFilter-haittaohjelmalla, joka on mahdollistaa niin kutsutut väliintulohyökkäykset (Man-in-the-middle).[311] Samaa ohjelmaa käytettiin vuonna 2018 yrityksessä tunkeutua Ukrainan vedenpuhdistamojärjestelmään.[312] GRU:n Strontium uhkatoimija on myös pyrkinyt käyttämään IoT-laitteiden haavoittuvuuksia tunkeutuakseen yritysten sisäverkkoihin.[313] SVR murtautui vuonna 2020 Solar Winds Orion palvelun päivityspalveluun ja syötti järjestelmään haittaohjelman, joka mahdollisti pääsyn palvelun asiakkaiden jär-

---

[304] NCSC: UK and partners condemn GRU cyber-attacks against Olympic and Paralympic Games. NCSC, 19.10.2020. [https://www.ncsc.gov.uk/news/uk-and-partners-condemn-gru-cyber-attacks-against-olympic-an-paralympic-games], luettu 4.2.2024.

[305] Stone, Jeff: Suspected Russian operatives tried using forged diplomatic documents, social media to create divisions. *Cyberscoop*, 8.4.2020. [https://cyberscoop.com/russia-disinformation-operation-pinball-georgia-moldova/], luettu 4.2.2024.

[306] GOV.UK: UK condemns Russia's GRU over Georgia cyber-attacks. GOV.UK, 20.2.2020. [https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks], luettu 4.2.2024; Roguski, Przemysław: Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace. Just Security, 6.3.2020. [https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/], luettu 4.2.2024.

[307] Ward, Alex: NATO troops say Russia is hacking their smartphones. *Vox*, 4.10.2017. [https://www.vox.com/world/2017/10/4/16424602/nato-russia-smartphone-hacking-report], luettu 4.2.2024.

[308] Foster, Lee, Mainor, David, Read, Ben, Riddell, Sam, Roncone, Gabby, Smith, Lindsay, & Wahlstrom, Alden: Ghostwriter Update: Cyber Espionage Group UNC1151 Likely Conducts Ghostwriter Influence Activity. Mandiant, 13.10.2024. [https://www.mandiant.com/resources/unc1151-ghostwriter-update-report], luettu 4.2.2024.

[309] Paul, Christopher & Matthews, Miriam: *The Russian "Firehose of Falsehood" Propaganda Model. Why It Might Work and Options to Counter It*. RAND, Santa Monica, 2016.

[310] Ward (2017).

[311] Goodin, Dan: VPNFilter malware infecting 500,000 devices is worse than we thought. *Ars Technica*, 6.6.2018. [https://arstechnica.com/information-technology/2018/06/vpnfilter-malware-infecting-50000-devices-is-worse-than-we-thought/], luettu 4.2.2024.

[312] Interfax: SBU thwarts cyber-attack from Russia against chlorine station in Dnipropetrovsk region. *Interfax*, 11.7.2018. [https://en.interfax.com.ua/news/general/517337.html], luettu 4.2.2024.

[313] Cimpanu, Catalin: Microsoft: Russian state hackers are using IoT devices to breach enterprise networks. *ZDNet*, 5.8.2019. [https://www.zdnet.com/article/microsoft-russian-state-hackers-are-using-iot-devices-to-breach-enterprise-networks/], luettu 4.2.2024.

jestelmiin. Tämän seurauksena se onnistui tunkeutumaan yli 250:een Yhdysvaltojen hallinnon ja yrityssektorin järjestelmään.[314] Yhdysvallat asetti hyökkäyksen johdosta Venäjälle sanktioita ja karkotti maasta kymmenen diplomaattia.[315]

Kaikesta globaalista aktiivisuudestaan huolimatta Venäjän pääkohde on vuosina 2015–2020 ollut Ukraina. Ukrainaan kohdistui vuonna 2016 pelkästään kahdessa kuukaudessa 6500 kyberhyökkäystä[316] Vuosina 2017–2018 Ukraina muun muassa ilmoitti Venäjän valmistelevan laaja-alaista kyberhyökkäystä maata vastaan, Ukrainan ortodoksikirkkoon kohdistuneesta vakoilusta ja useista hallinnon, asevoimien, pankkijärjestelmän, talouselämän ja yhteiskunnan kriittisiin järjestelmiin kohdistuneista hyökkäyksistä. Merkittävät kyberhyökkäykset ovat osuneet loma- tai merkkipäiville.[317] Kyberavusteinen informaatiovaikuttaminen oli Venäjän toiminnan keskiössä ja sillä pyrittiin heikentämään Ukrainan kansan yhtenäisyyttä ja Ukrainan lähentymistä Länteen.[318] Hyökkäyksiin ottivat väitetysti osaa myös kapinallisten maakuntien hakkerit.[319] Venäjä pyrki saastuttamaan Ukrainan asevoimien käyttämiä johtamisjärjestelmäohjelmistoja haittaohjelmilla ja vuonna 2014 GRU laski liikkeelle väärennetyn version Ukrainan käyttämästä tykistön tulenjohtamissovelluksesta.[320] Venäjän Ukrainaan kohdistuvan kybertoiminnan aktiivisuuteen ja laatuun on todennäköisesti vuosina 2019–2020 vaikuttanut lieventävästi, COVID-pandemian ohella, presidentti Volodymyr Zelenskyin presidenttikauden alkuvaiheen liennyttävä politiikka, joka kuitenkin loppusyksystä 2020 kääntyi vahvemmin venäjävastaiseksi.[321] Ukrainan operaatioiden avulla Venäjä pyrki vaikuttamaan Ukrainan sisäpoliittiseen tilanteeseen, kehitti kyberhyökkäyskykyjään ja todennäköisesti toteutti deterrenssiviestintää kriittiseen infrastruktuuriin kohdistuvien operaatioiden kautta. On mahdollista, että Venäjä oli liiankin aktiivinen kybertoiminnassaan ja tahtomattaan kehitti Ukrainan kyberpuolustusta ja henkistä resilienssiä kyberhyökkäyksiä kohtaan.

Turvallisuuspalveluiden ja asevoimien tiedustelun jo toimeenpannessa kyberoperaatioita Venäjän asevoimat aloittivat vasta 2010-luvulla operatiivisten kybersuorituskykyjen rakentamisen. Venäjän Yleisesikunnan 8. Direktoraatti oli ollut jo 1990-luvulta vastuussa mm. informaatioturvallisuudesta ja salausjärjestelmistä ja siellä työskenteleviä upseereita koulutti Krasnodarin kenraali S. Štemenkon Sotilasinstituutti.[322] Aikeet

---

[314] Hautala, Laura: SolarWinds hackers accessed DHS acting secretary's emails: What you need to know. *CNET*, 29.3.2021. [https://www.cnet.com/news/privacy/solarwinds-hackers-accessed-dhs-acting-secretarys-emails-what-you-need-to-know/], luettu 5.1.2024.

[315] Brandom, Russell: US institutes new Russia sanctions in response to SolarWinds hack / Other sanctions target Kremlin staffers who sought to undermine 2020 election results. *The Verge*, 15.4.2021. [https://www.theverge.com/2021/4/15/22385371/russia-sanctions-solarwinds-biden-white-house-putin-hack], luettu 4.2.2024.

[316] Sanger, David E.: *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. Scribe, Melbourne, 2018, s. 169.

[317] Cheravitch (2021), s. 31.

[318] Kerr (2023), s. 8–9.

[319] Polityuk, Pavel: Exclusive: Ukraine says Russian hackers preparing massive strike. *Reuters,* 27.6.2018. [https://www.reuters.com/article/us-ukraine-cyber-exclusive-idUSKBN1JM225], luettu 4.2.2024; House of Commons Library – UK Parliament: Conflict in Ukraine: A timeline (2014 – eve of 2022 invasion). 22.8.2023. [https://commonslibrary.parliament.uk/research-briefings/cbp-9476/], luettu 4.2.2024; Council on Foreign Relation (2024); CSIS (2024).

[320] CrowdStrike: Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units. CrowdStrike, 23.3.2017. [https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf], luettu 4.2.2024.

[321] House of Commons Library (2023).

[322] GlobalSecurity.org: Eighth Directorate of the General Staff State Secret Protection Service of the Armed Forces. GlobalSecurity.org, n.d. [https://www.globalsecurity.org/intell/world/russia/8gumo.htm], luettu 4.2.2024; Lysenko & Brooks (2018).

kyberkomentoportaan perustamisesta toi ensimmäisen kerran julkisuuteen varapääministeri Dmitri Rogozin vuonna 2012.[323] 2013 uutistoimisto Interfax raportoi, että asevoimiin perustettaisiin kyberjohtoporras vuoteen 2014 mennessä ja puolustusministeriön nimetön lähde totesi 2014, että asevoimat olivat perustaneet joukot puolustamaan omia verkkojaan kyberhyökkäyksiltä.[324] Vuonna 2014 puolustusministeri Šoigu ilmoitti informaatio-operaatiojoukkojen (Войска информационных операций – VIO) perustamisesta, jotka myöhemmin 2017 ilmoitti perustetuksi.

Šoigun ilmoituksen perusteella informaatio-operaatiojoukkojen tehtäviin kuului kybertoiminnan lisäksi strateginen kommunikaatio ja omien joukkojen suojaaminen vihamieliseltä propagandalta, mikä muodosti joukkojen tehtäväkentän varsin laveaksi. Ilmeisemmin VIO toimii Yleisesikunnan alla, mahdollisesti GRU:n johdossa. Sillä on kyber-, ELSO- ja psykologisten operaatioiden alayksiköt sotilaspiireissä ja joukot harjoittelevat osana joukkojen harjoituksia.[325] Puolustusministerin ilmoituksesta huolimatta Venäjällä ei virallisesti ole kyberaselajia tai johtoporrasta.[326] Tosin asevoimien erillinen informaatio-operaatiojoukkojen joukko-osasto perustettiin Krimille lokamarraskuussa 2015. Sen tehtäviin kuuluu vastustajan tietoverkkojen ja johtamisjärjestelmien häirintä.[327] Käytössä olevien tietojen perusteella VIO:n voi olettaa kuuluvan ns. erikoisjoukkoihin (специальные войска), joiden tehtävä on tukea (обеспечение военных (боевых) действий) asevoimien taistelutoimia tai toteuttaa erillisiä niille käskettyjä tehtäviä. Täten VIO:n yksiköt joko toteuttavat itsenäisesti taistelutoimia, taisteluita tai iskuja tai niiden toiminta liitetään osaksi taistelevien joukkojen toimintaa.[328] Sanakirjamääritelmän mukaisesti VIO täyttää aselajien määritelmän: sillä on omat taistelussa käytettävät välineet, muodot ja keinot.[329] Lisäksi osa aikaisemmin mainituista tiedekomppanioista on todennäköisesti osallistunut hyökkäykselliseen toimintaan tai ainakin kouluttanut hakkereita asevoimien tarpeisiin. Venäjä on tarkoituksella jättänyt

---

[323] Ведомости: Рогозин рассказал о планах создать киберкомандование. *Ведомости*, 12.3.2012. [https://www.vedomosti.ru/technology/news/2012/03/21/rogozin_rasskazal_o_planah_sozdat_kiberkomandovanie], luettu 4.2.2024.

[324] ТАСС: Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций. *ТАСС*, 12.5.2014 [https://tass.ru/politika/1179830], luettu 4.2.2024; Независимое военное обозрение: В бой идет новый род войск. Кибероперации приравняли к нанесению ядерного удара. *Независимое военное обозрение*, № 7 (938) 2017.

[325] Независимое военное обозрение: В бой идет новый род войск. Кибероперации приравняли к нанесению ядерного удара. *Независимое военное обозрение*, № 7 (938) 2017; Cheravitch (2021); Mil.ru: Военные связисты ЗВО отразили кибератаки «противника» на учении «Запад-2017». Mil.ru, 15.9.2017. [https://function.mil.ru/news_page/country/more.htm?id=12142419@egNews], luettu 4.2.2024; Интерфакс: Минобороны РФ создали войска информационных операций. *Интерфакс*, 22.2.2017. [https://www.interfax.ru/russia/551054; https://home.treasury.gov/news/press-releases/jy0126], luettu 4.2.2024; Dmitriev, Denis & Kovalev, Alexey: Psy-ops in high places Putin's new science adviser to Russia's National Security Council is a military intelligence agent accused of spreading disinformation about the coronavirus. *Meduza*, 17.5.2021. [https://meduza.io/en/feature/2021/05/17/psy-ops-in-high-places], luettu 4.23.2024; Agentura.Ru: Центр зарубежной военной информации и коммуникации (ЦЗВИК) ГУ ГШ. Agentura.ru, n.d. [https://agentura.ru/centr-zarubezhnoj-voennoj-informacii-i-kommunikacii-czvik-gu-gsh/], luettu 4.2.2024.

[326] Интерфакс: В Госдуме опровергли существование "кибервойск" в России. *Интерфакс,* 16.1.2017. [https://www.interfax.ru/russia/545640], luettu 5.1.2024.

[327] ТАСС: Отдельная часть Войск информационных операций появится осенью в Крыму. *ТАСС*, 17.4.2015. [https://tass.ru/armiya-i-opk/1911074], luettu 4.2.2024.

[328] Käsitteistöstä ks. Остапенко, Баушев & Морозов (2012); Министерство обороны Российской Федерации (MoD): *Справочник офицера*. Москва, 2017; Министерство обороны Российской Федерации (MoD): *Боевой устав сухопутных войск часть 2 батальон, рота*. Москва, 2013.

[329] Mil.ru: Военный энциклопедический словарь, 'Род войск (сил).' [https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=12348@morfDictionary], luettu 4.2.2024.

asevoimiensa kyberorganisaation julkistamatta, mikä yhtäältä tukee sen diplomaattisia pyrkimyksiä syyttää muita suurvaltoja kybertilan militarisoinnista ja toisaalta todistaa kybersuorituskyvyille annettua strategista painoarvoa ja samalla operaatioturvallisuudelle asetettuja vaatimuksia.

Länsi reagoi Venäjän operaatioihin vuodesta 2016 alkaen. Yhdysvallat liittolaisineen nimesi ja asetti pakotteita venäläisillä hakkereille.[330] Vuonna 2018 presidentti Donald Trump hyväksyi aktiiviset ja ennaltaehkäisevät kyberoperaatiot Yhdysvaltojen vastustajia vastaan ja samana vuonna U.S. Cyber Command esti IRA:n toiminnan kongressin välivaalien aikana. Vuonna 2020 presidentinvaalien alla U.S. Cyber Command yhdessä Microsoftin kanssa tuhosi Venäjän käyttämän bottiverkon.[331] Vuosina 2020–2021 läntiset tiedustelupalvelut ja palveluntarjoajat alkoivat aktiivisesti tuhota Venäjän disinformaatioalustoja ja niiden uskottavuutta identifioimalla, attribuoimalla, poistoilla, sanktioilla ja tutkimuksella yhteistyössä yksityisten ja kansalaisjärjestöjen kanssa.[332] Yhdysvallat, Nato- ja EU-maat tukivat taloudellisesti yli 1 miljardilla dollarilla Ukrainan kyberturvallisuuden kehittämistä ja monet kansainväliset yritykset, kuten Microsoft, Cisco ja Crowdstrike toimivat aktiivisesti Ukrainassa ja keräsivät kokemuksia venäläisten toiminnasta. EU tuki Ukrainaa lainsäädännöllisten ja normatiivisten valmiuksien kehittämisessä.[333] Ukrainan teleliikenneyritykset kasvattivat kyberturvallisuushenkilöstönsä vuodesta 2015 moninkertaiseksi.[334] Kun Venäjä sitten vuonna 2021 aloitti Ukrainan hyökkäysoperaation valmistelun kybertilassa, sillä oli vastassa kokenut ja valmistautunut vastustaja, josta oli vaikea saada yllätyksellistä etua ja joka oli varautunut tekemään tyhjäksi Venäjä operaatiot kyber- ja informaatiotilassa.[335]

Edellä esitettyjen ja aikaisemman tutkimuksen valossa on perusteita olettaa, että Venäjän hyökkäyksellinen kybertoiminta sai vaikutteita Venäjän turvallisuuspalveluiden historiallisista toimintatavoista. Vakoilun ja psykologisen vaikuttamisen korostuminen ei kuitenkaan ole ainut jatkuvuutta osoittava piirre. Määrätty teknologiafetisismi ja innokkuus uusien menetelmien käytössä edun saavuttamiseksi on myös ominaista venäläiselle strategiselle kulttuurille. Samoin aggressiivisuus ja voiman näyttäminen. Tämä näkyi etenkin 2010-luvun jälkimmäisen puoliskon kyberoperaatioissa.

Venäjän hyökkäykselliset toimet ovat osa kansallista informaatioturvallisuuden järjestelmää, jolla vaikutettiin potentiaalisiin vastustajiin ja turvallisuusympäristöön laajemminkin. Tämä ei ollut informaatiosotaa[336] vaan informaatiokamppailua osana valtioiden välistä jatkuvaa kamppailua. Kyseessä oli systeemien välinen, manipulointiin perustuva vuorovaikutus, jossa pääkeinot ja menetelmät olivat ei-sotilaallisia, ei-väkivaltaisia ja epäsuoria. Strategista ympäristöä ja siitä nousevia uhkia pyrittiin ennalta ehkäisemään strategisen deterrenssin periaatteiden mukaisesti. Samalla pyrittiin rapauttamaan vastustajien informaatiopotentiaalia. 2010-luvulla kybermenetelmät näyttivät tarjoavan kustannustehokkaan ja potentiaalisesti asymmetrisen edun. Venäjän toiminnassa näkyi kompensointi ja toiminnanvapauden hankkiminen koetun teknologisen,

[330] U.S. Department of State: Cyber Sanctions. n.d. [https://www.state.gov/cyber-sanctions/], luettu 4.2.2024.
[331] CSIS (2024).
[332] Cheravitch (2021), s. 36–37.
[333] Ks. Giles (2023).
[334] Bateman (2022).
[335] Warsaw Security Forum: Day 2: WSF2023 - Chicago room. 2023, [https://www.youtube.com/watch?v=g5A8jzR2ZJo], luettu 1.2.2024.
[336] Venäjän asevoimien määritelmän mukaan informaatiosotaan kuuluu avoin ja jyrkkä vastakkainasettelu, jossa informaatiovälineiden vaikutukset ovat tuhoavia ja käyttö massamaista (ks. Luku 2).

taloudellisen ja tavanomaisen sotilaallisen heikkouden tilassa. Nämä heikkoudet eivät väistyneet helmikuussa 2022, mutta voimankäytön reunaehdot ja päämäärä muuttuivat.

5. KYBERSODANKÄYNTIÄ UKRAINASSA 2022

Venäjän helmikuussa 2022 alkaneen Ukrainaan kohdistuneen hyökkäysoperaation jaottelu kybertilan tapahtumien osalta on haasteellista. Jaottelua vaiheisiin vaikeuttaa yhtäältä hyökkäysoperaation alkuvaiheen epäonnistuminen, minkä takia maaliskuun 2022 alkupuolen jälkeiset tapahtumat eivät ole asetettavissa millekään suunnitelmalliselle jatkumolle, ja toisaalta tiedon saatavuus myöhemmältä ajanjaksolta. Lisäksi vaiheistamista hankaloittaa se, että Venäjän asevoimat yrittivät toteuttaa mahdollisesti poliittisen johdon ohjaukseen ja virheelliseen tilanneymmärrykseen perustuen kaappaushyökkäyksen kaltaisen voimankäytöltään kuitenkin rajatun operaation ilman kunnollista valmistelua.[337] Toisaalta on toki mahdollista, kuten Viitaniemi ja Kytöneva väittävät, että asevoimien aseellisen taistelun kuva oli lähtökohtaisesti virheellinen eli Venäjän asevoimat lähti taisteluun, joka ei vastannut sen oletuksia.[338] Myöskin venäläisten sotilaiden 2000-luvulla kehittynyt kiinnostus epäsuoruutta, asymmetriaa ja oveluutta kohtaan eli ei-sotilaallisen väkivallan mahdollisuuksiin saattoi johtaa liialliseen riskinottoon.[339]

Edellä esitettyjen syitten takia sekä ajallisen kehityksen analysoimiseksi tarkastellaan Venäjän hyökkäyksellisiä kyberoperaatioita Ukrainassa ja Lännessä ja Venäjään kohdistuneita operaatiota tässä ja seuraavassa luvussa kronologisesti sitoen ne sotatoimien yleiseen kehitykseen.[340] Lukujen yhteenvedoissa tehtyjä havaintoja tarkastellaan sotataidollisesta näkökulmasta. Huomioitavaa on, että Venäjä jatkoi kybertoimintaa Ukrainan konfliktin ulkopuolellakin, mutta tämä toiminta rajataan tarkastelun ulkopuolelle.[341] Luvussa seitsemän tarkastellaan temaattisemmin jaoteltuna Venäjän puolustuksellista kybertoimintaa ja sen kehitystä hyökkäyssodan aikana.

---

[337] Dougherty, Christopher: Strange Debacle: Misadventures in Assessing Russian Military Power. *War on the Rocks*, 16.6.2022. [https://warontherocks.com/2022/06/strange-debacle-misadventures-in-assessing-russian-military-power/], luettu 4.2.2024; McDermott, Roger N. & Bartles, Charles K.: An Assessment of the Initial Period of War: Russia-Ukraine 2022 Part Two. Online report, August 2022. [https://www.researchgate.net/publication/371411326_An_Assessment_of_the_Initial_Period_of_War_Russia-Ukraine_2022_Part_II], luettu 4.2.2024; Baev (2022); Zabrodskyi, M., Watling, J., Danylyuk, O. & Reynolds, N.: *Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022*. RUSI, London, 2022; Watling, Jack & Reynolds, Nick: *Ukraine at War. Paving the Road from Survival to Victory*. RUSI. London, 2022; Congressional Research Service: Russia's War in Ukraine: Military and Intelligence Aspects. Updated September 14, 2022. [https://crsreports.congress.gov/product/pdf/R/R47068], luettu 4.2.2024.

[338] Viitaniemi & Kytöneva (2023). Vastaavan väitteen on esittänyt myös Pavel Baev (Baev (2022)).

[339] Kukkola (2022); Minic (2023).

[340] Vaihtoehtoisia jaotteluja: CERT-EU: valmisteluvaihe (Helmikuun 2022 3. viikkoon asti), nopea ja raivokas vaihe (Helmikuun viimeinen viikko – maaliskuu 2022) ja ylläpito vaihe nousuineen ja laskuineen (Huhtikuusta 2022) (CERT-EU: 1 Year Ukraine: Russia's War on Ukraine: One Year of Cyber Operations. CERT-EU, 24.2.2023 (a). [https://cert.europa.eu/blog/1yua-cyberops], luettu 5.1.2024.) Ukrainan asevoimat: 0. vaihe (ennen tammikuuta 2022), 1. vaihe (tammikuu 2022 – toukokuu 2022), 2. vaihe (Toukokuu 2022 – Joulukuu 2022) ja 3. vaihe (Joulukuusta 2022) (Zhukov, V. & Bespalov, M.: Cyber Operations in Russia's War against Ukraine Armed Forces Lessons learned. [Näyttöesitys]. USEUCOM Cyber Summit Briefing, 25 July 2023. Unclassified). Google / Mandiant: 1. Strateginen tiedustelu ja valmistelu (2019–2022 tammikuu), 2. Alkuvaiheen tuhoavat kyberoperaatiot ja sotilaallinen hyökkäys (helmikuu-huhtikuu), 3. Jatkuva maalittaminen ja hyökkäykset (toukokuu-heinäkuu), 4. Jalansijan ylläpito strategisen edun hankkimiseksi (elo-syyskuu), 5. Horjuttavien hyökkäysten kampanjan uudelleen käynnistäminen (loka-joulukuu). (Google: Fog of War. How the Ukraine Conflict Transformed the Cyber Landscape. Google, 16.2.2023. [https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf], luettu 5.1.2024).

[341] Tarkasteltaessa Venäjän hyökkäyksellisiä kyberoperaatioita on huomattava, että tiedot tapahtumista ovat tässä vaiheessa varsin puutteelliset ja yksittäiset tapahtumat saattavat saada suhteetonta huomiota suhteessa muuhun, jatkuvaan ja runsaaseen toimintaan.

5.1. Valmistelu 2021–2022

Venäjä ryhmitti ensimmäisen kerran merkittävän määrän joukkojaan Ukrainan vastaiselle rajalle huhtikuussa 2021 väittäen kyseessä olevan harjoituksen. Se kuitenkin aloitti strategisen hyökkäysoperaation valmistelun Ukrainaa vastaan kybertilassa viimeistään vuoden 2021 keväällä. Valmisteluun liittyvää tiedustelua ja vakoilua helpotti se, että venäläisillä oli ollut vuoteen 2014 asti melko vapaa pääsy Ukrainan teleliikenneverkkoon ja mahdollisesti sen jälkeenkin aina vuoteen 2022 asti.[342] Panostuksesta tiedustelun suorituskykyyn kertoo, että FSB:n Ukrainan tiedustelusta vastuussa olleen yksikön koko väitetysti nelinkertaistui 2019–2021.[343]

Venäjän tiedustelupalveluilla oli määrätty työnjako operaation tiedustelussa ja valmistelussa. FSB:n Gamaredon vakoili Ukrainan hallinnon dokumenttien jakelujärjestelmää[344] ja kohdisti tiedustelua yksilöityihin ukrainalaisviranomaisiin ja korkeimpaan valtionjohtoon ja tietoturvaluokiteltuun tietoon.[345] SVR:n Nobelium pyrki hankkimaan verkkourkintaoperaatiolla[346] tietoa Ukrainan ulko- ja puolustuspoliittisista asioista sekä Naton jäsenmaiden toiminnasta. GRU pyrki tunkeutumaan ainakin Ukrainan asevoimien verkkoihin ja myös valkovenäläinen Ghostwriter pyrki hankkimaan pääsyn Ukrainan asevoimien verkkoihin.[347] Kesällä Venäjän tiedustelupalvelut kohdistivat Ukrainaan kohdistuvan laajan verkkourkintakampanjan.[348] Microsoftin mukaan niin FSB, SVR kuin GRU tehostivat kybervakoilua tilanteen kiristyessä syksyllä 2021. Ne pyrkivät saavuttamaan pysyvän läsnäolon Ukrainan puolustuksen, puolustusteollisuuden, ulkohallinnon, valtion ja paikallishallinnon, poliisiviranomaisten ja humanitaaristen toimijoiden verkoissa.[349] Ukrainan lisäksi Venäjän tiedustelupalvelut kohdistivat jatkuvaa kybervakoilua mm. läntisiä hallituksia[350], avustusjärjestöjä, pilvipalveluita ja kyberturvallisuusyrityksiä vastaan hyödyntäen mm. Solarwinds-tietomurron tarjoamia mahdollisuuksia.[351] Microsoftin mukaan SVR:n Nobelium ryhmä pyrki hankkimaan pysyvän läsnäolon IT-palveluiden toimittajien järjestelmissä vakoillak-

[342] Bateman (2022); Mc Daid, Cathal: Cyberattacks & Data Breaches. Blogikirjoitus, 17.5.2022. [https://www.darkreading.com/attacks-breaches/how-mobile-networks-have-become-a-front-in-the-battle-for-ukraine], luettu 5.2.2024.
[343] Miller, Greg & Belton, Catherine: Russia's Spies Misread Ukraine and Misled Kremlin as War Loomed. *Washington Post*, 19.8.2022. [https://www.washingtonpost.com/world/interactive/2022/russia-fsb-intelligence-ukraine-war/], luettu 4.2.2024.
[344] Cimpanu, Catalin: Ukraine reports cyber-attack on government document management system. *ZDNet*, 24.2.2021. [https://www.zdnet.com/article/ukraine-reports-cyber-attack-on-government-document-management-system/], luettu 5.2.2024.
[345] Mele, Gage, Polozov, Yury & Gould, Tara: Primitive Bear (Gamaredon) Targets Ukraine with Timely Themes. Anomali Threat Research, 19.4.2021. [https://www.anomali.com/blog/primitive-bear-gamaredon-targets-ukraine-with-timely-themes], luettu 5.2.2024.
[346] Tiedonhankintatekniikka ja kyberhyökkäyksen tyyppi, jossa kohde pyritään huijaamaan luovuttamaan arkaluotoista tietoa. Voi hyödyntää teknisten menetelmien lisäksi sosiaalista manipulaatiota. Tunnetaan myös kalasteluna (phishing) (NIST: Glossary – Phishing. n.d. [https://csrc.nist.gov/glossary/term/phishing], luettu 5.2.2024.
[347] Microsoft: Special Report: Ukraine. An Overview of Russia's Cyberattack Activity in Ukraine. Microsoft, 27.4.2022 (a). [https://www.microsoft.com/cms/api/am/binary/RE4Vwwd], luettu 5.1.2024.
[348] Cimpanu, Catalin: Ukraine warns of 'massive' Russian spear-phishing campaign. The Record, 7.7.2021. [https://therecord.media/ukraine-warns-of-massive-russian-spear-phishing-campaign?web_view=true], luettu 4.2.2024.
[349] Microsoft (2022a).
[350] Ranskan hallinto ja sen liittolaiset (APT29), Saksan parlamenttia (GRU), Yhdysvaltojen ulkoministeriötä, puolalaiset poliitikot ja Slovakian hallitus. (Council on Foreign Relation (2024); CSIS (2024).
[351] Council on Foreign Relation (2024); Microsoft: New sophisticated email-based attack from NOBELIUM. Microsoft, 27.5.2021. [https://www.microsoft.com/en-us/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/], luettu 4.2.2024.

seen niiden asiakkaita.[352] GRU:n APT28 toteutti verkkourkintakampanjan 14000 Gmail-tiliä vastaan.[353] Verkkourkintakampanjat jatkuivat vuoden 2022 tammi-helmikuussa Venäjän sotilasoperaation alun lähestyessä.[354] Tiedustelutietojen keräämisellä pyrittiin todennäköisesti tukemaan sotilasoperaation toteuttamista eli Ukrainan hallinnon johdon horjuttamista, informaatiotilan hallintaa, hyökkäävien joukkojen tukea ja tuhoavien kyberhyökkäysten toteuttamista.[355] Valmisteluvaiheen operaatioita ovat voineet ohjata myös miehityshallinnon tarpeet. Vakoilulla pyrittiin selvittämään Venäjän käytettävissä olevat, sille myötämieliset, neutraalit ja haitalliset henkilöt.[356]

Vuoden 2021 kuluessa Venäjän suhteet Yhdysvaltoihin sekä Nato- ja EU-maihin kiristyivät entisestään. Venäjän valtiojohto julkaisi kirjoituksia, joissa kiistettiin itsenäisen Ukrainan valtion ja kansan olemassaolo. Kybervakoilun rinnalla Venäjän tiedustelupalvelut pyrkivät saamaan pysyvän jalansijan Ukrainan ja sen potentiaalisten liittolaisten valtionhallinnon ja kriittisen infrastruktuurin tietoverkoissa. Ukrainan sähköverkkoon ja ICT-yrityksiin kohdistuvia hyökkäyksiä valmisteltiin jo vuoden 2021 aikana.[357] HermeticWiper-haittaohjelman, jota käytettiin helmikuun 2022 hyökkäyksessä, koodi käännettiin 28.12.2021 ja IsaacWiper-haittaohjelman koodi 19.10.2021. Lisäksi hyökkääjät olivat erittäin todennäköisesti läsnä kohdeverkoissa ennen haittaohjelmien aktivointia. Samalla tavoin valmisteltiin helmikuussa käytetty CaddyWiper-haittaohjelma.[358] Tuntematon venäläistoimija pyrki saastuttamaan mm. Ukrainan turvallisuuspalvelun ja Kansallisen turvallisuuden ja puolustuksen komitean verkkopalvelimet viruksella, joka olisi tehnyt niistä osan palvelunestohyökkäyksissä käytettävää bottiverkkoa, jolloin teleoperaattorit olisivat hyökkäyksen havaitessaan estäneet tahattomasti näiden palvelinten toiminnan.[359] Sotatoimeen liittyvien kyberoperaatioiden valmistelu oli siis selvästi käynnissä loppuvuodesta 2021.

Venäjän operaatioita ulottuivat myös Ukrainan ulkopuolelle. Ranskan Kansallinen informaatiojärjestelmien turvallisuusvirasto (ANSSI) on ilmoittanut GRU:n APT28:n tunkeutuneen Ranskan kriittisiin tietoverkkoihin vuonna 2021.[360] Vuoden 2021 puoliväliin mennessä Venäjän valtioon sidoksissa olleet toimijat kohdistivat hyökkäyksiä Ukrainan ja Nato-maiden IT-palveluita tuottaviin yrityksiin todennäköisesti valmistel-

[352] Burt, Tom: New activity from Russian actor Nobelium. Microsoft, 24.10.2021. [https://blogs.microsoft.com/on-the-issues/2021/10/24/new-activity-from-russian-actor-nobelium/], luettu 5.2.2024.
[353] Cimpanu, Catalin: Google notifies 14,000 Gmail users of targeted APT28 attacks. *The Record*, 7.10.2021. [https://therecord.media/google-notifies-14000-gmail-users-of-targeted-apt28-attacks], luettu 5.2.2024.
[354] Google (2023); Schulze, Matthias & Kerttunen, Mika: Cyber Operations in Russia's War against Ukraine. SWP Comment, No 23, 2023. [https://www.swp-berlin.org/publications/products/comments/2023C23_CyberOperations_UkraineWar.pdf], luettu 5.1.2024.
[355] CISCO: Talos Year in Review. CISCO, 2023. [https://blog.talosintelligence.com/cisco-talos-2023-year-in-review/], luettu 5.1.2024.
[356] Willett, Marcus: The Cyber Dimension of the Russia–Ukraine War. *Survival*, 64(5) 2022, s. 7–26.
[357] The MOD of Lithuania: Regional Cyber Defence Centre: Report on Cyber Lessons Learned During the War in Ukraine. 2023, s. 20, s. 35. [https://www.nksc.lt/doc/rkgc/report_on_cyber_lessons_learned_during_the_war_in_ukraine.pdf], luettu 5.1.2024; SSSCIP: Russia's Cyber Tactics H1'2023. SSSCIP, 13.10.2023. [https://cip.gov.ua/services/cm/api/attachment/download?id=60068], luettu 5.1.2024; Microsoft (2022a).
[358] ESET: Threat Report T1 2022. ESET, 2.6.2022 (a). [https://www.welivesecurity.com/2022/06/02/eset-threat-report-t12022/], luettu 5.1.2024.
[359] Reuters: Ukraine accuses Russian networks of new massive cyber-attacks. *Reuters*, 22.2.2021. [https://www.reuters.com/article/us-ukraine-cyber/ukraine-accuses-russian-networks-of-new-massive-cyber-attacks-idUSKBN2AM1VF], luettu 4.2.2024.
[360] Toulas, Bill: France says Russian state hackers breached numerous critical networks. *Bleeping Computer*, 26.10.2023. [https://www.bleepingcomputer.com/news/security/france-says-russian-state-hackers-breached-numerous-critical-networks/], luettu 4.2.2024.

lakseen tuotantoketjuhyökkäystä.[361] Venäjä toteutti länsimaita vastaan aktiivisempiakin operaatioita. Venäläiset hakkerit pysäyttivät yhdysvaltalaisen Colonial Pipelines -polttoainetoimittajan putkiverkoston toiminnan DarkSide-kiristyshaittaohjelmalla[362] ja Irlannin kansallinen terveyspalvelu joutui venäläisen Conti-rikollisjärjestön kiristyshaittaohjelmahyökkäyksen uhriksi ja oli pakotettu sulkemaan kaikki IT järjestelmänsä.[363] Venäjän operaatioilla oli vahva yhteys informaatiovaikuttamiseen. Kesäkuussa kahden brittiläisen aluksen sijaintidata (AIS) väärennettiin niin, että ne näyttivät olevan Sevastopolin edustalla, joita Venäjä piti aluevesinään.[364] Heinäkuussa Venäjän valtiolliset hakkerit julkaisivat Ukrainan laivaston sivuilla väärennettyjä uutisia liittyen Sea Breeze harjoitukseen.[365] Syyskuussa 2021 EU syytti virallisesti Venäjää GhostWriterin – tosin mahdollisesti kyseessä oli valkovenäläinen UNC1151[366] uhkatoimija – kampanjasta, joka pyrki vaikuttamaan vaaleihin EU:n alueella ja rapauttamaan Naton sisäistä luottamusta levittämällä disinformaatiota vuosina 2017–2021.[367] Venäjä siis jatkoi informaatiokamppailua Länttä vastaan valmistellessaan Ukrainan hyökkäysoperaatiota. On mahdollista, että operaatioilla pyrittiin ylläpitämään määrättyä kohinatasoa ja harhauttamaan tiedustelupalveluita Venäjän todellisten aikeiden suhteen.

Joulukuussa 2021 Venäjä vaati Yhdysvalloilta ja Nato-mailta Naton sotilaallisen läsnäolon pois vetämistä Venäjän lähialueilta ja sitovaa sopimusta Naton laajentumisen lopettamisesta – käytännössä sopimusta uudesta, etupiireihin perustuvasta eurooppalaisesta turvallisuusrakenteesta. Neuvottelujen jatkuessa Venäjä ryhmitti Ukrainan rajalle uudelleen n. 130 000 sotilasta. Neuvottelukierros osapuolten välillä ei tuottanut tuloksia 14.1.2022 mennessä ja Yhdysvallat ja Nato hylkäsivät Venäjän vaatimukset virallisesti 26.1. Venäjän väitti vetävänsä joukkonsa pois Ukrainan rajoilta 16.2., mutta tunnusti Luhanskin ja Donetskin separatistialueiden itsenäisyyden 21.2. ja aloitti strategisen hyökkäysoperaation 24.2. aamuyöllä. Venäjän lopullisen hyökkäyspäätöksen tekohetkestä ei ole varmaa tietoa. Presidentti Putin teki sen mahdollisesti vasta helmikuun alussa.[368]

---

[361] Microsoft (2022a). Tuotantoketjuhyökkäys perustuu ohjelmistoon, järjestelmään tai palveluun tunkeutumiseen ennen kuin se asennetaan kohdetoimijan järjestelmiin (NIST: Glossary – Supply chain attack. n.d. [https://csrc.nist.gov/glossary/term/supply_chain_attack], luettu 5.2.2024.

[362] Woodruff, Swan, Betsy: Russia suspected of stealing thousands of State Department emails. *Politico*, 30.3.2021. [https://www.politico.com/news/2021/03/30/russia-suspected-emails-478541], luettu 5.2.2024. Kiristyshaittaohjelma kryptaa kohdejärjestelmän datan, jotta hyökkääjä voi vaatia lunnaita datan palauttamisesta. (NIST: Ransomware. n.d. [https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware], luettu 5.2.2024.

[363] Halpin, Padraic & Humphries, Conor: Irish health service hit by 'very sophisticated' ransomware attack. *Reuters*, 14.5.2021. [https://www.reuters.com/technology/irish-health-service-hit-by-ransomware-attack-vaccine-rollout-unaffected-2021-05-14/], luettu 5.2.2024.

[364] Sutton, H. I.: Positions of Two NATO Ships Were Falsified Near Russian Black Sea Naval Base. *USNI News*, 21.6.2021. [https://news.usni.org/2021/06/21/positions-of-two-nato-ships-were-falsified-near-russian-black-sea-naval-base], luettu 5.4.2024.

[365] RFE/RL: Ukraine Blames Russian Hackers For Attack On Navy Website. *RFE/RL*, 9.7.2021. [https://www.rferl.org/a/ukraine-hack-russia-navy-sea-breeze/31351045.html], luettu 5.4.2024.

[366] Cardiff University: The Ghostwriter Campaign. Cardiff University, 2023. [https://www.cardiff.ac.uk/__data/assets/pdf_file/0005/2699483/Ghostwriter-Report-Final.pdf], luettu 5.2.2024.

[367] Cimpanu, Catalin: EU formally blames Russia for GhostWriter influence operation. *The Record*, 24.9.2024. [https://therecord.media/eu-formally-blames-russia-for-ghostwriter-hack-and-influence-operation], luettu 5.2.2024.

[368] Risen, James: U.S. Intelligence Says Putin Made a Last-Minute Decision to Invade Ukraine. *The Intercept*, 11.3.3022. [https://theintercept.com/2022/03/11/russia-putin-ukraine-invasion-us-intelligence/], luettu 5.2.2024; Seddon, Max, Miller, Christopher & Schwartz, Felicia: How Putin blundered into Ukraine — then

Hyökkäystä edelsi joukko hyökkäyksellisiä kyberoperaatioita. 14.1.2022 seitsemänkymmentä Ukrainan valtionhallinnon verkkosivua sotkettiin ml. valtioneuvoston, puolustusministeriön, ulkoministeriön ja koulutus- ja tiedeministeriön verkkosivut ja niihin kohdistui palvelunestohyökkäyksiä. Hyökkäys ei ollut erityisen laajan tai hienostunut ja tekijäksi epäiltiin valkovenäläistä Ghostwriteria eli UNC1151-uhkatoimijaa.[369] Hyökkäyksiä käytettiin mahdollisesti haittaohjelman levittämisen peittämiseksi, sillä WhisperGate wiper-haittaohjelma[370] löydettiin samoista järjestelmistä kuin mihin palvelunestohyökkäys oli kohdistunut. Hyökkäys attribuoitiin myöhemmin GRU:n CadetBlizzard-operaatioksi ja Cisco Talos-kyberuhkatiedusteluryhmä on korostanut raportissaan hyökkääjän pyrkimystä käyttää disinformaatiota ja lavastusta attribuution hämärtämiseksi.[371] Viikko hyökkäyksen jälkeen 21.1. vuodettiin yli kahden miljoonan ukrainalaisen henkilötiedot internettiin.[372] Tammikuun puolivälissä toteutettiin myös hyökkäys ukrainalaista kaasuyhtiötä vastaan[373] ja helmikuun puolivälissä GRU teki kiristyshaittaohjelmahyökkäyksen yhdysvaltalaisia LNG-yrityksiä vastaan.[374] Tammikuun kyberhyökkäysoperaatiot liittyivät todennäköisesti käynnissä olleisiin neuvotteluihin sekä hyökkäysvalmisteluihin. Hyökkäykset kaasuyhtiöitä vastaan olivat osa taloudellista painostusta Ukrainaa ja sen potentiaalisia liittolaisia kohtaan. Tavoitteena oli joko pyrkimys poliittisstrategisten tavoitteiden saavuttamiseen ilman suoran aseellisen voiman käyttöä tai pyrkimys uskotella, että Venäjä pyrkisi edelleen tavoitteisiin ilman sotilaallisen voiman käyttöä eli harhautus, tai sitten molemmat.

Helmikuun puolivälissä Venäjä toteutti toisen kyberhyökkäysten sarjan. GRU teki laajan viisi tuntia kestäneen palvelunestohyökkäyksen Ukrainan hallintoa, turvallisuuspalveluita, asevoimia ja pankkeja vastaan[375] ja lisäksi Ukrainan itäosien mobiiliverkois-

---

doubled down. *Financial Times*, 23.2.2023. [https://www.ft.com/content/80002564-33e8-48fb-b734-44810afb7a49], luettu 5.2.2024.

[369] National Security Archive: Cyber Vault Ukraine Timeline. 30.5.2023. [https://nsarchive.gwu.edu/document/29562-cyber-vault-ukraine-timeline], luettu 5.2.2024; Beek, Christiaan, Kersten, Max & Samani, Raj: Return of Pseudo Ransomware. *Trellix*, 20.1.2022. [https://www.trellix.com/en-us/about/newsroom/stories/threat-labs/return-of-pseudo-ransomware.html], luettu 5.2.2024; Microsoft: Destructive Malware Targeting Ukrainian Organizations. Microsoft Threat Intelligence Center, 15.1.2022. [https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/], luettu 5.2.2024.

[370] Haittaohjelma, joka pyrkii hävittämään kohdejärjestelmässä olevan data pysyvästi (Iacob, Ioan & Ionit, Iulian Madalin: The Anatomy of Wiper Malware, Part 1: Common Techniques. CrowdStrike, 12.8.2022. [https://www.crowdstrike.com/blog/the-anatomy-of-wiper-malware-part-1/], luettu 5.2.2024.

[371] McLaughlin: More than 70 Ukrainian government websites have been defaced in cyberattacks. *NPR*, 19.1.2024. [https://www.npr.org/2022/01/19/1074172805/more-than-70-ukrainian-government-websites-have-been-defaced-in-cyber-attacks], luettu 5.2.2024; Microsoft Digital Security Unit: Destructive malware targeting Ukrainian organizations. Microsoft, 15.1.2022. [https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/], luettu 5.2.2024; CISCO (2023); CERT-EU (2023a); CISCO Talos: Ukraine Campaign Delivers Defacement and Wipers, in Continued Escalation. Cisco, 21.1.2022. [https://blog.talosintelligence.com/ukraine-campaign-delivers-defacement/].

[372] CERT-EU (2023a).

[373] Nykonorov, Oleg: Facebook teksti, 14.1.2022. [https://www.facebook.com/photo/?fbid=669565037387751&set=a.215320962812163], luettu 4.2.2024.

[374] Robertson, Jordan & Chapa, Sergio: Hackers Targeted U.S. LNG Producers in Run-Up to Ukraine War. *Bloomberg*, 7.3.2022. [https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine], luettu 5.2.2024.

[375] The White House: Press Briefing by Press Secretary Jen Psaki, Deputy National Security Advisor for Cyber and Emerging Technology Anne Neuberger, and Deputy National Security Advisor for International Economics and Deputy NEC Director Daleep Singh. The White House, 18.2.2022. [https://www.whitehouse.gov/briefing-room/press-briefings/2022/02/18/press-briefing-by-press-secretary-jen-psaki-d eputy-national-security-advisor-for-cyber-and-emerging-technology-anne-neuberger-and-deputy-national-security-a dvisor-for-international-economics-and-dep/], luettu 5.2.2024; The Economic Security Council of Ukraine: Cyber, Artillery, Propaganda. Comprehensive Analysis of Russian Warfare Dimensions.

sa oli häiriöitä 17.–18.2.[376] Venäjä pyrki todennäköisesti tunkeutumaan Ukrainan paikallishallinnon verkkoihin ja kriittisiin järjestelmiin mm. Sumyssä ja Odessassa.[377] Sekä tammi- että helmikuun hyökkäykset eivät olleet määrältään ja laadultaan sellaisia, että olisi syytä olettaa Venäjän pyrkineen korvaamaan niillä maahyökkäystä, enintään tukemaan maksimaalisia neuvottelutavoitteita. Helmikuun hyökkäys voidaan tulkita kuitenkin jo selvästi pelotteluksi ja painostamiseksi. Sillä mahdollisesti pyrittiin myös provosoimaan Ukrainaa ja hankkimaan perusteluja hyökkäysoperaation oikeuttamiseksi.[378] Venäjä kielsi sillä olevan mitään tekemistä kyberhyökkäysten kanssa.[379]

Lännessä Venäjän kyberhyökkäykset otettiin vakavasti.[380] Osa läntisestä kybertutkijoiden yhteisöstä ennusti Venäjän lamauttavan Ukrainan sähkö- ja tietoliikenneverkot ja iskevän lisäksi myös Lännen finanssi- ja öljyteollisuuden kohteisiin.[381] USA:n Kyberturvallisuusvirasto CISA julkaisi useita varoituksia liittyen Venäjän valtiosidonnaisten kybertoimijoiden operaatioihin tammi-helmikuussa 2022 ja hyökkäyksen alettua maaliskuussa.[382] Yhdysvallat ja Nato olivat käytännössä jo asettaneet tai asettivat heti sodan alettua omat ”punaiset viivansa” kyberhyökkäysten suhteen.[383] U.S. Cyber Command nosti valmiutta 11.2.[384] Ajan ilmapiiriä kuvaa, että 7.1.2022 tapahtuneesta Norjan Huippuvuorten datakaapelin katkeamisesta syytettiin mediassa Venäjää, vaikka inhimillisen tekijän vaikutusta ei ole kyetty osoittamaan.[385]

Aikaisemmista sotakokemuksista oppineena Venäjä pyrki ennen sotatoimien alkua tuottamaan oikeutuksen hyökkäykselleen informaatio-operaatioilla, joissa käytettiin hyväksi mm. Telegrammia ja Twitteriä. Tavoitteena oli informaatioylivoiman saavuttaminen jo ennen hyökkäyksen aloittamista. Yhdysvallat ja kansainvälinen OSINT-yhteisö pystyivät kuitenkin paljastamaan nämä yritykset riittävän nopeasti.[386] Microsoftin mukaan Venäjä käytti ns. Advanced Persistent Manipulator ryhmiä disinformaation levittämiseen. Ne levittivät valheellisia narratiiveja viestintäalustoilla esim. Yhdysvaltojen biolaboratorioista Ukrainassa. Valeuutiset levitettiin etukäteen yksittäisille verkkouutisalustoille, joista ne nostettiin laajemmin viestintäkanaville hyökkäyk-

---

The Economic Security Council of Ukraine, October 2022. [https://nsarchive.gwu.edu/document/30063-18-cyber-artillery-propaganda-comprehensive-analysis-russian-warfare-dimensions], luettu 5.1.2024; McLaughlin, Jenna: Ukraine Says Government Websites and Banks Were Hit with Denial of Service Attack. *NPR*, 15.2.2022. [https://www.npr.org/2022/02/15/1080876311/ukraine-hack-denial-of-service-attack-defense], luettu 5.2.2024.

[376] National Security Archive Cyber Vault: A Chronology of The Cyber Aspects of The War in Ukraine, 30.3.2023. [https://nsarchive.gwu.edu/document/29562-cyber-vault-ukraine-timeline], luettu 5.2.2024.

[377] Microsoft (2022a).

[378] Schulze & Kerttunen (2023).

[379] Sabbagh, Dan: Ukraine accuses Russia of cyber-attack on two banks and its defence ministry. *The Guardian*, 16.2.2022. [https://www.theguardian.com/world/2022/feb/16/ukraine-accuses-russia-of-cyber-attack-on-two-banks-and-its-defence-ministry], luettu 5.2.2024.

[380] Rundle, James: Russian Cyber Threat Remains High, U.S. Officials Say. *Wall Street Journal*, 7.6.2022. [https://www.wsj.com/articles/russian-cyber-threat-remains-high-us-officials-say-11654647242], luettu 5.2.2024.

[381] Kerr (2023), s. 10–11.

[382] CISA: Russia Cyber Threat Overview and Advisories. n.d. [https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia], luettu 5.2.2024.

[383] Willett (2022).

[384] National Security Archive (2023).

[385] Schia, Niels Nagelhus: The subsea cable cut at Svalbard January 2022: What happened, what were the consequences, and how were they managed? NUPI, 2.1.2023. [https://www.nupi.no/en/publications/cristin-pub/the-subsea-cable-cut-at-svalbard-january-2022-what-happened-what-were-the-consequences-and-how-were-they-managed], luettu 5.2.2024.

[386] Schulze & Kerttunen (2023).

sen alettua.[387] Informaatiovaikuttamista tukevilla kyberoperaatiolla nähtiin todennäköisesti olevan potentiaalista vaikutusta, koska Venäjän johto uskoi Ukrainan yhtenäisyyden olevan jo valmiiksi heikko.[388] Hyökkäyksissä käytettiin apuna kyberrikollisia. Esimerkiksi Zhadnost (ahneus) -bottiverkkoa, joka on todennäköisesti kyberrikollisten operoima, käytettiin Ukrainan valtionhallintoon ja finanssialaan kohdistuviin palvelunestohyökkäyksiin 15., 23. ja 28.2.[389] Palvelunestohyökkäysten lisäksi bottiverkkoja on käytetty laajasti konfliktia edeltäneestä ajasta lähtien sosiaalisen median alustoilla molempien osapuolten informaatio-operaatioiden tukena.[390]

Tammi-helmikuussa 2022 Venäjän näkyvässä kybertoiminnassa oli painostuksen, deterrenssiviestinnän ja harhautuksen piirteitä. Sillä myös pyrittiin tukemaan hyökkäystä edeltävän informaatioylivoiman hankkimista. Mielenkiintoinen lisä oli Venäjän ”kiristyshaittaohjelmadiplomatia.”[391] FSB pidätti Yhdysvaltojen pyynnöstä neljätoista kiristyshaittaohjelmiin erikoistuneen REvil kyberrikollisryhmän jäsentä 14.1. ikään kuin osoittaakseen olevansa valmis yhteistyöhön. Samana päivänä Ukrainaan tosin kohdistui laaja kyberhyökkäys ja jälkikäteen katsottuna REvilin jäsenten pidätys saattoi olla harhautus. Venäjä on käyttänyt kyberalan oikeusjuttuja ulkoisen viestinnän lisäksi sisäpiiriuhkien poistamiseen ja viestin välittämiseen venäläiselle alamaailmalle. Vuonna 2019 FSB:n kyberturvallisuusyksikön entinen johtaja ja tietoturvayhtiö Kasperskyn työntekijä tuomittiin maanpetoksesta syytettynä.[392] Syyskuussa 2021 pidätettiin merkittävän kyberturvallisuusyritys Group-IB:n perustaja Ilja Satškov ja hänet tuomittiin maanpetoksesta vuonna 2023.[393] Sekä FSB:n että Group-IB:n tapauksessa oli virallisesti kyse tietojen luovuttamisesta Yhdysvalloille. Epävirallisesti Venäjän kyberturvallisuusalan ammattilaisille ja kyberrikollisille tehtiin selväksi, että heitä valvottiin.

[387] Smith, Brad: Defending Ukraine: Early Lessons from the Cyber War. Microsoft, 22.6.2022. [https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/], luettu 4.2.2024; Microsoft: Defending Ukraine: Early Lessons from the Cyber War. Microsoft, 22.6.2022 (b). [https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/], luettu 5.1.2024.
[388] Mankoff, Jeffrey: Russia's War in Ukraine. Identity, History, and Conflict. CSIS, April 2022. [https://www.csis.org/analysis/russias-war-ukraine-identity-history-and-conflict], luettu 5.2.2024.
[389] Slaney, Ryan: SecurityScorecard discovers new botnet, 'Zhadnost,' responsible for Ukraine DDoS attacks. SecurityScoreCard, 3.10.2022. [https://securityscorecard.com/blog/securityscorecard-discovers-new-botnet-zhadnost-responsible-for-ukraine-ddos-attacks/], luettu 5.2.2024.
[390] Shen, Fei, Zhang, Erkun, Ren, Wujiong, He, Yuan, Jia, Quanxin & Zhang, Hongzhong: Examining the differences between human and bot social media accounts: A case study of the Russia-Ukraine War. *First Monday*, Volume 28, Number 2 (2023). [doi: https://dx.doi.org/10.5210/fm.v28i2.1277].
[391] Krebs: At Request of U.S., Russia Rounds Up 14 REvil Ransomware Affiliates. Krebs on Security, 14.1.2022. [https://krebsonsecurity.com/2022/01/at-request-of-u-s-russia-rounds-up-14-revil-ransomware-affiliates/], luettu 5.2.2024.
[392] Eckel, Mike: In Moscow Treason Trial, A Major Scandal For Russian Security Agency. *RFE/RL*, 27.2.2019. [https://www.rferl.org/a/russia-hacker-mikhailov-stoyanov-fsb-scandal-for-russian-security-agency/29794092.html], luettu 5.2.2024.
[393] Antoniuk, Daryna: Russia jails Group-IB co-founder for 14 years in treason case. The Record, 26.7.2023. [https://therecord.media/ilya-sachkov-group-ib-prison-sentence-treason-case-russia], luettu 4.2.2024.

5.2. Hyökkäyksen alkuvaihe: Helmikuun loppu 2022

Venäjä aloitti sotilaallisen erikoisoperaation Ukrainaan 24.2. yöllä ohjusiskuilla, ilmarynnäköllä Hostomeliin ja erikoisjoukkojen ja maavoimien yhtymien hyökkäyksellä. Kybertilassa hyökkäys alkoi jo vuorokautta aikaisemmin ja Venäjän valtiosidonnaisilla kybertoimijoilla oli päärooli informaatioiskuoperaation toteuttamisessa.[394] 23.2. havaittiin ”tärkeisiin verkkosivustoihin” kohdistuneen palvelunestohyökkäyksen jälkeen tietojärjestelmiä lamauttava ja tuhoava[395] HermeticWiper/FoxBlade-haittaohjelma, jota Sandworm käytti 19 valtionhallinnon ja kriittisen infrastruktuurin kohdetta vastaan.[396] Microsoftin mukaan kohdejärjestelmiä oli hallinnon, IT:n, energian, maatalouden ja finanssisektorin alalla kolmesataa.[397] HermeticWiperin rinnalla käytettiin HermeticWizard-haittaohjelmaperhettä, johon kuului levitysohjelma eli mato[398] ja valekiristysohjelma (HermeticRansom).[399] 24.2. havaittiin IsaacWiper-haittaohjelma, jota käytettiin eri verkkoja vastaan kuin HermeticWiperia ja josta se poikkesi koodiltaan, vaikkakin myös se pyrki datan hävittämiseen kohdejärjestelmistä.[400] Microsoft on nimennyt yhdeksi kohteista maatalousalan firman, jonka verkkodata tuhoamalla pyrittiin vaikuttamaan Ukrainan talouteen.[401]

Hyökkäyksen ensipäivien näkyvin operaatio oli Venäjän valtioon sidoksissa olleen toimijan toteuttama kyberhyökkäys noin tuntia ennen maahyökkäystä kansainvälisen satelliittiviestipalveluntarjoaja Viasatin KA-SAT modeemeihin. Hyökkäys vaikutti myös 5800 tuulivoimalaan Saksassa. Hyökkäys toteutettiin Acidrain-haittaohjelmalla ja tavoitteena oli Ukrainan asevoimien yhteyksien häirintä. Tiedot vaikutuksista ovat jääneet ristiriitaisiksi.[402] Ukrainan asevoimat käytti Viasatin palveluja vähintään varayhteytenä, joille hyökkäyksen ensimmäisinä päivinä oli varmasti tarvetta Venäjän elektronisen sodankäynnin ja kineettisen vaikuttamisen lamauttaessa johtamisjärjestelmiä.[403] Viasatin lisäksi internetpalveluntarjoaja Triolan järjestelmiin tunkeuduttiin ja sen tarjoamat yhteydet kärsivät häiriöistä vähintään kahden vuorokauden ajan.[404]

---

[394] U.S. Department of Health and Human Services: Major Cyber Organizations of the Russian Intelligence Services. N.d. [https://www.hhs.gov/sites/default/files/major-cyber-organizations-of-russian-intelligence-services.pdf], luettu 5.2.2024; Microsoft (2022a).

[395] Tuhoavalla haittaohjelmalla tarkoitetaan tässä luvussa tietoja tuhoavaa, tietojärjestelmiä toimintakyvyttömäksi tekevää tai toimintahäiriön kautta fyysistä tuhoa aiheuttavaa ohjelmaa. Englanninkielisissä lähteissä esiintyvät käsitteet disruptive tai destructive.

[396] Microsoft (2022b); ESET (2022a).

[397] Microsoft (2022a).

[398] Itsenäinen haittaohjelma, joka voi levittää itsestään kopioita tietoverkon välityksellä (NIST: Glossary – Worm. n.d. [https://csrc.nist.gov/glossary/term/worm], luettu 5.4.2024.

[399] ESET (2022a).

[400] Ibid.

[401] Microsoft (2022a).

[402] O'Neill, Patrick Howell: Russia hacked an American satellite company one hour before the Ukraine invasion. MIT Technology Review, 10.5.2022. [https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/], luettu 5.2.2024; Greig, Jonathan: NSA, Viasat say 2022 hack was two incidents; Russian sanctions resulted from investigation. *The Record*, 11.8.2023. [https://therecord.media/viasat-hack-was-two-incidents-and-resulted-in-sanctions], luettu 5.2.2024; Zetter, Kim: Viasat Hack 'Did Not' Have Huge Impact on Ukrainian Military Communications, Official Says. Substack newsletter, Zero Day (blog),26.9.2022. [https://zetter.substack.com/p/viasat-hack-did-not-have-huge-impact], luettu 5.2.2024; Satter, Raphael: Satellite outage caused 'huge loss in communications' at war's outset -Ukrainian official. *Reuters*, 15.3.2022. [https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/], luettu 5.2.2024; Schulze & Kerttunen (2023).

[403] Bateman (2022).

[404] Thomas Brewster: As Russia Invaded, Hackers Broke into a Ukrainian Internet Provider. Then Did It Again as Bombs Rained Down. *Forbes*, 10.3.2022. [https://www.forbes.com/sites/thomasbrewster/2022/03/10/cyberattack-on-major-ukraine-internet-provider-causes-major-outages/], luettu 5.1.2024;

Kyberhyökkäykset kohdistuivat myös sähköyhtiö Ukrenergoa vastaan, joka oli juuri testimielessä aloittanut Ukrainan verkon yhdistämisen eurooppalaiseen – ja samalla irrottautumisen venäläisestä verkosta.[405] Tilanne oli Ukrainan sähköhuollolle äärimmäisen vaarallinen, mutta maa onnistui 16.3. mennessä synkronoitumaan eurooppalaisen verkon kanssa.[406]

Tuhoavia hyökkäyksiä toteutettiin Microsoftin mukaan hyökkäyksen ensimmäisen viikon aikana kahtakymmentäkahta organisaatiota vastaan.[407] Hyökkäysten ensimmäisten päivien aikana Ukrainan internetyhteyksissä esiintyi merkittäviä, alueellisia häiriöitä.[408] GPS -yhteyksiä alettiin häiritä välittömästi operaation alettua ja tällä oli todennäköisesti vaikutusta moniin kriittisen infrastruktuurin kohteeseen.[409] Eräiden lausuntojen mukaan ainakin Kiovan suunnalla asevoimien johtamisjärjestelmät oli lamautettu.[410] Venäjän kyvystä vaikuttaa kybermenetelmin suoraan Ukrainan asevoimien asejärjestelmiin kuten ilmatorjunnan järjestelmiin sodan alkuvaiheessa ei ole havaintoja.

Microsoftin mukaan helmi-huhtikuussa Venäjän kyber- ja kineettisiä hyökkäyksiä koordinoitiin mm. Lvivissä, Vinnytsjassa, Kiovassa, Odessassa, Zaporižžjassa ja Dniprossa.[411] Kyber- ja kineettisten hyökkäysten painopiste oli Kiovan ja Itä-Ukrainan alueella. Ilmeisemmin Venäjä iski vähintään yhteen palvelinkeskukseen ohjuksilla.[412] Hyökkäysten välillä ei kuitenkaan ole selvää yhteyttä ja ne ovat luonteensa vuoksi voineet olla usean eri toimijan mielenkiinnon kohteena. Johtavat kyberasiantuntijat ovat arvostelleet Microsoftin raporttia epätarkaksi.[413] Microsoft onkin todennut kyberhyökkäysten tavoitteiden olleen pikemminkin poliittisella, taloudellisella ja sotilasstrategisella tasolla kuin asevoimien suorassa tukemisessa.[414] Kyberhyökkäysten vaikutuksia Ukrainan kriittiseen infrastruktuuriin on vaikea erotella ohjusiskuista. Niin tai näin, Venäjän tuhoavat kyberhyökkäykset eivät yksin tai yhdessä kineettisen vaikuttamisen kanssa tuottaneet strategisia vaikutuksia eli lamauttaneet Ukrainan valtiojohtoa, yhteiskuntaa tai asevoimia.

Ukrainaan kohdistuneet informaatiovaikuttamisen tukemisoperaatiot, jatkuvat palvelunestohyökkäykset ja verkkosivujen sotkemiset alkoivat välittömästi hyökkäysope-

---

NetBlocks: Twitter teksti, 23.2.2022. [https://twitter.com/netblocks/status/1496708402755559424], luettu 5.2.2024.

[405] The Economic Security Council of Ukraine (2022).

[406] Blaustein, Anna: How Ukraine Unplugged from Russia and Joined Europe's Power Grid with Unprecedented Speed. Scientific American, 23.3.2022. [https://www.scientificamerican.com/article/how-ukraine-unplugged-from-russia-and-joined-europes-power-grid-with-unprecedented-speed/], luettu 5.2.2024.

[407] Microsoft (2022a).

[408] Netblocks: Internet disruptions registered as Russia moves in on Ukraine. 24.2.2022. [https://netblocks.org/reports/internet-disruptions-registered-as-russia-moves-in-on-ukraine-W80p4k8K], luettu 5.2.2024.

[409] Harper, Jon: Space Force chief concerned about 'backdoor' for attacking satellite communications. Defensescoop, 31.1.2023. [https://defensescoop.com/2023/01/31/space-force-chief-concerned-about-backdoor-for-attacking-satellite-communications/], luettu 5.2.2024.

[410] Sonne, Paul, Khurshudyan, Isabelle, Morgunov, Serhiy & Khudov, Kostiantyn: Ukrainian Valor, Russian Blunders Combined to Save the Capital. *Washington Post*, 24.8.2022. [https://www.washingtonpost.com/national-security/interactive/2022/kyiv-battle-ukraine-survival/], luettu 5.2.2024.

[411] Microsoft (2022b).

[412] Giles, Keir: Russian cyber and information warfare in practice. Chatham House, 14.12.2023. [https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice/03-distinctive-features-war], luettu 5.2.2024.

[413] Smalley, Suzanne: Cybersecurity experts question Microsoft's Ukraine report. *Cyberscoop*, 1.7.2022. [https://cyberscoop.com/cybersecurity-experts-question-microsofts-ukraine-report/], luettu 5.2.2024.

[414] Microsoft (2022a).

raation alettua. Samaan aikaa alkoivat myös kyberhyökkäykset EU-maita kohtaan.[415] GRU:n ohjailema Killnet ryhmä aktivoitui helmikuussa 2022. Sen päätoimintamalli ovat olleet palvelunestohyökkäykset Ukrainaa ja sen liittolaisten julkista ja yksityistä sektoria vastaan. Kohdemaita ovat olleet muun muassa Yhdysvallat, Puola, Norja, Liettua, Italia, Romania, Viro ja Japani. Kohteet ovat yleensä olleet valtionhallinnon verkkosivuja ja menetelmät yksinkertaisia ja lähinnä tilapäistä häiriötä aiheuttavia.[416] Mandiant tietoturvayhtiön mukaan GRU ohjasi myös XakNet ryhmän toimintaa. Perusteluna yhteydelle on esitetty, että XakNet vuosi dataa GRU:n APT28:n wiper-haittaohjelmahyökkäysten kohdejärjestelmistä vuorokauden sisällä hyökkäysten tapahtumisesta osana informaatiovaikutuskampanjaa syksyllä 2022.[417]

Operaation alusta alkaen Venäjän tukena toimivat valkovenäläiset valtiosidonnaiset hakkerit ja haktivistit. Nämä olivat pääasiassa vastuussa palvelunestohyökkäyksistä.[418] Valkovenäläinen Ghostwriter aka Pushcha (UNC1151) suoritti verkkourkintaoperaation Ukrainan asevoimien työntekijöiden henkilökohtaisia tilejä vastaan. Tekstiviestikampanjalla peloteltiin sotilaita ja siviilejä. Ukrainan asevoimien johdon Facebook-tilejä kaapattiin. Bottiverkot käännettiin rokotevastaisesta propagandasta ukrainavastaiseen.[419] Venäjän operaation alku aiheutti myös sekaannusta ei-valtiollisten toimijoiden joukossa. Venäläinen Conti- kiristyshaittaohjelmaryhmä hajosi sisäisiin ristiriitoihin ja ryhmän sisäistä viestintää vuodettiin julkisuuteen.[420] Killnetin ja XakNetin kaltaisten ryhmien nopea järjestyminen ja aktivoituminen osoittaa, että operaatiota oli suunniteltu jo jonkin aikaa.

Ukraina ei jäänyt Venäjän kyberhyökkäysten edessä toimettomaksi. IT Army of Ukraine patrioottinen, valtiojohtoinen haktivistiryhmä perustettiin 26.2. Lisäksi sotaan osallistui vuoden 2023 alkuun mennessä ainakin kolmekymmentäkolme ukrainamielistä haktivistiryhmää. Näiden ryhmien toiminta on perustunut Venäjää vastaan tehtyihin palvelunestohyökkäyksiin, tietovuotoihin mm. DDoSecrets alustan kautta ja verkkosivujen sekä TV- ja radiolähetysten sotkemiseen.[421] Ukrainamieliset hakkerit ovat myös väittäneet toteuttaneensa Venäjän kriittiseen infrastruktuuriin kohdistuvia hyökkäyksiä ja tuhoavia kyberhyökkäyksiä, mutta todistusaineisto on puutteellista. Esimerkiksi Team OneFist on väittänyt hyökänneensä Venäjän runkoverkon reitittimiä vastaan, sähköverkon SCDA/ICS järjestelmiä vastaan ja Yamal viestisatelliittiverkkoa vastaan, mutta ei ole tarjonnut pitäviä todisteita operaatioistaan.[422] Ukrainan asevoimien kyberjoukot eivät ole virallisesti tai julkisesti toteuttaneet hyökkäyksellisiä

[415] CERT-EU (2023a).
[416] CISCO (2023); CERT-EU (2023a); Mandiant: Hacktivists Collaborate with GRU-sponsored APT28. Mandiant, 23.9.2023. [https://www.mandiant.com/resources/blog/gru-rise-telegram-minions], luettu 5.2.2024.
[417] Google (2023).
[418] Google (2023).
[419] Geers, Kenneth: Computer Hacks in the Russia-Ukraine War. Conference paper, DEFCON 30, 11.8.2022. [https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Kenneth%20Geers%20-%20Computer%20Hacks%20in%20the%20Russia-Ukraine%20War%20-%20paper.pdf], luettu 5.2.2024; National Security Archive Cyber Vault (2023); Google (2023).
[420] Burgess, Matt: The Workaday Life of the World's Most Dangerous Ransomware Gang. *WIRED*, 16.3.2022. [https://www.wired.co.uk/article/conti-leaks-ransomware-work-life], luettu 5.2.2024.
[421] CERT-EU (2023a); Soesanto, Stefan: The IT Army of Ukraine Structure, Tasking, and Ecosystem. CSS ETH Zürich, June 2022. [https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf], luettu 4.2.2024.
[422] CERT-EU (2023a); Béres, Katalin: Pro-Ukrainian hackers hacked more than 1 000 routers across Russia - "Operation Turn Ruzzia Off." CyberThreat.Report, 17.1.2023. [https://www.cyberthreat.report/pro-ukrainian-hackers-hacked-more-than-1-000-routers-across-russia-operation-turn-ruzzia-off/], luettu 5.2.2024.

kyberoperaatioita Venäjää vastaan, vaan operaatiot on toimeenpantu patrioottisten hakkereiden kautta.

Haktivistien tukemisen lisäksi Ukrainan valtio ryhtyi puolustuksellisiin toimiin. Ukrainassa oli jo ennen hyökkäystä säädetty laki valtion hallinnon ja yksityisen sektorin tietojen siirtämisestä pilvipalveluihin, joka tosin tuli voimaan vasta syksyllä 2022.[423] Sen lisäksi maaliskuussa säädettiin ja tuli voimaan toinen laki, joka mahdollisti valtion toiminnan kannalta kriittisen informaation siirtämisen pilveen sotatilan aikana.[424] Amazonin ja Microsoftin lausuntojen ja raporttien perusteella Ukrainan julkisen sektorin kriittinen data siirrettiin Amazonin (AWS) ja Microsoft pilvipalveluihin hyökkäyksen alusta kymmenen viikon kuluessa.[425] Operaatiota oli todennäköisesti valmisteltu jo jonkin aikaa. Lisäksi Yhdysvallat ja muut Nato-maat olivat lähettäneet Ukrainaan useiden vuosien ajan siviili- ja sotilaskyberasiantuntijoita, jotka olivat auttaneet järjestelmien ja toimintatapojen resilienssin parantamisessa ja pyrkineet torjumaan Venäjän tietoverkko- ja järjestelmäoperaatioita. Esimerkiksi U.S. Cyber Commandin ”hunt forward” -tiimit olivat Ukrainassa ainakin tammikuuhun asti ja auttoivat hyökkäysten torjumisessa.[426] EU aktivoi nopean toiminnan kybervasteryhmän (Cyber Rapid Response Team) auttamaan Ukrainaa[427] ja Nato hyväksyi Ukrainan kyberpuolustusosaamiskeskuksen (Cooperative Cyber Defense Centre of Excellence) osallistujamaaksi.[428] Järjestelmistä oli pyritty myös paikkaamaan viime aikoina paljastuneita merkittäviä tietoturvahaavoittuvuuksia kuten Log4j.[429] Ukraina sai merkittävää tukea läntisiltä ICT-alan yrityksiltä.[430] Kyberturvallisuusyritykset ovat tarjonneet datan siirron lisäksi ilmaiseksi muitakin palveluita, esimerkiksi Cloudflaren Project Galileo ja Googlen Project Shield, ja tuki on ulottunut myös yrityssektorille ja järjestökentälle.[431] Valmistautu-

---

[423] Верховна Рада України: Проект Закону про хмарні послуги, 2655 від 20.12.2019. [https://itd.rada.gov.ua/billInfo/Bills/CardByRn?regNum=2655&conv=9], luettu 5.2.2024; Верховна Рада України: Закон України Про хмарні послуги, Документ 2075-IX, чинний, поточна редакція — Редакція від 27.12.2023 [https://zakon.rada.gov.ua/laws/show/2075-20#Text], luettu 5.2.2024.

[424] Закон України: Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів, Документ 2130-IX, чинний, поточна редакція — Редакція від 29.07.2023 [https://zakon.rada.gov.ua/laws/show/2130-20/print], luettu 5.2.2024.

[425] Microsoft (2022b); Bateman (2022); Mitchell, Russ: How Amazon put Ukraine's 'government in a box' — and saved its economy from Russia. *Los Angeles Times*, 15.12.2022. [https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data], luettu 5.2.2024.

[426] Corera, Cordon: Inside a US military cyber team's defence of Ukraine. *BBC*, 30.10.2022. [https://www.bbc.com/news/uk-63328398?utm_source=substack&utm_medium=email], luettu 5.2.2024.

[427] Cerelus, Laurens: EU to mobilize cyber team to help Ukraine fight Russian cyberattacks. *Politico,* 21.2.2022. [https://www.politico.eu/article/ukraine-russia-eu-cyber-attack-security-help/], luettu 5.2.2024.

[428] Smalley, Suzanne: Ukraine, looking to fortify itself against Russian attacks, admitted to NATO cyber center. *Cyberscoop,* 4.3.2022. [https://cyberscoop.com/ukraine-admitted-nato-ccdcoe/], luettu 5.2.2024.

[429] Petkauskas, Vilius: Log4j used to deploy WhisperGate malware in Ukraine cyberattack. *Cybernews*, 15.11.2023. [https://cybernews.com/news/log4j-used-to-deploy-whispergate-malware-in-ukraine-cyberattack/], luettu 5.2.2024.

[430] Microsoft: Digital Defense Report 2022. Microsoft, Redmond, WA, 2022 (c) [https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us], luettu 5.2.2024; Microsoft (2022b); Olney, Matt: Cisco stands on guard with our customers in Ukraine. Cisco Talos blog, 3.3.2022. [https://blogs.cisco.com/news/cisco-stands-on-guard-with-our-customers-in-ukraine], luettu 5.2.2024; Huntley, Shane: Fog of war: how the Ukraine conflict transformed the cyber threat landscape. Google Threat Analysis Group Blog, 16.2.2023. [https://blog.google/threat-analysis-group/fog-of-war-howthe-ukraine-conflict-transformed-the-cyber-threat-landscape/], luettu 5.2.2024; Insikt Group: Themes and Failures of Russia's War Against Ukraine. Recorded Future, February 2023. [https://go.recordedfuture.com/hubfs/reports/ta-2023-0209.pdf.], luettu 4.2.2024.

[431] Garson, Melanie: From Script Kiddies to Cyber Warriors: The Private Lines of Defense in the Ukraine Conflict. *Evolving Cyber Operations and Capabilities*. Lewis, James A., Lonergan, Erica D., Voo, Julia, Garson Melanie & Ertan, Amy. CSIS, 2023 [https://www.jstor.org/stable/resrep49617.6]; Mueller, Grace B., Jensen,

minen ei kuitenkaan alkanut liian aikaisin. Ukrainan kyberturvallisuuskeskuksen (SSSCIP) edustaja on kertonut Ukrainan aloittaneen kansallisten kyberturvallisuusjärjestelmien rakentamisen vasta 2021.[432]

Hyökkäyksen jatkuessa kybereskalaation riski koettiin todelliseksi ja suurvaltojen deterrenssiviestintä jatkui. Yhdysvaltalaisen NBC News uutistoimiston mukaan presidentti Joe Bideniä informoitiin 24.2. Venäjää vastaan tarvittaessa toteutettavien kyberoperaatioiden luonteesta ja vaikutuksista. Näihin kuului mm. Venäjän verkko- ja sähköyhteyksien katkaiseminen.[433] Tilanne ei kuitenkaan eskaloitunut eikä Venäjään tai Nato- tai EU-maihin kohdistunut hyökkäyksen alkuvaiheessa merkittäviä hyökkäyksellisiä kybertoimia.

Venäjä yritti hyökkäysoperaation ensimmäisten vuorokausien aikana saavuttaa informaatioylivoiman omien sotataidollisten oppiensa mukaisesti. Tuhoavat hyökkäykselliset kyberoperaatiot olivat osa suunnitelmaa ja ne olivat uusi lisä Venäjän aikaisempiin operaatioihin, joissa kyberoperaatioita oli käytetty lähinnä häirintään ja informaatiooperaatioiden tukemiseen. Hyökkäyksellisen kybertoiminnan tavoitteena oli todennäköisesti yhteistoiminnassa muiden informaatiosodankäynnin joukkojen ja keinojen kanssa lamauttaa Ukrainan poliittinen päätöksenteko, synnyttää yhteiskunnallista sekasortoa, disorganisoida asevoimien johtaminen ja estää liikekannallepano, toisin sanoen saavuttaa informaatioylivoima Ukrainaan nähden. Osa tuhoavista hyökkäyksistä kohdistui Ukrainalle keskeisten talouden- ja finanssisektorin kohteisiin, joten niillä pyrittiin todennäköisesti myös pakottavaan vaikutukseen. Kyberhyökkäykset eivät kuitenkaan synkronoituneet ilmaiskujen ja elektronisen sodankäynnin kanssa, joilla oli omat haasteensa.[434] Lamauttava yhteisvaikutus jäi näin ollen toteutumatta.

5.3. Kaappaushyökkäys vaakalaudalla: Maaliskuun 2022 alku

Maaliskuun alkuun mennessä alkoi käydä selväksi, että kaappaushyökkäys oli epäonnistunut. Venäjä pyrki kuitenkin jatkamaan operaatiota ja valtaamaan Kiovan maajoukkojen taistelulla alkuperäisen suunnitelman etenemissuuntien ja käytössä olevien joukkojen mukaisesti. Taisteluiden jatkuessa tulitauko- ja rauhanneuvottelut olivat vielä käynnissä, eikä sodan pitkittyminen näyttänyt olevan Venäjän agendalla.[435]

Maaliskuun alussa Venäjä muutti hyökkäyksellisten kyberoperaatioidensa tavoitetta, kohteita ja menetelmiä. Venäjä ilmoitti 1.3. aikovansa tuhota disinformaatiokohteita Ukrainassa ja iski myöhemmin Kiovan TV-tornia vastaan ja käytti tuhoavaa DesertBlade-haittaohjelmaa radio- ja televisioyhtiötä vastaan.[436] Hyökkäykseen yhdistet-

---

Benjamin, Valeriano, Brandon, Maness, Ryan C. & Macias, Jose M.: *Cyber Operations During the Russo-Ukrainian War. From Strange Patterns to Alternative Futures*. CSIS, 13.7.2023. [https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war], luettu 5.2.2024.

[432] Warsaw Security Forum (2023).

[433] Dilanian, Ken & Kube, Courtney: Biden has been presented with options for massive cyberattacks against Russia. *NBC News*, 24.2.2022. [https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558], luettu 4.2.2024.

[434] Watling & Reynolds (2022); Watling, Jack, Danylyuk, Oleksandr V & Reynolds, Nick: *Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War, February 2022–February 2023*. RUSI, London, 2023; Jones, Seth G.: *Russia's Ill-Fated Invasion of Ukraine. Lessons in Modern Warfare*. CSIS, Washington, D.C., 2022; Bronk, Justin: *Russian Combat Air Strengths and Limitations: Lessons from Ukraine*. CNA, Washington, D.C., 2023.

[435] Vuosien 2022–2023 tapahtumien yleisestä kuvauksesta ks. House of Commons Library (2023).

[436] Microsoft Digital Security Unit (2022a).

tiin mahdollisesti disinformaation levittäminen eri menetelmillä.[437] Venäjä ilmoitti myös iskevänsä Ukrainan informaatio- ja psykologisen sodankäynnin joukkoihin torjuakseen hyökkäyksiä Venäjää vastaan.[438] CaddyWiper-haittaohjelma havaittiin ukrainalaisissa verkoissa 1.3. Se ei perustunut samaan koodiin kuin aikaisemmat HermeticWiper tai IsaacWiper. Viikkoa myöhemmin 17.3. havaittiin uudelleen DesertBlade ja HermeticRansom-haittaohjelmat ja uutena DoubleZero-haittaohjelma, joka oli myös wiper-tyyppinen.[439] CaddyWiperia käytettiin rajattuun määrään kohteina Ukrainassa. Kohteena oli ainakin yksi pankki.[440] Kyber- tai kineettisten hyökkäysten takia Ukrainassa oli 9.–10.3. merkittäviä internetyhteyksien häiriöitä.[441] Internet palveluntarjoaja Triolan järjestelmiin tunkeuduttiin ja vaikutettiin uudelleen 9.3. ja Vinasterisk yhtiöön kohdistui kyberhyökkäys 13.3.[442] Samoihin aikoihin Microsoft väitti Venäjällä olevan pääsy ukrainalaisen ydinvoimayhtiön verkkoihin.[443]

Tuhoavien hyökkäysten lisäksi maaliskuun puolivälissä Ukrainaan oli kohdistunut yli 3000 palvelunestohyökkäystä.[444] Cloudflaren mukaan palvelunestohyökkäysten määrä nousi 1300 % maaliskuun alkuun mennessä. Hyökkäyksissä oli paljon piikkejä ja ajallista vaihtelua, mutta käytännössä hyökkäykset ovat olleet jatkuvia aina 2022 vuodenvaihteeseen asti. Ajoittain liikenne laski .ua domainin osalta jopa 80 %. Hyökkäysten kohteena olivat hallinto, finanssiala ja media – etenkin TV- ja radioyhtiöt, ISP:t ja verkkomedia sekä kustannustoimittajat.[445] Venäjä ei kuitenkaan kyennyt hyökkäyksillään lamauttamaan Ukrainan teleliikenneverkkoja kuin paikallisesti ja tilapäisesti.[446]

Yhtenä syynä Ukrainan asevoimien johtamisyhteyksien kestämiseen oli yhdysvaltalaisen SpaceX-yrityksen Starlink-satelliitti-internetjärjestelmä. Ukraina sai käyttöönsä noin 500 Starlink-vastaanotinta helmi-maaliskuussa ja Starlinkin liikenne kasvoi 1600 % joulukuuhun 2022 mennessä.[447] Toukokuussa järjestelmällä oli 150000 päivittäistä käyttäjää ennen kaikkea rintamalla[448] ja sodan ensimmäisten kymmenen kuukauden

[437] The Economic Security Council of Ukraine (2022).
[438] TASS: Russian Defense Ministry warns about strikes being prepared on military sites in Kiev. TASS, 1.3.2022. [https:/tass.com/defense/1414199], luettu 5.2.2024.
[439] ESET: CaddyWiper: New wiper malware discovered in Ukraine. ESET, 15.3.2022 (b). [https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/], luettu 5.2.2024; ESET (2022a); CERT-UA: Кібератака на українські підприємства з використанням програми-деструктора DoubleZero (CERT-UA#4243). CERT-UA Computer Emergency Response Team of Ukraine, 22.32022. [https://cert.gov.ua/article/38088], luettu 5.2.2024; Malhotra, Asheer: Threat Advisory: DoubleZero. CISCO Talos Blog, 24.3.2022. [https://blog.talosintelligence.com/threat-advisory-doublezero/], luettu 5.2.2024; ESET: A year of wiper attacks in Ukraine. ESET Research, 24.2.2023 (a). [https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/], luettu 5.2.2024.
[440] Greenberg, Andy: Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless. *WIRED*, 10.11.2022 (a). [https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/], luettu 5.2.2024.
[441] CERT-EU (2023a).
[442] Cyber Peace Institute: Ukraine: Timeline of Cyberattacks on critical infrastructure and civilian objects. Cyber Peace Institute, 15.5.2022 (a). [https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/], luettu 5.2.2024.
[443] Microsoft (2022a).
[444] SSSCIP: Since February, 15, Ukraine has suffered over 3000 DDoS attacks. SSSCIP, 16.3.2022. [https://cip.gov.ua/en/news/vid-15-lyutogo-ukrayina-zaznala-ponad-3-000-ddos-atak], luettu 5.2.2024.
[445] Tomé, Joao, Belson, David & Berdan, Kristin: One year of war in Ukraine: Internet trends, attacks, and resilience. Cloudflare, 23.2.2023. [https://blog.cloudflare.com/one-year-of-war-in-ukraine/], luettu 5.2.2024.
[446] Sabin, Sam & Cerelus, Laurens: 3 reasons Moscow isn't taking down Ukraine's cell networks. *Politico*, 7.3.2022. [https://www.politico.com/news/2022/03/07/ukraine-phones-internet-still-work-00014487], luettu 5.2.2024.
[447] Tomé, Belson & Berdan (2023).
[448] Bateman (2022).

aikana Ukrainaan toimitettiin 22000 päätelaitetta.[449] Venäjä yritti häiritä Starlinkiä ensimmäisten viikkojen aikana, mutta epäonnistui.[450] Ukraina on käyttänyt johtamiseen myös ulkomaisia viestintäsovelluksia, joita Venäjä ei ole pystynyt, halunnut tai uskaltanut häiritä.[451]

Mandiantin mukaan GRU valmisteli maaliskuussa kevään ja kesän hyökkäyksiä murtautumalla verkkojen reunalaitteisiin verkkourkinnan sijaan, mikä mahdollisti nopeamman toiminnan, hyökkäyksien uusimisen ja pysyvyyden kohdeverkoissa.[452] Mandiantin mukaan Venäjä käytti tuhoavien hyökkäysten, kybervakoilun ja informaatiovaikuttamisen yhdistelmää useaan otteeseen. Esimerkiksi 16.3. Ukraine 24 TV-kanavan verkkosivuille ja tekstikanavalle syötettiin valeviesti Ukrainan antautumisesta ja sama teksti liitettiin presidentti Zelenskyistä tehtyyn deepfake-videoon. Lisäksi wiper-haittaohjelma oli alustettu tuhoamaan eräs järjestelmä kolme tuntia ennen Zelenskyin oikeaa puhetta.[453] Informaatiovaikuttamisoperaatiot eivät tuottaneet sodan alussa toivottuja tuloksia ja venäläinen informaatiosodankäynnin johtava tutkija Andrei Manoilo onkin todennut, että Venäjän joukoilla ei ollut tarvittavaa kuutta kuukautta aikaa valmistella informaatio-operaatiota, joten informaatiovaikuttaminen oli operaation alussa luonteeltaan yksinkertaista ja vanhanaikaista.[454]

Venäjän hyökkäykset ulottuivat myös Ukrainan rajojen ulkopuolelle. Esimerkiksi Ukrainan Lontoon lähetystön sähköiset palvelut olivat poissa käytöstä palvelunestohyökkäyksen vuoksi.[455] Eskalaatiouhka oli todellinen. Ukrainaa tukevien haktivistien yritettyä väitetysti päästä venäläisen Roskosmosin satelliittijärjestelmään yhtiön silloinen johtaja Dmitri Rogozin ilmoitti, että kyberhyökkäykset Venäjän satelliitteja vastaan olisivat syy sotaan.[456]

Maaliskuu oli kyberoperaatioiden osalta kiivain ajankohta vuosien 2022–2023 aikana.[457] Yllätyksellisen hyökkäyksen epäonnistuttua Ukrainan median häirinnästä palvelunestohyökkäyksillä siirryttiin hetkeksi tuhoamiseen ja informaatiotilan eristämiseen, mutta tästä operaatiolinjasta luovuttiin huhtikuun kuluessa.[458] Venäjä todennäköisesti pyrki estämään informaatiotilan käytön Ukrainan hallinnolta epäonnistut-

---

[449] Weatherbed, Jess: Ukraine nets 10,000 additional Starlink terminals, claims funding issues are 'resolved.' *The Verge*, 21.12.2022. [https://www.theverge.com/2022/12/21/23520412/ukraine-starlink-internet-terminals-spacex-funding-issues-russia-war], luettu 5.2.2024.

[450] Kan, Michael: Pentagon Impressed by Starlink's Fast Signal-Jamming Workaround in Ukraine. *PC Magazine UK*, 21.4.2022. [https://uk.pcmag.com/networking/139965/pentagon-impressed-by-starlinks-fast-signal-jamming-workaround-in-ukraine], luettu 5.2.2024.

[451] Trauthig, Inga Kristina: Chat and Encrypted Messaging Apps Are the New Battlefields in the Propaganda War. *Lawfare*, 27.3.2022. [https://www.lawfareblog.com/chat-and-encrypted-messaging-apps-are-new-battlefields-propaganda-war], luettu 5.2.2024.

[452] Greenberg (2022a).

[453] Google (2023).

[454] Manoilo, Andrey V.: Information operations before and after the armed conflict in Ukraine. SSRN, 11.1.2023. [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4296035]; Манойло, А. В.: Информационные диверсии в конфликте на украине. *Вестник академии военных наук*, 81(4) 2022, s. 54–58.

[455] Cook, James: Ukrainian embassy in London reportedly under constant cyber-attack. *Business Leader*, 4.3.2022. [https://www.businessleader.co.uk/ukrainian-embassy-in-london-reportedly-under-constant-cyberattack/], luettu 5.4.2022.

[456] Интерфакс: Рогозин: кибератаки на российские спутники - это casus belli. *Интерфакс*, 2.3.2022. [https://www.interfax-russia.ru/rossiya-i-mir/rogozin-kiberataki-na-rossiyskie-sputniki-eto-casus-belli], luettu 5.2.2024.

[457] Stupp, Catherine: Russian Cyberattacks Have Increased on Ukraine's Critical Infrastructure. *Wall Street Journal*, 5.4.2022. [https://www.wsj.com/livecoverage/russiaukraine-latest-news-2022-04-05/card/russian-cyberattacks-have-increasedon-ukraine-s-critical-infrastructurenSa3wDFQr3fbILlQ6dGf], luettu 5.2.2024.

[458] CERT-EU (2023a).

tuaan ensin hallinnon lamauttamisessa. Microsoftin mukaan maaliskuussa erilaisten verkko-operaatioiden määrä kaksinkertaistui kolmeen aikaisempaan kuukauteen verrattuna. Tuhoavia hyökkäyksiä ei kuitenkaan havaittu hyökkäyksen toisella viikolla (28.2.–6.3.) Maaliskuun toiselta viikolta eteenpäin huhtikuun ensimmäiselle viikolle tuhoavia hyökkäyksiä kohdistui kahdesta kuuteen organisaatioon viikossa, eniten aikajaksolla 17.–23.3.[459] Tämä kertoo siitä, että alkuperäinen kyberhyökkäyskampanja strategisen hyökkäysoperaation osana oli suunniteltu muutamia vuorokausia kestäväksi informaatioiskuoperaatioksi. Tilanteenarvion jälkeen Venäjä ryhtyi ns. symmetriseen taisteluun informaatiotilan hallinnasta. Kaappaushyökkäyksen uhkaava epäonnistuminen johti todennäköisesti ratkaisuun, jossa tiedustelupalvelut ja GRU käskettiin lamauttamaan Ukrainan valtiojohto, asevoimat ja yhteiskunta kaikilla käytettävissä olevilla keinoilla pois lukien joukkotuhoaseet. Venäjän maalis-huhtikuun kyberhyökkäyskampanjalla pyrittiin todennäköisesti myös taloudellisiin ja siten poliittisiin seurannaisvaikutuksiin.

5.4. Kaappaushyökkäys epäonnistuu: Maaliskuu 2022 loppu

Maaliskuun puolivälissä Venäjän maahyökkäys pysähtyi 15.–20.3. aikajaksolla ja Ukraina aloitti vastahyökkäykset Kiovan suunnalla 25.3. mennessä. Samoihin aikoihin Venäjä ilmoitti siirtävänsä taistelujen painopisteen Donetskin suunnalle. Taistelujen kestettyä muutamia viikkoja Ukrainan tueksi oli muodostunut Yhdysvaltojen ja Natomaiden liittouma, joka tuki Ukrainaa sotilaallisesti ja asetti Venäjälle tuntuvia talous- ja teknologiasanktioita.[460]

Venäjä jatkoi tuhoavia kyberhyökkäyksiä Ukrainan sähköverkkoa vastaan ja 19.3. Sandworm hyökkäsi Industroyer2-haittaohjelmalla Ukrainan sähköverkon tietojärjestelmiin pyrkien katkaisemaan sähkönsyötön ja tuhoamaan hallintatietokoneet – muutama päivä sen jälkeen, kun Ukraina oli liittynyt EU:n sähköverkkoon.[461] 28.3. hakkerit hyökkäsivät teleliikenneyhtiö Ukrtelecomia vastaan, joka on yksi kolmesta suuresta alan ukrainalaisesta yhtiöstä, ja sen tarjoamat yhteydet romahtivat 87 %. Yhteyksien palauttamiseen meni viisitoista tuntia.[462] Microsoftin mukaan Venäjän tuhoavat kyberhyökkäykset kohdistuivat ukrainalaisiin logistiikka- ja kuljetusalan yrityksiin sekä paikallishallintoon, millä pyrittiin tukemaan Venäjän painopisteen siirtoa Itä-Ukrainan alueelle. Lisäksi lamautettiin mm. valtionhallinon digitaalisen asioinnin portaali ja hyökkäykset mediaa vastaan jatkuivat.[463] Kyberhyökkäysten vakavuudesta huolimatta kineettisen vaikuttamisen seuraukset olivat maaliskuussa etenkin rintamalinjojen lähellä kybervaikuttamista merkittävämpiä.[464] Venäjän tuhoavien kyberhyökkäysten intensiteetti laski ja suunnitelmallisesta ja koordinoidusta informaatioiskusta siirryttiin ad hoc -operointiin käyttäen todennäköisesti pois ne hyökkäykset, jotka oli jätetty

[459] Microsoft (2022a).
[460] Vuosien 2022–2023 tapahtumien yleisestä kuvauksesta ks. House of Commons Library (2023).
[461] O'Neill, Patrick Howell: Russian hackers tried to bring down Ukraine's power grid to help the invasion. *MIT Technology Review*, 12.4.2022. [https://www.technologyreview.com/2022/04/12/1049586/russian-hackers-tried-to-bring-down-ukraines-power-grid-t o-help-the-invasion/], luettu 5.2.2024.
[462] NetBlocks (2022); Brewster, Thomas: 'Most Severe' Cyberattack Since Russian Invasion Crashes Ukraine Internet Provider. *Forbes*, 28.3.2022. [https://www.forbes.com/sites/thomasbrewster/2022/03/28/huge-cyberattack-on-ukrtelecom-biggest-since-russian-invasion-crashes-ukraine-telecom/?sh=1f1838767dc2], luettu 5.2.2024; Warsaw Security Forum (2023).
[463] Microsoft (2022a).
[464] Netblocks (2022).

aikaisemmin reserviin ja olivat vielä käytettävissä Ukrainan kyberpuolustuksen kovennutta.

Venäjän taistelutoimien tukemiseksi tehdyistä kyberhyökkäyksistä on maaliskuun lopulta vähän näyttöä. Mandiant on raportissaan väittänyt, että Sandworm olisi kyennyt maaliskuussa tunkeutumaan turkkilaisen Bayraktar lennokkien valmistajan tietoverkkoihin ja vaikuttamaan lennokkien käyttöön Ukrainassa.[465] Cisco puolestaan epäili Venäjän kyenneen asentamaan takaoven ukrainalaisen ohjelmistoyrityksen tuotteeseen tuotantoketjuhyökkäyksen mahdollistamiseksi.[466] Informaatiovaikuttamisen tukeminen sen sijaan jatkui aktiivisena. Mandiantin raportin mukaan Venäjä toteutti useita kyberavusteisia informaatio-operaatioita hyökkäyksen kahden ensimmäisen kuukauden aikana. Niihin liittyi epäautenttista käyttäytymistä sosiaalisessa mediassa, mediakanavien tilapäistä haltuunottoa ja tilien varastamista. Niiden tavoitteena oli Mandiantin mukaan ukrainalaisten yhtenäisyyden heikentäminen, Ukraina erottaminen ulkomaisista tukijoista ja Venäjän sotanarratiivien tukeminen.[467]

Venäjän Ukrainan ulkopuolelle kohdistuvat kyberhyökkäykset jatkuivat ja vahvistuivat. 23.3. ja maalis-huhtikuussa kolme eurooppalaista tuulivoimayhtiötä joutui kyberhyökkäysten kohteeksi – yksi VIASAT hyökkäyksen seurauksena ja kaksi kiristyshaittaohjelman kohteena.[468] Yhdysvaltojen johto näki parhaaksi varoittaa talouselämää ja yhteiskuntaa Venäjä kyberhyökkäyksen uhasta.[469] Hyökkäysten aikaan Lännessä käytiin keskustelua Venäjän energiayhteyksien korvaamisesta ja sanktioista sekä Ukrainalle annettavasta taloudellisesta ja sotilaallisesta avusta, mikä ei todennäköisesti ollut sattumaa.

Venäjällä ei aktiivisuudestaan huolimatta ollut täyttä toiminnanvapautta informaatiotilassa. 18.3. Yhdysvaltojen ja Iso-Britannian viranomaiset hävittivät Sandwormin operoiman bottiverkon ja 28.3. mennessä Ukrainan turvallisuuspalvelu (SBU) väitti hävittäneensä useita Venäjän bottiverkkoja, joilla oli tuhansia jäseniä.[470] Botit olivat lähettäneet propagandatekstiviestejä sotilaille ja poliiseille.[471] 28.3. Ukrainan turvallisuuspalvelut lopettivat viiden disinformaatiota levittävän bottifarmin toiminnan, jotka operoiva yli sataatuhatta tiliä.[472] Venäjän informaatiovaikuttamista haittasivat myös Metan, Redditin, TikTokin, Alphabetin, Microsoftin, Spotifyn ja Telegrammin disinformaation vastaiset toimet, kuten sisällön suodattaminen ja poistaminen sekä tilien sulkeminen. RT:n ja Sputnikin sovelluksia poistettiin sovelluskaupoista ja venäläisten

[465] Google (2023).
[466] Schultz, Jaeson: Attackers target Ukraine using GoMet backdoor, CISCO Talos Blog, 21.7.2022. [https://blog.talosintelligence.com/attackers-target-ukraine-using-gomet/], luettu 5.2.2024.
[467] Wahlstrom, Alden, Revelli, Alice, Riddell, Sam, Mainor, David & Serabian, Ryan: The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine. Mandiant, 25.11.2022. [https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine], luettu 5.2.2024;
[468] CERT-EU (2023a); Arghire, Ionut: German Wind Turbine Firm Hit by 'Targeted, Professional Cyberattack.' Security Week, 26.4.2022. [https://www.securityweek.com/german-wind-turbine-firm-discloses-targeted-professional-cyberattack/], luettu 5.2.2024.
[469] Demarest, Colin: Biden: Russia mulling cyberattacks on US. *C4ISRNET*, 22.3.2022. [https://www.c4isrnet.com/cyber/2022/03/22/biden-russia-mulling-cyberattacks-on-us/], luettu 5.2.2024.
[470] National Security Archive Cyber Vault (2023).
[471] Bateman (2022).
[472] Osborne, Charlie: Ukraine destroys five bot farms that were spreading 'panic' among citizens. *ZDnet,* 29.3.2022. [www.zdnet.com/article/ukraine-takes-out-five-bot-farms-spreading-panic-among-citizens/], luettu 5.2.2024.

toimijoiden mainostoimintaa rajoitettiin. Monet yritykset lisäsivät data-analytiikan käyttöä venäläisen disinformaation paljastamiseksi.[473]

Venäjään kohdistui maaliskuussa IT Army of Ukrainen ja muiden haktivistien ja mahdollisesti valtiosidonnaisten ryhmien ennennäkemätön kyberhyökkäysten kampanja. Suurin osa hyökkäyksistä oli palvelunestohyökkäyksiä tai verkkosivujen sotkemista, mutta myös useita tietomurtoja tapahtui ja niiden saalis vuodettiin internettiin. Monet verkkosivut ja palvelut olivat pitkiä aikoja pois käytöstä.[474] Maaliskuun lopulla Ukrainan ohjaamat patrioottiset hakkerit ja haktivistit ympäri maailmaa olivat nostaneet suorituskykynsä sille tasolle, että kykenivät siirtämään kybersodan Venäjän rajojen sisälle. Venäjän IT-sektori ei ollut valmistautunut sotilaallisen erikoisoperaation synnyttämään kyberhyökkäysten intensiteettiin. Tämä ei kuitenkaan johtanut strategisiin vaikutuksiin, sillä kyberhyökkäykset jäivät suurilta osin kiusanteon asteelle. Venäjän asevoimiin kohdistuneista operaatioista ei ole julkisuudessa tietoja ja on mahdollista, että osa Venäjään kohdistuneista hyökkäyksistä on jäänyt uutisoimatta.

5.5. Painopisteen siirto ja uudelleen ryhmittyminen: Huhtikuu 2022

Huhtikuun ensimmäisinä päivinä Venäjän joukot vetäytyivät Kiovan suunnalta, ja huhtikuun alusta Venäjän painopiste siirtyi Donetskin ja Luhanskin alueiden valtaamiseen ja Krimin maayhteyden varmistamiseen. Presidentti Putin totesi 12.4. että rauhanneuvottelut eivät olleet tarkoituksenmukaisia ja että Venäjän tulisi jatkamaan operaatiota loppuun asti.[475] Huhtikuussa Lännen sotilaallinen ja taloudellinen tuki Ukrainalle alkoi kiihtyä.[476]

Venäjän tuhoavat kyberhyökkäykset jatkuivat vielä huhtikuun alussa. CaddyWiper-haittaohjelmaa käytettiin uudelleen 1.4.[477] ja 8.4. Sandworm hyökkäsi Industroyer2 ja CaddyWiper-haittaohjelmilla vähintään yhdeksää Ukrainan sähköverkon muuntamoasemaa vastaan. Hyökkäystä oli todennäköisesti suunniteltu viikkoja ja se kykeni vaikuttamaan useaan eri käyttöjärjestelmään. Industroyer2:n käyttö oli tarkoitus salata. 1,5–2 miljoonaa ukrainalaista olisi jäänyt ilman sähköjä ja tietoliikenneyhteydet olisivat katkenneet, mikäli hyökkäys olisi onnistunut.[478] Matthias Schulzen ja Mika Kerttusen mukaan kyseessä oli ainut potentiaalisesti fyysistä tuhoa aiheuttava haittaohjelman käyttö 2022 aikana.[479] Telekommunikaatiosektori ja viestintä yleensäkin ml. mobiilioperaattorit olivat jatkuvien hyökkäysten kohteena.[480] Ukrainan SSSCIP:n mukaan

[473] Lewis et al. (2023).
[474] Zelenaya, Olexandra: Hacker Attacks on Russia Gain Attention but Cause Little Damage. *The Moscow Times*, 1.7.2022. [https://www.themoscowtimes.com/2022/04/29/hacker-attacks-on-russia-gain-attention-but-cause-little-damage-a77428], luettu 5.2.2024; Шпунт, Яков: Безопасность попала в сложную ситуацию. *Comnews*, 24.3.2022. [https://www.comnews.ru/content/219409/2022-03-24/2022-w12/bezopasnost-popala-slozhnuyu-situaciyu], luettu 5.2.2024.
[475] Gershkovich, Evan: Putin Says Peace Talks Have Reached Dead End, Vows War Will Go On. *The Wall Street Journal*, 12.4.2022. [https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-04-12/card/putin-says-peace-talks-have-reached-dead-end-vows-war-will-go-on-pstQwRdkQV1WiLl9kwAH], luettu 5.2.2024.
[476] Vuosien 2022–2023 tapahtumien yleisestä kuvauksesta ks. House of Commons Library (2023).
[477] ESET (2023a).
[478] Greenberg, Andy: Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine. *Wired*, 12.4.2022 (b). [https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru/], luettu 5.2.2024; ESET (2022a); The MOD of Lithuania (2023).
[479] Schulze & Kerttunen (2023).
[480] SSSCIP: During the war, telecom industry of Ukraine became one of the hackers' primary targets. SSSCIP, 3.4.2022. [https://cip.gov.ua/en/news/pid-chas-viini-telekom-galuz-ukrayini-stala-odniyeyu-z-klyuchovikh-mishenei-khakeriv], luettu 5.2.2024.

Venäjä pyrki tuhoamaan Ukrainan TV- ja radiolähetysinfrastruktuuria kineettisillä iskuilla.[481] Tuhoa aiheuttavat hyökkäykset kuitenkin vähenivät merkittävästi huhtikuun alun jälkeen, eikä niiden osalta voida enää puhua yhtenäisestä ja jatkuvasta kampanjasta. Tuhoavista hyökkäyksistä tuli yksittäisiä iskuja muun taistelutoiminnan lomassa.

Palvelunestohyökkäykset ja informaatiovaikuttamisen tukeminen jatkuivat. Telegramia pyrittiin käyttämään tiedusteluun lähettämällä haitallisia linkkejä käyttäjille.[482] GRU lähetti väärennettyjä sähköposteja Mariupolin puolustajien nimissä, joissa syytettiin hallitusta puolustajien hylkäämisestä.[483] EU-maihin kohdistui palvelunestohyökkäyksien aalto.[484] Kyberhyökkäykset Nato- sekä EU-maita vastaan alkoivat kuitenkin painottua kybervakoiluun.[485] Killnet ryhmän palvelunestohyökkäyksen kohteena olivat 14.4. kahdeksan puolalaisen lentokentän verkkosivut.[486]

Ukrainan onnistuttua mobilisoimaan kotimainen ja kansainvälinen haktivistirintama Venäjää vastaan alkoi kohdistua enemmän tietomurtoja ja -vuotoja palvelunestohyökkäysten hieman vähentyessä. Anonymous murtautui heikosti suojattuihin järjestelmiin ja vuosi internettiin suuret määrät Venäjän hallinnon ja yksityisyritysten tietoja.[487] Erityisesti hyökkäysten kohteeksi valikoituivat venäläiset pankit.[488] Rostelekom-Solarin mukaan 77 % kriittisistä hyökkäyksistä kohdistui verkkopalveluihin, millä oli vaikutusta venäläisten arkielämään.[489] Toukokuussa Venäjään kohdistui väitetysti jopa ICS/SCADA hyökkäyksiä.[490]

Microsoftin mukaan Ukrainaan oli kohdistunut lähes neljäkymmentä erillistä tuhoavaa kyberhyökkäystä huhtikuun loppuun mennessä.[491] Samalla kuitenkin vaikutti siltä, että Dmitri Alperovitch, yksi tietoturvayritys CrowdStriken perustajista, oli ollut melko oikeassa ennustaessaan, että taistelujen kestettyä aikansa Venäjä keskittyisi kybertilassa tiedusteluun, häirintään ja harhauttamiseen sekä psykologisiin operaatioihin.[492] Huhtikuussa oli jo nähtävissä, että kyberhyökkäykset alkoivat keskittyä palvelunestohyökkäyksiin ja informaatio-operaatioiden tukemiseen. Venäläiset todennäköisesti arvioivat, että tuhoavat kyberhyökkäykset olivat epäonnistuneet informaatioylivoiman tuottamisessa – yhdessä muiden informaatiosodankäynnin keinojen kanssa. Todennäköisesti tästä ja siitä syystä, että valmistellut hyökkäykset oli käytetty, informaatio-operaatioiden tukeminen ja tiedustelu vaikuttivat osuvammalta tehtävältä Venäjän kyberjou-

---

481 SSSCIP: Invaders are Destroying TV and Radio Broadcasting Infrastructure to Deny Access to Information. SSSCIP, 4.5.2022. [https://cip.gov.ua/en/news/okupanti-znishuyut-infrastrukturu-telebachennya-tamovlennya-shob-perekriti-dostup-do-pravdivoyi-informaciyi], luettu 5.2.2024.
482 SSSCIP: Please be careful! Cyber-attacks aimed at gaining access to Telegram accounts were detected. SSSCIP, 5.4.2022. [https://cip.gov.ua/en/news/please-be-careful-cyber-attacks-aimed-at-gaining-access-to-telegram-accounts-were-detected], luettu 5.2.2024.
483 Microsoft (2022a).
484 CERT-EU (2023a).
485 National Security Archive Cyber Vault (2023).
486 CERT-EU (2023a).
487 Fowler, Jeremiah: Is Anonymous Rewriting the Rules of Cyberwarfare? Timeline of Their Attacks Against the Russian Government. Website Planer, blogikirjoitus, n.d. [https://www.websiteplanet.com/blog/anonymous-cyberwarfare-report/], luettu 5.2.2024.
488 TVC.ru: Число атак хакеров на банки России выросло более чем в 20 раз. *TVC.ru*, 18.4.2022. [https://www.tvc.ru/news/show/id/238182], luettu 5.2.2024.
489 SecurityLab.ru: С конца февраля в России наблюдается резкий всплеск атак на веб приложения. *SecurityLab.ru*, 12.5.2022. [https://www.securitylab.ru/news/531584.php], luettu 5.2.2024.
490 CERT-EU (2023a).
491 Microsoft Digital Security Unit (2022a), s. 3.
492 Alperovich, Dmitri: How Russia Has Turned Ukraine into a Cyber-Battlefield. The Kremlin's Hackers Are Already Targeting Kyiv. *Foreign Affairs*, 28.1.2022. [https://www.foreignaffairs.com/articles/russia-fsu/2022-01-28/how-russia-has-turned-ukraine-cyber-battlefield], luettu 5.2.2024.

koille hyökkäysoperaation pidetessä. Vaikuttaa myös siltä, että informaatioylivoiman saavuttamisen tavoitteesta luovuttiin ja sen sijaan tavoitteeksi otettiin pidempi aikainen vaikuttaminen ukrainalaisiin ja heidän tukijoihinsa informaatiokamppailun hengessä.

5.6. Taistelut kaakossa: Touko-kesäkuu 2022

Touko-kesäkuussa Venäjä pyrki murtamaan Ukrainan puolustuksen Donetskin ja Luhanskin alueella tulenkäytöllä jatkaen samalla kaukovaikutteisten aseiden käyttöä. Kesäkuun alussa Yhdysvallat lähetti M142 HIMARS -järjestelmiä Ukrainaan, mikä aloitti edelleen jatkuvan yhä pidemmälle kantavien ohjusjärjestelmien luovuttamisen Ukrainalle. Ohjusiskujen lisäksi Ukraina käytti salamurhia, sabotaaseja ja erikoisjoukkojen iskuja Venäjän tukijärjestelmän heikentämiseen ja pettureiden eliminointiin kesästä 2022 lähtien.[493] Suomi ja Ruotsi päättivät hakeutua Natoon, ja EU päätti aloittaa Ukrainan kanssa jäsenhakemusneuvottelut. Venäjän strateginen ympäristö alkoi muuttua ei-toivotulla tavalla.[494]

Toukokuusta lähtien Venäjän kybertoimijat eli GRU, FSB, SVR ja näiden ohjaamat patrioottisen hakkerit pyrkivät uudelleen orientoimaan ja synkronoimaan kyberoperaatiot maaoperaation kanssa. Valmistellut operaatiot oli käytetty ja yllätys oli menetetty. Venäjä sotilasstrateginen toimintaympäristö oli muuttunut radikaalisti ja Ukrainan kybertilan luonne oli muuttunut voimakkaasti. Operaatioiden pääpaino siirtyi strategiseen tiedusteluun ja kohdetiedusteluun tulevia operaatioita silmällä pitäen.[495] Ukrainan mukaan viranomaisten puhelimia yritettiin hakkeroida ja FSB:n Turla kohdisti vakoilua Baltian maihin.[496] Lisäksi Venäjä tiedusteli Puolassa Ukrainan huoltoreittejä.[497] Microsoftin mukaan kesäkuuhun 2022 mennessä Venäjä oli tunkeutunut onnistuneesti 128 verkkoon 42 maassa. Kohteina olivat valtionhallinnon virastot, ajatushautomot, järjestöt, telekommunikaatio-, energia- ja puolustusalan yritykset.[498] Kybertoiminnan uudelleen orientaatio ei välttämättä ollut alussa suunnitelmallinen tai järjestelmällinen, eikä eri toimijoiden roolijako välttämättä ollut selvä epäonnistuneen hyökkäyksen jälkeen.

Sijaistoimijoiden ja aktivistien merkitys kasvoi loppukeväästä, vaikkakin hyökkäysten kokonaismäärä laski väliaikaisesti touko-kesäkuussa.[499] Palvelunestohyökkäykset olivat määrältään ja intensiteetiltään merkittävin kyberhyökkäysten muoto.[500] Ne ja ajoittain muunkin tyyppiset hyökkäykset olivat usein miten yhteydessä taistelukentän ulko-

[493] Liebermann, Oren: How Ukraine is using resistance warfare developed by the US to fight back against Russia. *CNN*, 27.8.2022. [https://edition.cnn.com/2022/08/27/politics/russia-ukraine-resistance-warfare/index.html], luettu 5.2.2024; Borsari, Federico: Ukrainian Special Forces — Preparing the Battlefield. CEPA, 22.5.2023. [https://cepa.org/article/ukrainian-special-forces-preparing-the-battlefield/], luettu 5.2.2024.
[494] Vuosien 2022–2023 tapahtumien yleisestä kuvauksesta ks. House of Commons Library (2023).
[495] SSSCIP: Russia's Cyber Tactics Lessons Learned 2022. SSSCIP, 2022 (a). [https://cip.gov.ua/services/cm/api/attachment/download?id=53466], luettu 5.2.2024.
[496] Satter, Raphael: Ukrainian Officials' Phones Targeted by Hackers —Cyber Watchdog. *Reuters*, 6.6.2022. [https://www.reuters.com/world/europe/ukrainian-officials-phones-targeted-by-hackers-cyber-watchdog-2022-06-06/], Luettu 5.2.2024; CERT-EU (2023a).
[497] Microsoft (2022b).
[498] Smith (2022).
[499] CyberPeace Institute: Cyber Dimensions of the Armed Conflict in Ukraine. Quarterly Analysis Report Q3 July to September 2022. CyberPeace Institute, 2022 (a). [https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q3-2023/], luettu 5.2.2024.
[500] National Security Archive Cyber Vault (2023).

puolisiin tapahtumiin, kuten esimerkiksi Alexander Duginin tyttären salamurhaan, ydinvoimaloiden turvallisuudesta käytyihin neuvotteluihin, kielikysymyksiin, miehitettyjen alueiden kansanäänestyksiin ja Ukrainan ortodoksisen kirkon asemaan liittyviin kiistoihin, juhlapäiviin tai Ukrainan poliittisen tai sotilasjohdon ulostuloihin.[501] Keväällä ja kesällä Venäjä käytti tekstiviestikampanjoita disinformaation levittämiseksi mm. rintaman läheisyydessä asuvan väestön keskuuteen.[502] Voiton päivänä 9.5. ukrainalaiset ja venäläiset hakkerit vaihtoivat iskuja. Ukrainalaisia teleliikenneyrityksiä vastaan tehtiin laaja palvelunestohyökkäys[503] ja toisaalta venäläinen RuTube-sisällönjakopalvelu lamautettiin kolmeksi vuorokaudeksi ja Venäjän voitonpäivän TV-lähetyksiä häirittiin.[504] Kesäkuussa Sandworm toteutti Ukrainan mediayrityksiä vastaan laajan Follina / CresentImp-haittaohjelmakampanjan samaan aikaan, kun Ukrainan EU-diplomatia oli aktiivista.[505] Informaatioiskuoperaation epäonnistuttua informaatiovaikuttamisen tukemisesta tuli näkyvien kyberoperaatioiden helppo, halpa ja tarvittaessa joustavasti toteutettava päätehtävä.

GRU:n ohjailema Killnet-ryhmä keskittyi Ukrainan ulkopuolisiin hyökkäyksiin. Toukokuussa se yritti sabotoida Italiassa järjestettyjä Eurovisio 2022 laulukilpailuja palvelunestohyökkäyksillä.[506] 27.6. se toteutti palvelunestohyökkäyksen liettualaisia verkkosivuja vastaan Liettuan keskeyttäessä EU:n sanktioimien tuotteiden viennin Venäjältä Kaliningradiin. Hyökkäys saattoi vaikuttaa myös viranomaisten turvaverkon toimintaan.[507] Myöhemmin heinäkuussa Killnet teki palvelunestohyökkäyksen Yhdysvaltojen kongressin verkkosivuja vastaan.[508]

Ukrainan tietoliikenneverkot palautuivat suhteellisen nopeasti ja hyvin kevään kyber- ja kineettisistä iskuista, vaikka esimerkiksi teleoperaattori Kyivstar on ollut jatkuvien hyökkäysten kohteena ja menettänyt kineettisissä iskuissa alueesta riippuen 10–30 % kiinteästä infrastruktuuristaan.[509] Ukrainan verkkoliikenne putosi 33 % helmikuun jälkeen, nousi 66 % syksyllä, mutta putosi noin 50 % vuodenvaihteessa sotaa edeltäneestä tasosta. Liikenne romahti Venäjän hyökkäysreiteillä muun muassa Tšernihivissä, Harkovassa ja Mariupolissa ja sen määrä nousi Länsi-Ukrainassa pakolaisten mukana. Starlink oli kriittinen asevoimille, mutta sen osuus kokonaisliikenteestä oli

[501] The Economic Security Council of Ukraine (2022).
[502] SSSCIP: Ukraine does not and will not disconnect Ukrainians from communication services. SSSCIP, 5.6.2022. [https://cip.gov.ua/en/news/ukrayina-ne-vidklyuchaye-i-ne-vidklyuchatime-ukrayinciv-vid-zv-yazku], luettu 5.2.2024.
[503] Zubkova, Daria: Russia Carried Out Large-Scale Cyber Attack on Ukrainian Telecom Operators Websites. *Ukrainian News Agency*, 11.5.2022. [https://ukranews.com/en/news/856131-russia-carried-out-large-scale-cyber-attack-on-ukrainian-telecom-operators-websites], luettu 5.2.2024.
[504] SecurityLab.ru: К атаке на Rutube могут быть причастны бывшие сотрудники видеохостинга. *SecurityLab.ru*, 13.5.2022. [https://www.securitylab.ru/news/531621.php], luettu 4.2.2024; Toulas, Bill: Hackers display "blood is on your hands" on Russian TV, take down RuTube. *Bleeping Computer*, 9.5.2022. [https://www.bleepingcomputer.com/news/security/hackers-display-blood-is-on-your-hands-on-russian-tv-take-down-rutube/], luettu 5.2.2024.
[505] Telychko, Veronika: CrescentImp Malware Detection: Russia-Linked Sandworm APT Targets Ukrainian Media Organizations. SOCPrime, 14.6.2022. [https://socprime.com/blog/crescentimp-malware-detection-russia-linked-sandworm-apt-targets-ukrainian-media-organizations/], luettu 5.2.2024.
[506] Askew, Joshua: Eurovision 2022: Russian hackers targeted contest, say Italian police. *Euronews*, 16.5.2022. [https://www.euronews.com/culture/2022/05/16/eurovision-2022-russian-hackers-targeted-contest-say-italian-police], luettu 5.2.2024.
[507] Lyngaas, Sean: Pro-Russia hackers claim responsibility for 'intense, ongoing' cyberattack against Lithuanian websites. *CNN*, 27.6.022. [https://edition.cnn.com/2022/06/27/politics/lithuania-cyber-attack-pro-russian-group/index.htm], luettu 5.2.2024.
[508] CERT-EU (2023a).
[509] Miller, Maggie: Ukraine's largest telecom stands against Russian cyberattacks. *Politico*, 9.7.2022. [https://www.politico.com/news/2022/09/07/hackers-ukraine-telecom-00055060], luettu 5.2.2024.

vain yhden prosentin luokkaa. Verkkojen resilienssiä on selitetty sillä, että vielä vuoden 2023 helmikuussa Ukrainassa oli 25 IXP:tä, jotka toimivat 50 kohteessa, eikä verkossa ollut ruuhkapisteitä. Lisäksi mobiililaitteiden käyttö lisääntyi sodan ensimmäisinä kuukausina.[510] Kesäkuun 2022 loppuun mennessä teleliikenneyhteydet Ukrainan hallussa olevilla alueilla oli virallisten lähteiden mukaan pääsääntöisesti palautettu.[511] Informaatioinfrastruktuuriin ei julkisten tietojen mukaan kohdistunut uusia, merkittäviä kyberhyökkäyksiä. Mandiantin mukaan CaddyWiper-haittaohjelmaa kuitenkin käytettiin viisi kertaa touko-kesäkuussa, mutta kohteista ei ole tietoa.[512] Venäjän ohjusiskut jatkuivat koko kesä ajan, mutta niiden vaikutuksista informaatioinfrastruktuuriin on saatavilla vain vähän tietoa.[513]

Mielenkiintoisen lisän sotaan toivat Venäjän toteuttamat informaatioinfrastruktuurin kaappaamiset. Vallattujen alueiden internetliikenne uudelleen reititettiin Venäjän kautta. Hersonin alueen liikenne reititettiin Venäjälle lokakuuhun asti, jonka jälkeen Ukraina valtasi alueen takaisin. Muiden miehitettyjen alueiden liikenteen reititys on jäänyt pysyväksi.[514] Tämä tarkoittaa, että verkkoliikenne noilta alueilta kulkee mm. SORM, GosSOPKA ja TSPU-järjestelmien läpi eli on suodatettavissa ja pääosin läpinäkyvää viranomaisille. Venäjä on myös pyrkinyt sulkemaan valloittamiensa alueiden informaatiotilan läntiseltä informaatiolta mm. estämällä Instagrammin, YouTuben, Viberin, Twitterin ja Googlen hakukoneen käytön Donestkin, Luhanskin, Zaporižžjan ja Hersonin alueilla.[515] Näin Venäjä liitti kaappaamansa alueet osaksi suvereenia aluettaan myös kybertilassa.[516]

Touko-kesäkuu oli suurvaltojen välisen deterrenssiviestinnän huippukohta. Toukokuussa Venäjä ilmoitti olevansa valmis toimimaan, mikäli se yritettäisiin irrottaa globaalista internetistä.[517] Yhdysvallat eivät halunneet eskaloida tilannetta ja ilmoitti, ettei Venäjän irrottaminen internetistä ollut sen intresseissään ja Venäjän pitäminen kansainvälisessä informaatiotilassa oli itse asiassa Lännen etujen mukaista.[518] Kesäkuun alussa U.S. Cyber Commandin komentaja kenraali Paul Nakasone myönsi Yhdysvaltojen tukeneen Ukrainaa hyökkäyksellisillä kyberoperaatioilla. Myöhemmin kesäkuussa Naton Madridin huippukokouksessa hyväksytyssä strategisessa konseptissa sotilasliitto ilmoitti pitävänsä kyberhyökkäyksiä 5. artiklan aktivointiin mahdollisesti johtavana tapahtumana.[519] Venäjän ulkoministeriö vastasi pitkäaikaisen kyberdiplomaatti Andrei Krutskihin suulla Lännen pyrkimysten militarisoida informaatiotilan voivan johtaa suoraan sotilaalliseen yhteenottoon ja arvaamattomiin seurauksiin, ja

[510] Tomé, Belson & Berdan (2023).
[511] SSSCIP: Latest SSSCIP update on mobile communication, Internet, and digital television broadcasting in Ukraine as of 18:00, June 27, 2022. SSCIP, 27.6.2022. [https://cip.gov.ua/en/news/operativna-informaciya-derzhspeczv-yazku-pro-robotu-mobilnogo-zv-yazku-internetu-ta-cifrovogo-telebachennya-v-ukrayini-stanom-na-18-00-27-chervnya-2022-roku], luettu 5.2.2024.
[512] Greenberg (2022a).
[513] Missile Threat CSIS: Russian Missile Attacks on Ukraine. Kuva. n.d. [https://missilethreat.csis.org/wp-content/uploads/2022/03/Russian-Missile-Attacks-on-Ukraine-3.21.png], luettu 5.2.2024.
[514] Tomé, Belson & Berdan (2023).
[515] Lewis et al. (2023).
[516] Ristolainen, Mari: *Voiko informaatioajan valtio vapautua maantieteestä?* Puolustusvoimien tutkimuslaitos, Tutkimuskatsaus 3–2024. Riihimäki, 2024.
[517] РИА Новости: Пушков не исключил отключение России от глобального интернета. *РІА Новости*, 26.5.2022. [https://ria.ru/20220526/pushkov-1790880043.html], luettu 5.2.2024.
[518] SecurityLabs.ru: США призвали посредников со всего мира не отключать Россию от интернета. *SecurityLabs.ru*, 26.5.2022. [https://www.securitylab.ru/news/531896.php], luettu 5.2.2024.
[519] NATO: NATO 2022 Strategic Concept. Adopted by Heads of State and Government at the NATO Summit in Madrid 29 June 2022. [https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf], luettu 5.2.2024.

että Venäjä ei jätä vastaamatta aggressiivisiin toimiin.[520] Venäläiset eivät kuitenkaan ilmoittaneet toimiensa olevan asymmetrisiä, mikä osoitti, että he eivät itsekään halunneet antaa aihetta eskalaatiolle. Kesän kyberdeterrenssiviestintä sekoittui osaltaan Venäjän uhkailuun ydinaseiden käytöstä.[521] Venäjä pyrki rajoittamaan Lännen tukea Ukrainalle ja painostamaan sitä ja sen liittolaisia neuvotteluihin. Vaaralliseksi tilanteen teki se, että Venäjän ydinasedoktriini varaa oikeuden ydinaseiden käyttöön, mikäli sellaisiin valtion tai asevoimien kriittisiin objekteihin vaikutetaan, joiden vahingoittuminen voi estää ydinaseiden käytön.[522] Tahallaan, tahaton tai vahingossa tehty kyberhyökkäys Venäjän ydinasejärjestelmää vastaan kesän kiihtyneessä tilanteessa olisi voinut johtaa raskaisiin seurauksiin.

Ukrainalaiset valtiosidonnaiset haktivistit vastasivat Venäjän hyökkäyksiin. Sberpankin mukaan 65 miljoonan venäläisen tiedot oli vuodettu Internettiin kesäkuuhun mennessä erikoisoperaation alun jälkeen ja se kutsui Ukrainaa ”kansainvälisen terrorismin keskukseksi.”[523] Massiivisista palvelunestohyökkäyksistä oli tullut venäläisille arkipäivää.[524] Ukrainalaisten tai heidän sijaistoimijoidensa tai liittolaistensa tuhoavien kyberhyökkäysten puute venäläisiä kohteita vastaan kesällä 2022 on merkittäviä osoitus Venäjän sodan aikaisen deterrenssin tai sitten kyberpuolustuksen toimivuudesta. Viimeistään alkusyksystä olisi voinut olettaa Ukrainan kykenevän iskemään Venäjää vastaan merkittävällä tavalla. Vaikka osa hyökkäyksistä olisikin jäänyt salaisiksi, voidaan jälkikäteen sanoa, että niillä ei ollut vaikutusta Venäjän poliittisen päätöksentekoon. Asevoimiin kohdistuneista vaikutuksista on mahdoton sanoa mitään käytettävissä olevan aineiston perusteella. Venäjä asevoimien yleiseen kaaokseen keväällä ja kesällä ovat toki saattaneet tuoda oman lisänsä asevoimien johtamisjärjestelmien ja - verkkojen häiriöt.

5.7. Pitkä sota alkaa: Heinä-elokuu 2022

Heinäkuun puolivälissä Venäjä aloitti puoliviralliset mobilisaatiotoimet suurten tappioiden korvaamiseksi ja sitoutui poliittisesti pitkään sotaan. Voimakkaista tykistötaisteluista huolimatta rintamalinjat eivät juurikaan liikkuneet, eikä diplomatia edistynyt paitsi Mustanmeren viljatoimitusten osalta. Elokuun alusta viljakuljetukset pääsivät lähtemään Odessasta, mutta Venäjä hallitsi edelleen Mustaamerta. Venäjän hyökkäysvoima oli ehtynyt heinäkuun alkuun mennessä. Zaporižžjan ydinvoimalan kohtalo ja siihen liittyvä uhat hallitsivat diplomaattisia keskusteluja. Iran lupasi aloittaa lennokki-

[520] Исакова, Татьяна & Тишина, Юлия: МИД РФ видит угрозу прямого киберстолкновения с США. *Коммерсантъ*, 6.6.2022. [https://www.kommersant.ru/doc/5392410], luettu 5.2.2024.
[521] Sanger, David E. & Broad, William J.: Putin's Threats Highlight the Dangers of a New, Riskier Nuclear Era. *The New York Times*, 1.6.2022. [https://www.nytimes.com/2022/06/01/us/politics/nuclear-arms-treaties.html], luettu 5.2.2024.
[522] Lonergan, Erica & Yarhi-Milo, Keren: Cyber Signaling And Nuclear Deterrence: Implications For The Ukraine Crisis. *War on the Rocks*, 21.4.2022. [https://warontherocks.com/2022/04/cyber-signaling-and-nuclear-deterrence-implications-for-the-ukraine-crisis/], luettu 5.2.2024; Указ Президента Российской Федерации от 02.06.2020 no 355 Об Основах государственной политики Российской Федерации в области ядерного сдерживания. [http://static.kremlin.ru/media/events/files/ru/IluTKhAiabLzOBjIfBSvu4q3bcl7AXd7.pdf], luettu 5.2.2024.
[523] SecurityLab.ru: Хакеры с начала спецоперации на Украине украли данные 65 млн россиян. *SecurityLab.ru*, 16.6.2022. [https://www.securitylab.ru/news/532340.php], luettu 5.2.2024; Сбербанк: Украина – центр международного кибертерроризма. *SecurityLab.ru*, 16.6.2022. [https://www.securitylab.ru/news/532342.php], luettu 5.2.2024.
[524] Урманцева, Анна & Кильдюшкин, Роман: О дивный новый DDoS. Кто координирует кибератаки на Россию. *Газета.Ru*, 26.5.2022. [https://m.gazeta.ru/tech/2022/05/26/14903480.shtml], luettu 5.2.2024.

toimitukset Venäjälle, mikä oli ensimmäinen selkeä merkki Venäjän kyvystä hankkia merkittävää sotilaallista tukea ulkomailta operaatiolleen.[525]

FSB- ja SVR-sidonnaiset APT-ryhmät Gamaredon, InvisiMole, Dukes, Turla jatkoivat kesän ja syksyn aikana Ukrainan hallinnon, kriittisen infrastruktuurin toimijoiden ja asevoimien sekä Ukrainan liittolaisten aktiivista vakoilua.[526] Heinäkuussa 2022 Putin käski SVR:n työskentelemään sanktioiden vaikutusten vähentämiseksi. Tämä ei ainakaan välittömästi näkynyt SVR:n teollisuusvakoilun lisääntymisenä.[527] Edelleen APT29-uhkatoimija suoritti elokuussa verkkourkintahyökkäyksiä Teamsin kautta valtiollisia kohteita vastaan.[528] FSB levitti heinäkuussa Android sovellusta nimeltään CyberAzov, joka oli väitetysti tarkoitettu Venäjän hakkerointiin, mutta todellisuudessa pyrki selvittämään potentiaalisten käyttäjien henkilöllisyyden.[529] Vuodesta 2016 toiminut, henkilökohdennettuun verkkourkintaan erikoistunut Callisto/Coldriver/Seaborgium APT-uhkatoimija pyrki vakoilemaan ukrainalaista ja sen liittolaisten puolustusteollisuutta ja ajatuspajoja. Microsoft lamautti sen verkkourkintainfrastruktuurin elokuussa.[530] Myöhemmin joulukuussa 2023 Yhdysvallat nosti syytteet kahta FSB:n 18. Keskuksen työntekijää kohtaan samaisen kybervakoilukampanjan toteuttamisesta vuosina 2016–2022.[531] Yleisesti ottaen FSB:n ja GRU:n kybervakoiluoperaatiot eivät edes pyrkineet salaamaan toimintaansa ja osa operaatioista paljastui varsin nopeasti.[532]

GRU:n ohjaama XakNet tunkeutui energiayhtiö DTEK Groupin tietoverkkoihin kesällä 1.7., mutta ei aiheuttanut merkittävää vahinkoa. Samoihin aikoihin tehtiin risteilyohjusisku Kryvorizkan lämpövoimalaa vastaa.[533] Vastaavia tapauksia Microsoftin ja Ukrainan hallinto on käyttänyt todisteena kyber- ja kineettisen vaikuttamisen koordinoinnista.[534] Kuitenkin heinä-syyskuussa 71,3 % hyökkäyksistä oli palvelunestohyök-

---

[525] Vuosien 2022–2023 tapahtumien yleisestä kuvauksesta ks. House of Commons Library (2023).
[526] ESET: APT Activity Report T2 2022. ESET, 1.11.2022 (c). [https://www.eset.com/us/business/resource-center/reports/eset-apt-activity-report-t2-2022/], luettu 5.1.2024; Mahotra, Asheer & Venere, Guilherme: Gamaredon APT targets Ukrainian government agencies in new campaign, CISCO Talos Blog, 15.9.2022. [https://blog.talosintelligence.com/gamaredon-apt-targets-ukrainian-agencies/], luettu 5.2.2024; Unit 42: Russia's Trident Ursa (aka Gamaredon APT) Cyber Conflict Operations Unwavering Since Invasion of Ukraine. Unit 42, 20.12.2022. [https://unit42.paloaltonetworks.com/trident-ursa/], luettu 4.2.2024; Sharma, Srivathsa: Examining the Activities of the Turla APT Group. Trend Micro, 22.9.2023. [https://www.trendmicro.com/en_us/research/23/i/examining-the-activities-of-the-turla-group.html], luettu 5.2.2024.
[527] Martin, Alexander: Fears grow of Russian spies turning to industrial espionage. *The Record*, 14.9.2022. [https://therecord.media/fears-grow-of-russian-spies-turning-to-industrial-espionage], luettu 5.2.2024; Kremlin.ru: Владимир Путин поздравил сотрудников и ветеранов СВР со столетием нелегальной разведки. Kremlin.ru, 30.6.2022. [http://kremlin.ru/events/president/news/68790], luettu 5.2.2024.
[528] Gatlan, Sergiu: Russian hackers target govt orgs in Microsoft Teams phishing attacks. *Bleeping Computer*, 2.8.2023. [https://www.bleepingcomputer.com/news/security/russian-hackers-target-govt-orgs-in-microsoft-teams-phishing-attacks/], luettu 5.2.2024.
[529] Franceschi-Bicchierai, Lorenzo: Russia Released a Ukrainian App for Hacking Russia That Was Actually Malware. *Motherboard*, 19.7.2022. [https://www.vice.com/en/article/bvmnxd/russia-released-a-ukrainian-app-for-hacking-russia-that-was-actually-malware], luettu 5.2.2024.
[530] Microsoft: Disrupting Seaborgium's ongoing phishing operations. Digital Threat Analysis Center (DTAC), 15.8.2022. [https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/], luettu 5.2.2024; Page, Carly: Meet the prolific Russian espionage crew hacking spymasters and lawmakers. *TechCrunch*, 8.2.2023. [https://techcrunch.com/2023/02/08/seaborgium-cold-river-hacking/], luettu 5.2.2024.
[531] Greig, Jonathan: US charges two Russians in hacks of government accounts. The Record, 7.12.2023. [https://therecord.media/us-indictment-fsb-alleged-hacking-government-officials], luettu 5.1.2024.
[532] Smith (2022).
[533] CyberDaily.au: Russian hackers blamed for cyber-attack on Ukrainian energy firm DTEK Group. CyberDaily.au, 8.7.2022. [https://www.cyberdaily.au/critical-infrastructure/8008-russian-hackers-blamed-for-cyber-attack-on-ukrainian-energy-firm-dtek-group], luettu 5.2.2024.
[534] The Economic Security Council of Ukraine (2022).

käyksiä ja 80 % hyökkäyksistä oli haktivistien toteuttamia. Hyökkäysten kohteena olivat julkishallinto, media- ja ICT-sektorit. [535] Muunkin tyyppisiä operaatioita tehtiin. Sandworm käytti CaddyWiperia ainakin kahta Ukrainan paikallishallinnon kohdetta vastaan.[536] 21.7. kaksi ukrainalaista radioasemaa hakkerointiin ja ne lähettivät valheellista viestiä Zelenskiin joutumisesta sairaalaan.[537] 25.7. Ukrainalainen ISP joutui tietomurron kohteeksi ja siltä varastettiin 300GB dataa.[538] 19.8. Ukrainan hallintoon kohdistui tietomurto, jonka yhteydessä varastettiin satojentuhansien ihmisten henkilötietoja.[539] 16.8. tehtiin kyberhyökkäys Energoatomia vastaan.[540] Yhtiö julkaisi samana päivänä tietoja Zaporižžjan ydinvoimalan säteilyvaarasta ja IAEA valmistautui lähettämään tarkastajia voimalaan.[541] Kaikki mikä tapahtui Ukrainan ydinvoimaloiden ympärillä sai julkisuutta, joten kyberoperaatioita todennäköisesti käytettiin informaatiovaikuttamisen tukemiseen enemmän kuin oikeiden hyökkäysten valmisteluun. Kyberhyökkäykset, potentiaalisesti myös tuhoavat siis jatkuivat, mutta ne olivat aikaisempaa hajanaisempia ja usein kytkettyjä informaatiovaikuttamiseen. Kohteena olivat mediayritykset, teleliikenneyritykset ja energia-alan yritykset.

Kybertoimien käytöstä taistelun tukemiseksi kesällä 2022 on vähän todisteita. Venäläiset hakkerit pyrkivät tunkeutumaan useita kertoja kesän ja syksyn aikana eri menetelmillä taktisen tason johtamisjärjestelmä Kropyvaan sekä Delta tilannekuvajärjestelmään. Nämä järjestelmät tukeutuivat osaltaan sosiaaliseen mediaan ja internetyhteyksiin ja niitä käytettiin taistelijoiden omilta mobiililaitteilta. Ukrainalaisten mukaan hyökkäykset epäonnistuivat.[542] Lisäksi CERT-UA mukaan komissariaattien henkilötietojärjestelmät, rajavartioston satelliittipalvelut ja hallinnollinen Shliakh-järjestelmä sekä sisäiseen viestintään käytetyt Signal-viestintäpalvelun tilit ovat olleet etenkin FSB:n Gamaredonin hyökkäysten kohteena.[543] Lännen tiedustelusuorituskykyjen merkitys Ukrainan puolustukselle oli selvää, mutta niiden häirinnästä (satelliitit, signaalitiedustelu) ei ole julkisuudessa havaintoja. Todennäköisesti niihin kohdistettiin vähintään elektronista häirintää.[544] Kesään mennessä Venäjä oli saanut elektronisen sodankäynnin suorituskykynsä järjestykseen ja Ukrainan alkuvaiheen etulyöntiasema

[535] CyberPeace Institute (2022a).
[536] ESET (2022c).
[537] Antoniuk, Daryna: Ukrainian radio broadcaster hacked to spread fake news about Zelensky's health. *The Record*, 22.7.2022. [https://therecord.media/ukrainian-radio-broadcaster-hacked-to-spread-fake-news-about-zelenskys-health/], luettu 5.2.2024.
[538] CyberPeace Institute (2022a).
[539] CyberPeace Institute (2022a).
[540] The MOD of Lithuania (2023).
[541] The Economic Security Council of Ukraine (2022).
[542] The MOD of Lithuania (2023).
[543] SSSCIP (2022a).
[544] Satam, Parth: Russia's TOBOL EW System "Cuts Off" Starlink from It's Ground Terminals; How Did Moscow Delink the Starlink. *The Eurasian Times*, 24.4.2023. [https://www.eurasiantimes.com/russias-tobol-ew-system-cuts-off-starlink-from-its-ground-terminals/], luettu 5.2.2024; Stashevskyi, Oleksandr & Bajak, Frank: They're jamming everything: How secretive electronic warfare shapes war in Ukraine. The *Times of Israel*, 3.6.2022. [https://www.timesofisrael.com/theyre-jamming-everything-secretive-electronic-warfare-shapes-war-in-ukraine/], luettu 5.2.2024; Clark, Bryan: The Fall and Rise of Russian Electronic Warfare the Ukraine invasion has become an old-fashioned slog, enabling Russia to unleash its electronic weapons. *Spectrum IEEE*, 20.7.2022. [https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare], luettu 5.2.2024; Peck, Michael: Russia's electronic warriors are intercepting Ukrainian troops' communications and jamming their GPS-guided bombs, experts say. *Business Insider*, 4.7.2023. [https://www.businessinsider.com/russian-electronic-warfare-interfering-with-ukrainian-radios-bombs-2023-7?r=US&IR=T], luettu 5.2.2024.

lennokkien käytössä oli menetetty.[545] Elektronisen sodankäynnin suorituskykyjen palautuminen on saattanut vaikuttaa kyberoperaatioiden tehtäväkenttään ja koettuun hyödyllisyyteen informaatiosodankäynnin välineenä.

Venäläiset toimijat jatkoivat hyökkäyksiä Ukrainan liittolaisia vastaan. Heinäkuun puoliväliin mennessä Killnet oli julistanut ”sodan” kymmenelle valtiolle.[546] Venäjä jatkoi koko kesän kestäneitä informaatiovaikuttamisoperaatioitaan läntisillä sosiaalisen median alustoilla huolimatta yritysten lupauksista rajoittaa Venäjän vaikutusmahdollisuuksia.[547] Gamaredon yritti epäonnistuneesti tunkeutua Nato-maan öljynjalostamon tietoverkkoihin 30.8.[548] ja ColdRiver APT-uhkatoimija yritti päästä käsiksi Yhdysvaltojen ydinteknologiatutkimuslaitosten verkkoihin.[549] Nämä hyökkäykset saattoivat olla aitoja vakoiluyrityksiä tai sitten osa deterrenssiviestintää.

Taistelu informaatiotilan hallinnasta jatkui kiivaana. 5.8.2022 Ukraina hävitti ”miljoonavahvuisen” bottiverkon, jota oli käytetty Ukrainan johdon halventamiseen ja yhteiskunnallisten ristiriitojen lietsomiseen. Operaatiossa otettiin haltuun 5000 SIM-korttia ja 200 välityspalvelinta.[550] Venäjän tietoverkkoihin kohdistui ennen näkemätön määrä palvelunestohyökkäyksiä.[551] Kyberhyökkäykset teollisuutta vastaan kasvoivat Positive Technologies yrityksen mukaan 53 %.[552] Heinä-syyskuussa hyökkäysten painotus vaihtui Venäjän julkishallinnosta ja energiasta mediaan finanssisektorin pysyessä suosittuna kohteena. IT Army of Ukraine oli aktiivisin toimija. Sen ja Anonymousin tehtailemista tietovuodoista alkoi tulla Venäjän hallitukselle kiusallinen aihe.[553] Vaikka kyberhyökkäykset puolin ja toisin jatkuivat heinä-elokuussa, aikajakso oli kehittyneempien operaatioiden osalta selvästi rauhallisin koko vuonna. Huolimatta siitä, että palvelunestohyökkäykset kohosivat ennen näkemättömiin määriin, kestoihin ja intensiteettiin, ne eivät lamauttaneet kummankaan osapuolen yhteiskuntien toimintaa tai edistäneet informaatioylivoiman saavuttamista. Toisaalta informaatiokamppailu jatkui keskeytymättömänä ja hyökkäyksellisellä kybertoiminnalla oli siinä tehtävänsä.

---

[545] Watling & Reynolds (2022); Antoniuk, Daryna: How electronic warfare is reshaping the war between Russia and Ukraine. *The Record*, 16.8.2022. [https://therecord.media/how-electronic-warfare-is-reshaping-the-war-between-russia-and-ukraine], luettu 5.2.2024.

[546] Burgess, Matt: Russian ‘Hacktivists’ Are Causing Trouble Far Beyond Ukraine. *WIRED*, 11.7.2022. [https://www.wired.com/story/russia-hacking-xaknet-killnet/], luettu 5.2.2024.

[547] Oremus, Will & Zakrzewski: Big Tech Tried to Quash Russian Propaganda. Russia Found Loopholes. *The Washington Post*, 10.8.2022. [https://www.washingtonpost.com/technology/2022/08/10/facebook-twitter-russian-embassy-accounts-propaganda/?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202], luettu 5.2.2024.

[548] Unit 42 (2022).

[549] Pearson, James & Bing, Christopher: Exclusive: Russian hackers targeted U.S. nuclear scientists. *Reuters*, 7.1.2023. [https://www.reuters.com/world/europe/russian-hackers-targeted-us-nuclear-scientists-2023-01-06], luettu 5.2.2024.

[550] Petkauskas, Vilius: Ukraine dismantled million-strong disinformation bot farm. *Cybernews*, 5.8.2022. [https://cybernews.com/cyber-war/ukraine-dismantled-million-strong-disinformation-bot-farm/], luettu 5.2.2024.

[551] Ошанина, Олеся: Защищаясь от киберугроз. Как компании внедряли решения по информбезопасности от «Мегафона». *Ведомости*, 29.7.2022. [https://www.vedomosti.ru/partner/articles/2022/07/29/933346-zaschischayas-kiberugroz], luettu 5.2.2024.

[552] SecurityLab.ru: Positive Technologies: число атак на промышленность выросло на 53%. *SecurityLab.ru*, 8.9.2022 (a). [https://www.securitylab.ru/news/533812.php], luettu 5.2.2024.

[553] CyberPeace Institute (2022a).

5.8. Harkovan vastahyökkäys ja ohjusiskut: Syys-lokakuu 2022

Ukraina aloitti vastahyökkäyksen Hersonin suunnalla elokuun lopussa ja toteutti yllätyshyökkäyksen Harkovan suunnalla syyskuun alussa. Putin julisti puolittaisen mobilisaation 21.9. ja syyskuun lopussa Venäjä liitti valtaamansa alueet itseensä ja Itämerellä kulkevat Nord Stream-kaasuputket räjäytettiin. Venäjä johdon ydinaseen käyttöön liittyvät vihjailut kiristivät diplomaattista ilmapiiriä ja aiheuttivat huolta eskalaatiosta.[554] Lokakuun 10. päivä Venäjä teki ohjusiskun, joka oli alku talven kestäneelle Ukrainan sähköinfrastruktuuriin kohdistuneelle hyökkäysten sarjalle. Iskut aiheuttivat sähkökatkoja ympäri Ukrainaa. Voidakseen jatkaa iskuja Venäjä alkoi täydentää ohjusvarastojaan Iranilta hankituilla lennokeilla.[555]

SSSCIP:n tietojen mukaan kyberhyökkäysten määrä Ukrainaa vastaan, mukaan lukien kriittiset tietoturvatapahtumat, jatkoi kasvamistaan syksyllä 2022. SSSCIP tulkinnan mukaan hyökkäysten päätavoitteina oli vakoilu, ukrainalaisten pääsyn estäminen julkisiin informaatiopalveluihin ja informaation tuhoaminen. Valtiolliset tai niihin sidonnaiset toimijat olivat aktiivisimpia ja niiden kohteina olivat finanssi- ja kaupanala.[556] Esimerkiksi Mandiant paljasti FSB:n Turlan kybervakoiluoperaation, joka oli jatkunut ukrainalaisissa verkoissa joulukuusta 2021.[557] Cisco Talos puolestaan ilmoitti Gamaredonin kohdistaneen Ukrainan valtionhallintoon kybervakoilukampanjan.[558]

Venäjä aloitti lokakuussa ohjus- ja lennokki-iskujen sarjan Ukrainan sähköenergiainfrastruktuuria vastaan, joka kiihtyi talven edetessä.[559] Lokakuun iskut energiainfrastruktuuriin vaikuttivat merkittävästi internetyhteyksiin, mutta liikenne palasi lähes normaaliksi 12–24 tunnissa.[560] Kineettiseen vaikuttamiseen liittyi kyberhyökkäyskampanja. Todennäköisesti 10.10. Sandworm hyökkäsi energiasektorin kohteita vastaan samaan aikaan risteilyohjusiskun[561] kanssa uudella NikoWiper-haittaohjelmalla ja onnistui aiheuttamaan lyhyen sähkökatkon.[562] Sandworm tunkeutui Ukrainan sähköverkon OT-järjestelmiin aiheuttaen katkoksen ja sitten 12.10. käytti CaddyWiper-haittaohjelman uutta versiota hävittääkseen hyökkäyksen jäljet.[563] CaddyWiperia käytettiin ainakin neljä kertaa lokakuun aikana.[564] Ukrainan tiedustelupalvelun mukaan myös

[554] Pifer, Steven: Russia, nuclear threats, and nuclear signaling. Brookings, blogikirjoitus, 13.10.2023. [https://www.brookings.edu/articles/russia-nuclear-threats-and-nuclear-signaling/], luettu 5.2.2024.
[555] Vuosien 2022–2023 tapahtumien yleisestä kuvauksesta ks. House of Commons Library (2023).
[556] SSSCIP: The number of cyberattacks on Ukraine keeps increasing. SSSCIP, 10.11.2022. [https://cip.gov.ua/en/news/kilkist-kiberatak-na-ukrayinu-prodovzhuye-zrostati], luettu 5.2.2024.
[557] Groll. Elias: Notorious Russian hacking group appears to resurface with fresh cyberattacks on Ukraine. *Cyberscoop*, 6.1.2023. [https://cyberscoop.com/ukraine-turla-russia-cyberattacks/?utm_source=substack&utm_medium=email], luettu 5.2.2024.
[558] Mahotra & Guilherme (2022).
[559] Watts, Clint: Preparing for a Russian cyber offensive against Ukraine this winter. Microsoft, blogikirjoitus, 3.12.2022. [https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/], luettu 5.2.2024.
[560] Tomé, Belson & Berdan (2023).
[561] Hunder, Max & Landay, Jonathan: Russia launches biggest air strikes since start of Ukraine war. *Reuters*, 11.10.2022. [https://www.reuters.com/world/europe/russias-ria-state-agency-reports-fuel-tank-fire-kerch-bridge-crimea-2022-10-08/], luettu 5.2.2024.
[562] ESET: APT Activity Report T3 2022: Sandworm Deploying its Enhanced Wiper Arsenal. ESET, January 2023 (b). [https://www.eset.com/int/business/resource-center/reports/eset-apt-activity-report-t3-2022/], luettu 5.2.2024.
[563] Greenberg, Andy: Sandworm Hackers Caused Another Blackout in Ukraine—During a Missile Strike. *WIRED*, 9.11.2023. [https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/], luettu 5.2.2024.
[564] Greenberg (2022a).

marras-joulukuun ohjusiskuihin liittyi kyberhyökkäyksiä energiasektoria vastaan.[565] Syksyn 2023 energiainfrastruktuuriin kohdistunut hyökkäys oli selvin esimerkki kyber- ja kineettisten hyökkäysten vaikutusten koordinoinnista sitten maaliskuun.[566] Vaikka hyökkäysten päätavoitteena oli Ukrainan kansan taistelutahdon murtaminen, pakottaminen antautumaan, sähkökatkot vaikuttivat myös kybertilaan ja sitä kautta Ukrainan kykyyn toimia informaatiotilassa. Mikäli Venäjä ei voinut valloittaa Ukrainan informaatiotilaa, se saattoi estää sen käytön tuhoamalla tilan materiaalisen perustan. Venäjän valmius tuhota laaja-alaisesti yhteiskunnallista infrastruktuuria poliittisten päämäärien saavuttamiseksi näkyi niin syksyllä 2022 kuin syksyllä 2023.

Energiasektoriin kohdistuvien kyberhyökkäysten rinnalla Venäjä toteutti muitakin operaatioita. Ukrainan tiedustelupalvelun mukaan Venäjä pyrki saastuttamaan kaasu- ja vesihuoltoyritysten käyttämän ohjelmiston tuotantoketjuhyökkäyksellä. Hyökkäyksen ajankohta ei ole tiedossa.[567] 14.10. Sandworm teki kiristyshaittaohjelmahyökkäyksen liikenne- ja logistiikkayhtiöitä vastaan Ukrainassa ja Puolassa Prestige-haittaohjelmalla.[568] Prestige-hyökkäys oli poikkeava, koska aikaisemmin Venäjä ei ollut käyttänyt tuhoavaa haittaohjelmaa Ukrainan liittolaisia vastaan.[569] Caddywiper ja HermeticWiper-haittaohjelmista ilmestyi uusi versioita lokakuun alussa.[570] Huolimatta uusista, tuhoavista hyökkäyksistä, Ukrainan kyberturvallisuusjohtaja Victor Zhora totesi lokakuussa, että Venäjän kybertoiminta oli opportunistista ja vailla strategiaa.[571] Ydinasepuhe ja Venäjän kyberhyökkäykset Ukrainan tukijoita vastaan kuitenkin osoittivat Venäjän pyrkivän maksimoimaan toiminnan vapautensa ydinasepelotteen suojissa.

Haktivistien hyökkäykset Ukrainan tukijoita vastaan kasvoivat merkittävästi. Kohteina olivat etenkin Puola, Latvia ja Yhdysvallat. Hyökkäykset olivat lähes yksinomaan palvelunestohyökkäyksiä.[572] Haktivistit myös altistivat aktiivisuudella itsensä vastatoimille. Syyskuussa Meta purki alustoiltaan venäläisen informaatiovaikuttamiskampanjan. Siihen kuului kuusikymmentä valeverkkosivustoa ja tuhansia tilejä Metan palveluissa. Kampanja pyrki edistämään Venäjän narratiivia Ukrainan sodasta.[573] 23.9. SBU ilmoitti neutraloineensa ukrainalaisen hakkeriryhmän, joka oli välittänyt varastamiaan tietoja venäjämyönteisille propagandisteille.[574] Ukrainan ja Venäjän sodassa valtioiden

---

[565] АрміяInform: рф щодня здійснює понад 10 кібератак на стратегічні об'єкти України — керівник Департаменту кібербезпеки СБУ. АрміяInform, 9.11.2022. [https://armyinform.com.ua/2022/11/09/ponad-10-kiberatak-na-strategichni-obyekty/], luettu 5.2.2024.
[566] The MOD of Lithuania (2023), s. 9.
[567] Warsaw Security Forum (2023).
[568] Gatlan, Sergiu: Microsoft: New Prestige ransomware targets orgs in Ukraine, Poland. *Bleeping Computer*, 14.10.2022. [https://www.bleepingcomputer.com/news/security/microsoft-new-prestige-ransomware-targets-orgs-in-ukraine-poland/], luettu 5.2.2024.
[569] Google (2023).
[570] ESET (2023b).
[571] Nichols, Shaun: Ukraine: Russian cyber-attacks aimless and opportunistic. *TechTarget*, 26.10.2022. [https://www.techtarget.com/searchsecurity/news/252526575/Ukraine-Russian-cyber-attacks-aimless-and-opportunistic], luettu 5.2.2024.
[572] Cyber Peace Institute: Cyber Dimensions of the Armed Conflict in Ukraine. Quarterly Analysis Report Q4 October to December 2022. Cyber Peace Institute, 16.12.2022 (b). [https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q4-2022/], luettu 5.1.2024; CERT-EU (2023a).
[573] O'Sullivan, Donie: Meta shuts down covert influence campaigns it says were run from China and Russia. *CNN*, 27.9.2022. [https://edition.cnn.com/2022/09/27/tech/meta-china-russia-influence-campaigns/index.html], luettu 5.2.2024.
[574] Служба безпеки України: СБУ нейтралізувала хакерське угруповання, яке «зламало» майже 30 млн акаунтів громадян України та ЄС. Служба безпеки України, 23.9.2022. [https://ssu.gov.ua/novyny/sbu-neitralizuvala-khakerske-uhrupovannia-yake-zlamalo-maizhe-30-mln-akauntiv-hromadian-ukrainy-ta-yes?utm_source=substack&utm_medium=email], luettu 5.2.2024.

fyysiset rajat eivät asettaneet esteitä kybertoimijoille ja sisäpiiriuhka on todennäköisesti ollut etenkin sodan ensimmäisenä vuonna varsin korkea.

Kolmansiin maihin kohdistuneiden kyberhyökkäysten intensiteetti oli yhteydessä Ukrainan sotilaalliseen tukemiseen tai osallistumiseen Venäjä-vastaisiin sanktioihin.[575] Disinformaatio-operaatiot liittyivät usein taistelukentän tai poliittisiin tapahtumiin. Esimerkiksi lokakuussa Nord Stream -kaasuputkien räjähdyksen yhteydessä Venäjä toteutti disinformaatio-operaatioita.[576] Vaikuttamiselle oli mahdollisuuksia. Sota oli jo lokakuun puolivälissä kestänyt niin pitkään, että Lännen tuessa Ukrainalle alkoi esiintyä rakoilua. Ukrainan asevoimien tietoliikenneyhteydet olivat hetken aikaa vaarassa, kun Elon Musk harkitsi Starlink tuen lopettamista. Tuki kuitenkin lopulta jatkui, vaikkakin siinä myöhemmin esiintyi maantieteellisiä rajoituksia.[577] Myöhemmin Elon Muskin Twitteristä, tai X:stä, on sittemmin tullut kiistanalainen alusta omistajansa näkemysten vuoksi, mikä vain osoittaa, että Läntiset sosiaalisen media alustat eivät ole olleet suojassa sodan poliittisilta vaikutuksilta – eivätkä sodat sosiaaliselta medialta.

Venäjään kohdistuneiden kyberhyökkäysten vakavuudesta kertoo se, että maa menetti kuusi sijaa QuartorLabsin ylläpitämässä kansallisten internetsegmenttien kestävyyden tilastossa syyskuussa.[578] Alati jatkuvien palvelunestohyökkäysten lisäksi hakkerit onnistuivat murtautumaan Yandex Taxi -palveluun ja aiheuttivat sekasorron väärennetyillä tilauksilla.[579] Nöyryyttävintä lienee oli Roskomnadzoriin kohdistunut tietomurto ja sitä seurannut tietovuoto.[580] Viimeistään syksyllä maasta paenneiden IT-alan ammattilaisten puute alkoi aiheuttaa ongelmia koko yrityskentälle.[581]

5.9. Voimien kerääminen ohjusten varjossa: Marras-joulukuu 2022

Venäjä jatkoi vuodenvaihteen yli pommituskampanjaansa tavoitteenaan murtaa Ukrainan kansan puolustustahto tuhoamalla Ukrainan sähköverkko. Marraskuun alussa Ukraina vapautti hitaasti edenneiden taisteluiden jälkeen Hersonin ja alkoi vastaanottaa ulkomailta kehittyneitä ilmatorjuntajärjestelmiä, joiden avulla se kykeni rajoittamaan Venäjän pommituskampanjan vaikutuksia. Molemmat osapuolet pyrkivät palauttamaan joukkojensa taistelukyvyn ja rakentamaan uusia joukkoja voidakseen jatkaa sotaa seuraavana vuonna. Venäjä yrittäisi iskeä ensin.[582]

Ukrainan kyberturvallisuudesta vastaavien viranomaisten mukaan vuoden 2022 kyber- ja risteilyohjushyökkäykset oli synkronoitu vaikuttamaan sähköverkon eri osiin vaikutusten yhdistämiseksi.[583] Iskuilla oli vaikutusta Ukrainan tietoliikenneyhteyksiin.

---

[575] CyberPeace Institute (2022a).
[576] CERT-EU (2023a).
[577] Wikipedia: Starlink in the Russo-Ukrainian War. Wikipedia, 25.1.2024. [https://en.wikipedia.org/wiki/Starlink_in_the_Russo-Ukrainian_War], luettu 5.2.2024.
[578] Исакова, Татьяна: Один за сеть. *Коммерсантъ*, 7.9.2022. [https://www.kommersant.ru/doc/5548136], luettu 5.2.2024.
[579] Gordon, Aaron & Franceschi-Bicchierai, Lorenzo: Hackers Create Traffic Jam in Moscow by Ordering Dozens of Taxis at Once Through App. *VICE*, 2.9.2022. [https://www.vice.com/en/article/y3pbgy/hackers-create-traffic-jam-in-moscow-by-ordering-dozens-of-taxis-at-once-through-app], luettu 5.2.2024.
[580] Mozur, Paul, Satariano, Adam, Krolik, Aaron & Aufrichtig, Aliza: 'They Are Watching': Inside Russia's Vast Surveillance State. *The New York Times*, 22.9.2022. [https://www.nytimes.com/interactive/2022/09/22/technology/russia-putin-surveillance-spying.html], luettu 5.2.2024.
[581] SecurityLab.ru: В России не хватает десятков тысяч специалистов по кибербезопасности. *SecurityLab.ru*, 6.9.2022. [https://www.securitylab.ru/news/533776.php], luettu 5.2.2024.
[582] Vuosien 2022–2023 tapahtumien yleisestä kuvauksesta ks. House of Commons Library (2023).
[583] Warsaw Security Forum (2023).

Esimerkiksi marraskuun 23. päivän isku johti 50 % liikenteen vähenemiseen koko Ukrainassa puoleksitoista päiväksi. Joulukuusta eteenpäin liikenne ei enää palautunut yhtä nopeasti tai samalle tasolle.[584] Vaikuttaa kuitenkin siltä, että vuoden lopun lähestyessä pääosa Venäjän kyberhyökkäyksistä jäi haktivistien ja sijaistoimijoiden toteutettavaksi ja tiedustelupalvelut sekä asevoimat keskittyivät tiedonhankintaan. Risteilyohjuksia ja lennokkeja oli yksinkertaisesti helpompi käyttää sähköenergiainfrastruktuurin kohteita vastaan. Iskuja oli vuoden loppuun mennessä tehty yli seitsemäänsataan kriittisen infrastruktuurin kohteeseen.[585]

Marras-joulukuussa Ukrainaan kohdistuvien kyberhyökkäysten määrä jatkoi kasvuaan. Pääosa eli 87.3 % oli edelleen palvelunestohyökkäyksiä ja haktivistien, etenkin People's CyberArmyn, tekemiä. Pääkohteeksi nousi finanssisektori. Sitä seurasivat hallinto ja kuljetusala.[586] Mandiantin mukaan lokakuusta joulukuulle kestänyt GRU:n aktivoituminen perustui pitkälti rikollistyyppisten kiristyshaittaohjelmien käyttöön.[587] Marras-joulukuussa Sandworm hyökkäsi Ukrainan aseteollisuusalan yrityksiä vastaan ja käytti toisessa operaatiossa kiristysohjelmaa nimeltään RansomBoggs datan tuhoamiseen kohdejärjestelmissä.[588] Haktivistiryhmä NoName057(16) toteutti 3.12. alkaen kolme päivää kestäneen DDoS hyökkäyksen ukrainalaisen telekommunikaatioyrityksen palvelimia vastaan.[589] Marraskuussa Blackberry ilmoitti RomCom APT-uhkatoimijan jatkavan Ukrainan ja Nato-maiden asevoimiin kohdistuvaa kybervakoiluoperaatiota.[590] Taistelukentälle kyberoperaatiot eivät kuitenkaan vieläkään kunnolla ulottuneet. Joe Batemanin mukaan joulukuussa 2022 tiedossa ei ollut yhtään tapausta, jossa Venäjä olisi käyttänyt kyberhyökkäystä kentällä olevan sotilaskaluston toimintaan vaikuttamiseen.[591]

Microsoft varoitti vuoden lopulla Venäjän mahdollisesti valmistelevan uusi tuhoavia hyökkäyksiä ukrainalaista ja eurooppalaista kriittistä infrastruktuuria vastaan.[592] Microsoftin mukaan Killnet aloittikin sairaaloihin kohdistuvan palvelunestohyökkäysten sarjan marraskuussa, joka jatkui ainakin helmikuulle 2023.[593] 23.11. Killnet väitti toteuttaneensa palvelunestohyökkäyksen Euroopan parlamentin verkkosivuja kohtaan.[594] Aikaisemmin lokakuussa se väitti iskeneensä usean Yhdysvaltojen osavaltion

[584] Purtill, James: The battle to keep Ukraine connected to the Internet Amid Russian missile attacks. *ABC News*, 26.2.2023. [https://www.abc.net.au/news/science/2023-02-27/ukraine-internet-russia-rocket-strikes-connected-kyiv/102009234?utm_source=substack&utm_medium=email], luettu 5.2.2024.
[585] Жерновская, Людмила: Стало известно, сколько объектов критической инфраструктуры повредила РФ. *УНІАН*, 28.12.2022. [https://www.unian.net/war/skolko-obektov-kriticheskoy-infrastruktury-postradali-iz-za-atak-rf-12092418.html], luettu 5.2.2024.
[586] Cyber Peace Institute (2022b).
[587] Freedberg, Sydney J.: Faltering against Ukraine, Russian hackers resort to ransomware: Researchers. *Breaking Defense*, 18.4.2023. [https://breakingdefense.com/2023/04/faltering-against-ukraine-russian-hackers-resort-to-ransomware-researchers/], luettu 5.2.2024.
[588] Google (2023); ESET (2023b); Lakshmanan, Ravie: New Report Reveals NikoWiper Malware That Targeted Ukraine Energy Sector. *The Hacker News*, 31.1.2023. [https://thehackernews.com/2023/01/new-report-reveals-nikowiper-malware.html], luettu 5.2.2024.
[589] Cyber Peace Institute (2022b).
[590] BlackBerry: RomCom Threat Actor Abuses KeePass and SolarWinds to Target Ukraine and Potentially the United Kingdom. BlackBerry, blogikirjoitus, 11.2.2022. [https://blogs.blackberry.com/en/2022/11/romcom-spoofing-solarwinds-keepass], luettu 5.2.2024.
[591] Bateman (2022).
[592] Cyber Peace Institute (2022b).
[593] Greig, Jonathan: Pro-Russia hackers are increasingly targeting hospitals, researchers warn. *The Record*, 19.3.2023. [https://therecord.media/killnet-ddos-hospitals-healthcare-russia?utm_source=substack&utm_medium=email], luettu 5.2.2024.
[594] CERT-EU (2023a).

lentoaseman verkkoihin.[595] Merkittävää tuhoavien kyberhyökkäysten sarjaa ei kuitenkaan tehty ja vuoden 2022 aikana ei lopulta tapahtunut pelättyä vakavien venäläisten kyberoperaatioiden laajentumista EU- ja Nato-maihin. Mielenkiintoinen muutos oli kuitenkin häiritsevien ja lamauttavien hyökkäysten kohdistuminen finanssisektoriin ja yhteiskunnallisiin palveluihin. Joko näiden katsottiin tarjoavan parempia vaikutusmahdollisuuksia kuin energia- ja teleliikennejärjestelmien häirintä, patrioottisille hakkereille piti löytää sopivampia kohteita tai sitten ohjusiskuihin liitetyn kyberhyökkäyskampanja ”ammukset” oli nopeasti käytetty.

Venäjän informaatiovaikuttamista tukevat kyberoperaatiot jatkuivat vuoden loppuun, mutta eivät ilman vastarintaa. Joulukuussa Ukraina hävitti 13 bottiverkkoa, jotka käyttivät 1.5 miljoonaa venäjämyönteistä propagandaa levittävää tiliä.[596] Google väitti keskeyttäneensä 1950 Venäjän informaatiovaikuttamistapahtumaa alustoillaan vuonna 2022.[597] Päätoimijoiksi se nimesi Internet Research Agencyn, Krymskybridge-konsulttifirman ja FSB/GRU sidonnaisen News Frontin. Huolimatta siitä, että Lännessä kiinnitettiin paljon huomiota Venäjän Länteen kohdistuneeseen informaatiovaikuttamiseen, joka oli todellinen ilmiö[598], sen pääkohteina ovat olleet Venäjän sisäinen yleisö ja sisältökieli on ollut suurilta osin venäjä.[599] Sota ja sen herättämät intohimot ja tarpeet eri ihmisryhmissä alkoivat alkuhämmennyksen jälkeen vetää puoleensa rikollisia. Kyberrikolliset pyrkivät hyötymään Ukrainan sodasta levittäen tietoja varastavia haittaohjelmia Telegram kanavilla. Haittaohjelmat teeskentelivät olevansa Venäjän vastaisen taistelun välineitä.[600]

Cyber Peace Instituten mukaan loka-joulukuussa Venäjään kohdistuneet hyökkäykset vähenivät ja pääosa kohdistui ICT-sektoria vastaan. Taustalla lienee vaikuttanut kansainvälisten haktivistien innon laantuminen. 11.10.2022 IT Army of Ukraine hyökkäsi Pietarin alueella toimivaa sähköverkkoyritystä vastaan, mutta vahingot jäivät vähäisiksi. Toisen hyökkäyksen tuloksena kolmen miljoonan venäläisen henkilötiedot päätyivät internettiin eri tietovuotojen takia. 31.12.2022 IT Army of Ukraine pyrki sabotoimaan Venäjän presidentin uuden vuoden puhetta.[601] 17.12. VTB pankkiin kohdistui sen historian suurin palvelunestohyökkäys, eikä pääosa sen palveluista ollut käytettävissä.[602] Selvä poikkeus aikaisempaan oli Venäjän oikeus- ja paikallishallintoon kohdistunut tuhoava CryWiper-haittaohjelmahyökkäys joulukuussa.[603] Venäjän sisäisistä

---

[595] SecurityWeek: US Airport Websites Hit by Suspected Pro-Russian Cyberattacks. *SecurityWeek*, 10.10.2022. [https://www.securityweek.com/us-airport-websites-hit-suspected-pro-russian-cyberattacks/], luettu 5.2.2024.

[596] Кіберполіції України: Кіберполіція провела загальнонаціональну операцію з припинення діяльності ворожих ботоферм. Кіберполіції України, 20.12.2024. [https://cyberpolice.gov.ua/news/kiberpolicziya-provela-zagalnonaczionalnu-operacziyu-z-prypynennya-diyalnosti-vorozhyx-botoferm-7521/?utm_source=substack&utm_medium=email], luettu 5.2.2024.

[597] Google (2023).

[598] Geissler, D., Bär, D., Pröllochs, N. (et al.): Russian Propaganda on Social Media During the 2022 Invasion Of Ukraine. *EPJ Data Science*, 12/2023. [https://doi.org/10.1140/epjds/s13688-023-00414-5]

[599] OECD: Disinformation and Russia's war of aggression against Ukraine. Threats and governance responses. OECD, 3.11.2022. [https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/], luettu 5.2.2024.

[600] CISCO (2023).

[601] Cyber Peace Institute (2022b).

[602] Toulas, Bill: Massive DDoS attack takes Russia's second-largest bank VTB offline. *Bleeping Computer*, 6.12.2022. [https://www.bleepingcomputer.com/news/security/massive-ddos-attack-takes-russia-s-second-largest-bank-vtb-offline/], luettu 5.2.2024.

[603] Goodin, Dan: Never-before-seen malware is nuking data in Russia's courts and mayors' offices. *ARS Technica*, 2.12.2022. [https://arstechnica.com/information-technology/2022/12/never-before-seen-malware-is-nuking-data-in-russias-courts-and-mayors-offices/], luettu 5.2.2024; Securelist: Новый троянец CryWiper

jännitteistä tai mahdollisesti Ukrainan epäsuorien keinojen käytöstä kertoi se, että ensimmäistä kertaa konfliktin alun jälkeen venäläismieliset toimijat hyökkäsivät venäläiskohteita vastaan ja XakNet ja Killnet ottivat yhteen käyttäen palvelunestohyökkäyksiä hyökkäyksillä.[604] Käytettävän lähdeaineiston valossa näyttää siltä, että Ukrainan kybertoiminta muuttui hetkeksi aikaa aggressiivisemmaksi vuoden 2022 lopulla. Tämä oli todennäköisesti seurausta halusta kostaa Venäjän ohjus- ja lennokki-iskut.

5.10. Yhteenveto vuodesta 2022

Venäjä pyrki sotataidollisten oppiensa mukaisesti hankkimaan informaatioylivoiman jo ennen hyökkäysoperaation alkua tai aivan viimeistään hyökkäyshetkellä. Tässä se epäonnistui. Venäjä pyrki oikeuttamaan hyökkäyksensä kansainvälisen yleisön silmissä, provosoi ja pyrki harhauttamaan Ukrainaa ja sen tukijoita kyberoperaatioilla ja tuki Ukrainan puolustustahdon rapauttamista informaatiovaikuttamisella kyberhyökkäyksin. Voidaan pohtia, oliko tammi-helmikuun hyökkäysoperaatioiden tarkoitus pelkästään painostaa vai virittää ukrainalaiset pelko- ja tappiomielialaan, kun voimaa lopulta käytettäisiin? Kybermenetelmin toteutettu tiedonhankinta ja kyberhyökkäysten valmistelu oli keskeinen osa Venäjän toimintaa ennen operaation alkua. Hyökkäyksen alkuvaiheen kyberoperaatioiden oli tarkoitus yhdessä kineettisen vaikuttamisen kanssa taata tilapäinen, mutta riittävä informaatioylivoima.

Hyökkäysoperaation edetessä Venäjän kyberhyökkäysten tavoite muuttui kaappaushyökkäyksen tukemisesta, informaatioylivoiman varmistamiseen ja Ukrainan neuvotteluihin pakottamiseen ja sitten tiedonhankintaan ja laaja-alaiseen informaatiopsykologisen vaikuttamisen tukemiseen, kunnes lopulta palasi ohjusiskujen yhteydessä antautumiseen pakottamiseen kriittiseen infrastruktuurin vahingoittamisen kautta. Venäjän toiminnasta on erotettavissa ainakin kolme selkeää kampanjaa: hyökkäyksen ensivaihe, sitä seurannut pakottaminen ja kamppailu informaatiotilasta ja syksyn ohjusiskuja tukenut toiminta, joka saattoi myös olla sidoksissa Ukrainan vastahyökkäykseen Harkovan ja Hersonin suunnilla. Kampanjoista huolimatta deterrenssiviestintä, tiedonhankinta ja informaatiovaikuttaminen olivat jatkuvasti osa Venäjän toimintaa ja ne laajensivat sodan vaikutukset Ukrainan ja Venäjän rajojen ulkopuolelle. Ajan kuluessa valmistelluista ja suunnitelluista hyökkäyksistä siirryttiin nopeammin toimeenpantuihin operaatioihin ja kriittiseen infrastruktuuriin kohdistuvat operaatiot vähenivät suhteessa palvelunestohyökkäyksiin ja informaatiovaikuttamisen tukemiseen.[605]

Venäjän kybertoiminnan kehitys ei ollut suoraviivaista tai vailla merkittäviä poikkeuksia. Venäjä pyrki uusimaan tuhoavien kyberhyökkäysten kampanjan maalis-huhtikuussa, jolloin kyberhyökkäyksillä oli vielä mahdollisuus vaikuttaa operaation kehittymiseen. Se jatkoi yksittäisiä tuhoavia kyberhyökkäyksiä tai niiden valmistelua kesän ajan ja syksyllä kyberhyökkäyksiä käytettiin osana Ukrainan sähköinfrastruktuuriin kohdistuvaa kampanjaa. Ukrainan asevoimien johtamisyhteydet olivat todennäköisesti jatkuvasti kyberoperaatioiden ja elektronisen häirinnän kohteena. Häiritsevien ja informaatiovaikutuksia tukevien hyökkäysten intensiteetti laski kesällä, mutta nousi jälleen syksyllä ja alkoi kohdistua Ukrainaa tukevia maita kohtaan. Joulukuussa nähtiin tällaisten hyökkäysten huippu. Haktivistien näkyvä rooli kasvoi jatkuvasti – erilaiset

прикидывается шифровальщиком. Securelist, 1.12.2022. [https://securelist.ru/novyj-troyanec-cry-wiper/106114/?utm_source=substack&utm_medium=email], luettu 5.2.2024.

[604] Cyber Peace Institute (2022b).

[605] Giles (2023), s. 8–10.

ryhmät liittoutuivat keskenään ja erosivat. Painotusten muutokset vastasivat yhtäältä venäläistä informaatiosodankäyntiin liittyvää ajattelua, mutta olivat myös yhteydessä taistelukentän tapahtumiin ja heijastelivat kybersodankäynnin realiteettien muutoksia. Syksyn ohjusiskut heijastelivat ajatuksia kriittiseen infrastruktuuriin kohdistuvasta strategisesta operaatiosta, jolla Ukraina olisi pakotettu lopettamaan sota Venäjälle suotuisilla ehdoilla. Se myös osoitti, että ideat epäsuoruudesta ja asymmetriasta, ainakin vahvemman asymmetriasta, vaikuttivat edelleen Venäjän asevoimien ajatteluun. Yhteenvetona voidaan todeta, että Venäjän hyökkäyksellinen kybertoiminta ei ollut kaavamaista vaan kehittyi jatkuvasti. Se ei kuitenkaan johtajanut hyökkäysten vaikuttavuuden kasvuun.

Ukraina rekisteröi vuonna 2022 lähes kolme kertaa enemmän kyberturvallisuuspoikkeamia kuin vuonna 2021 ja virallisesti havaittuja kyberhyökkäyksiä oli 2194.[606] CERT-UA mukaan eniten kyberhyökkäyksiä Ukrainassa kohdistui vuonna 2022 energia- ja logistiikkayhtiöihin, keskeisiin ministeriöihin ja asevoimiin sekä rajavartiolaitokseen.[607] Kybertoiminnasta 36 % oli kybervakoilua ja 12 % tuhoavia hyökkäyksiä.[608] Vakavuudeltaan kriittiset ja korkeat tietoturvatapahtumat keskittyivät tammi-huhtikuuhun. Touko-kesäkuu olivat hiljaisempaa aikaa, mutta heinäkuusta erityyppisten hyökkäysten aktiivisuus alkoi kasvaa. Syksyllä intensiteetissä esiintyi vaihtelua mutta, joulukuussa vakavien tietoturvatapahtumien määrä nousi lähes sodan alun tasolle.[609] CERT-UA ja Mandiant ovat väittäneet, että kesäkausi käytettiin uusien operaatioiden valmisteluun – kyberoperaatiot yritettiin synkronoida sotatoimen osaksi – jotka toimeenpantiin syksyllä ja loppuvuodesta. Venäjän kyberhyökkäysten painopiste siirtyi 2022 syksyllä media- ja teleliikennepalveluista energiajärjestelmään, yhteiskunnallisiin palveluihin ja finanssisektoriin.[610] Mandiant jäljitti 19 Venäjän tekemään tuhoavaa kyberhyökkäystä vuonna 2022.[611] Toisen tutkimuksen mukaan ensimmäisen neljän kuukauden aikana Venäjä käytti 8–10 uutta tuhoavaa haittaohjelmaa, pääsääntöisesti wiper-tyyppisiä, tai versioita niistä 48–56 kohdetta vastaan. Ensimmäisen viikon aikana 22 organisaatiota joutui kohteeksi. Seuraavan viiden viikon aikana hyökkäyksiä oli kolme viikossa, minkä jälkeen enää yksi viikossa, eikä uusia haittaohjelmia juurikaan esiintynyt. Syksyllä esiintyi jälleen muutamia uusia tuhoavia hyökkäyksiä. Yleisesti ottaen hyökkäyksistä tuli ajan kuluessa vähemmän sofistikoituneempia. Tarkat kohteet tai haittaohjelmien vaikutukset eivät ole tiedossa.[612] Mandiantin mukaan etenkin GRU pyrki sitomaan tuhoaviin kyberoperaatioihinsa informaatiopsykologisen vaikutuksen julkistamalla tietoa operaatioistaan sijaistoimijoiden kautta.[613] Microsoft on raportoi-

[606] Eri lähteet määrittelevät hyökkäykset hyvin eri tavoin, joten hyökkäyksien numeraaliset määrä eivät anna kuvaa todellisesta tilanteesta tai vaikutuksista. Saman lähdesarjan sisällä ne toimivat parhaiten suhdelukuina. Esimerkiksi Ukrainan tiedustelupalvelu on ilmoittanut hyökkäyksiä olleen vuonna 2022 4200 ja vuonna 2021 1400 (Nilsson (2023))
[607] SSSCIP (2022a).
[608] CERT-EU (2023a).
[609] Freedberg, Sydney J.: Faltering against Ukraine, Russian hackers resort to ransomware: Researchers. *Breaking Defense*, 18.4.2023. [https://breakingdefense.com/2023/04/faltering-against-ukraine-russian-hackers-resort-to-ransomware-researchers/], luettu 5.2.2024; SSSCIP (2022a); CERT-EU (2023a).
[610] SSSCIP (2022a); Cyber Peace Institute (2022b); Black, Dan & Roncone, Gabby: The GRU's Disruptive Playbook. Mandiant, 12.7.2023. [https://www.mandiant.com/resources/blog/gru-disruptive-playbook], luettu 5.2.2024.
[611] Greenberg (2022a).
[612] Bateman (2022).
[613] Black & Roncone (2023).

nut samasta menettelytavasta.[614] Tietoturvayhtiöiden raporteista ei saa täsmällistä kuvaa hyökkäysten määristä, kohteista tai vaikutuksista. Ajoittain ne ovat keskenään ristiriitaisia. Yleiset trendit ja painotuksen muutokset niistä ovat kuitenkin pääteltävissä.

Venäjään kohdistui huomattavasti vähemmän tuhoavia kyberhyökkäyksiä kuin Ukrainaan, vaikka osa TV- ja radiolähetysten sotkemisista saavuttikin varmasti näkyvyyttä. Kybersodan luonteesta kertoo se, että vuosi 2022 oli huippuvuosi Venäjällä niin palvelunestohyökkäyksissä, tietovuodoissa kuin piratismin kasvussakin, millä oli suora vaikutus kyberturvallisuuden heikkenemiseen.[615] Venäjä joutui kiistatta voimakkaiden kyberhyökkäysten kohteeksi, joita todennäköisesti koordinoitiin Ukrainan valtion toimesta. Toiminta oli kuitenkin opportunistista, pyrki näkyvyyteen ja oli todennäköisesti eskalaatiouhan rajoittamaa. Käytössä olevan aineiston perusteella vaikuttaa siltä, että Ukrainan valtion ja sitä tukevien aktivistien hyökkäysten päämääränä oli informaatiovaikuttamisen tukeminen. Ehkä osittain siksi, että muuhun ei ollut ehditty valmistautua, ja ehkä osittain Ukrainan liittolaisten asettamien epävirallisten rajoitusten johdosta.

Mobiiliverkkoihin kohdistuneilla kyberoperaatioilla oli vaikutusta niin Ukrainaan kuin Venäjään. Molemmat yrittivät käyttää hyökkäyksen alkuvaiheessa Ukrainan mobiiliverkkoja joukkojen johtamiseen ja vastapuolen tiedusteluun. Näistä syistä ja siksi, että Venäjän kaappaushyökkäys ei sitä edellyttänyt, Venäjä ei mahdollisesti edes pyrkinyt täysin tuhoamaan Ukrainan mobiiliverkkoja.[616] Toisaalta Venäjä kohdisti teleliikenneoperaattoreihin lamauttavia kyberiskuja eli niiden merkitys informaatiosodankäynnille tunnistettiin. Kenties vaikuttamista ei haluttu tehdä kineettisin keinoin tai kybertoimet vaikuttivat lupaavammilta. Ukrainan kokoisen maan mobiiliverkkojen kineettinen tuhoaminen olisi vaatinut pidempää ja intensiivisempää pommituskampanjaa kuin mihin Venäjä oli varautunut ja mihin sillä oli lopulta mahdollisuus. Venäjä kylläkin pyrki hyökkäyksen myöhemmissä vaiheissa tuhoamaan ja häiritsemään Ukrainan teleliikenneverkkoja rintaman lähellä. Syksyn 2022 ohjushyökkäykset vaikuttivat suoraan teleliikenteen toimivuuteen. Mobiiliverkkoihin kohdistunut vaikuttaminen seurasi siis operaation kehitystä. Sitä ei ainakaan täysin ohjannut Venäjän tiedustelun tarpeiden asettaminen vastustajan johtamisyhteyksien lamauttamisen edelle.

Venäjä oli jo 2014 kaapannut ja siirtänyt osaksi omaa informaatiotilaansa Krimin ja osan Donetskin ja Luhanskin alueen informaatioinfrastruktuurista. Vuoden 2022 aikana se irrotti Ukrainan informaatiotilasta valloittamansa alueet ottamalla haltuun kiinteän infrastruktuurin ja mobiiliverkot ja reitittämällä niiden liikenteen Venäjälle omien valvonta- ja hallintamekanismiensa läpi. Informaatioinfrastruktuurin kaappaaminen mahdollisti vallattujen alueiden informaatiotilan eristämisen.[617] Toimenpide myös ulotti Venäjän informaatiosuvereniteetin Ukrainan alueelle ja osoitti, kuinka

[614] Microsoft: Microsoft Digital Defense Report. Building and improving cyber resilience. Microsoft, October 2023 (a). [https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023], luettu 5.2.2024.
[615] Roskomsvoboda: «Сетевые свободы»: 2022 год стал рекордным по количеству и объёму утечек. *Roskomsvoboda*, 22.12.2022. [https://roskomsvoboda.org/post/setevye-svobody-utechki/], luettu 5.2.2024; Roskomsvoboda: Правообладатели зафиксировали в 2022 году рост пиратства в России. *Roskomsvoboda*, 19.1.2023. [https://roskomsvoboda.org/post/s-feb-2022-vyroslo-piratstvo/], luettu 5.2.2024; Toulas, Bill: Russia's largest ISP says 2022 broke all DDoS attack records. *Bleeping Computer*, 23.1.2023. [https://www.bleepingcomputer.com/news/security/russia-s-largest-isp-says-2022-broke-all-ddos-attack-records/], luettu 5.2.2024.
[616] Giles (2023), s. 21–24.
[617] Saman ajatuksen on esittänyt myös Giles (2023), s. 22–23.

kybertilan kautta myös informaatiotila voidaan valloittaa ja pitää.[618] Toki myöhemmin Venäjän menetti osan Hersonin ja Harkovan alueesta takaisin Ukrainalle.

Pitkäaikainen mobiiliverkkojen, teleliikennesatelliittien ja GPS-signaalin häirintä rintama-alueiden läheisyydessä on osoittanut, että kyber- ja informaatiotilan käytön kiistämisellä voi olla maantieteellisesti laaja-alainen ja ajallisesti pitkäaikainen ulottuvuus. Ukrainan käyttöön ottama Starlink-järjestelmä on taas osoittanut, kuinka hankalaa informaatiotila on saada tottelemaan suvereniteetin rajoja ja että avaruus on huomioitava uudella tavalla rajoja tai puolustuslinjoja rakennettaessa. Informaatiosodankäynnin informaatioteknologisilla toimilla ja kääntäen informaatioteknologian kehityksellä on geopoliittisia ja -ekonomisia vaikutuksia, jotka eivät ole täysin valtioiden käsissä.

EU-CERT:n mukaan vain 32 % kaikista Venäjään liitetyistä kyberhyökkäyksistä kohdistui Ukrainaan. Muista maista eniten hyökkäyksiä kohdistui Puolaan ja Baltian maihin. Hyökkäykset Euroopassa ja Yhdysvalloissa kohdistuivat julkishallintoon, puolustussektoriin, ICT-alaan, järjestökenttään, energia- ja mediasektoriin sekä logistiikkaan ja kuljetuksiin.[619] Googlen mukaan verkkourkintakampanjoiden määrä Nato-maissa nousi sodan alettua 300 %.[620] Tietoa etsittiin mm. valloitettujen alueiden asukkaista ja energiasektorin haavoittuvuuksista.[621] Vuonna 2022 haktivistien hyökkäykset olivat pääsääntöisesti palvelunestohyökkäyksiä ja jossain määrin tietovuotoja ja verkkosivujen sotkemisia. Kohteet vaihtelivat julkishallinnosta kriittisen infranoperaattoreihin ja hyökkäykset liittyivät yleensä poliittisiin tapahtumiin.[622] Ukrainan tuen eturintamassa olleeseen Viroon kohdistui aikaisempaan vuoteen verrattuna vuonna 2022 neljä kertaa enemmän hyökkäyksiä. Hyökkäysten vaikutus oli marginaalinen.[623] Jopa eri maiden ja EU:n parlamentteihin kohdistuneet hyökkäykset jäivät vaikutuksiltaan vähäisiksi.[624] Varsinaisia tietovuotoja on dokumentoitu vain viisi ja niistäkin kolme XakNetin toimesta. Venäjään on kohdistunut samaan aikaan 63 tietovuotoa.[625] Haktivistienkin toiminnassa painopiste muodostui lopulta informaatiovaikuttamisen tukemiseen. Atlantic Councilin tutkijoiden mukaan Venäjä harrasti ”narratiivista sodankäyntiä”, jossa pyrittiin rapauttamaan luottamusta Ukrainaan sosiaalisen median valetilien, bottien ja sisältöhakujen manipulaation kautta.[626] Näillä operaatioilla oli globaali luonne.[627]

Kybersodankäynnin toimijakentän laajentuminen vaikutti kybersodan kuvaan. Haktivistiorganisaatiot kehittyivät sodan kuluessa ja Venäjän tiedustelupalveluiden kybertoimijat muuttuivat kulutussodan iskujoukoiksi. On mahdollista, että osa sodan myöhempien vaiheiden operaatioista perustui eri toimijoiden pyrkimykseen osoittaa oma hyödyllisyytensä.[628] Tällöin kaikkea haktivistien toimintaa ei voi pitää ohjattuna. Venä-

[618] Ristolainen (2024).
[619] CERT-EU (2023a).
[620] Google (2023).
[621] The MOD of Lithuania (2023), s. 58.
[622] CERT-EU (2023a).
[623] Oyetunde, Blessing: Estonia saw a record number of cyber-attacks in 2022. E-Estonia, 27.3.2023. [https://e-estonia.com/in-2022-estonia-had-the-highest-number-of-cyber-attacks/], luettu 5.2.2024.
[624] Lonergan (2023); The Economic Security Council of Ukraine (2022).
[625] CyberPeace Institute: Timeline. CyberPeace Institute, 13.11.2023 (a). [https://cyberconflicts.cyberpeaceinstitute.org/threats/timeline], luettu 5.2.2024.
[626] Osadchuk, Roman: *Undermining Ukraine. How the Kremlin employs information operations to erode global confidence in Ukraine*. Atlantic Council, February 2023. [https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine/], luettu 5.2.2024.
[627] Mueller et al. (2023); The MOD of Lithuania (2023).
[628] Levite, Ariel E.: *Integrating Cyber into Warfighting: Some Early Takeaways From the Ukraine Conflict*. Carnegie Endowment for International Peace, April 2023. [https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine/], luettu 5.2.2024.

jällä käytiin jonkin verran keskustelua haktivistien yhdistämisestä yhden organisaation alle ja heidän roolinsa virallistamisesta.[629] Nämä keskustelut eivät vielä vuoden 2022 aikana johtaneet mihinkään. Ukrainan IT Army jatkoi toimimista valtiosta erillisenä organisaationa, mikä asetti sen kansainvälisen lain osalta suojattomaan tilaan.[630]

Venäjän hyökkäysoperaation seurauksena globaali kybertila muuttui. Esimerkiksi kyberrikollisten ekosysteemi järkkyi. ESET ja Ciscon Talos ovat todenneet vuoden 2022 raporteissa globaalin kyberrikollisuuden vähentyneen vuoden 2022 aikana osittain sodasta johtuneista syistä. Myös kyberrikollisten kiristyshaittaohjelmapalvelut (Ransomware-as-a-Service – RaaS) ovat joutuneet hyökkäysten kohteeksi, kenties osittain sivullisina uhreina.[631] Vuoden 2022 aikana rikollisryhmät pyrkivät toimimaan matalalla profiililla ja keskittyivät Ukrainan sekä Venäjän ulkopuolisiin kohteisiin.[632] Tilanne alkoi palautua normaaliksi seuraavana vuonna, kun sota itsessään alkoi ”normalisoitua.”

[629] Cyber Peace Institute (2023a).
[630] Biggerstaff, William C.: The Status of Ukraine's "It Army" Under the Law of Armed Conflict. Lieber Institute, blogikirjoitus, 10.5.2023. [https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/], luettu 5.2.2024.
[631] ESET: Threat Report T3 2022. ESET, February 2023 (c). [https://www.eset.com/int/business/resource-center/reports/eset-threat-report-t3-2022/], luettu 5.2.2024; CISCO (2023).
[632] Weber, Valentin: Financial Incentives May Explain the Perceived Lack of Ransomware in Russia's Latest Assault on Ukraine. *Council on Foreign Relations*, 26.7.2022. [https://www.cfr.org/blog/financial-incentives-may-explain-perceived-lack-ransomware-russias-latest-assault-ukraine], luettu 5.2.2024; Pearson, James & Satter, Raphael:Analysis: Russian Ransomware Attacks on Ukraine Muted by Leaks, Insurance Woes. *Reuters*, 1.3.2022. [https://www.reuters.com/technology/russian-ransomware-attacks-ukraine-muted-by-leaks-insurance-woes-2022-03-01/], luettu 5.2.2024.

6. KYBERSODANKÄYNTIÄ UKRAINASSA 2023

Venäjän hyökkäysoperaation toisena vuonna sota muuttui kulutussodankäynniksi tai asemasodankäynniksi.[633] Venäjän yritys murtaa Ukrainan puolustustahto sähköinfrastruktuuri tuhoamalla epäonnistui kevääseen mennessä. Ukrainan kesän vastahyökkäys epäonnistui, eikä kumpikaan osapuoli onnistunut palauttamaan sotaan sellaista liikettä, jolla vastustajan asevoimat olisi voitu lyödä tai strategiset kohteet vallata. Nato- ja EU-maiden sotilaallinen ja taloudellinen apu vakiintui, vaikkakin vuoden lopussa liittolaisissa alkoikin esiintyä sotaväsymystä. Venäjä mobilisoi yhteiskuntansa ja taloutensa osittain ja rajoituksin, mikä voi sekin riittää voimasuhteiden kääntämiseen Venäjälle edullisiksi 1–2 vuoden aikana. Kiina on jatkanut Venäjän epäsuoraa tukemista, ja Lännen asettamat sanktiot vuotavat siinä määrin, että niiden vaikutus on jäänyt puutteelliseksi. Yhdysvallat ja Nato eikä toisaalta Venäjä ole ollut valmis eskaloimaan tilannetta sotilaalliseksi vastakkainasetteluksi niiden välillä. Tässä strategisessa tilanteessa hyökkäykselliset kyberoperaatiot näyttävät evolutionäärisesti löytäneen oman paikkansa, tosin niiden vaikuttavuus on jäänyt kyseenalaiseksi.

6.1. Aloite kääntyy Ukrainalle: Tammi-huhtikuu 2023

Vuoden 2023 helmikuussa Venäjä yritti temmata aloitteen hyökkäämällä Luhanskin alueella, mutta epäonnistui. Tämän jälkeen taisteluiden painopiste siirtyi Bakhmutin alueelle, jossa ne muotoutuivat hitaasti eteneväksi kulutustaisteluksi. Talven ja kevään aikana Ukrainan joukkoja koulutettiin Nato-maissa ja vastaanotti sotilaallista apua kesän suunnitellun vastahyökkäyksen mahdollistamiseksi ja vastaavasti Venäjän ja Valko-Venäjän sotilaallinen yhteistyö tiivistyi.[634]

CERT-UA mukaan vuoden 2023 ensimmäisen kuuden kuukauden aikana kyberhyökkäykset Ukrainaa kohtaan lisääntyivät edelleen +123 %, mutta kriittiset tapahtumat vähenivät 81 %. Hyökkäysten päämotiivina oli kybervakoilu ja etenkin siviilisektorin ja poliisi- ja oikeusjärjestelmän vakoilu. Tavoitteena oli saada tietoja sotarikostutkinnoista, Ukrainan vastavakoilun toiminnasta, tuotantoketjuista ja kineettisten iskujen vaikutuksista. Onnistuessaan operaatiot pyrkivät välittömästi varastamaan kohdejärjestelmien datan. Taktiikkaa on kutsuttu ”spray and pray” -tyyliseksi.[635] CyberPeace Instituten mukaan vuoden ensimmäisen neljänneksen osalta 76,9–87,5 % hyökkäyksistä Ukrainaa vastaan oli palvelunestohyökkäyksiä. Hyökkäykset kohdistuivat pääasiassa ICT- ja finanssisektorin, julkishallinnon ja teollisuuskohteita vastaan. Haktivistit kohdistivat hyökkäyksiä myös kansalaisjärjestöjen verkkosivuja vastaan.[636] Ukrainalaisten mukaan hyökkäykset kohdistuivat sodan edetessä entistä enemmän energiajärjestelmään.[637] Huhti-toukokuun taitteessa Ukrainaan kohdistuneissa hyökkäyksillä esiintyi piikki, joka saattoi liittyä Venäjän uudelleen aktivoituneeseen ohjushyökkäys-

[633] Valery Zaluzhny: The commander-in-chief of Ukraine's armed forces on how to win the war. Technology is the key as the war becomes "positional", says Valery Zaluzhny. *The Economist*, 1.11.2023. [https://www.economist.com/by-invitation/2023/11/01/the-commander-in-chief-of-ukraines-armed-forces-on-how-to-win-the-war], luettu 5.2.2024.
[634] Vuosien 2022–2023 tapahtumien yleisestä kuvauksesta ks. House of Commons Library (2023).
[635] SSSCIP (2023).
[636] CyberPeace Institute: Cyber Dimensions of the Armed Conflict in Ukraine. Quarterly Analysis Report Q1 January to March 2023. CyberPeace Institute, 4.9.2023 (b). [https://cpi.link/CATC-2023-Q1-report], luettu 5.1.2024.
[637] Antoniuk, Daryna: Ukraine's cyber chief on the ever-changing digital war with Russia. *Recorded Future*, 21.5.2023 (a). [https://therecord.media/ukraine-ssscip-yurii-shchyhol-interview], luettu 5.2.2024.

operaatioon, Ukrainan vastahyökkäyksen valmisteluun tai käynnissä olleisiin viljanvientineuvotteluihin.[638]

Verkkourkinta- ja haittaohjelmien levittäminen olivat toiseksi yleisimmät hyökkäystyypit. CERT-UA:n mukaan yksi ryhmä on kyennyt toteuttamaan suunnilleen yhden vakavan operaation kuukaudessa, ja operaatiot kohdistuvat usein samoihin kohteisiin. Pääkohteita ovat olleet Ukrainan yksityiset media ja telekommunikaatioyritykset, valtiollinen ja paikallishallinto, turvallisuus- ja puolustusala ja valtion instituutiot. Venäläiset hakkerit pyrkivät hankkimaan erityisesti ukrainalaisten henkilötietoja. Energiasektoriin kohdistui tiedustelua ja vähintään yksi tuhoa aiheuttavat hyökkäys.[639] Cisco Talosin mukaan sekä FSB:n Gamaredon että Turla toteuttivat keskitettyjä vakoilukampanjoita vuoden 2023 aikana, mutta hyökkäysten määrä laski selvästi vuodesta 2022 ja Gamaredonin kohdevalikoima oli huomattavasti laajempi kuin Turlan. Snake-haittaohjelmaoperaation lamauttaminen toukokuussa vaikutti merkittävästi Turlan toimintaan.[640]

Venäjän tiedustelupalvelut vaikuttavat vuoden 2023 alussa keskittyneen poliittiseen vakoiluun, mikä oli ymmärrettävää, koska Ukrainan vastarinnan jatkuminen perustui länsimaiden tukeen. Vuoden 2023 alkupuolella Gamaredon laajensi kohdevalikoimaansa Ukrainan lisäksi EU-maihin. Se jatkoi kybervakoilumenetelmiensä kehittämistä ja kykeni pysyttelemään kohdeverkoissa kuukausia.[641] SVR:n Dukes-kampanja vakoili EU-maan diplomaatteja[642] ja GRU vakoili keväällä 2023 EU ja Nato-maiden ulkoministeriöitä ja diplomaattiedustustoja.[643] Mediasektori on ollut erityisesti GRU:n hyökkäysten kohteena ja niillä on pyritty tukemaan informaatio-operaatioita ja informaatiotilan hallintaa.[644] CERT-UA löysi helmikuussa Venäjän joulukuussa 2021 Ukrainan keskus- ja paikallishallinon järjestelmiin asentaman takaoven, mikä todistaa vakoiluoperaatioiden merkittävää kykyä pysyä kohdejärjestelmissä huolimatta Ukrainan vastatoimista.[645]

Venäjä jatkoi hieman yllättäen tuhoavia kyberhyökkäyksiä heti vuodenvaihteessa. 1.1., kun tuntematon toimija hyökkäsi SDelete-ohjelmaa käyttäen ukrainalaista ohjelmistoalan yritystä vastaan.[646] Tammikuussa 2023 Sandworm käytti uutta SwiftSlicer wiper-haittaohjelmaa yksityisorganisaatiota vastaan.[647] Samoihin aikoihin CERT-UA ilmoitti Sandwormin hyökänneen tammikuun puolivälissä viidellä eri wiper-haittaohjelmalla –

---

[638] CyberPeace Institute: Cyber Dimensions of the Armed Conflict in Ukraine. Quarterly Analysis Report Q3 July to September 2023. CyberPeace Institute, 21.12.2023 (c). [https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q3-2023/], luettu 5.2.2024.
[639] SSSCIP (2023).
[640] CISCO: Talos Year in Review. CISCO, 2023 (a). [https://blog.talosintelligence.com/cisco-talos-2023-year-in-review/], luettu 5.1.2024.
[641] Symantec: Shuckworm: Inside Russia's Relentless Cyber Campaign Against Ukraine. Symantec, 15.6.2023. [https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/shuckworm-russia-ukraine-military], luettu 5.2.2024; SSSCIP (2023).
[642] ESET: APT Activity Report Q4 2022 – Q1 2023. ESET, 1.5.2023 (d). [https://www.eset.com/us/business/resource-center/reports/eset-apt-activity-report-q4-2022-q1-2023/], luettu 5.1.2024.
[643] Antoniuk, Daryna: Kremlin-backed hackers blamed in spying campaign on EU and NATO diplomatic agencies. *The Record*, 13.4.2023. [https://therecord.media/nobelium-apt29-russia-cyber-spying-campaign-targeting-nato-eu], luettu 5.2.2024.
[644] SSSCIP (2023).
[645] Gatlan, Sergiu: Ukraine says Russian hackers backdoored govt websites in 2021. *Bleeping Computer*, 23.2.2023. [https://www.bleepingcomputer.com/news/security/ukraine-says-russian-hackers-backdoored-govt-websites-in-2021/?utm_source=substack&utm_medium=email], luettu 5.2.2024.
[646] ESET (2023a).
[647] ESET: SwiftSlicer: New destructive wiper malware strikes Ukraine. ESET, 27.1.2023. [https://www.welivesecurity.com/2023/01/27/swiftslicer-new-destructive-wiper-malware-ukraine/], luettu 5.2.2024.

SDelete, AwfulShred, BidSwipe, CaddyWiper ja ZeroWipe – Ukrainan kansallista uutispalvelua Ukrinformia vastaan.[648] Operaatioon liittyi myös tietovuoto, joka toteutettiin Cyber Army of Russia Reborn haktivistipeitteen takaa. Vastaava sijaistoimijoiden taakse naamioituminen yleistyi tietovuototapauksissa vuoden 2023 aikana. [649] GRU:n Sandworm hyökkäsi vielä kevään aikana CaddyWiper-haittaohjelmalla Ukrainan valtiohallinnon kohteita vastaan[650] ja RoarBat wiper-haittaohjelmalla huhtikuussa Ukrainan valtionhallinnon organisaatiota vastaan.[651] Alkutalven ja kevään tuhoavien hyökkäysten sarjan jälkeen GRU vaikutti keskittyneen kybervakoiluun.[652]

Kevään 2023 hyökkäykset mukaan lukien operaation ensimmäisen vuoden aikana Venäjä käytti kuuttatoista wiper-haittaohjelmaperhettä. Niitä on ilmestynyt lähes kaikille käyttöjärjestelmille, mutta koodin taso ja toteutus on heikentynyt merkittävästi sodan edetessä.[653] Venäjä alkoi hyödyntää operaatioissaan yhä enemmän ns. Living-of-the-Land (LOTL) tekniikoita ja huhtikuussa Yhdysvaltojen ja Iso-Britannian turvallisuuspalvelut ilmoittivat GRU:n APT28-uhkatoimijan käyttävän Ciscon reitittimien haavoittuvuutta haittaohjelmien levittämiseen.[654] Voitaneen todeta, että Venäjän kyberhyökkäyskyky todennäköisesti kehittyi vuoden 2022 kokemusten perusteella. Tuhoavien kyberhyökkäyksien tekijä oli säännönmukaisesti GRU:n Sandworm ryhmä, josta viimeistään sodan toisena vuonna näyttää attribuutioiden perusteella kehittyneen Venäjän asevoimien pääkybertoimija. Ukrainan yhteiskunta ja kybertila oli kuitenkin jo siirtynyt sotatilaan, eikä Sandwormin yksittäisillä hyökkäyksillä näyttänyt olevan mahdollisuutta saavuttaa merkittäviä vaikutuksia. Tämä ei kuitenkaan estänyt Venäjää jatkamasta Ukrainan yhteiskunnan suunnitelmallista ja pitkäaikaista horjuttamista entistä kehittyneemmillä hyökkäyksillä.

Venäjä aloitti taistelutoimien tukemiseen liittyen viimeistään vuodenvaihteessa 2023 Starlink-järjestelmän häirinnän rintama-alueilla.[655] Lisäksi Sandworm yritti tunkeutua Ukrainan asevoimien verkkoihin kerätäkseen tietoa Starlink-järjestelmää käyttävistä

---

[648] ESET (2023d); CERT-EU: Cyber Security Brief (January 2023). CERT-EU, 1.2.2023 (b). [https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CB-23-02.pdf], luettu 5.2.2024; Gatlan, Sergiu: Ukraine: Sandworm hackers hit news agency with 5 data wipers. *Bleeping Computer*, 27.1.2024. [https://www.bleepingcomputer.com/news/security/ukraine-sandworm-hackers-hit-news-agency-with-5-data-wipers/], luettu 5.2.2024; Gatlan, Sergiu: Ukraine links data-wiping attack on news agency to Russian hackers. *Bleeping Computer*, 18.1.2023. [https://www.bleepingcomputer.com/news/security/ukraine-links-data-wiping-attack-on-news-agency-to-russian-hackers/], luettu 5.2.2024.

[649] SSSCIP (2023).

[650] CERT-UA: Kiberataka na informacijno-komunikacijnu sistemu Ukrinform (CERT-UA#5850). CERT-UA, 18.1.2023. [https://cert.gov.ua/article/3639362], luettu 5.2.2024; CyberPeace Institute: Cyber Dimensions of the Armed Conflict in Ukraine. Quarterly Analysis Report Q2 April to June 2023. CyberPeace Institute, 4.9.2023 (d). [https://cyberpeaceinstitute.org/news/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q2-2023/], luettu 5.1.2024.

[651] ESET: APT Activity Report. Government Espionage and Unpatched Vulnerabilities. April 2023 – September 2023. ESET, 1.10.2023 (e). [https://www.eset.com/fileadmin/ESET/IL/ESET-APT-Activity-Report-Q2_2023-Q3_2023.pdf], luettu 5.1.2024; SSSCIP (2023).

[652] CyberPeace Institute (2023d).

[653] Greebnberg, Andy: Ukraine Suffered More Data-Wiping Malware Last Year Than Anywhere, Ever. *WIRED*, 22.2.2023. [https://www.wired.com/story/ukraine-russia-wiper-malware/], luettu 5.2.2023.

[654] CISA: APT28 Exploits Known Vulnerability to Carry Out Reconnaissance and Deploy Malware on Cisco Routers. CISA, 18.4.2023. [https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-108], luettu 5.2.2024.

[655] Skove, Sam: Using Starlink Paints a Target on Ukrainian Troops. Units scramble for solutions as Russia learns to locate and jam the vital comsat links. *Defense One*, 23.3.2023. [https://www.defense-one.com/threats/2023/03/using-starlink-paints-target-ukrainian-troops/384361/], luettu 5.2.2024.

joukoista.[656] Venäjä jatkoi valloittamiensa alueiden liittämistä omaan informaatiotilaansa ja käski 16.3. Venäjään liitettyjen alueiden muuttaa IP osoitteensa venäläisiksi ja raportoida asiasta RIPE:een.[657] Valloitettujen alueiden informaatioinfrastruktuurin haltuunotto ja valvonta todennäköisesti vaikeutti Ukrainan erikoisjoukkojen ja partisaanien toimintaa. Sodan pitkittyessä informaatiotilan hallinta helpotti alueelle jääneen väestön kontrollointia.

Keväällä 2023 rikollisryhmät Trickbot/Conti toteuttivat hyökkäyksiä etenkin energiasektorin kriittisen infrastruktuurin kohteita vastaan. Killnet, XakNet, Zarya, NoName057, Anonymous Russia tekivät väitetysti yhteistyötä ja vuosivat räätälöityä dataa ja toteuttivat informaatio-operaatioita sosiaalisessa mediassa.[658] Uusina ryhminä ilmaantuivat People's CyberArmy, National Hackers of RUssia, Netside Group, Russian Clay, Solntsepek, mutta ne olivat pääosin lyhytikäisiä. Ryhmät kommunikoivat ja mobilisoivat osallistujia pääosin Telegramin kautta.[659] Vuoden 2023 heinäkuussa venäjämielisiä ryhmiä oli yhden lähteen mukaan yli seitsemänkymmentä.[660] Esimerkiksi Wagner-palkkasotilasyrityksellä raportoitiin olevan omat kyberjoukkonsa.[661] Kyberhyökkäyksiä suorittivat monet muutkin toimijat, mutta niiden sidonnaisuudet ovat jääneet epäselviksi.[662]

Keväällä paljastui venäläisiä tietoturvayrityksiä koskeva tietovuoto, niin kutsuttu Vulkan files leak, joka vahvisti epäilykset venäläisten kyberturvallisuusalan yritysten osallistumisesta Venäjän valtion kybersuorituskykyjen kehittämiseen ja altisti ne Lännen lisäsanktioille.[663] Läntinen media raportoi myös Venäjän ja Iranin tiivistyneistä kybersuorituskykyjen rakentamiseen liittyvästä yhteistyöstä.[664] Sijaistoimijakenttä eli voimakkaasti vuoden 2023 keväällä ja jos mahdollista muuttui entistä sekavammaksi. Yhtäältä geopoliittinen asetelma, ja näin ollen operaatioiden kiistettävyyden vaikeus, oli kehittynyt niin vahvaksi, että sijaistoimijoiden käytöllä oli enää pikemmin organisatoriset ja resurssipoliittiset kuin poliittiset ja strategiset syyt. Toisaalta niiden ylläpito mahdollisti vastapuolen uhkaamisen "tahattomilla", eli sanktioimattomilla tuhoavilla kyberhyökkäyksillä. Tällainen epäsuorauhkailu oli osa edelleen jatkuvaa kyberdeterrenssiviestintää.

SSSCIP:n mukaan haktivistien hyökkäykset vähenivät merkittävästi 2023 ensimmäisellä neljänneksellä pääosan ollessa edelleen palvelunestohyökkäyksiä. Niiden kohtee-

---

[656] Microsoft: Russian threat actors dig in, prepare to seize on war fatigue. Microsoft, 8.12.2023 (b). [https://www.microsoft.com/en-us/security/business/security-insider/reports/russian-threat-actors-dig-in-prepare-to-seize-on-war-fatigue/], luettu 5.2.2024.

[657] Устинова, Анна: IP-адреса пользователей новых регионов станут российскими. *Ведомости*, 16.3.3023. [https://www.vedomosti.ru/technology/articles/2023/03/16/966729-ip-adresa-polzovatelei-novih-regionov-stanut-rossiiskimi], luettu 5.2.2024.

[658] SSSCIP (2023).

[659] CyberPeace Institute (2023b).

[660] Cyberknow: Update 24. 2023 Russia-Ukraine War — Cybertracker. 20 JULY. Medium, blogikirjoitus, 20.7.2023. [https://cyberknow.medium.com/update-24-2023-russia-ukraine-war-cybertracker-20-july-ec64cfef38a0], luettu 5.2.2024.

[661] Досье: Кибервойска Пригожина. Как устроена IT-инфраструктура «Вагнера», «Фабрики троллей» и «Конкорда». Досье, 18.3.2023. [https://dossier-center.appspot.com/prig-it/], luettu 5.2.2024.

[662] Haktivisti ja sijaisryhmiä on nimetty seuraavasti: UAC-0010 (Gamaredon/FSB), UAC-0056 (GRU), UAC-0028 (APT28/GRU), UAC-0082 (Sandworm/GRU), UAC-0144 / UAC-0024 / UAC-0003 (Turla), UAC-0029 (APT29/SVR), UAC-0109 (Zarya), UAC-0100, UAC-0106 (XakNet), UAC-0107 (CyberArmyofRussia). (SSSCIP (2023).

[663] Antoniadis, Nikolai et al. (2023).

[664] Lieber, Dov, Faucon, Benoit & Amon, Michael: Russia Supplies Iran with Cyber Weapons as Military Cooperation Grows. *The Wall Street Journal*, 27.3.2023. [https://www.wsj.com/articles/russia-supplies-iran-with-cyber-weapons-as-military-cooperation-grows-b14b94cd?mod=djemalertNEWS], luettu 5.2.2024.

na olivat etenkin kaupallinen ja energiasektori.[665] Yleisesti ottaen venäläisten haktivistien hyökkäykset lisääntyivät Euroopan kohteissa 2023 aikana.[666] Killnet jatkoi hyökkäyksiä Ukrainan ulkopuolisia kohteita vastaan ja kaatoi esimerkiksi helmi- ja huhtikuussa osan Naton verkkosivuista ja teki palvelunestohyökkäyksen Euroopan ilmatilanhallintavirastoa vastaan huhtikuussa.[667] 25.2. Haktivistiryhmä Zarya teki väitetysti kyberhyökkäyksen kanadalaista kaasuputkiyritystä vastaan ja pääsi käsiksi sen OT-järjestelmiin. Hyökkäys ei aiheuttanut fyysistä tuhoa.[668] 13.4. Puola syytti Venäjää virallisesti laajasta kybervakoilukampanjasta, joka kohdistui Nato-maiden diplomaatteihin ja ulkohallinnon alaan. Puola attribuoi operaation APT29-uhkatoimijaan.[669] Venäläisten haktivistien hyökkäykset Nato- ja EU-maita kohtaan eivät ylittäneet häirinnän tasoa. Osa niistä oli varmasti itsenäisten, aggressiivisten, patrioottisten hakkereiden operaatioita, mutta Venäjän valtion kyvystä ohjata näitä operaatioita kertoi se, että merkittävään vaikutukseen päässeitä operaatioita ei esiintynyt. Tosin salaiseksi jääneitä epäonnistuneita tai onnistuneita hyökkäyksiä on saattanut tapahtua.

Ukrainalaishakkerit jatkoivat aktiivisesti hyökkäyksiään Venäjää vastaan ja aiheuttivat mm. ilmahälytyksiä Venäjällä, mikä oli mahdollista väärentämällä (*signal spoofing*) Yamal-402 tietoliikennesatelliitin signaalin.[670] Radio- ja TV-lähetyksiin kohdistui edelleen häirintää.[671] Yandexin lähdekoodia vuodettiin internettiin[672] ja Venäjän tullin tietojärjestelmät lamautettiin useaksi vuorokaudeksi[673] ja ainakin yhden puolustusteollisuuden alan yrityksen tietokannat tuhottiin.[674] Venäläisiin yrityksiin tehtiin aikaisempaa enemmän valekiristysohjelmahyökkäyksiä, jotka olivat aikaisemmin olleet venäläishakkereiden työkaluja.[675] Tietovuodot jatkuivat, mutta palvelunestohyökkäykset väitetysti lyhenivät edellisvuodesta.[676] Uutena keinona Ukraina käytti lennokki-iskuja

---

[665] Cyber Incidents Response Operational Centre: 2023 Report on Vulnerability Detection and Cyber Incidents/ Cyber Attacks Response System. SSSCIP, 2023. [https://scpc.gov.ua/api/files/4625437d-9981-4e9d-b8ce-c1077f36ba3e], luettu 5.2.2024.

[666] Rautaheimo, Kaisa: Venäläiset hakkerit muuttaneet strategiaansa – kyberiskut lisääntyneet Euroopassa, kertoo tuore raportti. *Helsingin Sanomat*, 28.3.2023. [https://www.hs.fi/ulkomaat/art-2000009482398.html], luettu 5.2.2024.

[667] Paganini, Pierluigi: Pro-Russia Hacker Group Killnet Targets Nato Websites with DDoS Attacks. *Security Affairs*, 13.2.2023. [https://securityaffairs.com/142192/hacking/killnet-targets-nato-websites.html], luettu 5.2.2024; National Security Archive Cyber Vault (2023).

[668] Paganini, Pierluigi: Pro-Russia Hacking Group Executed a Disruptive Attack Against a Canadian Gas Pipeline. *Security Affairs*, 26.4.2023. [https://securityaffairs.com/145307/cyber-warfare-2/canadian-gas-pipeline-disruptive-attack.html], luettu 5.2.2024.

[669] CERT-EU: Cyber Security Brief (April 2023). CERT-EU, 3.5.2023 (c). [https://cert.europa.eu/publications/threat-intelligence/cb23-05/], luettu 5.2.2024.

[670] Мингазов, Сергей: «Ведомости» узнали о подмене сигнала для спутника «Ямал-402» «Газпрома». *Forbes,* 1.3.2024. [https://www.forbes.ru/tekhnologii/485530-vedomosti-uznali-o-podmene-signala-dla-sputnika-amal-402-gazproma], luettu 5.2.2024.

[671] CyberPeace Institute (2023d).

[672] Toulas, Bill: Yandex denies hack, blames source code leak on former employee. *Bleeping Computer*, 26.1.2023. [https://www.bleepingcomputer.com/news/security/yandex-denies-hack-blames-source-code-leak-on-former-employee/], luettu 5.2.2024.

[673] SecurityLab.ru: Российские таможенные органы под атакой: масштабные сбои вызваны внешним воздействием (обновлено). *SecurityLab.ru*, 12.4.2023. [https://www.securitylab.ru/news/537510.php], luettu 5.2.2024.

[674] Безпалько, Ульяна & Кучерявец, Мария: ГУР провело масштабную кибератаку на оборонный завод РФ, - источники. *РБК-Украина*, 30.5.2023. [https://www.rbc.ua/ukr/news/gur-provelo-masshtabnu-kiberataku-oboronniy-1685433575.html], luettu 5.2.2024.

[675] Lenta.ru: Раскрыт новый вид хакерских атак в России. Lenta.ru, 22.3.2023. [https://lenta.ru/news/2023/03/22/hackers/], luettu 5.2.2024.

[676] Исакова, Татьяна: Атаки эконом-класса. Хакеры начали экономить свое время и ресурсы. *Коммерсантъ*, 25.4.2023. [https://www.kommersant.ru/doc/5952992?from=top_main_3], luettu 5.2.2024; Solar

informaatioinfrastruktuuria vastaan, mikä paljasti merkittäviä puutteita venäläisten teleliikenneyritysten varautumisessa.[677] FSB:n mukaan Venäjän kriittistä infrastruktuuria vastaan oli vuodesta 2022 lähtien tehty yli 5000 kyberhyökkäystä.[678]

FSB syytti huhtikuussa Yhdysvaltoja ja Nato-maita Venäjän kriittiseen infrastruktuuriin kohdistuvista hyökkäyksistä.[679] Sen mukaan Ukrainan alueelta oli tehty hyökkäyksiä Venäjää vastaan.[680] Vastaavasti Yhdysvallat ja Iso-Britannia asettivat helmikuussa sanktiota yhdeksälle venäläiselle, joita syytettiin Trickbot-kyberrikollisryhmään kuulumisesta ja hyökkäyksistä mm. sairaaloita vastaan.[681] Maaliskuussa Ukrainan SBU lopetti väitetysti Venäjän tiedustelupalveluiden operoiman disinformaatiota levittävän bottifarmin toiminnan.[682] Kevät 2023 oli siis kybertaistelutilassa kiihkeää aikaa, mutta yksikään operaatio ei vaikutuksiltaan noussut taktiselta tasolta operatiiviselle tai strategiselle. Venäläisen sotataidollisen ajattelun näkökulmasta kyberoperaatioista oli tullut pääsääntöisesti jatkuvan ei-aseellisen ja ei-väkivaltaisen vaikuttamisen keino, jolla hitaasti mutta vakaasti pyrittiin informaatiovaikuttamisen tukemisen kautta vastustajan heikentämiseen. Jatkuvat kyberoperaatiot myös loivat kohinaa ja painetta, jonka taustalla kyettiin valmistelemaan uusia merkittävämpiä operaatioita. Toisaalta osa venäläisistä operaatioista on saattanut syntyä vain organisaatioiden, valtiollisten tai aktivistien, tarpeesta tehdä jotain ollakseen hyödyllisiä.

6.2. Vastahyökkäys epäonnistuu: Touko-elokuu 2023

Venäjä jatkoi lyhyen tauon jälkeen ohjusiskujaan huhtikuun loppupuolella ja Ukraina aloitti satunnaiset lennokki-iskut Moskovaan. Ukraina menetti lopulta Bakhmutin hallinnan toukokuun lopussa, mutta sai Lännеltä lupauksia F-16 hävittäjistä. Valko-Venäjä ja Venäjä sopivat taktisten ydinaseiden sijoittamisesta Valko-Venäjän alueelle. Kiinan presidentti Xi Jiaping vieraili Venäjällä ja Kansainvälinen rikostuomioistuin julkaisi pidätysmääräyksen Putinista. Kesäkuun alussa Ukraina aloitti vastahyökkäyksensä, joka oli ohi viimeistään lokakuun alkuun mennessä. Ukraina sai kesän aikana yhä kauaskantoisempia ohjuksia lännеltä ja iski niillä, lennokeilla ja miehittämättömillä aluksilla mm. Moskovaan ja Venäjän asevoimien kohteisiin Venäjän selustassa sekä Mustanmeren laivaston kohteisiin. Venäjä vähensi ohjus- ja lennokki-iskujaan kesällä, mutta korosti ydinasepelotettaan sopimusteknisillä ja retorisilla toimilla. Naton Vilnan huippukokous ei edistänyt Ukrainan jäsenyyttä ja EU-jäsenyysehdokkuusprosessi eteni hitaasti.[683]

JSOC CERT: Техники и тактики киберпреступников. Solar JSOC CERT, 2023. [https://rt-solar.ru/analytics/reports/3416/], luettu 5.2.2024.

[677] Ларина, Анастасия: Сети связи развернут против дронов. *Коммерсантъ,* 21.9.2023 (a). [https://www.kommersant.ru/doc/6225913?tg], luettu 5.2.2024; 93.ru: Власти подтвердили причину взрывов в центре Краснодара — это падение беспилотников (онлайн). *93.ru*, 26.5.2023 (a). [https://93.ru/text/incidents/2023/05/26/72338669/], luettu 5.2.2024.

[678] ФСБ России: ФСБ России с начала 2022 года зафиксировано более пяти тысяч хакерских атак на критическую инфраструктуру Российской Федерации. ФСБ России, 13.4.2024. [http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439694%40fsbMessage.htm], luettu 5.2.2024.

[679] CERT-EU (2023c).

[680] ФСБ России (2023).

[681] CERT-EU: Cyber Security Brief (February 2023). CERT-EU, 1.3.2023. [https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CB-23-03.pdf], luettu 5.2.2024.

[682] CERT-EU: Cyber Security Brief (March 2023). CERT-EU, 3.4.2023. [https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CB-23-04.pdf], luettu 5.2.2024.

[683] Vuosien 2022–2023 tapahtumien yleisestä kuvauksesta ks. House of Commons Library (2023).

Ukrainan vastahyökkäyksen alku lisäsi epäilyttävää verkkoliikennettä Euroopassa, Lähi-idässä ja Afrikassa.[684] Toisella vuosineljänneksellä palvelunestohyökkäykset kattoivat 88.8 % tapahtumista. Kohteina olivat julkishallinto, media, ICT, finanssi- ja kuljetussektorit.[685] Cyber Peace Instituten mukaan kesäkuuhun 2023 mennessä selvästi eniten hyökkäyksiä oli kohdistunut Ukrainan julkishallintoon, jota seurasivat finanssisektoriin ja media. Venäjän osalta järjestys oli sama.[686] ESET-tietoturvayhtiön raportoinnin mukaan Sandworm-ryhmä jatkoi kesällä tuhoavia kyberhyökkäyksiä ja hyökkäsi mm. kesäkuussa nimeämätöntä mediaorganisaatiota vastaan. Sandworm käytti NikoWiper-haittaohjelmaa valtionhallinnon ja yrityssektorin kohteita vastaan kahdessa kampanjassa heinäkuussa ja SharpNikoWiperia-haittaohjelmaa elokuussa. Sandworm otti käyttöön Telegram kanavan, jossa se levitti tietoa operaatioistaan sijaistoimijapeitteellä. Se pyrki viesteissään heikentämään CERT-UA:n uskottavuutta.[687] Sandworm tunkeutui toukokuun ja syyskuun välisenä aikana yhdentoista ukrainalaisen teleliikenneoperaattorin verkkoihin. Tavoitteena lienee ollut vakoilu ja tämän jälkeen järjestelmien lamauttaminen.[688] Microsoft ilmoitti kesäkuussa GRU:n Cadet Blizzard-kybervakoilukampanjasta Ukrainan valtionhallintoa ja IT-palveluntarjoajia vastaan[689] ja 20.6. GRU:n ilmoitettiin murtautuneen Ukrainan valtion käyttämille sähköpostipalvelimille.[690] 25.8. yli 20 puolalaista junaa pysähtyi, kun rautatiejärjestelmän radio-ohjausverkkoa häirittiin valesanomilla. Kyseessä ei varsinaisesti ollut kyberhyökkäys, mutta tapaus paljasti Puolan rautatieverkon heikkoudet.[691] NSA:n kyberturvallisuusjohtajan mukaan Venäjä keskittyi kyberhyökkäyksissään logistiikkaan ja tuotantoketjuihin.[692]

Microsoftin mukaan Venäjä toteutti kesä-syyskuussa kyberhyökkäyskampanjan Ukrainan maataloussektoria vastaan. Se pyrki hankkimaan tietoa Ukrainan viljanviennistä ja jopa tuhoamaan järjestelmiä. Vakoiluoperaation takana oli FSB:n Gamaredon ja tuhoavat hyökkäykset toteutti GRU:n Sandworm. Hyökkäykset ajoittuivat yhteen Venäjän vetäytymiseen viljanvientisopimuksesta ja viljainfrastruktuurin kohdistuneiden ohjusiskujen kanssa. Ohjusiskut pyrittiin oikeuttamaan informaatio-operaatiolla.[693] Kesä 2023 ei siis ollut erityisen hiljaista aikaa GRU:n operaatioiden osalta, mutta tuhoavat kyberhyökkäykset jäivät yksittäisiksi vakoiluoperaatioiden ollessa yleisempiä. Pyrkimykset päästä käsiksi palveluntarjoajien ja teleliikenneoperaattoreiden verkkoihin saattoivat kuitenkin olla osa laajempien, tuhoavien tai lamauttavien hyökkäysten

[684] CISCO (2023a).
[685] CyberPeace Institute (2023d).
[686] CyberPeace Institute (2023c).
[687] ESET (2023e); SSSCIP (2023).
[688] Stahie, Silviu: 11 Ukrainian Telcom Operators Hit by the Same Threat Actor. *Bitdefender*, 18.10.2023. [https://www.bitdefender.com/blog/hotforsecurity/11-ukrainian-telcom-operators-hit-by-the-same-threat-actor/], luettu 5.2.2024.
[689] Burt, Tom: Ongoing Russian cyberattacks targeting Ukraine. Microsoft, 14.6.2023. [https://blogs.microsoft.com/on-the-issues/2023/06/14/russian-cyberattacks-ukraine-cadet-blizzard/], luettu 5.2.2024.
[690] Gatlan, Sergiu: Russian APT28 hackers breach Ukrainian govt email servers. *Bleeping Computer*, 20.6.2023. [https://www.bleepingcomputer.com/news/security/russian-apt28-hackers-breach-ukrainian-govt-email-servers/], luettu 5.2.2024.
[691] Greenberg, Andy: The Cheap Radio Hack That Disrupted Poland's Railway System. *WIRED*, 27.8.2023. [https://www.wired.com/story/poland-train-radio-stop-attack/], luettu 5.2.2024.
[692] Matishak, Martin: NSA cyber director warns of ransomware attacks on Ukraine, Western supply chains. *The Record*, 26.4.2023. [https://therecord.media/russia-ransomware-attacks-logistics-supply-chain-ukraine?utm_source=substack&utm_medium=email], luettu 5.2.2024.
[693] Microsoft (2023b).

valmistelua. Joulukuussa GRU:n hyökkäys lamautti Kiyvstar teleliikenneoperaattorin useaksi päiväksi.

ESET-tietoturvayhtiön mukaan FSB:n Gamaredonin tiedonkeruukyvyt kehittyivät huomattavasti vuoden 2023 kuluessa. Gamaredon jatkoi Ukrainan asevoimien ja puolustusteollisuuden kybervakoilua.[694] FSB:hen liitetty Sednit-uhkatoimija vakoili mm. Ukrainan, Puolan, Armenia, Tadzikistanin, Kreikan, Serbian ja Tsekin tasavallan hallituksia.[695] Heinäkuussa venäläishakkerit onnistuivat murtautumaan Norjan kahdentoista eri ministeriön järjestelmiin.[696] FSB:n Turla suoritti heinäkuussa kybertiedustelua Ukrainan asevoimien ja puolustusteollisuuden kohteita vastaan Capibar/Kazuar-haittaohjelmalla.[697] Myös GRU:n APT28 jatkoi Ukrainan valtionhallinnon ja asevoimien kybervakoilua.[698] Venäläishakkerit yrittivät edelleen päästä käsiksi ukrainalaisten käyttämiin mobiililaitteisiin.[699] Mandiantin ilmoituksen mukaan SVR:n APT29 osallistui aktiivisesti kybervakoiluun koko kesän ajan pyrkien hankkimaan tietoa Ukrainan liittolaisten näkemyksistä Ukrainan vastahyökkäykseen liittyen.[700] Venäjän toteutti kybervakoilua ja -tiedustelua kesällä 2023 taisteluteknisestä strategiselle tasolle asti. Ukrainan asevoimien mobiililaite- ja palveluperustaisiin johtamisjärjestelmiin tunkeutuminen olisi ollut merkittävä tiedusteluvoitto ja taannut informaatioylivoiman taistelukentällä. Eheän tilannekuvan muodostaminen Ukrainan kesän vastahyökkäyksestä olisi mahdollistanut sen heikentämisen etukäteen ja torjumisen. Jälkikäteen ajateltuna on mahdollista, että näin osittain kävikin. Ukrainan tukijoiden onnistunut vakoilu olisi auttanut arvioimaan Ukrainan kykyä jatkaa sotaa ja Venäjän mahdollisuuksia kiertää pakotteita entistä paremmin. Panostaminen kybervakoiluun ja -tiedusteluun oli taisteluiden tila huomioiden Venäjän näkökulmasta järkevää.

Venäläisten haktivistiryhmien hyökkäykset Ukrainan tukijoita vastaan lisääntyivät vuoden 2023 ensimmäisen puolikkaan aikana. Hyökkäykset olivat lähes täysin palvelunestohyökkäyksiä ja kohdistuivat mm. Puolaa, Saksaa, Ranskaa, Kanadaa, Italiaa ja Baltian maita kohtaan. Joitain disinformaatiokampanjoita toteutettiin valeverkkosivujen avulla.[701] Ilmoitukset sotilasavusta, mm. MiG-29 ja Leopard 2-panssarivaunujen toimitukset, aiheuttivat piikkejä Ukrainan liittolaisiin kohdistuneessa hyökkäyksissä.[702] NoName057(16) toteutti kaksi päivää kestäneen palvelunestohyökkäyksen Ruotsin

---

[694] Toulas, Bill: Russian hackers use PowerShell USB malware to drop backdoors. *Bleeping Computer*, 15.6.2023. [https://www.bleepingcomputer.com/news/security/russian-hackers-use-powershell-usb-malware-to-drop-backdoors/], luettu 5.2.2024.
[695] ESET (2023e); SSSCIP (2023).
[696] Reuters: Norway government ministries hit by cyber attack. *Reuters*, 24.7.2023. [https://www.reuters.com/technology/norway-government-ministries-hit-by-cyber-attack-2023-07-24/], luettu 5.2.2024.
[697] Antoniuk, Daryna: Russia's Turla hackers target Ukraine's defense with spyware. *The Record*, 19.7.2023. [https://therecord.media/turla-hackers-targeting-ukraine-defense], luettu 5.2.2024; The Hacker News: Turla's New DeliveryCheck Backdoor Breaches Ukrainian Defense Sector. *The Hacker News*, 20.7.2023. [https://thehackernews.com/2023/07/turlas-new-deliverycheck-backdoor.html], luettu 5.2.2024.
[698] Insikit Group: BlueDelta Exploits Ukrainian Government Roundcube Mail Servers to Support Espionage Activities. Recorded Future, 20.6.2023. [https://www.recordedfuture.com/bluedelta-exploits-ukrainian-government-roundcube-mail-servers], luettu 5.2.2024.
[699] Banfield-Nwachi, Mabel, Belam, Martin & Sullivan, Helen: Russia-Ukraine war: Kyiv claims to have foiled Russian hacking of armed forces combat system – as it happened. *The Guardian*, 8.8.2023. [https://www.theguardian.com/world/live/2023/aug/08/russia-ukraine-war-live-updates-moscow-missile-attack-pokrovsk-injuries-deaths], luettu 5.2.2024.
[700] Jenkins, Luke, Atkins, Josh & Black, Dan: Backchannel Diplomacy: APT29's Rapidly Evolving Diplomatic Phishing Operations. Mandiant, 21.9.2023. [https://www.mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing], luettu 5.2.2024.
[701] CyberPeace Institute (2023d); CyberPeace Institute (2023c).
[702] CyberPeace Institute (2023d); CERT-EU (2023a).

parlamenttia ja viittä muuta organisaatiota vastaan vastauksena Venäjän ja Ruotsin kiristyneistä diplomaattisuhteista.[703] Venäjä kohdisti Vilnan Naton huippukokoukseen disinformaatiokampanjan, johon liittyi mm. väärennettyjen dokumenttien levittämistä. Ukrainan presidentti Zelenskin puhuessa etänä Sveitsin parlamentille venäläismieliset haktivistit toteuttivat laajan palvelunestohyökkäyksen useita sveitsiläisiä kohteita vastaan.[704] Kesäkuun puolivälissä Killnet, REvil ja Anonymous Sudan uhkasivat kaataa Euroopan pankkijärjestelmän, mutta hyökkäyksen tulokset jäivät heikoiksi.[705] Ryhmien julistuksellinen yhteistyö kuitenkin osoittaa, miten Venäjä onnistui mobilisoimaan haktivistit, rikolliset ja terroristiset sijaistoimijat sotatoimensa tueksi.

Ukrainalaisten kohteiden osalta patrioottisten haktivistien toiminta keskittyi palvelunestohyökkäyksiin.[706] Haktivistiryhmä Solntsepek häiritsi Ukrainan televisio- ja radiolähetyksiä kesäkuussa.[707] NoName057(16) kohdalla oli havaittavissa organisoitu, säännöllinen ja järjestelmällinen palvelunestotoiminta, mikä viittasi valtiolliseen kontrolliin ja toisaalta haktivismitoiminnan vakiintumiseen osaksi sodan kuvaa.[708] CyberPeace Instituten mukaan palvelunestohyökkäykset eivät olleet pelkkää kiusantekoa vaan saattoivat johtaa lisäkustannuksiin, tulon- ja maineen menetyksiin, olennaisten palveluiden häiriöihin ja halvaannuttaa tilapäisesti kokonaisia taloudellisen toiminnan aloja.[709] Näin ollen niillä oli selvä rooli kaikessa ”arkipäiväisyydessään” Ukrainan painostamisessa ja heikentämisessä. Ryhmien sisällä tapahtui uudelleen järjestelyjä ja ilmeni sisäisiä kiistoja, jotka mahdollisesti vaikuttivat joidenkin ryhmien aktiivisuuteen. Samalla osa ryhmistä alkoi rahastaa palveluillaan.[710]

Venäjä jatkoi vuonna 2023 sijaistoimijoiden käyttämistä kyberoperaatioidensa peitteenä. Esimerkiksi Void Rabisu -kyberrikollisryhmä attribuoitiin keväällä 2023 Venäjän tiedustelupalveluiden työkaluksi tai vähintään alihankkijaksi. Rikollisen toimintansa lisäksi ryhmän vakoilutoiminta oli selvästi geopoliittisesti motivoitunutta.[711] Heinäkuussa 2023 Anonymous Sudan ryhmän yhteydet Venäjän valtioon alkoivat näyttää yhä selvemmiltä.[712] Venäjän sijaistoimijana operoinut valkovenäläinen Ghoswriter-uhkatoimija jatkoi edelleen toimintaansa ja sen vuoden kestänyt Ukrainaan ja Puolaan

[703] CERT-EU (2023c).
[704] Miller, Maggie & Cerelus, Laurens: How Russian hackers targeted NATO's Vilnius summit. *Politico*, 21.8.2023. [https://www.politico.eu/article/russia-hackers-targeted-nato-vilnius-summit-graphika/], luettu 5.2.2024; Swissinfo.ch: Pro-Russian hackers step up attacks against Swiss targets. *Swissinfo.ch*, 14.6.2023. [https://www.swissinfo.ch/eng/politics/pro-russian-hackers-step-up-attacks-against-swiss-targets/48588976], luettu 5.2.2024.
[705] Lenta.ru: Хакеры обещают уничтожить банковскую систему Европы в ближайшие 48 часов. Они анонсируют сильнейшую кибератаку в истории. *Lenta.ru*, 14.6.2023. [https://lenta.ru/news/2023/06/14/killnet/], luettu 5.2.2024.
[706] CyberPeace Institute (2023c).
[707] CyberPeace Institute (2023d).
[708] Antoniuk, Daryna: What's in a NoName? Researchers see a lone-wolf DDoS group. *The Record*, 5.9.2023. [https://therecord.media/noname-hacking-group-targets-ukraine-and-allies], luettu 5.2.2024.
[709] CyberPeace Institute (2023d); CyberPeace Institute (2023c).
[710] CyberPeace Institute (2023c).
[711] Ahmed, Deeba: ROMCOMLITE: Stealthier Version of ROMCOM Backdoor Targets Female Politicians. *HackRead*, 16.10.2024. [https://www.hackread.com/romcomlite-romcom-backdoor-female-politicians/#:~:text=Hackread.com%20had%20reported%20in,backdoor%20RAT%20delivered%20via%20malicious], luettu 5.2.2024.
[712] CyberCX: A bear in wolf's clothing: Insights into the infrastructure used by Anonymous Sudan to attack Australian organisations. CyberCX, 19.6.2023. [https://cybercx.com.au/blog/a-bear-in-wolfs-clothing/], luettu 5.2.2024.

kohdistunut vakoilukampanja paljastui heinäkuussa.[713] Vaikka suoranaista ohjaussuhdetta Venäjän valtioon ei olisi ollut, rikollisryhmien toiminta kohdistui useassa tapauksessa Lännen Ukraina-avulle tärkeitä kohteita vastaan. Black Basta -kyberrikollisryhmä teki kiristyshaittaohjelmahyökkäyksen saksalaista Rheinmetallia vastaan huhtikuussa. Ryhmä oli yhteyksiä Venäjää avoimesti tukeneeseen Conti-ryhmään ja kohdeyritys oli kriittinen Saksan Ukraina-avulle.[714] 16.6. Venäläinen hakkeriryhmä Slor väitti toteuttaneensa laajan kyberhyökkäyksen länsimaisia kohteita vastaan.[715] Huolimatta edellä esitellystä aktiivisesta toiminnasta venäläisten patrioottisten hakkereiden toiminta näyttää hieman laantuneen vuoden 2023 ensimmäisen puolikkaan aikana.[716]

Venäläiset toimijat jatkoivat informaatiovaikuttamista Ukrainan tukijoita kohtaan. Ranska paljasti 13.6. venäläisen disinformaatiokampanja Doppelgängerin. Kampanjaan kuului valesivustojen rakentaminen ja valeuutisten levittäminen mukaan lukien valtionhallin verkkosivujen väärentäminen ja väärennettyjen uutisten kaiuttaminen sosiaalisen median kautta.[717] EU asetti elokuussa sanktioita operaation taustalla olleille venäläisille henkilöille. Ukraina pidätti 100 henkilöä venäläisen online-propagandan ja disinformaation levittämisen takia. Joukko oli operoinut bottiverkkoa ja pyrki salaamaan toimintansa käyttämällä erityisesti toimintaan sopivaa ohjelmistoa ja laitteistoja.[718]

Ukraina ja Länsi pyrkivät kiistämään Venäjän toiminnan vapauden informaatiotilassa. Yhdysvallat teki toukokuussa toimintakyvyttömäksi 20 vuotta sitä ja sen liittolaisia vakoilleen Venäjän kyberoperaation – FSB:n Turlan Snake-kampanjan.[719] Venäjään kohdistuneiden palvelunestohyökkäysten määrä kasvoi toukokuussa 50 % edellisestä vuodesta ja kesäkuuhun mennessä niiden kesto oli pidentynyt 150 %. Tuhoavat hyökkäykset ja tietovuodot lisääntyivät edellisestä vuodesta.[720] Positive Technologies yrityksen mukaan vuoden 2023 yhdeksän ensimmäisen kuukauden aikana hyökkäykset verkkoresursseja vastaan kasvoivat 44%. Kohteena olivat etenkin teleliikenne, mutta myös pankki- ja liikenneala. Venäjää vastaan on Positive Technologiesin mukaan käy-

---

[713] The Hacker News: Ukraine's CERT Thwarts APT28's Cyberattack on Critical Energy Infrastructure. *The Hacker News*, 6.9.2023 (a). [https://thehackernews.com/2023/09/ukraines-cert-thwarts-apt28s.html?m=1], luettu 5.2.2024.

[714] Martin, Alexander: German arms company Rheinmetall confirms Black Basta ransomware group behind cyberattack. *The Record*, 22.5.2023. [https://therecord.media/rheinmetall-confirms-black-basta-ransomware-group-behind-cyberattack], luettu 5.2.2024.

[715] Lenta.ru: Русские хакеры напали на сотни западных компаний и госорганы. Среди их жертв — «Би-би-си», Shell и Минэнерго США. *Lenta.ru*, 16.6.2023. [https://m.lenta.ru/news/2023/06/16/clop/], luettu 5.2.2024.

[716] CyberPeace Institute (2023c).

[717] Reynaud, Florian & Leloup, Damien: 'Doppelgänger': The Russian disinformation campaign denounced by France. *Le Monde*, 13.6.2023. [https://www.lemonde.fr/en/pixels/article/2023/06/13/doppelganger-the-russian-disinformation-campaign-denounced-by-france_6031227_13.html#:~:text=Russia-,'Doppelg%C3%A4nger'%3A%20The%20Russian%20disinformation%20campaign%20denounced%20by%20France,'], luettu 5.2.2024.

[718] CERT-EU: Cyber Security Brief (July 2023). CERT-EU, 1.8.2023. [https://cert.europa.eu/publications/threat-intelligence/cb23-08/], luettu 5.2.2024.

[719] Stein, Perry: U.S. Says It Has Disabled Major Cyberespionage Operation. *The Washington Post*, 9.5.2023. [https://www.washingtonpost.com/national-security/2023/05/09/russian-cyberespionage-disrupted-snake/], luettu 5.2.2024; Greenberg (2023a).

[720] Исакова, Татьяна & Послaвская, Юлия: Хакеры работают по площадям. География атак расширяется, а их число растет. *Коммерсантъ*, 29.5.2023. [https://www.kommersant.ru/doc/6012555?from=top_main_3], luettu 5.2.2024; Бевза, Дмитрий: Количество кибератак на российские организации в 2023 году заметно выросло. *Российская газета*, 27.7.2023. [https://rg.ru/2023/07/27/kolichestvo-kiberatak-na-rossijskie-organizacii-v-2023-godu-zametno-vyroslo.html], luettu 5.2.2024.

tetty erityisesti vakoiluohjelmia ja tekoälyn käyttö sosiaalisen manipulaation tukena on lisääntynyt.[721] Tiedot ovat kuitenkin ristiriitaisia sillä tietoturvayhtiö Kaspersky on taas väittänyt Venäjään kohdistuneiden hyökkäysten vähentyneen merkittävästi,[722] Venäjän pankin mukaan palvelunestohyökkäysten määrä romahti alkuvuodesta[723] ja tietovuotojen määrän väitetään vähentyneen.[724]

Niin tai näin ukrainalaishakkerit tekivät 11.6. tuhoavan kyberiskun venäläisen internetpalveluntarjoaja Infotelin infrastruktuuriin, mikä vaikutti mm. venäläispankkien toimintaan.[725] Venäjän teknologiapuisto Skolkovia vastaan tehtiin kyberhyökkäys ja sen tietoja vuodettiin internettiin[726] ja useisiin venäläisiin teleliikennealan yrityksiin kohdistui häiritseviä ja tuhoavia kyberhyökkäyksiä.[727] Kesällä 2023 Kaspersky löysi valtion ja teollisuuden verkoista takaoven, jota olivat todennäköisesti käyttäneet valtiosidonnaiset hakkerit.[728] Kaspersky myös paljasti Applen puhelimiin kohdistuneen Triangulaatio-vakoilukampanjan. Venäjän turvallisuusviranomaiset syyttivät Yhdysvaltoja operaatiosta. Neljä vuotta kestäneen kampanjan kohteena olivat Kaperskyn lisäksi mm. Venäjällä toimivat ulkomaiset lähetystöt.[729] Kesän pitkään jatkuneiden ja teknisesti kehittyneiden vakoilukampanjoiden paljastusten takana saattaa olla tarveharkintaisuus. Sekä Yhdysvallat että Venäjä olivat valmiita paljastamaan ja lopettamaan pitkään jatkuneet vakoiluoperaatiot, joko koska niistä oli tullut liian riskialttiita, hyödyttömiä, viestittääkseen päättäväisyyttä tai mustamaalatakseen vastustajiaan.

Huolimatta aktiivisuudestaan ukrainalaiset hakkerit ovat rajoittaneet tuhoavia hyökkäyksiään Venäjä kriittisiä teollisuuden aloja, terveydenhuoltoa ja turvaluokiteltuja järjestelmiä kohtaan.[730] Cyber Peace Instituten mukaan pääosa hyökkäyksistä huhti-kesäkuussa oli palvelunestohyökkäyksiä.[731] Ukrainalaiset ovat silti tavoitelleet näyttävyyttä. Poliittisesti merkittävät tapahtumat ja päivät ovat toimineet edelleen hyökkäysten aktivoijina. Esimerkiksi 17.7. Hakkerit hyökkäsivät Pietarissa järjestettyä Kansain-

---

[721] SecurityLab.ru: Шпионское ПО, уязвимости в системах передачи данных и нейросети в киберпреступности: аналитика Positive Technologies за 2023 год. *SecurityLab.ru*, 13.12.2023. [https://www.securitylab.ru/news/544568.php], luettu 5.2.2024.
[722] Kaspersky: Ландшафт угроз для систем промышленной автоматизации. Первое полугодие 2023. Kaspersky, 13.9.2023. [https://ics-cert.kaspersky.ru/publications/reports/2023/09/13/threat-landscape-for-industrial-automation-systems-statistics-for-h1-2023/], luettu 5.2.2024.
[723] Ошанина, Олеся: Почему DDoS-атаки становятся более избирательными. *Ведомости*, 27.7.2023. [https://www.vedomosti.ru/partner/articles/2023/07/27/986567-ddos-ataki-izbiratelnimi], luettu 5.2.2024.
[724] D-Russia: InfoWatch: за год зафиксированных утечек информации в мире стало больше на 141,2%, в России – меньше на 17,5%. *D-Russia*, 29.9.2023. [https://d-russia.ru/infowatch-za-god-zafiksirovannyh-utechek-informacii-v-mire-stalo-bolshe-na-141-2-v-rossii-menshe-na-17-5.html], luettu 5.2.2024.
[725] Antoniu, Daryna: Pro-Ukraine hackers claim to take down Russian internet provider. *The Record*, 9.6.2023 (a). [https://therecord.media/proukraine-hackers-claim-to-take-down-russian-isp], luettu 5.2.2024.
[726] Волкова, Юлия & Ясакова, Екатерина: «Сколково» сообщило о хакерской атаке «украинского киберфронта». *РБК*, 29.5.2023. [https://www.rbc.ru/politics/29/05/2023/647486eb9a79475a4c770c45], luettu 5.2.2024.
[727] SecurityLab.ru: Хакеры взломали расписание телепрограммы в нескольких кабельных сетях. *SecurityLab.ru*, 9.5.2023.[https://www.securitylab.ru/news/531524.php], luettu 5.2.2024.
[728] SecureList: Атаки на индустриальный и государственный секторы РФ. SecureList, 24.10.2023. [https://securelist.ru/ataki-na-industrialnyj-i-gosudarstvennyj-sektory-rf/108229/], luettu 4.2.2024.
[729] Faulconbridge, Guy: Russia says US hacked thousands of Apple phones in spy plot. *Reuters*, 2.6.2023. [https://www.reuters.com/technology/russias-fsb-says-us-nsa-penetrated-thousands-apple-phones-spy-plot-2023-06-01/], luettu 4.2.2024; Goodin, Dan: 4-year campaign backdoored iPhones using possibly the most advanced exploit ever. *Ars Technica*, 27.12.2023. [https://arstechnica.com/security/2023/12/exploit-used-in-mass-iphone-infection-campaign-targeted-secret-hardware-feature/], luettu 4.2.2024.
[730] Fendorf, Kyle: The Dynamics of the Ukrainian IT Army's Campaign in Russia. *Lawfare*, 15.6.2023. [https://www.lawfaremedia.org/article/the-dynamics-of-the-ukrainian-it-army-s-campaign-in-russia], luettu 4.2.2024.
[731] CyberPeace Institute (2023c).

välistä talousfoorumia vastaan.[732] Venäjän televisiolähetyksiin on kohdistunut jatkuvaa häirintää joko kyber- tai satelliittisignaalin häirinnän keinoin.[733] Toisin kuin olisi voinut olettaa venäläisen Wagner palkkasotilasyrityksen kapina juhannuksena 2023 ei aiheuttanut kybertilassa julkiseksi tullutta poikkeavaa toimintaa.[734] Toki tapahtuman informaatioarvo hyödynnettiin täysimääräisesti läntisessä mediassa. Sen sijaan tapahtumat todennäköisesti johtivat Jevgeni Prigožiniin sidoksissa olleen IRA:n toiminnan lopettamiseen silloisessa muodossaan.[735] Sinällään yhden toimijan poistuminen kyber- ja informaatiosodankäynnin kentältä ei ollut millään tavoin ratkaisevaa. Sodan toisena vuotena monet alkuvaiheen organisaatioista ja toimijoista olivat muuttuneet, kadonneet näkyvistä tai jatkaneet toimintaa uuden nimikkeen alla.

6.3. Kulutussotaa: Syys-joulukuu 2023

Syyskuussa Pohjois-Korean ja Venäjän johto tapasivat ja Pohjois-Korea aloitti tykistön ampumatarvikkeiden toimitukset Venäjälle. Lokakuussa Venäjä aloitti oman hyökkäyksien sarjan aloitteen tempaamiseksi. Taistelut keskittyivät Harkovan ja Donetskin alueille. Marraskuussa Venäjä aloitti jälleen lennokki- ja ohjusiskut Ukrainan valmiiksi heikossa kunnossa ollutta sähkö- ja yhteiskunnallista infrastruktuuria vastaan.[736] Vastavuoroisesti Ukrainan lennokki- ja ohjusiskut Venäjän sotilaskohteisiin ja lennokki-iskut infrastruktuurikohteisiin jatkuivat. Loka-marraskuun taitteessa Ukrainan poliittinen ja valtiojohto totesi sodan muuttuneet kulutussodaksi, jossa Venäjällä tulisi olemaan aikaetu puolellaan.[737] Gazan Hamas-järjestön ja Israelin välille syttynyt sota vei kansainvälisen huomion Ukrainan ja Venäjän välisestä sodasta. Venäjä vuodenvaihteessa toteuttamat massiiviset ohjusiskut palauttivat sen vähintään hetkeksi huomion keskipisteeseen.[738]

Syyskuussa GRU:n APT28 pyrki ilman menestystä tunkeutumaan ukrainalaisen energialaitoksen verkkoihin, mahdollisesti pyrkien toisintamaan syksyn 2022 hyökkäykset, kun ohjushyökkäykset alkoivat uudelleen.[739] Ukrainan sähköjärjestelmään kohdistuneisiin kyberhyökkäyksiin kuitenkin varauduttiin, sillä CISCO toimitti Ukrainalle GPS -riippumaton reititinkalustoa sähköverkon synkronoinnin ylläpitämiseksi.[740] Sandworm onnistui kuitenkin 12.12. toteuttamaan harvinaisen menestyksekkään tuhoavan kyberhyökkäyksen teleliikenneoperaattori Kiyvstaria vastaan. Hyökkäys kohdistui yri-

---

[732] Интерфакс: Хакеры атаковали ИТ-инфраструктуру ПМЭФ-2023, все попытки взлома отражены. *Интерфакс*: 17.6.2023. [https://www.interfax.ru/russia/906884], luettu 4.2.2024.
[733] Нотченко, Вероника: Россияне почти месяц живут без нормального телевидения. *ГлавСовет*, 7.7.2023. [https://sovetov.su/news/2023/7/7/35395], luettu 4.2.2024.
[734] CyberPeace Institute (2023d).
[735] Greenberg, Andy: Security News This Week: Russia's Notorious Troll Farm Disbands. *WIRED*, 8.7.2023. [https://www.wired.com/story/russia-internet-research-agency-disbands/], luettu 5.2.2024.
[736] Méheut, Constant: Ukraine heads into winter with a fragile power grid. *The Spokesman-Review*, 22.11.2023. [https://www.spokesman.com/stories/2023/nov/22/ukraine-heads-into-winter-with-a-fragile-power-gri/], luettu 4.2.2024; Harmash, Olena: Russian drone attack hits Ukraine infrastructure, causes power outage. *Reuters*, 18.11.2023. [https://www.reuters.com/world/europe/russia-launches-major-drone-attack-ukraine-infrastructure-hit-2023-11-18/], luettu 4.2.2024.
[737] Zaluzhny (2023).
[738] Vuosien 2022–2023 tapahtumien yleisestä kuvauksesta ks. House of Commons Library (2023).
[739] Antoniuk, Daryna: Ukraine says an energy facility disrupted a Fancy Bear intrusion. *The Record*, 5.9.2023. [https://therecord.media/ukraine-energy-facility-cyberattack-fancy-bear-email], luettu 4.2.2024; The Hacker News (2023a)
[740] Jones, Connor: Cisco whips up modded switch to secure Ukraine grid against Russian cyberattacks. The Register, 22.11.2023. [https://www.theregister.com/2023/11/22/cisco_modded_switch_ukraine/], luettu 4.2.2024.

tyksen runkoverkkoon ja tuhosi osan palveluista ja aiheutti jopa kahden päivän palvelukatkon asiakkaille eli puolelle ukrainalaisista. Tuhojen korjaamiseen meni yli viikko. Lisäksi Sandworm oli ollut Kiyvstarin verkoissa jo toukokuusta ja päässyt käsiksi yrityksen ja mahdollisesti asiakkaiden tietoihin. Vaikka Solntsepek-ryhmä otti vastuun hyökkäyksestä, mutta kyseessä oli todennäköisesti peiteoperaatio.[741] Kyivstarin kyberhyökkäystä seurasi tykistöohjusisku mm. Kiovaan.[742] Kyberhyökkäysten lisäksi vuodenvaihteen ohjus- ja lennokki-iskut katkoivat teleliikenneyhteyksiä kaikkialla Ukrainassa.[743]

Venäjän kybervakoilun kohteena olivat syksyllä 2023 ukrainalaisten mukaan muun muassa sotarikostutkintoihin liittyvä materiaali.[744] Tämä materiaali kiinnosti kaikkia venäläisiä tiedustelupalveluita.[745] Lisäksi ukrainalaisiin sotilaisiin kohdistettiin verkkourkintahyökkäyksiä mm. saastutettujen lennokkimanuaalien avulla.[746] Ainakin GRU ja SVR toteuttivat verkkovakoilua käyttäen hyväkseen ohjelmistohaavoittuvuuksia. Kohteena olivat lähetystöt, yritykset ja maatalousalan toimijat.[747] FSB:n Gamaredon jatkoi myös vakoilua ja sen käyttämä USB-mato levisi Ukrainan ulkopuolelle.[748]

Venäläismieliset haktivistiryhmät jatkoivat palvelunestohyökkäyksiään ja verkkosivujen sotkemista. Tekijänä oli usein People's CyberArmy -ryhmä ja kohteena olivat median, yliopistojen ja valtionhallinnon sivustot.[749] NoName 057(16) teki palvelunestohyökkäyksiä saksalaisia, hollantilaisia ja kanadalaisia valtiohallinnon, finanssialan ja

---

[741] Antoniuk, Daryna: Ukraine telecom cyberattack one of 'highest-impact' hacks of the war. *The Record*, 18.12.2023. [https://therecord.media/ukraine-kyivstar-hack-high-impact], luettu 4.2.2024; RFE/RL: Ukraine's Kyivstar Says All Problems Fixed. *RFE/RL*, 20.12.2023. [https://www.rferl.org/a/ukraine-kyivstar-cyberattack/32739897.html], luettu 4.2.2023; Шакиров, Олег: Официальный взлом: почему в Москве и Киеве начинают открыто говорить о кибервойне. *Forbes*, 20.12.2023. [https://www.forbes.ru/mneniya/502767-oficial-nyj-vzlom-pocemu-v-moskve-i-kieve-nacinaut-otkryto-govorit-o-kibervojne], luettu 4.2.2024; Кагалтынов, Эрдни: СБУ: российские хакеры уничтожили почти все в «Киевстаре». *Коммерсантъ*, 4.1.2024. [https://www.kommersant.ru/doc/6442061?from=top_main_1], luettu 5.2.2024.

[742] Balmforth, Tom: Exclusive: Russian hackers were inside Ukraine telecoms giant for months. *Reuters*, 5.1.2024. [https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/], luettu 20.2.2024.

[743] Netblock: Twiitti 1.2.2024. [https://twitter.com/netblocks/status/1742095412025065566?t=r-wtqao-Flo8KNOKJ_VXs1A&s=19], luettu 4.2.2024.

[744] Balmforth, Tom & Pearson, James: Exclusive: Russian hackers seek war crimes evidence, Ukraine cyber chief says. *Reuters*, 23.9.2023. [https://www.reuters.com/world/europe/russian-hackers-seek-war-crimes-evidence-ukraine-cyber-chief-says-2023-09-22/], luettu 4.2.2024.

[745] Microsoft (2023b), s. 6.

[746] The Hacker News: Ukrainian Military Targeted in Phishing Campaign Leveraging Drone Manuals. *The Hacker News*, 25.9.2023. [https://thehackernews.com/2023/09/ukrainian-military-targeted-in-phishing.html?m=1], luettu 4.2.2024.

[747] Greig, Jonathan: Russian foreign intelligence service spotted exploiting JetBrains vulnerability. *The Record*, 13.12.2023. [https://therecord.media/russia-svr-exploiting-jetbrains-vulnerability], luettu 5.2.2024; CERT-UA: APT28: від первинного ураження до створення загроз для контролеру домену за годину (CERT-UA#8399). CERT-UA, 28.12.2023. [https://cert.gov.ua/article/6276894], luettu 4.2.2024; Antoniuk, Daryna: Kremlin-backed hackers attacking unpatched Outlook systems, Microsoft says. *The Record*, 4.12.2023. [https://therecord.media/unpatched-microsoft-outlook-email-attacks-fancy-bear], luettu 4.2.2024; Antoniuk, Daryna: Cyber-espionage operation on embassies linked to Russia's Cozy Bear hackers. *The Record*, 14.11.2023. [https://therecord.media/cyber-espionage-campaign-embassies-apt29-cozy-bear], luettu 4.2.2023.

[748] CERT-EU: Cyber Security Brief 23-12 - November 2023. CERT-EU, 4.12.2023 (d). [https://cert.europa.eu/publications/threat-intelligence/cb23-12/], luettu 4.2.2024.

[749] CyberPeace Institute (2023a).

kuljetusalan kohteita vastaan.[750] Killnet ja NoName 057(16) kiihdyttivät uudelleen palvelunestohyökkäyksiään EU-maihin Israelin ja Hamasin välisen sodan alettua 7.10. ja venäläiset haktivistiryhmät kohdistivat kyberhyökkäyksiä Israelia vastaan ja tukivat Hamasin propagandan levittämistä.[751] Marraskuussa Venäjään liitetty Anonymous Sudan väitti hakkeroineensa Cloudflaren internetsivustot, mutta hyökkäyksellä ei yrityksen mukaan ollut vaikutusta palvelutoimintaan.[752] Syyskuussa venäläishakkerit tunkeutuivat Kansainvälisen rikostuomioistuimen järjestelmiin ja vuosivat tuhansia Iso-Britannian puolustusministeriön dokumentteja internettiin.[753] Haktivistien palvelunestohyökkäyksiä tehtiin todennäköisesti lähinnä häirintätarkoituksessa. Ukrainan tukijoille voitiin aiheuttaa lisäkuluja ja muistuttaa heitä tuen jatkamisen hinnasta. Venäjä viestitti sallivansa määrättyjen kyberrikollisten toiminnan venyttäessään REvil-kyberrikollisryhmän oikeusjuttua.[754]

Venäjän kyberoperaatioiden tuki informaatiovaikuttamiselle oli jatkuvaa. Doppelgänger-kampanja jatkoi väärennösten ja valeuutisten levittämistä huolimatta paljastumisestaan ainakin Ranskassa, Yhdysvalloissa, Saksassa ja Ukrainassa. Se käytti hyväkseen tekoälyteknologiaa ja sen tavoitteena oli todennäköisesti hajaannuksen aiheuttaminen. Kampanja ei kuitenkaan tavoittanut merkittävästi yleisöä[755] Venäjä pyrki käyttämään Israelin ja Hamasin lokakuussa syttynyttä sotaa Ukrainan mustamaalaamiseen sosiaalisessa mediassa. Lisäksi venäläinen Storm-1099-uhkatoimija yrtti mustamaalata Ukrainan presidenttiä manipuloimalla yhdysvaltalaisten näyttelijöiden Cameo-palveluun lataamia videoita. Microsoftin mukaan Venäjä vaikuttaa panostavan erityisesti väärennettyihin videoihin ukrainavastaisen propagandansa levittämisessä.[756]

GRU jatkoi yrityksiä Ukrainan asevoimien käyttämien mobiililaitteiden saastuttamiseksi. Sen Infamous Chisel -haittaohjelma pyrki pysyvään läsnäoloon kohdejärjestelmässä ja käytti Tor-verkkoa viestintään. Ukraina on ilmoittanut torjuneensa hyökkäyksen.[757] Toista haittaohjelmaa on yritetty käyttää Ukrainan joukkojen seurantaan saastutettujen mobiililaitteiden Starlink-yhteyden avulla.[758] Solntsepek-haktivistiryh-

---

[750] Arghire, Ionut: Canadian Government Targeted With DDoS Attacks by Pro-Russia Group. *SecurityWeek*, 18.9.2023. [https://www.securityweek.com/canadian-government-targeted-with-ddos-attacks-by-pro-russia-group/], luettu 5.2.2024; CERT-EU (2023d).

[751] CERT-EU: Cyber Security Brief (October 2023). CERT-EU, 3.11.2023. [https://cert.europa.eu/publications/threat-intelligence/cb23-11/], luettu 4.2.2024.

[752] Gatlan, Sergiu: Cloudflare website downed by DDoS attack claimed by Anonymous Sudan. *Bleeping Computer*, 9.11.2023. [https://www.bleepingcomputer.com/news/technology/cloudflare-website-downed-by-ddos-attack-claimed-by-anonymous-sudan/], luettu 4.2.2024.

[753] CSIS (2024).

[754] Кучеров, Андрей: Окружной военный суд решил, кому какое дело. Расследование деятельности группы REvil признано соответствующим УПК. *Коммерсантъ*, 29.10.2023. [https://www.kommersant.ru/doc/6310318], luettu 4.2.2024.

[755] Microsoft (2023b); Antoniuk, Daryna: Russia-linked 'Doppelgänger' social media operation rolls on, report says. *The Record*, 5.12.2023. [https://therecord.media/doppelganger-influence-operation-new-activity], luettu 4.2.2024; CERT-EU: Cyber Security Brief (December 2023). CERT-EU, 4.1.2024. [https://cert.europa.eu/publications/threat-intelligence/cb24-01/], luettu 4.2.2024.

[756] Vicens, AJ.: Russian information operation uses US celebrity Cameos to attack Zelensky. *Cyberscoop*, 7.12.2023. [https://cyberscoop.com/russia-hollywood-actors-zelensky/], luettu 5.2.2024.

[757] CISA: Infamous Chisel Malware Analysis Report. CISA, 31.8.2023. [https://www.cisa.gov/news-events/analysis-reports/ar23-243a], luettu 4.2.2024; CISA: U.S. and International Partners Release Report on Russian Cyber Actors Using "Infamous Chisel" Malware. CISA, 31.8.2023. [https://www.cisa.gov/news-events/news/us-and-international-partners-release-report-russian-cyber-actors-using-infamous-chisel-malware], luettu 4.2.2024.

[758] Corfield, Gareth: Russian spy agencies targeting Starlink with custom malware, Ukraine warns. *The Telegraph*, 12.8.2023. [https://www.telegraph.co.uk/business/2023/08/12/russian-spy-agencies-targeting-elon-musk-starlink-malware/], luettu 4.2.2024.

mä väitti elokuussa tehneensä huomattavasti vakavamman kyberhyökkäyksen Ukrainan elektronisen tiedustelun järjestelmien vastaan mm. lamauttamalla radiotiedusteluasemia ja satelliittiyhteyksiä. Väitteille ei kuitenkaan ole esitetty todisteita.[759] Molemmat osapuolet ovat ryhmittäneet kyberjoukkojen toimintaryhmiä lähemmäs rintamaa tukemaan mm. mobiili- ja langattomien verkkojen tiedustelua ja lennokkien torjuntaa.[760] Taistelukentällä elektroninen sodankäynti on kuitenkin edelleen johtamisjärjestelmäsodankäynnin pääväline.

Käytettävissä olevan aineiston pohjalta pääteltynä vaikuttaisi siltä, että huolimatta muutamasta näyttävästä operaatiosta kybersodankäynti oli siirtymässä haktivistien vastuulle ja että informaatiovaikuttamisen tukeminen ja tiedonhankinta nousivat entistä keskeisempään rooliin.[761] Kulutus- tai asemasodan kehyksessä tuhoavilla kyberhyökkäyksillä oli vaikea saavuttaa operatiivista tai strategista vaikutusta. Patrioottisiin hakkereihin tai muihin ryhmiin tukeutumisessa oli kuitenkin haasteensa. Vuoden 2023 kuluessa loppuun yhä useammat niistä palasivat rikollisen toiminnan pariin tai hajosivat sisäisiin riitoihin.[762]

IT Army of Ukraine ja muut ukrainalaismieliset haktivistiryhmät jatkoivat syksyllä palvelunestohyökkäyksiä ja verkkosivujen sotkemista hyökkäysten määrän kuitenkin laskiessa edellisvuodesta. Tekniikat tosin olivat jonkin verran kehittyneempiä.[763] Esimerkiksi syyskuun Moskovan paikallisvaalien online-äänestystä häirittiin palvelunestohyökkäyksellä[764] ja marraskuussa Sber-yhtiötä vastaan tehtiin sen historian suurin palvelunestohyökkäys.[765] Ukraina pyrki häiritsemään Venäjän satelliittiviestintää ja häiritsi satelliitti-TV:n lähetyksiä etenkin Krimillä useita kertoja.[766] Krimin internetpalvelutarjoajiin kohdistui voimakas hyökkäys 21.–22.9. samaan aikaan Ukrainan tekemän lennokki-iskun kanssa.[767] Venäjän pankkisektori samoin kuin puolustusteollisuus olivat edelleen hyökkäysten kohteena, jotka nekin kehittyivät tekniikaltaan määrän vähetessä.[768] Lokakuussa venäläisteleoperaattori Transtelekomia vastaan tehtiin kyber-

---

[759] CERT-EU: Cyber Security Brief (August 2023). CERT-EU: 1.9.2023. [https://cert.europa.eu/publications/threat-intelligence/cb23-10/], luettu 4.2.2024.

[760] Corera, Gordon: Ukraine war: Cyber-teams fight a high-tech war on front lines. *BBC*, 6.9.2023. [https://www.bbc.com/news/world-europe-66686584], luettu 4.2.2024.

[761] Näin totesi myös korruptiosyytösten takia joulukuussa 2023 erotettu SSSCIP:n johtaja Viktor Zhoran (Temple-Raston, Dina: In recent interview, ousted Ukrainian cyber official spoke about new Russian attacks, long-term plans. *The Record*, 20.11.2023. [https://therecord.media/victor-zhora-interview-click-here-ousted], luettu 5.2.2024.

[762] Antoniuk, Daryna: Leader of Russian hacktivist group Killnet 'retires,' appoints new head. *The Record*, 8.12.2023. [https://therecord.media/killnet-killmilk-announces-retirement], luettu 8.12.2023; CyberPeace Institute (2023c); Microsoft (2023b).

[763] Нефёдова, Мария: Qrator Labs: рекорд по длительности DDoS-атак составил более 70 часов. *Xakep.ru*, 02.11.2023. [https://xakep.ru/2023/11/02/ddos-stats-2023-q3/], luettu 4.2.2024.

[764] ТАСС: DDoS-атаки стали причиной задержки СМС для участников онлайн-голосования в Москве. *ТАСС*, 8.9.2023. [https://tass.ru/politika/18683863], luettu 4.2.2024.

[765] Paganini, Pierluigi: The Largest Russian Bank Sberbank Hit by A Massive DDoS Attack. *Security Affairs*, 9.11.2023. [https://securityaffairs.com/153888/hacking/russian-bank-sberbank-massive-ddos-attack.html], luettu 5.2.2024.

[766] Интерфакс: Минцифры и другие ведомства борются с попытками заглушить российские спутники. *Интерфакс*, 6.9.2023. [https://www.interfax.ru/russia/919465], luettu 5.2.2024; Jason Jay Smart: Twiitti 5.11.2023. [https://twitter.com/officejjsmart/status/1721261370031644682?t=44gzOCqWqQAzl-c4XuybiQ&s=19], luettu 5.2.2024.

[767] Александров, Егор: В Крыму возникли перебои с интернетом из-за кибератаки. *Коммерсантъ*, 22.9.2023. [https://www.kommersant.ru/doc/6235858], luettu 5.2.2024.

[768] SecurityLab.ru: 21 миллион строк «откровений»: группировка NLB взломала МТС Банк. *SecurityLab.ru,* 7.9.2023. [https://www.securitylab.ru/news/541592.php], luettu 5.2.2023; D-Russia: Positive Technologies сообщила об атаках новой хакерской группировки на российский ОПК. *D-Russia*, 27.9.2023. [https://d-russia.ru/positive-technologies-soobshhila-ob-atakah-novoj-hakerskoj-gruppirovki-na-

hyökkäys kiristyshaittaohjelmalla[769] ja miehitettyjen alueiden teleoperaattoreita vastaan tehtiin palvelunestohyökkäyksiä.[770] Loppuvuodesta Ukrainan tuhoavissa kyberhyökkäyksissä esiintyi piikki, sen iskiessä Venäjän liittovaltion veropalvelun, lentoyhtiö Rosaviatsian ja Rosvodokanal vesihuoltoyhtiön järjestelmiä vastaan.[771]

Loppukesästä ja alkusyksystä on Krimille kohdistuneissa Ukrainan lennokki-, ohjus- ja kyberhyökkäyksissä havaittavissa, jos ei koordinoinnin piirteitä, niin useiden saman aikaisten menetelmien käyttöä Venäjän aseman heikentämiseksi Krimillä. Todennäköisesti hyökkäysten oli myös tarkoitus osoittaa, että Venäjä ei kyennyt varmistamaan valloittamiensa alueiden turvallisuutta ja näin legitimoimaan valtaansa siellä. Joulukuussa tapahtuneet kyberhyökkäykset Venäjän kriittistä infrastruktuuria kohtaan olivat selvä kosto Venäjän ohjusiskuista. Hyökkäykset jatkuivat tammi-helmikuussa 2024 ja niillä pyrittiin todennäköisesti vaikuttamaan yhteiskunnalliseen ilmapiiriin Venäjällä ennen maaliskuun presidentinvaaleja.[772] Venäjään vaikuttaa vuoden 2024 alussa kohdistuneen aikaisempaa enemmän kriittisiä hyökkäyksiä, tietovuotojen määrä on jatkanut kasvuaan ja kansallisessa internetsegmentissä on esiintynyt vakavia häiriöitä.[773] Tapahtumat osoittavat yhdessä vuoden 2023 aikaisempien kyber- sekä lennokkihyökkäysten kanssa Ukrainan toiminnan muuttuneen aggressiivisemmaksi sen pyrkiessä vaikuttamaan Venäjän kotirintamaan.

Lännessä Venäjän informaatiovaikuttamisoperaatioiden torjumista vaikeuttivat viestintäpalvelu X:n uudistuneet säännöt ja Elon Muskin henkilökohtaiset näkemykset.[774] Muskin haluttomuus tukea Ukrainan lennokkioperaatioita Starlinkin yhteyksillä Venäjän selustassa aiheutti myös ajoittaista kitkaa liittolaisten välille.[775] Deterrenssiä rakentaakseen Yhdysvallat jatkoi venäläisten hakkereiden nimeämistä ja sanktiointia ja

---

rossijskij-opk.html], luettu 5.2.2023; Antoniuk, Daryna: XDSpy hackers attack military-industrial companies in Russia. *The Record*, 1.12.2023. [https://therecord.media/xdspy-hackers-target-russian-military-industrial-companies], luettu 5.2.2024.

[769] Исакова, Татьяна & Тишина, Юлия: Оператор связи «Транстелеком» подвергся кибератаке. *Коммерсантъ*, 30.10.2023. [https://www.kommersant.ru/doc/6311071], luettu 5.2.2024.

[770] Manuel, Rojoef: Hacktivists Disable Russian Internet in Occupied Ukraine Territories Over the Weekend. *The Defense Post*, 30.10.2023. [https://www.thedefensepost.com/2023/10/30/ukraine-hacktivists-disable-russian-internet/], luettu 5.2.2024.

[771] Костирін, Володимир & Акимова, Юлія: Українські хакери атакували "Росводоканал" і отримали його дані, - джерела. *РБК-Україна*, 20.12.2023. [https://www.rbc.ua/rus/news/ukrayinski-hakeri-atakuvali-rosvodokanal-1703104226.html], luettu 5.2.2024; Беляев, Михаил: ФНС опровергла взлом украинскими хакерами налоговой системы России. *Коммерсантъ*, 12.12.2023. [https://www.kommersant.ru/doc/6396113], luettu 5.2.2025; Antoniuk, Daryna: Ukraine claims cyber operation against Russian aviation agency. *The Record*, 27.11.2023. [https://therecord.media/ukraine-cyber-operation-russian-aviation-agency], luettu 5.2.2024.

[772] Khalilova, Dinara: Media: Ukrainian hackers hit Russian internet provider, claim they are preparing 'revenge for Kyivstar.' *The Kyiv Independent*, 9.1.2024. [https://kyivindependent.com/media-ukrainian-hackers-hit-russian-internet-provider-claim-they-are-preparing-revenge-for-kyivstar/], luettu 6.2.2024; Deeba, Ahmed: Ukraine Claims Destruction of 280 Russian Servers, 2 Petabytes Lost. *Hackread*, 28.1.2024. [https://www.hackread.com/ukraine-destruct-280-russian-servers-petabytes-lost/], luettu 6.2.2024.

[773] Исакова, Татьяна: У контролеров глаза велики. *Коммерсантъ*, 28.02.2024. [https://www.kommersant.ru/doc/6533510], luettu 28.2.2024; Известия: С начала года число высококритичных кибератак в РФ выросло более чем в три раза. *Известия*, 22.2.2024. [https://iz.ru/1653921/2024-02-22/s-nachala-goda-chislo-vysokokritichnykh-kiberatak-v-rf-vyroslo-bolee-chem-v-tri-raza], luettu 28.2.2024; ТАСС: Что известно о массовом сбое в работе Telegram. *ТАСС*, 27.2.2024. [https://tass.ru/ekonomika/20094623], luettu 28.2.2024.

[774] Ramirez, Isabella: Elon Musk's Changes to Twitter Helped Spread Russian Propaganda: EU. *Daily Beast*, 1.9.2023. [https://www.thedailybeast.com/elon-musks-changes-to-twitter-helped-spread-russian-propaganda-eu?source=twitter&via=desktop], luettu 6.2.2024.

[775] Ilkka, Ilmo: Ukraina kommentoi vihaisesti väitettä, jonka mukaan Musk sammutti Starlinkin kesken hyökkäyksen Krimillä. *Helsingin Sanomat*, 8.9.2023. [https://www.hs.fi/ulkomaat/art-2000009840641.html], luettu 6.2.2024.

asetti, tosin kyberrikollisuuden tukemisesta, yhdelletoista Trickbot-ryhmän jäsenelle pakotteita 8.9.[776] Marraskuussa Yhdysvallat asetti venäläisille IT-alan yrityksille lisää sanktioita.[777] Vuoden 2023 loppupuoliskolla Nato- ja EU-maat jatkoivat Venäjän disinformaatio- ja kyberhyökkäysten torjuntaa ja ehkäisyä, mutta eivät olleet valmiita eskaloimaan tilannetta. Tämän tutkimuksen tarkastelun ulkopuolelle jäävät kuitenkin mahdolliset Venäjän tukijoihin tai sitä taloussanktioiden kiertämisessä auttaviin maihin kohdistuneet operaatiot.

Suomi on vuosina 2022–2023 saanut osansa Venäjän kyberhyökkäyksistä. Suomeen kohdistuneet kiristyshaittaohjelmahyökkäykset ovat nelinkertaistuneet maan liityttyä Natoon.[778] Maahan on kohdistunut myös jatkuvia venäläishaktivistien palvelunestohyökkäyksiä.[779] Venäjän GPS-häirintä on vaikuttanut Suomen alueen lentoliikenteeseen.[780] Lisäksi Suomen, Viron, Ruotsin ja Venäjän väliset tietoliikennekaapelit katkesivat lokakuussa mahdollisesti tahallisesti noin viikko sen jälkeen, kun Venäjän tietoliikennekaapelissa Ohotanmerellä oli väitetysti havaittu häiriöitä.[781] Vaikuttaisikin siltä, että Suomen kansallisesta kybertilasta on viimeistään vuonna 2023 mennessä tullut osa suurvaltojen välisen jatkuvan kamppailun toimintakenttää. Muutos on venäläisen strategisen kulttuurin näkökulmasta looginen.

6.4. Yhteenveto vuodesta 2023

Vuoden 2023 osalta ei ole erotettavissa yhtä selkeitä kyberhyökkäyskampanjoita tai vaiheita kuin vuonna 2022. Kevään 2022 jälkeen tapahtunut siirtymä vakoiluun ja informaatiovaikuttamisen tukemiseen vahvistui vuoden 2023 aikana palvelunestohyökkäysten ja yksittäisten tuhoavien operaatioiden intensiteetin noustessa ja laskiessa Ukrainassa operatiivisen tason tapahtumia seuraten ja ulkomailla strategisen tilanteen muutosten mukaan. Cyber Peace Instituten seurannan mukaan yksittäisten hyökkäyksien määrä kasvoi merkittävästi vuoden alussa, laski kiihtyäkseen uudelleen toukokuussa, minkä jälkeen säilyi suhteellisen matalana kesän. Syksyllä Ukrainaan kohdistui kolme kampanjanomaista hyökkäyssarjaa.[782]

---

[776] The Hacker News: U.K. and U.S. Sanction 11 Russia-based TrickBot Cybercrime Gang Members. *The Hacker News*, 8.9.2023. [https://thehackernews.com/2023/09/uk-and-us-sanction-11-russia-based.html?m=1], luettu 6.2.2024.

[777] Королев, Игорь: Америка ввела санкции против знаменитых российских ИТ-компаний, замглавы Минцифры и хозяев МТС. *CNews*, 3.11.2023. [https://www.cnews.ru/news/top/2023-11-03_amerika_vvela_sanktsii_protiv], luettu 6.2.2024.

[778] Paganini, Pierluigi: The Number Of Ransomware Attacks Targeting Finland Increased Fourfold Since It Started The Process To Join NATO. *Security Affairs*, 7.8.2023. [https://securityaffairs.com/149244/hacking/ransomware-attacks-against-finland.html], luettu 6.2.2024.

[779] Sinkko-Westerholm, Pipsa: Venäläinen hakkeriryhmä ottaa nimiinsä keskiviikkona tehdyt palvelunestohyökkäykset. *Helsingin Sanomat*, 11.10.2024. [https://www.hs.fi/kotimaa/art-2000009916111.html], luettu 6.2.2024.

[780] Rummukainen, Anu: Katkennut yhteys. *YLE MOT*, 31.1.2023. [https://yle.fi/a/74-20015375], luettu 6.2.2024.

[781] Chiappa, Claudia: Russia finds damage to its Baltic Sea telecoms cable. *Politco,* 6.11.2023. [https://www.politico.eu/article/russia-find-damage-baltic-sea-telecoms-cable/], luettu 6.2.2024; Любавина, Анна: Внезапные аварии на магистральных кабелях. Два региона России остались без интернета. *CNews*, 11.10.2023. [https://www.cnews.ru/news/top/2023-10-11_srazu_dva_uchastka_optovolokonnoj], luettu 6.2.2024; Королев, Павел: "Ростелеком" вернет связь на Курильские острова. *Comnews*, 12.10.2023. [https://www.comnews.ru/content/229406/2023-10-12/2023-w41/1007/rostelekom-vernet-svyaz-kurilskie-ostrova], luettu 6.2.2024.

[782] CyberPeace Institute (2023a).

Vuoden 2023 hyökkäykset voidaan liittää Venäjän hyökkäystoiminnan aktivoitumiseen: Vuhledarin hyökkäys tammi-helmikuussa, risteilyohjusiskut huhti-toukokuussa ja vastahyökkäykset Donbassissa sekä ohjus- ja lennokki-iskujen lisääntyminen syyskuusta alkaen. Pääosa tunnetuista hyökkäyksistä oli kuitenkin jatkuvia palvelunestohyökkäyksiä ja verkkourkintaa. Sotilaskohteisiin kohdistuneista hyökkäyksistä ei ole tietoa. Tietoturvayhtiöiden raporttien mukaan on pääteltävissä, että ennen kaikkea haktivistien palvelunesto- ja sotkemishyökkäykset säilyivät korkealla tasolla vielä keväällä 2023, mutta niiden määrä alkoi hieman laskea vuoden jälkimmäisellä puoliskolla. Raporttien perusteella hyökkäykset ammattimaistuivat, kehittyivät ja muuttuivat jossain määrin järjestelmällisemmiksi.

Vuoden 2023 aikana Venäjän kyberhyökkäysoperaatioissa on painottunut vakoilu ja valtiosidonnaisten haktivistien kautta toteutettu informaatiovaikuttamisen tukeminen. Vakoilulla on pyritty hankkimaan operatiivistaktista tietoa Ukrainan asevoimien toiminnasta ja strategisella tasolla Ukrainan sisäisen tilanteen kehittymisestä ja sen liittolaisten näkemyksistä ja tuen määrästä ja laadusta. Vakoilua ovat toteuttaneet useat niin valtiolliset kuin ei-valtiolliset toimijat sekä ainakin Venäjän valkovenäläiset liittolaiset. Informaatiovaikuttamista on tuettu tekemällä näyttäviä tuhoavia hyökkäyksiä, vaikuttamalla Ukrainan yhteiskunnan toimintaan, vaikeuttamalla talouselämän normaalia toimintaa, häiritsemällä ukrainalaisen median toimintaa ja hankkimalla ja vuotamalla arkaluontoista materiaalia. Patrioottiset hakkeriryhmät, tai paremminkin sijaistoimijat, NoName057(16) ja Killnet ovat olleet pääosin vastuussa palvelunestohyökkäyksistä. Taloudellinen ja sotilaallinen tuki Ukrainalle sekä poliitikkojen lausunnot näyttävät olleen pääsyitä haktivistien hyökkäyksille Ukrainan ulkopuolisia kohteita vastaan.[783]

Tuhoavien haittaohjelmien tai kiristysohjelmien käyttö Venäjän sotilasoperaation ensimmäisen kahdentoista kuukauden aikana on ollut määrältään ja laadultaan ennen näkemätöntä, muttei ole tuottanut merkittäviä näkyviä vaikutuksia.[784] Vuoden 2023 osalta tuhoavat hyökkäykset vaikuttavat keskittyneen media- ja teleliikennealaan, joilla on todennäköisesti tähdätty informaatiopsykologisiin vaikutuksiin, sillä niihin ei ole liittynyt merkittäviä operatiivisstrategisia sotatoimia. Tosin teleliikenneoperaattoreihin kohdistuneilla hyökkäyksillä on mahdollisesti valmisteltu vakavampia hyökkäyksiä. Mandiantin arvion mukaan ainakin GRU on pyrkinyt operaatioiden nopeampaa valmisteluun ja toimeenpanoon vakioitujen toimintatapojen ja menetelmien avulla.[785] Toisaalta ukrainalaisten mukaan Venäjä on lisännyt tuotantoketjuhyökkäyksiä ohjelmistoalan yrityksiä vastaan, mikä viestiin huolellisemmasta ja hienostuneemmasta valmistelusta.[786]

Haktivistien hyökkäykset OT-järjestelmiä vastaan eivät ole tuottaneet todistettavia tuloksia.[787] Palvelunestohyökkäykset ovat olleet koko operaation ajan erittäin suosittuja, mutta niiden vaikutus on ollut rajallinen. Hyökkäykset ovat myöhemmin painottuneet kriittisiin palveluihin ja infrastruktuuriin, jossa lyhytaikainenkin häiriö voi tietenkin vaikuttaa asevoimien tai yhteiskunnan toimintaan.[788] Tuhoaviin ja häiritseviin kyberhyökkäyksiin on joissain tapauksissa liitetty erillinen informaatiovaikuttamiskom-

[783] CyberPeace Institute (2023c).
[784] ESET (2023a).
[785] Black & Roncone (2023).
[786] Antoniuk (2023a).
[787] Kapellmann Zafra, Daniel, Lunden, Keith & Brubaker, Nathan: We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems. Mandiant, 22.3.2023. [https://www.mandiant.com/resources/blog/hacktivists-targeting-ot-systems], luettu 6.2.2024.
[788] The MOD of Lithuania (2023).

ponentti. Venäjän valtiotoimijoiden hyökkäyksiä on ”mainostettu” haktivistien avulla luovuttamalla niille varastettuja tietoja tai antamalla niiden ottaa kunnia hyökkäyksistä.[789]

Vuoden 2023 aikana haktivistikenttä on yhtäältä hajaantunut rikollisten ja kansainvälisten toimijoiden mielenkiinnon siirtyessä muualle. Toisaalta eräiden valtiosidonnaisten haktivistiryhmien toiminta näyttää vakiintuneen samalla, kun uusia ryhmiä on syntynyt tai synnytetty harhauttamistarkoituksessa. Osa ryhmistä on erikoistunut määrätyn kaltaisiin operaatioihin.[790] Microsoftin mukaan vähintäänkin Solntsepek, InfoCenter ja Cyber Army of Russia -ryhmät ovat olleet aktiivisessa yhteydessä GRU:hun ja ovat pyrkineet levittämään disinformaatiota Venäjän kyberhyökkäyksiin liittyen.[791] Venäjän rinnalla toimii valkovenäläisen Ghostwriterin ja kazakstanilaisen YoroTrooperin kaltaisia ryhmiä, joiden tavoitteet ovat vähintään osittain yhteneviä Venäjän kanssa.[792] Tämän kehityksen seurauksena Ukrainan kybertilassa toimii useita eri valtiollisia ja ei-valtiollisia toimijoita, joista osa on ystävällismielisiä, osa vihamielisiä ja osa pyrkii vain hankkimaan tiedustelutietoa konfliktista ja sen osapuolista tai hyötymään tilanteesta taloudellisesti. Taistelutilana se on siis sekava ja jatkuvassa muutoksessa.

Vaikka pääosa Venäjän kyberhyökkäyksistä vuonna 2023 onkin kohdistunut Ukrainaan, merkittävä osa niistä on kohdistunut Nato-maihin.[793] Sodan siirtyessä kulutussotavaiheeseen Venäjälle on ollut entistä tärkeämpää hankkia tietoa Ukrainan liittolaisista, joiden tuesta Ukraina on riippuvainen, ja toisaalta pyrkiä tuon tiedon varassa toteuttamaan operaatioita, jotka rapauttavat Ukrainan saamaa tukea. Tämän lisäksi Venäjälle on edelleen tärkeää estää Lännen suora sotilaallinen osallistuminen sotaan. Vaikka deterrenssiviestintä ei ole ollut yhtä vahvaa kuin vuonna 2022, on sekin näytellyt osaa Venäjän operaatioissa. Venäjä todennäköisesti katsoo sodan siirtyneen vaiheeseen, jossa informaatiosodankäynnin teknologisilla keinoilla on enemmän saavutettavaa ei-sotilaallisen ja ei-väkivaltaisen voimakäytön välineinä kuin aseellisen voimankäytön tukena tai osana. Informaatioylivoiman hankkiminen tarjoaa mahdollisuuden muuttaa voimatasapaino ratkaisevasti ja nopeastikin Venäjän hyväksi ja täten mahdollisuuden sodan lopettamiseen Venäjän etujen mukaisella tavalla.[794]

Läntisissä tutkijapiireissä on Venäjän vuosien 2022–2023 kyberhyökkäysten tavoitteeksi arvioitu pikemminkin Ukrainan valtiojohdon viestinnän häirintää ja lamauttamista, disinformaation levittämistä ja yhteiskunnan poliittiseen johtoon koetun luottamuksen horjuttamista sekä ennen kaikkea tiedustelua ja vakoilua kuin kriittisen infrastruktuurin tuhoamista tai koko informaatioyhteiskunnan romahduttamista. Tutkijat ovat olleet eri mieltä siitä, pyrkikö ja kykenikö Venäjä koordinoimaan kyber- ja kineettisiä vaikutuksia taistelukentällä.[795] Keskustelua on usein miten käyty taktisella tasolla, jolloin huomio on ollut kyber- ja kineettisten vaikutusten käyttämisessä samaa kohdetta vastaan määrätyssä aikaikkunassa. Toisaalta Harry Kantola on esittänyt, että Venäjä pyrki suunnitelmallisesti käyttämään hyökkäysoperaation alkuvaiheessa kyberhyökkäyksiä tietojärjestelmiä vastaan yhdistääkseen kineettisen ja ei-kineettisen

[789] Microsoft (2023a).
[790] The MOD of Lithuania (2023).
[791] Microsoft (2023b).
[792] CISCO (2023a).
[793] Microsoft (2023a).
[794] Kerr (2023), s.34.
[795] Schulze & Kerttunen (2023); The MOD of Lithuania (2023); Mueller et al. (2023); Schulze & Kerttunen (2023); Levite (2023); Bateman (2022).

vaikuttamisen, mutta muutti painotuksen informaatiovaikuttamista tukeviin hyökkäyksiin alkuperäisin suunnitelman epäonnistuttua.[796] Tämä tutkimus vaikuttaisi vahvistavan Kantolan päätelmän.

Olennaista Venäjän kyberoperaatioiden arvioinnissa on asettaa ne kulloisenkin sodan vaiheen kontekstiin. Vuoden 2022 helmikuun, huhtikuun ja syksyn tuhoavat operaatiot toteutettiin eri tilanteessa kuin vuoden 2023 operaatiot. Tavoitteiden muuttumisen lisäksi Venäjän sotilas- ja poliittisen johdon näkemykset kybervälineiden käytettävyydestä todennäköisesti muuttuivat ja organisaatioillakin oli omat kokemuksensa ja intressinsä, jotka vaikuttavat operaatioiden toteutukseen. Venäjän hyökkäyksellisten kyberoperaatioiden luonne käy järkeen, jos ne asetetaan historiallisten muotojen, keinojen ja tavoitteiden kehykseen: operaatio Tonavan (Tšekkoslovakia 1968) ja Štorm 333:n (Afganistan 1978) malliin. Niihin kuului informaatio-operaatio vastustajan heikentämiseksi ja hämäämiseksi sekä yllätyksellinen isku, johon liittyi epäsuorien keinojen käyttö ja pyrkimys vaikuttaa suoraan valtion johtoon. Niihin liittyi myös häikäilemätöntä väkivaltaa, joka tosin Ukrainan tapauksessa on ollut alusta lähtien merkittävästi intensiivisempää.[797]

Todennäköisesti Venäjän kyberhyökkäykset Ukrainassa koordinoitiin alkuperäisessä Venäjän suunnitelmassa yllätykselliselle kaappaushyökkäykselle asetettujen vaatimusten kanssa informaatioiskuoperaatioksi, jonka oli tarkoitus hetkellisesti lamauttaa valtiojohto, asevoimat ja edistää vallanvaihtoa.[798] Ennen alkutalvea 2022 niillä pyrittiin manipuloimaan Ukrainaa poliittisstrategisten tavoitteiden saavuttamiseksi ei-sotilaallisin ja ei-väkivaltaisin keinoin. Tammi-helmikuutta 2022 voidaan hyvällä syyllä pitää jo sotaa edeltävänä aikana, jossa tulevan sodan reunaehdot pyrittiin saattamaan Venäjälle edullisiksi samalla heikentäen ja hämäten vastustajaa ja sen liittolaisia. Kyberoperaatiolla pyrittiin tukemaan yllätyksen saavuttamista ja mahdollisesti peitettiin helmimaaliskuun tuhoavien kyberhyökkäysten valmistelu. Niillä toteutettiin myös deterrenssiviestintää osoittamalla Venäjän kykyä ja valmiutta toteuttaa tuhoaviakin kyberhyökkäyksiä. Sodan alkuvaiheessa kaappaushyökkäyksen alettua kyberoperaatioiden piti lamauttaa Ukrainan valtiojohto ja tukea informaatioylivoiman saavuttamista sekä disorganisoida turvallisuuspalveluiden ja asevoimien johto. Informaatioylivoiman hankkiminen nähtiin varmasti tärkeänä operaation onnistumiselle. Siitä kertoo se, kuinka Venäjä operaation alkuvaiheen epäonnistuttua pyrki entistä voimakkaammin lamauttamaan Ukrainan valtion informaatioinfrastruktuurin, viestinnän ja median kyberhyökkäyksillä.

Toisaalta, operaatiotaidolliseen tulkintaan ei tule luottaa liikaa, koska mitä ilmeisemmin Venäjän asevoimat ja turvallisuuspalvelut eivät saaneet ja ehtineet suunnitella yhteisoperaatiota, jossa kyberoperaatiot olisi tuotu riittävän hyvin osaksi operatiivisia suunnitelmia.[799] Jos Venäjän asevoimilta, mukaan lukien GRU, puuttuivat vaihtoehtosuunnitelmat hyökkäyksen epäonnistuessa, niitä ei todennäköisesti ollut kyberope-

[796] Kantola (2023).
[797] DeBenedictis, Kent: *Russian 'Hybrid Warfare' and the Annexation of Crimea. The Modern Application of Soviet Political Warfare*. Bloomsbury, London, 2022; Braithwaite, Rodric: *Afgantsy. The Russians in Afghanistan 1979–89*. Oxford University Press, New York, 2011.
[798] Saman näkemyksen esittäneet: Lonergan, Erica D., Smith, Margaret W. & Mueller, Grace B.: Evaluating Assumptions About the Role of Cyberspace in Warfighting: Evidence from Ukraine. *2023 15th International Conference on Cyber Conflict*. T. Jančárková, D. Giovannelli, K. Podiņš, I. Winther (Toim.) NATO CCDCOE Publications, Tallinn, 2023, s. 85–102.
[799] Schulze & Kerttunen (2023); Watling & Reynolds (2022); Lin, Herbert: Russian Cyber Operations in the Invasion of Ukraine. *The Cyber Defense Review*, 7(4) 2022, s. 31–4.

raatioiden osalta tiedustelupalveluillakaan.[800] Viimeistään viikon kuluttua hyökkäyksen alkamisesta kyberhyökkäyksien luonne erosi alkuperäisestä suunnitelmasta. Maalis-huhtikuussa pyrittiin saavuttamaan sekä informaatioteknologisia että -psykologisia vaikutuksia, Ukrainan johdon ja yhteiskunnan halvaannuttamiseksi ja pakottamiseksi neuvotteluihin. Sotatoimen kehittyessä epäsuotuisasti muissa toimintaympäristöissä, valmisteltujen ”kyberaseiden” loppuessa, Ukrainan vastarinnan tiivistyttyä ja kyberpuolustuksen vahvistuttua sekä läntisen avun merkityksen kasvaessa oli loogista siirtää operaatioiden painopiste tiedusteluun ja informaatiovaikuttamisen tukemiseen haktivistien eli massan avulla. Tuhoavilla hyökkäyksillä kriittistä infrastruktuuria vastaan ei taistelujen tässä vaiheessa ollut saavutettavissa merkittävää vaikutusta. Viimeistään kesän 2022 loppupuolella Yhdysvaltojen ja Venäjän välinen deterrenssiviestintä oli tasoittanut tilanteen niin, että Länteen suunnatun ennaltaehkäisevän iskun tai Venäjän internetistä irti kytkemisen pelko oli lieventynyt.

On kyseenalaista, nähtiinkö helmi-maaliskuun 2022 hyökkäykseen kuuluvaksi infrastruktuuriin kohdistuvaa strategista iskua, mutta syksyn ohjusiskut Ukrainan sähköinfrastruktuuriin olivat strateginen pommituskampanja vastustajan syvyydessä – samoin 2023 loppuvuoden hyökkäykset. Ohjushyökkäyksiin liittyvät tuhoavat kyberoperaatiot on nähtävä osana uutta strategiaa – ei enää kaappauksena tai uusien alueiden haltuunottoon tähtäävänä vaan Ukrainan uuvuttamiseen pyrkivänä – ja sitä toteuttavaa operaatiota, jossa pyrittiin strategiseen vaikutukseen kriittistä infrastruktuuria vastaan informaatio- ja kineettisten menetelmien yhteiskäytöllä. Tässä yhteydessä kyberhyökkäykset voidaan nähdä venäläisittäin asymmetrisenä, kustannustehokkaana ja epäsuorana keinona, osana Ukrainan sähköverkon lamauttamiseen kohdistuvaa operaatiota. Vuoden 2023 tuhoavat kyberhyökkäykset ovat olleet enemmän sidoksissa kostoiskuihin vastauksena Ukrainan kyber- tai muihin operaatioihin, deterrenssiviestintään, poliittisiin tapahtumiin, menetelmien testaamiseen ja kulutussodankäyntiin kybertilassa. Tällaista kybersodankäyntiä venäläiset sotataidolliset kirjoitukset eivät ole visioineet – koska tavanomainen kulutussodankäynti ei kuulunut oletetun tulevaisuuden sodankäynnin luonteeseen – lukuun ottamatta informaatiopsykologisia vaikutuksia painottavia kirjoittajia. Hekin ovat epäilemättä tyytymättömiä informaatiovaikuttamisen tukemisoperaatioiden tuottamiin tuloksiin.

Venäjän hyökkäyksellisten, tuhoavien ja lamauttavien kyberoperaatioiden puutteelle ei ole vain yhtä syytä. Sodan ja taistelujen luonne sekä operatiivisen tason tavoitteet ovat muuttuneet kahden vuoden aikana useasti. Sodan ensi vaiheen selitys tapahtumille ei päde enää vuoden päästä havaittuihin tapahtumiin. Kybertoimien tarkoituksenmukaisuus ja suhde muihin sotilaallisen ja ei-sotilaallisen voimankäytön muotoihin on täten myös vaihdellut. Osapuolten suorituskyvyt ja kybertilan ominaisuudet ovat muuttuneet. Vuoden 2023 aikana oli todennäköisesti paljon tarkoituksenmukaisempaa pyrkiä hankkimaan tietoa Ukrainan asevoimista, sotataloudesta, poliittisen johdon näkemyksistä ja liittolaisten sitoutumisesta kuin paljastaa ja menettää hankittu pääsy Ukrainan verkkoihin lyhyt aikaista etua tavoittelevilla hyökkäyksillä. Haktivistien palvelunestohyökkäykset, tietovuodot ja verkkosivujen sotkemiset riittivät Ukrainan horjuttamiseen ja sodan ulkopuolella jatkuvan suurvaltakamppailun tavoitteiden saavuttamiseen. Venäjä ei kuitenkaan luopunut pyrkimyksestä disorganisoida Ukrainan asevoimien johtamista vaan Ukrainan johtamisjärjestelmien häirintää ja johtamisen mani-

[800] Zabrodskyi, Watling, Danylyuk & Reynolds (2022).

pulointia on pidetty tärkeänä koko operaation ajan. Tämän pohjalta voi päätellä, että Venäjällä kyberoperaatioita toimeenpanevat useat tahot, eri tasoilla ja eri tavoittein.

Venäjän hyökkäyksellisten kyberoperaatioiden luonne ja heikko menestys ei vastannut niitä odotuksia, joita läntisillä tutkijoilla ja laajemmalla yleisöllä kybersodankäynnistä ennakkoon oli. ”Kyber Pearl Harbor”, ”Shock and Awe” tai ”Thunder run” -skenaario ei toteutunut, Venäjä ei toteuttanut tuhoavia kyberhyökkäyksiä Länttä vastaan kostoksi pakotteista ja näytöt kineettisten ja kyberoperaatioiden koordinaatiosta ovat jääneet vähäisiksi.[801] Kybereskalaatiota suurvaltojen väliseksi taisteluksi ei tapahtunut. Sodan alkuvaiheessa pelättiin kyberoperaatioiden ns. spill-over vaikutuksia eli leviämistä taistelutilan ulkopuolelle ja haktivistien toiminnan nähtiin voivan johtaa tahattomaan eskalaatioon ja olevan ristiriidassa sodan lakien kanssa. Uhat eivät ole toteutuneet ja haktivistit ovat jatkaneet matalan ja hallitun tason, ilmeisemmin käytännössä aseellisten hyökkäysten alle jäävää, toimintaansa.[802]

Odotusten ja todellisuuden ristiriidan seurauksena käynnistyi edelleen jatkuva keskustelu tutkijoiden kesken yhtäältä Venäjä kybersuorituskykyjen tasosta ja toisaalta kybermenetelmien sotilaallisesta käytettävyydestä yleensäkin.[803] Keskustelu heijastelee laajempaa Ukrainan tapahtumiin liittyvää itsekriittistä keskustelua läntisten sotatieteilijöiden keskuudessa.[804] Vuoden 2022 huhtikuussa Naton edustajat pyrkivät väittämään, että Venäjän kyberhyökkäys oli ennen näkemättömän laaja ja tuhovoimainen, mutta Venäjän asevoimat eivät kyenneet käyttämään sen menestystä hyväkseen. Heidän narratiivinsa on jäänyt vähemmistöön.[805] Eräät tutkijat ovat pyrkineet haastamaan näkemyksen läntisen avun merkityksestä Ukrainan kyberpuolustuksen onnistumisessa ja etsineet selityksiä Venäjän tietoisesta pidättäytymisestä.[806] Kaikista pessimistisimmissä arvoissa on haluttu poistaa kybertilalta ”domainin” asema.[807] Tunnettu kybertutkija James A. Lewis on jopa todennut, että kyberhyökkäykset ovat ”yliarvostettuja.”[808]

---

[801] Tästä keskustelusta paras summaus: Kerr (2023); Nilsson (2023).
[802] Willett (2022).
[803] Lin (2022); Willett (2022); Mueller et al. (2023); Lonergan (2023); Levite (2023); Maschmeyer, Lennart & Kostyuk, Nadiya: There Is No Cyber ‘Shock and Awe’: Plausible Threats in The Ukrainian Conflict. *War on the Rocks*, 8.2.2022. [https://warontherocks.com/2022/02/there-is-no-cyber-shock-and-awe-plausible-threats-in-the-ukrainian-conflict/], luettu 6.2.2024; Healey, Jason: Preventing Cyber Escalation in Ukraine and After. *War on the Rocks*, 9.3.2022. [https://warontherocks.com/2022/03/preventing-cyber-escalation-in-ukraine-and-after/], luettu 6.2.2024; Kostyuk, Nadiya & Gartzke, Erik: Why Cyber Dogs Have Yet to Bark Loudly in Russia’s Invasion of Ukraine. *Texas National Security Review,* 5(3) 2022, s. 113–126; Rovner, Joshua: Sabotage and War in Cyberspace. *War on the Rocks*, 19.7.2022. [https://warontherocks.com/2022/07/sabotage-and-war-in-cyberspace/], luettu 6.2.2024; Lewis, James A.: Cyber War and Ukraine. CSIS, June 2022. [https://www.csis.org/analysis/cyber-war-and-ukraine], luettu 6.2.2024.
[804] Driedger, Jonas J.: Utility-based predictions of military escalation: Why experts forecasted Russia would not invade Ukraine. *Contemporary Security Policy*, 44(4) 2023, s. 544-560; Renz, Bettina: Western Estimates of Russian Military Capabilities and the Invasion of Ukraine. *Problems of Post-Communism*, 2023. [DOI:10.1080/10758216.2023.2253359].
[805] Cattler, David & Black, Daniel: The Myth of the Missing Cyberwar. Russia’s Hacking Succeeded in Ukraine—And Poses a Threat Elsewhere, too. *Foreign Affairs*, 6.4.2022. [https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar], luettu 6.2.2024.
[806] Kostyuk, Nadiya & Brantly, Aaron: War in the borderland through cyberspace: Limits of defending Ukraine through interstate cooperation. *Contemporary Security Policy*, 43(3) 2022, s. 498–515.
[807] Bateman, Jon, Beecroft, Nick & Wilde, Gavin: What the Russian Invasion Reveals About the Future of Cyber Warfare. Carnegie Endowment for International Peace, 9.12.2022. [https://carnegieendowment.org/2022/12/19/what-russian-invasion-reveals-about-future-of-cyber-warfare-pub-88667], luettu 6.2.2024.
[808] Lewis (2022).

Venäjän kyberhyökkäysoperaatioista käyty keskustelu osoittaa, että oikea sota harvoin vastaa ennakko-oletuksia.[809] Samalla se näyttää, kuinka vaikeaa on esittää johtopäätöksiä sodasta, jonka menneiden tapahtumien lähdeaineisto on merkittäviltä osin tavoittamattomissa ja tulevaisuus edelleen avoin. Pyrittiinpä Venäjän vuosien 2022–2023 hyökkäyksellisten kybertoimien arvioinnissa kuinka ehdottomaan objektiivisuuteen tahansa, sodan lopputulos tulee lopulta värittämään tulevaisuuden päätelmiä niin Lännessä kuin Venäjällä.

[809] Saman tematiikan pohdinnasta ks. Kerr (2023).

7. VENÄJÄN KYBERTURVALLISUUS JA -PUOLUSTUS UKRAINAN SODASSA 2022–2023

Vuoden 2022 toukokuussa Putin totesi Venäjän olevan sodassa informaatiotilassa.[810] Samana vuonna kyberhyökkäysten määrä venäläisiä kohteita vastaan kasvoikin väitetysti 80–100 %. Virallisten lähteiden mukaan valtionhallinnon resursseihin kohdistui 25 000 hyökkäystä ja kriittiseen infrastruktuuriin 1200 hyökkäystä.[811] Palvelunestohyökkäykset, häirintäsoitot ja -viestit sekä uutislähetysten häirintä näkyivät venäläisten arjessa. Niiden määrä nousi, tosin kriittisyys väheni, vuoden 2022 loppupuolella yritysten kyberturvallisuuden parantuessa.[812] Tietovuotojen määrä moninkertaistui vuoteen 2021 verrattuna.[813] Vuonna 2022 Venäjään kohdistui vain muutama merkittävä tuhoava kyberhyökkäys, eikä niillä ollut näkyvää vaikutusta yhteiskunnan toimintaan tai Venäjän politiikkaan.[814] Poikkeuksena olivat rautateihin kohdistuneet hyökkäykset, jotka saattoivat vaikuttaa asevoimien joukkojen siirtoihin.[815]

Vuoden 2023 aikana kyberhyökkäysten kokonaismäärä jatkoi kasvamista, mutta kriittisten tapausten määrä väheni edelleen. Toisaalta hyökkäystekniikat kehittyivät ja yhä useampi hyökkäys pyrki aiheuttamaan tuhoa kohdejärjestelmissä. Vuoden 2023 kolmannella neljänneksellä tietoturvatapahtumien määrä oli 85 % korkeampi kuin vastaavalla ajanjaksolla vuonna 2022. Tietovuotojen määrä jatkoi kasvamistaan ja vuoden 2023 aikana venäläisiltä yrityksiltä vuodettiin internetiin dataa n. 92 terabittiä. Rostelekom-Solar -kyberturvallisuusyrityksen mukaan ”huligaanit” ja APT-ryhmät vastasivat 50 % hyökkäyksistä. Hyökkäyksistä pääosa kohdistui julkishallintoon ja noin kymmenys teleliikennealaan, maatalouteen, finanssialaan ja teollisuuteen kuhunkin. NKTsKI:n edustajan mukaan hyökkäykset muuttuivat huolellisemmiksi ja pyrkivät maksimaaliseen vaikutukseen.[816] Vuoden 2024 alussa Venäjään kohdistuneet kyber-

---

[810] Kremlin.ru: Заседание Совета Безопасности. Kremlin.ru, 20.5.2022. [http://kremlin.ru/events/president/news/68451], luettu 6.2.2024.

[811] Тишина, Юлия: Без учений — тьма. *Коммерсантъ*, 13.12.2022. [https://www.kommersant.ru/doc/5705859], luettu 6.2.2024; SecurityLab.ru (2022a); Roskomsvoboda: Минцифры: 100 тысяч IT-специалистов уехало из страны с начала года. *Roskomsvoboda*, 20.12.2022. [https://roskomsvoboda.org/post/otiezd-100tys-specov/], luettu 6.2.2024.

[812] Rostelekom-Solar: Отчет «Кибератаки на российские компании в 2022 году». Rostelekom-Solar. Москва, 2023. [https://rt-solar.ru/analytics/reports/3332], luettu 6.2.2024; Srivastava, Mehul: Russia hammered by pro-Ukrainian hackers following invasion. *Ars Technica*, 6.5.2022. [https://arstechnica.com/information-technology/2022/05/russia-hammered-by-pro-ukrainian-hackers-following-invasion/], luettu 6.2.2024; SecurityLab.ru: Россия-Украина, хроники киберконфликта. *SecurityLab.ru*, 6.6.2022. [https:/www.securitylab.ru/news/532111.php], luettu 6.2.2024.

[813] Ясакова, Екатерина: В России за год утекло более 660 млн записей с персональными данными. *РБК*, 17.4.2023. [https://www.rbc.ru/technology_and_media/17/04/2023/643936229a7947134f0ce21c], luettu 6.2.2024.

[814] CyberPeace Institute (2023b); CyberPeace Institute (2023d).

[815] Gallagher, Ryan: Belarus Hackers Allegedly Disrupted Trains to Thwart Russia. *Bloomberg*, 28.2.20022. [https://www.bloomberg.com/news/articles/2022-02-27/belarus-hackers-allegedly-disrupted-trains-to-thwart-russia], luettu 6.2.2024.

[816] Rostelekom-Solar: Атаки на российские компании во II квартале 2023 года. Rostelekom-Solar, 2023. [https://rt-solar.ru/analytics/reports/3610/], luettu 6.2.2024; Бевза, Дмитрий: Количество кибератак на российские организации в 2023 году заметно выросло. *Российская газета*, 27.7.2023. [https://rg.ru/2023/07/27/kolichestvo-kiberatak-na-rossijskie-organizacii-v-2023-godu-zametno-vyroslo.html], luettu 6.2.2024; Известия: В России почти в 40 раз увеличились случаи утечки личных данных. *Известия*, 7.8.2023. [https://iz.ru/1555263/2023-08-07/v-rossii-pochti-v-40-raz-uvelichilis-sluchai-utechki-lichnykh-dannykh], luettu 6.2.2024; Бевза, Дмитрий: В третьем квартале 2023 года выросло количество хакерских атак на российские компании и госорганы. *Российская газета*, 15.11.2023. [https://rg.ru/2023/11/15/kiborgrabota.html], luettu 6.2.2024.

hyökkäykset ovat saaneet vakavamman luonteen, mikä osoittaa, että tilanne ei ole vakiintunut, vaikka siihen olisikin jollain tavalla totuttu. On selvää, että kyberhyökkäysten kasvu on ollut sidoksissa Ukrainan tapahtumiin ja ne ovat olleet osa sotaa, mutta Putin ei vuoden 2022 toukokuun lausunnostaan huolimatta ole sitonut tapahtumia sotatoimiin.

Venäjän hyökkäyksen alettua useat ICT-alan yritykset vetäytyivät Venäjältä ja mm. Facebookin, Instagramin ja Twitterin käyttö estettiin Venäjällä, koska näiden katsottiin levittävän disinformaatiota. Läntisten uutistoimistojen sivuille pääsy estettiin.[817] EU:ssa vastavuoroisesti kiellettiin venäläisten RT:n ja Sputnikin toiminta.[818] Globaaleista teleliikenneoperaattoreista Cogent ja Lumen lopettivat toimintansa Venäjällä.[819] Venäläispankkeja estettiin käyttämästä maksujärjestelmä SWIFT:iä ja Visa sekä Mastercard lopettivat toimintansa Venäjällä.[820] Yhdysvallat liittolaisineen asetti sanktioita mm. Venäjän ICT- ja kyberturvallisuusalan yrityksiä vastaan.[821] Venäjän laaja-alainen mobiiliverkkojen ja GPS-signaalin häirintä Ukrainan lähialueilla on todennäköisesti vaikuttanut sen oman siviili-infrastruktuurin toimintaan.[822] Venäjän kybertoimintaympäristö muuttui täten radikaalisti Ukrainan hyökkäyksen alettua.

Uudenlaiseen kyberuhkatilanteeseen, läntisten yritysten markkinoilta poistumiseen ja teknologiasanktioihin vastaamiseksi Venäjä on turvautunut valtiovetoiseen politiikkaan. Tavoitteena on teknologisen suvereniteetin turvaaminen ja rakentaminen ja tilanne on pyritty esittämään positiivisena mahdollisuutena Venäjän kansalaisille ja yrityksille.[823] Tavoiteaikataulua suvereenisuuden saavuttamisesta tosin uudelleen arviointiin 10–20 vuoden päähän.[824] Käytännössä valtiojohto yritti yhtäältä pakottaa valtionhallinnon ja -yritykset sekä kriittistä informaatioinfrastruktuuria operoivat yksityisyritykset siirtymään kotimaisten palveluiden, laitteistojen ja ohjelmistojen käyttöön mahdollisimman pian.[825] Tälle oli olemassa lakiperusta jo vuoden 2019 niin kutsutussa

---

[817] Freedom House: Freedomon the Net – Russia, 2023. [https://freedomhouse.org/country/russia/freedom-net/2023], luettu 6.2.2024; SecurityLab.ru: Более 1000 компаний свернули свою деятельность в России. *SecurityLab.ru*. 2.8.2022. [https://www.securitylab.ru/news/533068.php], luettu 6.2.2024.

[818] Chee, Foo Yun: EU bans RT, Sputnik over Ukraine disinformation. *Reuters*, 2.3.2022. [https://www.reuters.com/world/europe/eu-bans-rt-sputnik-banned-over-ukraine-disinformation-2022-03-02/], luettu 6.2.2024.

[819] Iyengar, Rishi: 'This is different': Why internet backbone services are cutting off Russia. *CNN*, 14.3.2022. [https://edition.cnn.com/2022/03/11/tech/russia-internet-backbone-cogent-lumen/index.html], luettu 6.2.2024.

[820] Roth, Emma: Visa and Mastercard suspend their services in Russia / Cards issued in Russia will no longer work outside of the country. *The Verge*, 6.3.2022. [https://www.theverge.com/2022/3/5/22963433/visa-mastercard-suspend-services-russia-ukraine], luettu 6.2.2024.

[821] Tadviser: High-tech sanctions and restrictions against Russia. Tadviser, 19.12.2023 (a). [https://tadviser.com/index.php/Article:High-tech_sanctions_and_restrictions_against_Russia], luettu 6.2.2024.

[822] Тадтаев, Георгий & Ясакова, Екатерина: «Ситидрайв» и «Яндекс» сообщили о сбоях GPS в центре Москвы. *РБК*, 4.5.2023. [www.rbc.ru/technology_and_media/04/05/2023/6453c94c9a7947056a04e6b3?from=from_main_10], luettu 6.2.2024.

[823] ТАСС: Обеспечить технологическую независимость России. Заявления нового главы РАН. *ТАСС*, 20.9.2022. [https://nauka.tass.ru/nauka/15810819], luettu 5.1.2024.

[824] Уварчев, Леонид: Спецпредставитель президента: РФ может достичь технологического суверенитета за 10–20 лет. *Коммерсантъ*, 27.6.2022. [https://www.kommersant.ru/doc/5434318?from=top_main_9], luettu 5.1.2024.

[825] Литвиненко, Юрий & Тишина, Юлия: Губернаторов ведут на контакт. *Коммерсантъ*, 1.6.2022. [https://www.kommersant.ru/doc/5381031], luettu 5.1.2024; Известия: В Минпромторге заявили о переходе ряда госкомпаний на отечественное ПО. *Известия*, 16.8.2022. [https://iz.ru/1380115/2022-08-16/v-minpromtorge-zaiavili-o-perekhode-riada-goskompanii-na-otechestvennoe-po], luettu 5.1.2024; Пашкова, Лилия & Соколов, Кирилл: Сотрудникам российского министерства запретят использовать iPhone.

suvereenin internetin laissa.[826] Käytännössä esimerkiksi FSTEK poisti sertifioinnit Oraclen, Microsoftin ja SAP:n tuotteilta, jolloin niiden käyttö valtionhallinnossa ei enää ollut mahdollista.[827] Toisaalta valtiojohto pyrki ohjaamaan nopealla aikataululla budjettivaroja kotimaiseen laitteisto- ja ohjelmistotuotantoon ja edistämään hankkeita luomalla kompetenssikeskuksia ja julkishallinnon ja yritysmaailman yhteisiä työryhmiä.[828] Näin pyrittiin riippuvuuksien eliminoimisen lisäksi luomaan keinotekoista kysyntää Venäläisille tuotteille. Venäjän IT-sektorin onkin väitetysti kasvanut 2022–2023 yli 6 % ja internettalouden osuus Venäjän GPD:stä nousi vuonna 2023 35 %.[829] Näihin lukuihin on toki suhtauduttava varauksella, sillä Venäjän valtio on salannut merkittäviä osia maan talousluvuista Ukrainan hyökkäysoperaation alettua.[830]

Toukokuussa 2022 presidentti Putin käski turvallisuusneuvostoa huolehtimaan valtion informaatioinfrastruktuurin resilienssistä ja turvallisuudesta.[831] Turvallisuusneuvosto laatikin 2022 kesän aikana suunnitelmia kansallisen informaatioinfrastruktuurin ja maan teknologisen kehityksen turvaamiseksi.[832] Mahdollisesti tämän salaisen suunnitelman pohjalta Putin käski hallituksen laatia suunnitelman Venäjä riippumattomuuden turvaamiseksi ulkomaisista ohjelmistoista lokakuuhun mennessä.[833] Joulukuussa Venäjän hallitus hyväksyi tiekartat kotimaisen ohjelmistoperustan turvaamiseksi. Nämä yhdessä muiden korkeateknologian tiekarttojen, mm. kvanttilaskenta ja -kommunikaatio, AI ja tulevaisuuden mobiiliverkot, kanssa liitettiin osaksi Digitaalisen talouden ohjelmaa.[834] Huhtikuussa 2023 Venäjän hallitus hyväksyi asetuksen teknologisen suvereniteetin projektien pääsuunnista, joihin kuului mm. mikroprosessorien valmistaminen, mobiiliverkkolaitteisto ja ICT-teknologia laajemminkin.[835]

РБК, 5.7.2023. [https://www.rbc.ru/technology_and_media/05/07/2023/64a4e8f69a794747898acaaf], luettu 5.1.2024

[826] Федеральный закон № 90-ФЗ (2019).

[827] Холупова, Кристина: У Microsoft, Oracle, SAP и IBM отзывают сертификаты ФСТЭК. Cnews, 28.3.2022. [https://www.cnews.ru/news/top/2022-03-28_u_ibmmicrosoftoraclesap_otzyvayut], luettu 6.2.2024.

[828] Известия: Правительство ускорит работу по выводу на рынок российских разработок по ПО. *Известия*, 20.7.2022. [https://iz.ru/1367630/2022-07-20/pravitelstvo-uskorit-rabotu-po-vyvodu-na-rynok-rossiiskikh-razrabotok-po-po], luettu 5.1.2024.

[829] Тюняева, Марина: Вклад интернета в экономику России вырос на треть в 2023 году. *Ведомости*, 13.12.2023. [https://www.vedomosti.ru/economics/articles/2023/12/13/1010924-interneta-ekonomiku-viros], luettu 6.2.2024; Tadviser: ICT market of Russia. Tadviser, 5.9.2023. [https://tadviser.com/index.php/Article:ICT_market_of_Russia], luettu 5.1.2024.

[830] Stognei, Anastasia, Seddon, Max & Mosolov, Daria: Black box economics: Russia's internal struggle over classified financial data. *Financial Times*, 29.1.2023. [https://www.ft.com/content/42b53987-8280-469e-8014-9ddb0c98463b], luettu 6.2.2024.

[831]Совет Безопасности Российской Федерации: О повышении устойчивости и безопасности функционирования информационной инфраструктуры государства. СБРФ, 20.5.2022. [http://www.scrf.gov.ru/council/session/3241/], luettu 6.2.2024.

[832] ИнтерФакс: Документ о госполитике в сфере инфобезопасности вскоре представят Путину для утверждения. *ИнтерФакс*, 20.5.2022. [https://www.interfax.ru/russia/842023], luettu 6.2.2024; Совет Безопасности Российской Федерации: В Санкт-Петербурге Секретарь Совета Безопасности Российской Федерации Николай Патрушев провел совещание по вопросам участия высших учебных заведений в обеспечении технологической независимости России. СБРФ, 31.8.2022. [http://www.scrf.gov.ru/news/allnews/3327/], luettu 6.2.2024.

[833] SecurityLab.ru: Путин поручил обеспечить независимость России от иностранного софта. *SecurityLab.ru*, 6.9.2022. [https://www.securitylab.ru/news/533754.php], luento 6.2.2024.

[834] Правительство России: Утверждены «дорожные карты» «Новое индустриальное программное обеспечение» и «Новое общесистемное программное обеспечение». Правительство России, 16.12.2022. [http://government.ru/news/47353/], luettu 6.2.2024.

[835] Правительство России: Правительство определило приоритетные направления проектов технологического суверенитета и структурной адаптации экономики России. Правительство России,

Toukokuussa 2023 Venäjän hallitus hyväksyi konseptin maan teknologisesta kehityksestä vuoteen 2030 asti. Sen mukaan maalle pitäisi rakentaa kotimainen tieteellinen, henkilöstöllinen ja kriittisen ja läpileikkaavien teknologioiden perusta 2030-luvun loppuun mennessä.[836] Ulkomaan markkinoiksi venäläisille tuotteille kaavailtiin BRICS:n ja Euraasian unionin maita.[837] Heinäkuussa Putin totesikin, että Venäjän ei pidä linnoittautua vaan kehittää teknologisia liittokuntia.[838] Vuoden 2023 loppuun mennessä hallituksen piti hyväksyä uusi Datatalouden ohjelma, joka koskee datan keruuta, turvallisuutta ja käyttöä.[839] Putin hyväksyi syyskuussa uuden ohjelman suuntalinjat ja samalla valmisteluaikaa pidennettiin vuodelle 2024.[840] Mintsifri on ilmoittanut aikovansa kohdentaa Datatalouden ohjelmaan vuosina 2025–2023 1,5 triljoonaa ruplaa.[841] Datatalouteen liittyen Putin on vuosina 2022–2023 antanut useita määräyksiä tekoälyteknologian kehityksestä, mikä kertoo sen koetusta tärkeydestä Venäjä taloudelle ja kansalliselle turvallisuudelle.[842] Vuoden 2019 tekoälystrategia päivitettiin helmikuussa 2024 vastaamaan entistä paremmin teknologisen suvereniteetin vaatimuksia.[843] Strategioiden ja investointien lisäksi innovaatioita etsittiin esimerkiksi nimittämällä eliitin jälkikasvua uuden sukupolven edustajina teknologiayritysten johtoon.[844]

Strategisten suunnitelmien rinnalla Venäjällä on työstetty muitakin käytännöllisiä ratkaisuja sodan tuomiin, etenkin maksuliikenteellisiin, ongelmiin. Venäjä on edistänyt SWIFT:lle vaihtoehtoisen maksujen välitysjärjestelmän kehittämistä ja monet Venäjän kanssa kauppaa tekevät maat ovatkin liittyneet siihen.[845] Lisäksi Venäjä on pyrkinyt laajentamaan kotimaisen Mir maksu- ja luottokortin käytettävyyttä kansainvälisessä maksuliikenteessä.[846] Kryptorupla hyväksyttiin sanktioiden tuoman paineen takia Venäjällä viralliseksi valuutaksi, tosin se ei todennäköisesti auta Venäjää lyhyellä aikavälillä kiertämään finanssisektorin sanktiota.[847] Jo aikaisemmin kehitettyjen kansallisten

17.4.2023. [http://publication.pravo.gov.ru/Document/View/0001202304170025?index=43], luettu 6.2.2024.

[836] Правительство России: Правительство утвердило Концепцию технологического развития до 2030 года. Правительство России, 25.5.2023. [http://government.ru/news/48570/], luettu 6.2.2024.

[837] Королев, Никита: ПО неширокому кругу друзей. *Коммерсантъ*, 5.7.2023. [https://www.kommersant.ru/doc/6083548], luettu 6.2.2024.

[838] ТАСС: Мегагранты и независимость от зарубежных технологий. О чем Путин говорил с учеными. *ТАСС*, 13.7.2023. [https://tass.ru/ekonomika/18270781], luettu 6.2.2024.

[839] Министерство цифрового развития, связи и массовых коммуникаций РФ: В России появится новый нацпроект — «Экономика данных». Минцивры, 13.7.2023. [https://digital.gov.ru/ru/events/45686/], luettu 6.2.2024.

[840] Roskomsvoboda: В России создают нацпроект по формированию экономики данных. *Roskomsvoboda*, 5.9.203. [https://roskomsvoboda.org/post/nacproect-po-formirovaniyu-economiki-dannyh/], luettu 6.2.2024.

[841] Roskomsvoboda: Минцифры потратит на «Экономику данных» 1,5 триллиона рублей. *Roskomsvoboda*, 27.11.2023. [https://roskomsvoboda.org/post/econ-dannyh/], luettu 6.2.2024.

[842] D-Russia.ru: Президент России поручил обеспечить поддержку деятельности исследовательских центров в сфере ИИ до 2030 года. *D-Russia.ru*, 7.9.2023. [https://d-russia.ru/vladimir-putin-poruchil-obespechit-podderzhku-dejatelnosti-issledovatelskih-centrov-v-sfere-ii-do-2030-goda.html], luettu 6.2.2024.

[843] Указ Президента РФ от 10 октября 2019 г. N 490 "О развитии искусственного интеллекта в Российской Федерации" (с изменениями и дополнениями). [https://base.garant.ru/72838946/], luettu 24.2.2024.

[844] Soldatov, Andrei & Borogan, Irina: Success Eludes the Kremlin's Chosen Children. CEPA, 27.9.2023. [https://cepa.org/article/success-eludes-the-kremlins-chosen-children/], luettu 6.2.2024.

[845] ИнтерФакс: К Системе передачи финансовых сообщений Банка России подключено 514 участников. *ИнтерФакс,* 1.9.2023. [https://www.interfax.ru/business/918936], luettu 6.2.2024.

[846] Reuters: Russia pursues payment solutions as Mir card used in just 9 countries. *Reuters*, 13.4.2023. [https://www.reuters.com/article/russia-payments-idUSL8N36G4HQ/], luettu 6.2.2024.

[847] Банк России: Принят закон о цифровом рубле. Банк России, 11.7.2023. [https://www.cbr.ru/press/event/?id=16896], luettu 6.2.2024; Cordell, Jake: Russia's Digital Ruble Won't Help It Evade Sanctions Anytime Soon. *The Moscow Times*, 1.8.2023.

käyttöjärjestelmien muun muassa Auroran kehittämistä ja käyttöönottoa on tuettu nopeutetussa aikataulussa.[848] Venäjällä on jopa esitetty, mukaillen Kiinan aikaisempaa esitystä, TCP/IP-protokollaperheen korvaamista uudella venäläisellä versiolla.[849] Hieman yllättäen Telegram-viestintäpalvelusta on tullut niin Venäjän valtion kuin venäjänkielisen oppositionkin pääviestintäkanava internetissä, jota Lännessäkin seurataan suurella mielenkiinnolla.[850] Valtiojohtoisen byrokratian ja suurten hankkeiden rinnalla tapahtuu virastojen, valtionyritysten ja yksityisen sektorin joustavaa sopeutumista uuteen tilanteeseen.

Suunnitelmat ovat perinteiseen tapaan olleet ylioptimistisia. ICT-alan valtionyhtiöt ja valtiota lähellä olevat yritykset ovat osallistuneet niiden laadintaan, mikä herättää kysymyksiä budjettivarojen allokoinnin perusteista.[851] Nämä yritykset esimerkiksi esittivät, että päästökseen hyväksyttyjen kotimaisten ohjelmiston listalle, jollaista Mintsifri ylläpitää ja jolla olevien ohjelmistojen käyttö oli sallittua valtionhallinnolle ja -yrityksille, ohjelmien piti tukea kotimaisia laiteratkaisuja.[852] Läpileikkaavien teknologioiden edistäminen on jaettu määrättyjen valtionyhtiöiden tehtäväksi.[853] Tällainen politiikka edistää helposti korruptiota ja toisaalta hidastaa kehitystä, koska Venäjältä puuttuu kotimainen laitetuotanto. Käskyjen ja suunnitelmien äkkipikaisuus on aiheuttanut haasteita yrityssektorille. Esimerkiksi Putinin informaatioturvallisuusukaasia keväältä 2022 tullaan korjaamaan käytännön toteutuksen hankaluuksien takia.[854] Maaliskuussa 2023 Mintsifri joutui jo esittämään pidempää siirtymäkautta ulkomaisista ohjelmistoista luopumiselle ja syksyllä 2023 finanssisektori pyysi lisää aikaa kotimaisiin ohjelmistoihin siirtymisessä.[855] Tosin Mintsifri väitti samaan aikaan, että 80 %:lle ohjelmis-

[https://www.themoscowtimes.com/2023/08/01/russias-digital-ruble-wont-help-it-evade-sanctions-anytime-soon-a82024], luettu 6.2.2024.

[848] Коммерсантъ: «Аврора» не тонет. *Коммерсантъ*, 14.8.2023. [https://www.kommersant.ru/doc/6159874], luettu 6.2.2024; CNews: Российские министерства повально тестируют смартфоны на ОС «Аврора». *CNews*, 6.10.203. [https://www.cnews.ru/news/top/2023-10-06_posle_otkaza_ot_iphone_ministerstva], luettu 5.1.2024.

[849] Roskomsvoboda: Путин поддержал импортозамещение протокола TCP/IP. Реакция экспертов. Roskomsvoboda, 2.5.2023. [https://roskomsvoboda.org/post/otech-tcp-ip/], luettu 6.2.2024; ТАСС: Путин поддержал создание российских протоколов связи, альтернативных зарубежным. *ТАСС*, 28.4.2023. [https://tass.ru/politika/17633161], luettu 6.2.2024.

[850] Романова, Елена: Заказной Telegram. *Новая газета*, 14.8.2023.
[https://novayagazeta.eu/articles/2023/08/14/zakaznoi-telegram], luettu 6.2.2024.

[851] Королев, Игорь: Как в России потратят ₽100 млрд на новое общесистемное ПО и интернет-сервисы. *Cnews*, 7.4.2023. [https://www.cnews.ru/articles/2023-03-29_kak_v_rossii_potratyat_100_mlrd_na], luettu 6.2.2024.

[852] Roskomsvoboda: Отечественное ПО обяжут работать на российских процессорах и операционных системах. *Roskomsvoboda*, 21.4.2023. [https://roskomsvoboda.org/post/importozameshenie-procev/], luettu 6.2.2024.

[853] Российкая газета: На сквозные "цифровые" технологии в РФ нужен почти триллион рублей. *Российкая газета*, 14.10.2019. [https://rg.ru/2019/10/14/na-skvoznye-cifrovye-tehnologii-v-rf-nuzhen-pochti-trillion-rublej.html], luettu 6.2.2024.

[854] Швецова, Анна:Указ о мерах информационной безопасности РФ будет доработан по спорным позициям. *Comnews*, 13.11.2023. [https://www.comnews.ru/content/230097/2023-11-13/2023-w46/1008/ukaz-o-merakh-informacionnoy-bezopasnosti-rf-budet-dorabotan-spornym-poziciyam], luettu 5.1.2014.

[855] Коммерсантъ: Банкирам софт не дописан. Кредитные организации просят отсрочить импортозамещение. *Коммерсантъ*, 8.9.2023. [https://www.kommersant.ru/doc/6199827], luettu 6.2.2024; SecurityLab.ru: Российские власти предложат новые условия для использования ПО от ушедших из России вендоров. *SecurityLab.ru*, 1.3.2023. [https://www.securitylab.ru/news/536673.php], luettu 5.1.2024; Кодачигов, Валерий: Пересдача данных: скорость мобильного интернета в России снизилась на 7%. *Известия*, 1.3.2023 (a). [https://iz.ru/1476492/valerii-kodachigov/peresdacha-dannykh-skorost-mobilnogo-interneta-v-rossii-snizilas-na-7], luettu 6.2.2024.

toista löytyy venäläinen vastine.[856] Yhtenä ratkaisuna ohjelmistoalan ongelmiin ja toisaalta ulkomaisten riippuvuuksien ehkäisemiseksi esitettiin venäläisen avoimen lähdekoodin tietovaraston perustamista.[857]

Ohjelmistojen osalta tilanne on parempi kuin ICT-laitteistojen, joiden osalta Venäjällä on ollut vähän osaamista, tuotantoa tai tuotekehitystä.[858] Lisäksi Yhdysvallat on pyrkinyt kohdennetuilla sanktiolla estämään Venäjää hankkimasta ICT-teknologiaa ulkomailta.[859] Vuoden 2022 syksyllä ilmoitettiin mobiiliyhteyksien hidastumisesta laitteiden puutteen takia ja tilanne jatkoi heikentymistä syksyllä 2023.[860] Venäjällä valmistettujen, eli koottujen, mobiilitukiasemien testaamista suunniteltiin aloitettavaksi 2025.[861] Prosessorivalmistuksen osalta Venäjän tilanne näytti heikolta vuoden 2023 syksyllä. Yksi kotimainen valmistaja ajautui konkurssiin ja loppujen tuotanto oli vähäistä ja vanhakantaista.[862] Venäjällä oli hankaluuksia tuoda maahan ICT-laitteistoja kesällä 2022, mutta jo 2023 viiden ensimmäisen kuukauden aikana maahan tuotiin 10 % enemmän palvelimia kuin aikaisemmin.[863] Virallisten lausuntojen ja alan uutislähteiden mukaan Venäjän kotimainen tuotanto oli 2023 syksyllä kehittymässä vastaamaan kysyntää, mutta lähteiden tarkkuutta, todenperäisyyttä ja laitteistojen ”venäläisyyden astetta” on syytä epäillä.[864] Vaikuttaa siltä, että ainakin lyhyellä aikavälillä Venäjän ICT-tuotanto perustuu ulkomailta sanktioita kiertäen hankittujen laitteistojen uudelleen kokoamiseen.

Epäilemättä talouden siirtyminen kohti sotatilaa ja asevoimien tarpeet ovat vaikuttaneet ICT-alan tutkimukseen, kehittämiseen ja tuotantoon.[865] Digitaalisen talouden

[856] Уварчев, Леонид: Чернышенко: российские аналоги есть у 80% зарубежного программного обеспечения. *Коммерсантъ*, 11.9.2023. [https://www.kommersant.ru/doc/6210030], luettu 6.2.2024.
[857] SecurityLab.ru: Создание российского аналога GitHub начнется 1 ноября 2022 года. *SecurityLab.ru*, 13.10.2022. [https://www.securitylab.ru/news/534352.php], luettu 6.2.2024.
[858] Cnews: Сергей Шилов, «Лига цифровой экономики»: Процесс трансформации сферы ИТ только набирает обороты. *CNews*, 13.2.2023. [https://www.cnews.ru/reviews/cnews_trendy_2023/interviews/sergej_shilov_1?erid=Pb3XmBtzt5g4DDmv8eLKfv6QYqzDYcyWiwM7Gez], luettu 6.2.2024.
[859] Tadviser (2023a).
[860] SecurityLab.ru: Российские власти предложат новые условия для использования ПО от ушедших из России вендоров. *SecurityLab.ru*, 1.3.2023. [https://www.securitylab.ru/news/536673.php], luettu 5.1.2024; Кодачигов (2023a); Федонин, Дмитрий: Количество БС в России сократилось, но деградации сетей связи пока нет. *Comnews*, 11.9.2023. [https://www.comnews.ru/content/228741/2023-09-11/2023-w37/1008/kolichestvo-bs-rossii-sokratilos-no-degradacii-setey-svyazi-poka-net], luettu 6.2.2024.
[861] ТАСС: Минцифры планирует пилотный запуск 5G на российских базовых станциях в 2025 году. *ТАСС*, 2.3.2023. [https://tass.ru/ekonomika/17181413], luettu 6.2.2024.
[862] Петрова, Венера & Галиева, Диана: Чипонезависимость со скидкой. *Коммерсантъ*, 15.11.2022. [https://www.kommersant.ru/doc/5667792?from=top_main_8], luettu 6.2.2024; Королев, Игорь: Российская микроэлектроника перейдет на топологию 28 нм. Много это или мало? *Cnews*, 11.10.2023. [https://www.cnews.ru/news/top/2023-10-11_rossijskaya_mikroelektronika], luettu 6.2.2024; Дорофеев, Георгий: «Байкалы» выставлены на аукцион. Связанные с российскими чипами наработки уйдут с молотка из-за банкротства «Т-платформ». *Cnews*, 24.8.2023. [https://www.cnews.ru/news/top/2023-08-24_bajkaly_ujdut_s_molotka], luettu 6.2.2024.
[863] Коммерсантъ: Серверы примерно импортируются. *Коммерсантъ*, 19.7.2023. [https://www.kommersant.ru/doc/6110850], luettu 6.2.2024.
[864] Cnews: В 2024 году доля отечественных ИТ-продуктов в сетевых проектах вырастет на 25–30%: тренды на рынке сетей и ИТ-инфраструктуры. *CNews*, 16.11.2023. [https://import-free.cnews.ru/news/line/2023-11-16_v_2024_godu_dolya_otechestvennyh?erid=2SDnjdYL3i8], luettu 6.2.2024; Niskanen (2023).
[865] Vesala, Lauri: Sota kasvattaa Venäjän taloutta hyvinvoinnin kustannuksella. Suomen Pankki, blogikirjoitus, 14.9.2023. [https://www.eurojatalous.fi/fi/blogit/2023/sota-kasvattaa-venajan-taloutta-hyvinvoinnin-kustannuksella/], luettu 6.2.2024.

ohjelman budjettia leikattiin vuodelta 2024 11 suunnitellusta.[866] Toisaalta kyberturvallisuus alana saattaa tulla priorisoiduksi turvallisuustilanteen johdosta ja vastarinta kansallisen internetsegmentin rakentamiselle on todennäköisesti lientynyt, vaikkakin yksityissektori edelleen valittaa nousevista kustannuksista.[867] Venäjällä on myös havahduttu siihen, että kotimaisen ICT-ekosysteemin luominen edellyttää tuotteiden yhteensovittamista, joka luonnollisesti halutaan toteuttaa valtiojohtoisesti.[868] Olennainen kysymys on venäläisen kyberturvallisuusalan osaamisen varmistaminen koskien uusia kotimaisia ohjelmistoja, joiden koodi ja haavoittuvuudet ovat uusia ja vähän tunnettuja.

Digitaalisen talouden kasvuhankkeiden taakse kätkeytyy korruptiota, tehottomuutta, innovaatiopohjan rapautumista ja kasvavaa riippuvuutta Kiinasta.[869] Venäläisten ohjelmistojen hinnat nousivat 30 % ulkomaisen kilpailun puutteessa 2022.[870] Saatavuus on ollut ongelma ja jopa ohjelmistopiratismin sallimista pohdittiin apukeinona.[871] Vaihtoehtona on esitetty ohjelmistojen käyttämistä ilman lisenssiä.[872] Kiinalaistuotteiden markkinaosuus on kasvanut vuosina 2022–2023 huomattavasti, eivätkä saatavilla olevat luvut kerro venäläisinä myytävien kiinalaistuotteiden määrää.[873] Kiinariippuvuuden uhat ymmärretään Venäjällä ja Roskomnadzor varoitti jo 2022 liiallisesti teknologisesta riippuvuudesta Kiinasta[874] ja venäläisyritykset ovat pyytäneet suojelua kii-

---

[866] D-Russia: Минцифры сформировало бюджет развития IT на 2024 год в размере 277 млрд рублей – министр. *D-Russia*, 11.10.2023. [https://d-russia.ru/mincifry-sformirovalo-bjudzhet-razvitija-it-na-2024-god-v-razmere-277-mlrd-rublej-ministr.html], luettu 6.2.2024.

[867] Кинякина, Екатерина & Курашева, Анастасия: Региональные интернет-провайдеры нашли обход закона «О связи». *Ведомости*, 9.6.2022. [https://www.vedomosti.ru/media/articles/2022/06/10/926003-internet-provaideri-nashli-obhod-zakona], luettu 6.2.2024; Известия: В ФСБ недовольны темпами исполнения требований "пакета Яровой" операторами связи. *Известия*, 25.10.2023. [https://www.interfax.ru/russia/927494], luettu 6.2.2024.

[868] ТАСС: Минцифры хочет создать центры тестирования совместимости отечественных софта и ПО. *ТАСС*, 28.6.2023. [https://tass.ru/ekonomika/18137265], luettu 6.2.2024.

[869] Кинякина, Екатерина & Курашева, Анастасия: Эксперимент по созданию государственного репозитория ПО перенесен на неопределенный срок. *Ведомости*, 9.8.2022. [https://www.vedomosti.ru/technology/articles/2022/08/08/935090-gosudarstvennogo-repozitoriya-po-perenesen], luettu 6.2.2024; Тишина, Юлия & Корнев, Тимофей: Операторы прорубают волокно в Азию. Инфраструктуре связи предложили маршрут развития. *Коммерсантъ*, 23.5.2023. [https://www.kommersant.ru/doc/5999898], luettu 6.2.2024; Тишина, Юлия & Корнев, Тимофей: Операторы прорубают волокно в Азию. *Коммерсантъ*, 23.5.2023. [https://www.kommersant.ru/doc/6070240?tg], luettu 6.2.2024; Любавина, Анна: Бывший топ-менеджер «Ростелекома» получил 6 лет и 25 млн руб. штрафа за взятки в нацпроекте «Цифровая экономика». *Cnews*, 7.7.2023. [https://www.cnews.ru/news/top/2023-07-07_byvshij_top-menedzher_rostelekoma], luettu 6.2.2024.

[870] Корнев, Тимофей, Исакова, Татьяна & Королев, Никита: ПО дороже денег. Цены на российский софт растут вне конкуренции. *Коммерсантъ*, 30.3.2023. [https://www.kommersant.ru/doc/5902157], luettu 6.2.2024.

[871] Литвиненко, Юрий: Софт требует жесткости. Российские разработчики против легализации иностранного ПО. *Коммерсантъ*, 12.9.2022. [https://www.kommersant.ru/doc/5558200], luettu 6.2.2024.

[872] Перцева, Евгения & Кодачигов, Валерий: Программное проявление: в РФ разрешат принудительное лицензирование ПО. *Известия,* 1.3.2023. [https://iz.ru/1526187/evgeniia-pertceva-valerii-kodachigov/programmnoe-proiavlenie-v-rf-razreshat-prinuditelnoe-litcenzirovanie-po], luettu 6.2.2024.

[873] Корнев, Тимофей: Станционные риски. Китайское оборудование вызвало вопросы у российских операторов связи. *Коммерсантъ*, 8.9.2023. [https://www.kommersant.ru/doc/6199811], luettu 6.2.2024; Simola, Heli & Röyskö, Aino: Russia's Technology Imports from East Asia. *Asian Economic Papers*, 22(1) 2023, s. 1–10; Смирнова, Софья: Кладите трубку: Китай сократил поставки смартфонов в Россию. *Известия,* 13.3.2022. [https://iz.ru/1303814/sofia-smirnova/kladite-trubku-kitai-sokratil-postavki-smartfonov-v-rossiiu], luettu 6.2.2024.

[874] Nardelli, Alberto: Russian Memo Said War Leaves Moscow Too Reliant on Chinese Tech. *Bloomberg*, 19.4.2023. [https://www.bloomberg.com/news/articles/2023-04-19/russia-china-worries-set-out-in-private-memo-on-tech-risk?srnd=premium-europe&leadSource=uverify%20wall#xj4y7vzkg], luettu 6.2.2024.

nalaiselta kilpailulta.[875] Toisaalta ne tuotteet, joita Kiina on ollut halukas viemään Venäjälle – Kiinan kansallinen turvallisuus ja sanktioiden pelko vaikuttavat vientihalukkuuteen[876] – eivät ole tyydyttäneet venäläisiä kaikilta osin.[877] Yhtenä ratkaisuna on ollut kiinalaistuotannon siirtäminen Venäjälle ”yhteistyön” nimikkeen alle verhottuna.[878] Kiina on siis sekä uhka että mahdollisuus Venäjän digitaalisen ja teknologisen suvereniteetin tavoittelulle ja tätä Ukrainan sodan pahentamaa ristiriitaa maa ei ole pystynyt ratkaisemaan.

Venäjän kyberturvallisuusala joutui merkittäviin ongelmiin Venäjän hyökkäyksen alettua, kun maasta poistui yli 100 000 teknologia-alan työntekijää.[879] Sberpankin mukaan Venäjältä puuttui syyskuussa 2022 viisituhatta kyberalan ammattilaista.[880] Mintsifrin johto totesi 2023 syksyllä, että Venäjältä puuttui yli puoli miljoonaa IT-alan työntekijää, jotka olisi tarvittu alan kasvun varmistamiseksi.[881] Seurauksena työvoimapulasta ja alan voimakkaasta kasvusta IT-työläisten palkat nousivat merkittävästi vuosina 2022–2023.[882] Tämä on todennäköisesti houkutellut osan maasta lähteneistä IT-alan ammattilaisista takaisin ja auttanut uusien työntekijöiden rekrytoinnissa. Toisaalta 35 % IT-alan työntekijöistä ilmoitti tulojensa laskeneen vuonna 2023, mikä on ristiriidassa Minstifrin ilmoitusten kanssa.[883] Osaamisen rakentamisen ja säilyttämisen näkökulmasta tilanne on siis todennäköisesti epävakaa. Vuonna 2023 Digitaalisen talouden kansalliseen ohjelmaan säädettiin tavoite miljoonan IT-työläisen kouluttamisesta muutamassa vuodessa, mutta jo vuoden 2024 budjetista leikattiin nimenomaan koulutukseen kohdennettuja varoja.[884] Osaajien puute heikentää Venäjän kansallista kyberturvallisuuttaa ja asevoimien tarpeet todennäköisesti pahentavat tilannetta entisestään. Valtion ja asevoimien kriittisen informaatioinfrastruktuurin puolustamiselle löy-

---

[875] Королев, Никита: Оптоволокно оборвут на границе. *Коммерсантъ*, 20.3.2023. [https://www.kommersant.ru/doc/5886686?tg], luettu 6.2.2024.

[876] Kot, Brian: Hong Kong's Technology Lifeline to Russia. Carnegie Endowment for International Peace, 17.5.2023. [https://carnegieendowment.org/2023/05/17/hong-kong-s-technology-lifeline-to-russia-pub-89775], luettu 6.2.2024.

[877] Cnews: Базовые станции из КНР оказались бесполезными. В России дефицит оборудования для сотовых сетей. *Cnews*, 8.9.2023. [https://www.cnews.ru/news/top/2023-09-08_kitaj_ne_pomogv_rossii_defitsit], luettu 6.2.2024

[878] Dzen.ru: В Иннополисе запустят российско-китайское производство телеком-оборудования. *Dzen.ru*, 23.9.2023. [https://dzen.ru/a/ZREnBc78KBMo3abu], luettu 6.2.2024.

[879] Захарова, Нина: При путинизме мы жить не согласны. Массовая эмиграция IT-кадров. *Сибирь.Реалии*, 21.4.2022. [https://www.sibreal.org/a/massovaya-emigratsiya-it-kadrov/31797774.html], luettu 6.2.2024; Шпунт, Яков: Безопасность попала в сложную ситуацию. *Comnews*, 24.3.2022. [https://www.comnews.ru/content/219409/2022-03-24/2022-w12/bezopasnost-popala-slozhnuyu-situaciyu], luettu 6.2.2024; Шпунт, Яков: Вектор атак кардинально изменился. *Comnews*, 24.3.2022. [https://www.comnews.ru/content/219408/2022-03-24/2022-w12/vektor-atak-kardinalno-izmenilsya], luettu 6.2.2024.

[880] SecurityLab.ru: В России не хватает десятков тысяч специалистов по кибербезопасности. *SecurityLab.ru*, 6.9.2022. [https://www.securitylab.ru/news/533776.php], luettu 6.2.2024.

[881] Федотова, Мария: Минцифры оценило дефицит кадров в IT-отрасли в 500–700 тыс. человек. *Коммерсантъ*, 16.8.2023. [https://www.kommersant.ru/doc/6161948], luettu 6.2.2023.

[882] Дорофеев, Георгий: Российским ИТ-шникам платят почти миллион в месяц, лишь бы не уехали. Зарплаты в отрасли рекордно выросли. *Cnews*, 3.11.2023. [https://www.cnews.ru/news/top/2023-11-03_rossijskim_it-shnikam_platyat], luettu 6.2.2024.

[883] Исакова, Татьяна & Жабин, Алексей: В IT творится что-то неокладное. Профильные специалисты жалуются на снижение доходов. *Коммерсантъ*, 14.12.2023. [https://www.kommersant.ru/doc/6397006], luettu 6.2.2024.

[884] Comnews: Миллион дефицитных ИТ-специалистов – за 4 года. *Comnews*, 28.10.2022. [https://www.comnews.ru/projects/it-is-priority/case-study/222761/million-deficitnykh-it-specialistov-za-4-goda], luettu 6.2.2024; D-Russia: Минцифры сформировало бюджет развития IT на 2024 год в размере 277 млрд рублей – министр. *D-Russia*, 11.10.2023. [https://d-russia.ru/mincifry-sformirovalo-bjudzhet-razvitija-it-na-2024-god-v-razmere-277-mlrd-rublej-ministr.html], luettu 6.2.2024.

tynee riittävä työvoima, vaikka pakolla, mutta Venäjän laaja paikallis- ja aluehallinto ja yksityissektori voivat jäädä haavoittuviksi. Rekrytointihaasteet voivat myös lisätä sisäpiirihyökkäysten uhkaa poliittisesti lautuneessa ilmapiirissä. Työvoimapulan takia epäluotettavaa henkilöstöä voi päätyä kriittisiin tehtäviin.

Sodan seuraukset ovat johtaneet Venäjän IT-alan yrityskentän muutoksiin. Yandex joutui todellisiin ongelmiin ja jakautui kahteen osaan voidakseen jatkaa toimintaansa. Sen venäläisyydestä ja yhteistyöstä FSB:n kanssa on tullut mainehaitta ja kansainväliset toiminnot ovat kärsineet. Heikentyneenä se on joutunut kilpailijoidensa hampaisiin.[885] JARUS sosiaalisen median palvelu, jonka piti korvata YouTube ja Facebook, lopetti toimintansa vuoden jälkeen.[886] Toisaalta Sber on noussut pankista yhdeksi IT-alan johtavista yrityksistä.[887] Rostelekom on entisestään vahvistanut asemiaan kaikilla informaatioteknologiaan liittyvillä talouden sektoreilla. Se on hyötynyt merkittävästi Digitaalisen talouden ohjelman hankkeista ja toimii valtion tuonninkorvausohjelman veturina ICT-alalla.[888] Rostelekom on myös saanut osansa Venäjän valloittamien Ukrainan alueiden informaatioinfrastruktuurin rakentamishankkeista, tosin valtionyritys ei haluaisi vastata kustannuksista täysimääräisesti yksin ja on yrittänyt houkutella mukaan yksityisyrityksiä.[889] Yrityskentän muutokset eivät ole välttämättä olleet autoritaarisen valtiovallan näkökulmasta haitallisia, mutta innovaatio- ja investointi-ilmapiiriin ne ovat todennäköisesti vaikuttaneet heikentävästi.

Venäjän vastaus hyökkäysoperaation synnyttämiin kyberuhkiin ja teknologiasanktioihin on ollut valtiokeskeinen. Vuoden 2022 toukokuussa Putin antoi käskyn lisätoimista informaatioturvallisuuden takaamiseksi, jonka piti luoda maahan FSB:hen sidoksissa oleva, hallinnon tasot vertikaalisti läpäisevä kyberhyökkäysten torjuntaorganisaatio. Kriittistä informaatioinfrastruktuuria operoivien tahojen johtoporras asetettiin henkilökohtaiseen vastuuseen kyberturvallisuudesta.[890] Käskyn mukaisesti Venäjälle on perustettu virasto- ja sektorikohtaiset kyberturvallisuusosaamiskeskukset

---

[885] Borak, Masha: How Russia killed its tech industry. *MIT Technology Review*, 4.4.2023. [https://www.technologyreview.com/2023/04/04/1070352/ukraine-war-russia-tech-industry-yandex-skolkovo/], luettu 5.1.2024; Marrow, Alexander & Devitt, Polina: Exclusive: Fear of tech 'brain drain' prevents Russia from seizing Yandex for now, sources say. *Reuters*, 10.8.2023. [https://www.reuters.com/technology/fear-tech-brain-drain-prevents-russia-seizing-yandex-now-sources-2023-08-10/], luettu 6.2.2024.

[886] Пламенев, Илья: Соцсеть ЯRUS объявила о закрытии. *РБК*, 29.6.2023. [https://www.rbc.ru/technology_and_media/29/06/2023/649db9b69a79475ebaec5369?from=from_main_7], luettu 6.2.2024.

[887] Tadviser: Information technology at Sberbank. Tadviser, 19.1.2023. [https://tadviser.com/index.php/Article:Information_technology_at_Sberbank], luettu 6.2.2024.

[888] Niskanen (2023); Российкая газета: Ростелеком увеличил инвестиции в отечественное программное обеспечение до 90 %. *Российкая газета*, 8.8.2023. [https://rg.ru/2023/08/08/reg-ufo/rostelekom-uvelichil-investicii-v-otechestvennoe-programmnoe-obespechenie-do-90.html], luettu 6.2.2024; Шишулин, Денис: Magnum opus для "Ростелекома." *Comnews*, 20.3.2023. [https://www.comnews.ru/content/224860/2023-03-20/2023-w12/magnum-opus-dlya-rostelekoma], luettu 6.2.2024; Матвеев, Дмитрий: Чудес не бывает: импортозамещение на новом производстве «Ростелекома» оказалось не совсем полным. *Телеспутник*, 14.6.2023. [https://telesputnik.ru/materials/hipe/article/cudes-ne-byvaet-importozameshhenie-na-novom-proizvodstve-rostelekoma-okazalos-ne-sovsem-polnym], luettu 6.2.2024.

[889] ГРЧЦ: Глава Роскомнадзора призвал операторов связи помочь новым регионам. ГРЧЦ, 24.10.2023. [https://portal.noc.gov.ru/ru/news/2023/10/24/glava-roskomnadzora-prizval-operatorov-svyazi-pomoch-novym-regionam/], luettu 6.2.2024.

[890] SecurityLab.ru: Путин подписал указ о дополнительных мерах по обеспечению информационной безопасности России. *SecurityLab.ru*, 1.5.2022. [https://www.securitylab.ru/news/531409.php], luettu 6.2.2024; Указ Президента Российской Федерации от 01.05.2022 № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации" [http://publication.pravo.gov.ru/Document/View/0001202205010023], luettu 6.2.2024; SecurityLab.ru: Минцифры создаст методику работы штабов по кибербезопасности в регионах. *SecurityLab.ru*, 6.6.2022. [https://www.securitylab.ru/news/532127.php], luettu 6.2.2024.

vuonna 2023.[891] Rakenteiden ja prosessien kehittämisen lisäksi Mintsifri halusi maaliskuussa 2023 koventaa sellaisten yritysten rangaistuksia, joiden tietoja oli vuodettu internettiin.[892] Tällaisten käskyjen ja rangaistusten antaminen kertoo lähtökohtaisesti epäonnistumisesta aikaisemmissa valtiohallinnon ja strategisen teollisuuden kohteiden kyberturvallisuuden rakentamisessa. Alemman tason johtajien henkilökohtaisen vastuun korostaminen ja rangaistusten koventaminen ovat perinteisiä venäläisiä, ja kenties autoritaarisia yleensäkin, valtionhallinnon tapoja yrittää ratkaista rakenteellisia ongelmia kriisitilanteissa.

Sota on lisännyt valtion turvallisuuselinten hallintaa venäläisestä informaatiotilasta. FSB:n ja Roskomnadzorin oikeus saada asiakkaiden tietoja teleoperaattoreilta ja palveluntarjoajilta on vahvistunut niin hallinnollisesti kuin teknisesti. Tämä koskee myös valloitettuja alueita. Valvontaa on edes auttanut alati laajeneva lista aiheista, joiden käsittely voidaan katsoa valtion vastaiseksi toiminnaksi.[893] Venäjä on ottanut käyttöön tai kehittänyt jo olemassa olevia järjestelmiä kansallisen internetsegmentin sisällön valvomiseksi, esimerkiksi Okulus ja Vepr-järjestelmä.[894] Venäläisestä informaatiotilasta on myös vuoden 2022 aikana poistettu ne ulkomaalaiset ja kotimaiset viestintäpalvelutai sosiaalisen median alustat, jotka eivät ole taipuneet Venäjän valtion vaatimuksiin sensuurista tai käyttäjien tietojen luovuttamisesta.[895] Kesään 2023 mennessä Roskomnadzor oli blokannut 170 000–206 000 ”verkkoresurssia” sotilaalliseen erikoisoperaatioon liittyen.[896] Lisäksi Venäjä on kyennyt estämään usean VPN-palvelun toiminnan

[891] Roskomsvoboda: Совет Безопасности РФ анонсировал создание центров компетенций для защиты госресурсов от кибератак. *Roskomsvoboda*, 17.1.2023. [https://roskomsvoboda.org/post/centr-kompetenciy-sovbez/], luettu 6.2.2024; Правительство России: Заседание Правительства. Правительство России, 10.8.2023. [http://government.ru/news/49251/], luettu 6.2.2024.

[892] Исакова, Татьяна & Королев, Никита: В личные данные подгружают ответственность. Госдума приступила к ужесточению правил работы с информацией. *Коммерсантъ*, 17.3.2023. [https://www.kommersant.ru/doc/5876276], luettu 6.2.2024.

[893] Уварчев, Леонид: Роскомнадзор заявил о нарушениях в данных владельцев минимум 9,5 млн симкарт. *Коммерсантъ*, 8.8.2023. [https://www.kommersant.ru/doc/6148115], luettu 6.2.2024; Burgess, Matt: Leaked Yandex Code Breaks Open the Creepy Black Box of Online Advertising. *WIRED*, 10.8.2023. [https://www.wired.com/story/yandex-leaks-crypta-ads/], luettu 6.2.2023; Устинова, Анна: Крупные телекомоператоры ДНР и ЛНР начали устанавливать СОРМ. *Ведомости*, 19.7.2023. [https://www.vedomosti.ru/technology/articles/2023/07/19/985936-krupnie-telekomoperatori-dnr-i-lnr-nachali-usta-navlivat-sorm], luettu 6.2.2024; Burgess, Matt: Shadowy Russian Cell Phone Companies Are Cropping Up in Ukraine. *WIRED*, 21.9.2022. [https://www.wired.co.uk/article/ukraine-war-mobile-networks-russia], luettu 5.1.2024; Roskomsvoboda: «Аэрофлот», «Островок», «Кассы.Ру» и другие сервисы расскажут о своих пользователях ФСБ. R*oskomsvoboda*, 26.10.2023. [https://roskomsvoboda.org/post/popolnenie-ori-okt-2023/], luettu 6.2.2024; Litvinova, Dasha: The cyber gulag: How Russia tracks, censors and controls its citizens. *AP*, 23.5.2023. [https://apnews.com/article/russia-crackdown-surveillance-censorship-war-ukraine-internet-dab3663774feb666d6d0025bcd082fba], luettu 5.1.2024; Roskomsvoboda: Путин подписал закон о запрете дискредитировать Росгвардию. *Roskomsvoboda*, 26.12.2023. [https://roskomsvoboda.org/post/putin-podpis-dirkred-rosguard/], luettu 6.2.2024.

[894] Roskomsvoboda: Роскомнадзор запустил систему автоматического поиска запрещённого контента. *Roskomsvoboda*, 13.2.2023. [https://roskomsvoboda.org/post/okulus-otyshet-zapreshionku/], luettu 1.5.2024; ТАСС: Систему "Вепрь" для выявления угроз в интернете запустят во второй половине 2023 года. *TACC*, 20.2.2023. [https://tass.ru/obschestvo/17091419?utm_source=substack&utm_medium=email], luettu 5.1.2024; Toulas, Bill: Russia's Rostec allegedly can de-anonymize Telegram users. *Bleeping Computer*, 25.3.2023. [https://www.bleepingcomputer.com/news/security/russia-s-rostec-allegedly-can-de-anonymize-telegram-users/], luettu 6.2.2024.

[895] Freedom House (2023).

[896] РБК: Роскомнадзор заблокировал 206 тыс. ресурсов из-за фейков о спецоперации. *РБК*, 9.6.2023. [https://www.rbc.ru/rbcfreenews/6482d21a9a79471b72e389c5], luettu 5.1.2024; Roskomsvoboda: 15,000 websites — a new “record” for wartime censorship. *Roskomsvoboda*, 27.11.2023. [https://roskomsvoboda.org/analysis/new-record-for-wartime-censorship/], luettu 6.2.2024.

alueellaan, mikä on hankaloittanut tavallisten kansalaisten tiedonsaantia.[897] VPN-palvelujen käytön estämisestä kokonaan vuoden 2024 aikana on käynnissä hanke liittoneuvostossa.[898] Venäjällä on jopa esitetty ajatusta ”passikäyttöisestä” internetistä, jossa jo pelkän internettiin pääsyn tulisi perustua tunnistautumiseen ja tuolloinkin pääsy olisi rajattu vain määrättyihin palveluihin.[899] Hankkeiden taustalla on yhtäältä etenkin nuorison lisääntynyt VPN-palveluiden käyttö[900] ja toisaalta Venäjän johdon periaatteellinen vastenmielisyys internetin anonymiteettia kohtaan. Nimettömyys mahdollistaa yhtäältä sisäisen opposition ja toisaalta ulkoisten, vieraiden valtojen vaikuttajien toiminnan. Se on suora haaste venäläiselle valtion suvereniteetille.

Venäjä on jatkanut suorituskyvyn rakentamista internetistä irrottautumiseksi tai irrotetuksi tulemisesta selviämiseksi. Tämä siitä huolimatta, että poliitikot ovat väittäneet, ettei Venäjä aio luoda suljettua internettiä ”Kiinan mallin mukaan.”[901] Perusteluna on ollut valtion turvallisuus. Marraskuussa 2023 pääministeri Mihail Mišustin totesi, että lisääntyneet kyberhyökkäykset edellyttävät kriittisen digitaalisen infrastruktuurin suojauksen kehittämistä.[902] Kyberhyökkäysten alettua keväällä 2022 Mintsifri käski pikatoimena internetpalveluntarjoajat ottamaan käyttöön kotimaiset nimipalvelimet, .ru domainit ja siirtämään palvelunsa kotimaisille palvelemille.[903] TSUP-järjestelmää testattiin Venäjän globaalista internetistä irrottamiseksi virallisten tietojen mukaan onnistuneesti sekä kesällä 2022 että 2023 ja talvella 2024.[904] Tosin harjoituksissa havaittiin myös vakavia ongelmiakin.[905] Harjoituksiin ovat osallistuneet FSB, FSO, puolustusministeriö, Mintsifri, hätätilaministeriö, FSTEK, finanssiala, teleoperaattorit ja osa sosiaalisen median palvelutuottajista.[906] Roskomnadzorin mukaan TSUP:tä on käytetty

[897] Roskomsvoboda: В России продолжается тестирование блокировки протоколов VPN? *Roskomsvoboda*, 23.1.2023. [https://roskomsvoboda.org/post/blok-protokol-vpn-01-2023/;], luettu 6.2.2024; Кагалтынов, Эрдни: РКН: с 2021 года в России заблокировали 167 VPN-сервисов. *Коммерсантъ*, 25.10.2023. [https://www.kommersant.ru/doc/6297540?tg], luettu 5.1.2024.

[898] Ларина, Анастасия: Сенатор Шейкин: VPN-сервисы смогут заблокировать в России с 1 марта 2024 года. *Коммерсантъ*, 3.101.2023. [https://www.kommersant.ru/doc/6252625], luettu 5.1.2024.

[899] Dzen.ru: В Госдуме анонсировали появление персонального идентификатора для входа в интернет. *Dzen.ru*, 3.62023. [https://govoritmoskva.ru/news/366561/], luettu 5.1.2024.

[900] SecurityLab.ru: Власти бессильны: количество пользователей VPN в России выросло на 37% за год. *SecurityLab.ru*, 6.12.2023. [https://www.securitylab.ru/news/544351.php], luettu 6.2.2024.

[901] Ведомости: Хинштейн заявил об отсутствии планов строить закрытый рунет. *Ведомости*, 6.7.2023. [https://www.vedomosti.ru/technology/news/2023/07/06/984044-hinshtein-zayavil-ob-otsutstvii-planov-stroit-zakritii-runet], luettu 5.1.2024.

[902] ТАСС: Мишустин призвал усилить защиту национальной цифровой инфраструктуры. *ТАСС*, 21.11.2023. [https://tass.ru/ekonomika/19340569], luettu 6.2.2024.

[903] Славин, Алексей: В России правда собираются отключить «внешний» интернет? Что это значит? Зайти на зарубежные сайты будет невозможно? *Meduza*, 6.3.2022. [https://meduza.io/feature/2022/03/06/v-rossii-pravda-sobirayutsya-otklyuchit-vneshniy-internet-chto-eto-znachit-zayti-na-zarubezhnye-sayty-budet-nevozmozhno], luettu 5.1.2024; Тишина, Юлия, Гаврилюк, Анастасия, Петрова, Венера & Королев, Никита: Власти изолируют сети. *Коммерсантъ*, 6.3.2022. [https://www.kommersant.ru/doc/5249500], luettu 6.2.2024.

[904] CNews: Россия приготовилась к полному отключению от интернета. *CNews*, 26.10.2022. [https://www.cnews.ru/news/top/2022-10-26_rossiya_prigotovilas_k_polnomu], luettu 5.1.2024; Eckel, Mike: Another Brick in The Great Kremlin Firewall: Mass Internet Outages Part Of 'Sovereign Internet'. *RFE/RL*, 31.1.2024. [https://www.rferl.org/a/russia-mass-internet-outages-kremlin-firewall/32799971.html], luettu 24.2.2024.

[905] CNews: Суверенный Рунет слабоват. Изъяны в его инфраструктуре могут сломать Сеть в России. *CNews*, 24.10.2023. [https://www.cnews.ru/news/top/2023-10-24_suverennyj_runet_slabovat], luettu 5.1.2024.

[906] Тишина, Юлия: Без учений — тьма. Как готовят рунет к автономной работе в случае его отключения извне. *Коммерсантъ*, 13.12.2022. [https://www.kommersant.ru/doc/5705859], luettu 6.2.2024.

jo vuodesta 2022 kyberhyökkäysten torjumiseen.[907] TSUP-järjestelmää operoivan Radiotaajuuspääkeskuksen johtajan mukaan pelkkä TSUP ei kuitenkaan riitä autonomisen kansallisen segmentin toiminnan takaamiseksi vaan tarvitaan myös kansallinen ohjelmistokirjasto ja kansallisten salaussertifikaattien ottaminen laajaan käyttöön sekä kansallinen palvelunestohyökkäysten torjuntajärjestelmä.[908] Nämä vaatimukset on sisällytetty Venäjän hallituksen joulukuussa 2023 hyväksymään Viestiliikennealan kehitysstrategiaan vuodelle 2035. Strategia sisältää aloitteen luotettavan maakohtaisen IP-osoitteiden tietokannan rakentamiseksi ”maan digitaalisen ulkokehän suojaamiseksi”; yhtenäisen ja keskitetyn DDoS-hyökkäysten suojajärjestelmän rakentamisen; GosSOPKA-järjestelmän alakohtaisten keskusten kehittämisen; kvanttisalauksen ja postkvanttisalauksen hyödyntämisen; normiperustaisen siirtymisen kotimaisiin salausjärjestelmiin; sekä mm. Starlinkin haastavan satelliittijärjestelmän rakentamisen. Strategian päämäärä on teknologisen suvereniteetin saavuttaminen, joka etenkin runko- ja mobiililiikenneverkkojen osalta on heikko. Strategia myöntää Venäjän ongelmat.[909] Kansallisten salausratkaisujen kehittämiseksi perustettiin Kansallinen digitaalisen kryptografian teknologiakeskus.[910] Tavoitetilassa vuoden 2023 loppuun mennessä kaiken venäläisen verkkoliikenteen pitäisi kulkea TSUP:n läpi, tosi virallisesti pääosa liikenteestä jo kulkee sen läpi.[911] Ongelmiakin on, sillä teleoperaattoreita on uhattu vankeustuomioilla ja miljoonaluokan sakoilla, mikäli nämä eivät asenna TSUP-järjestelmää verkkoihinsa.[912]

TSUP:iin ja sen rinnalle on vallitsevan tilanteen johdosta haluttu luoda lisää informaatiotilan hallintaa parantavia järjestelmiä ja järjestelyjä. Vuoden 2024 alusta 160 kriittistä informaatioinfrastruktuuria operoivaa organisaatiota tulisi liittää kansalliseen palvelunestohyökkäyksien torjuntajärjestelmään.[913] TSUP:ta halutaan kehittää 1,2 miljardilla ruplalla rakentamalla kansallinen dataliikenteen valvonta- ja hallintajärjestelmä.[914] Radiotaajuuspääkeskus on joulukuussa 2022 ottanut käyttöön Antifrod-järjestelmän huijauspuheluiden estämiseksi operaattoreiden omien järjestelmien rinnalle. Roskomnadzorin mukaan vuoteen 2024 mennessä kaikki operaattorit on liitetty järjestel-

[907] Roskomsvoboda: Роскомнадзор хочет ограничить сканирование Рунета на уязвимости из-за рубежа. *Roskomsvoboda*, 9.6.2023. [https://roskomsvoboda.org/post/rkn-ip-i-scan/], luettu 6.2.2024; Roskomsvoboda: Роскомнадзор создаёт систему противодействия DDoS-атакам. *Roskomsvoboda*, 13.6.2023. [https://roskomsvoboda.org/post/systema-protiv-ddos-atak/], luettu 6.2.2024.

[908] ТАСС: Эксперт сообщил о возможности автономной работы Рунета при отключении от глобальной сети. *ТАСС*, 1.5.202. [https://tass.ru/ekonomika/16157169], luettu 6.2.2024; Известия: Документ о госполитике в сфере инфобезопасности вскоре представят Путину для утверждения. *Известия*, 20.5.2022. [https://www.interfax.ru/russia/842023], luettu 6.2.2024.

[909] Распоряжение Правительства РФ 24.11.2023 № 3339-р Стратегия развития отрасли связи Российской Федерации на период до 2035 года. [http://government.ru/docs/50304/], luettu 5.1.2024; SecurityLab.ru: Стратегия 2035: Россия создаст свою систему гео-IP-локации и защиты от DDoS-атак. *SecurityLab.ru*, 22.12.2023. [https://www.securitylab.ru/news/544804.php], luettu 6.2.2024.

[910] SecurityLab.ru: Минцифры и ФСБ объявили о создании Центра цифровой криптографии. *SecurityLab.ru*, 26.1.2023. [https://www.securitylab.ru/news/536093.php], luettu 6.2.2024.

[911] Капранов, Олег: Глава Роскомнадзора Липов: В России все узлы связи на 100% закрыты при помощи ТСПУ. *Российская газета*, 24.10.2023. [https://rg.ru/2023/10/24/glava-roskomnadzora-lipov-v-rossii-vse-uzly-sviazi-na-100-zakryty-pri-pomoshchi-tspu.html], luettu 6.2.2024.

[912] Кодачигов, Валерий: Трафик виноват: не подключившихся к «суверенному интернету» провайдеров ждут штрафы. *Известия*, 20.7.2023. [https://iz.ru/1546502/valerii-kodachigov/trafik-vinovat-ne-podkliuchivshikhsia-k-suverennomu-internetu-provaiderov-zhdut-shtrafy], luettu 6.2.2024.

[913] Исакова, Татьяна: К системе по борьбе с DDoS-атаками на базе ТСПУ подключат 160 субъектов КИИ. *Коммерсантъ*, 9.11.2023. [https://www.kommersant.ru/doc/6323505], luettu 6.2.2024.

[914] Курашева, Анастасия: Государство потратит 1,2 млрд рублей на создание новейшей системы контроля трафика в интернете. *Ведомости*, 6.11.2022. [https://www.vedomosti.ru/technology/articles/2022/11/07/949049-gosudarstvo-potratit-12-mlrd-rublei-na-sozdanie-sistemi-kontrolya-trafika], luettu 6.2.2024.

mään.[915] Perustettavaksi esitetyt järjestelmät noudattavat valtiojohtoista keskittämisen logiikka, joka oli nähtävissä jo ennen vuotta 2022. Sota toiminee venäläisen internetin kansallistamisen lopullisena katalyyttinä ja on linjassa venäläisen strategisen kulttuurin ideoiden kanssa.

Sodan seurauksena Venäjän sijoitus on Qrator Labsin ylläpitämällä kansallisen internetreitityksen resilienssin tilastolla pudonnut sijalta kuusi sijalle kolmetoista.[916] Roskomnadzor ei ole yleisesti ottaen ollut tyytyväinen teleoperaattoreiden infrastruktuurin resilienssiin, jonka puutteet ovat korostuneet Ukrainan Venäjälle tekemien lennokki-iskujen seurauksena.[917] Iskujen johdosta moskovalaiset yritykset ovat siirtäneet dataansa turvaan Jekaterinburgin ja Novosibirskin palvelinkeskuksiin.[918] Kriittisen informaatioinfrastruktuurin turvaamisessa on ollut muitakin haasteita. Yksityiset toimijat eivät ole halunneet listauttaa infrastruktuuriaan kriittiseksi siitä seuraavien lisävelvoitteiden takia.[919] Kriittistä informaatioinfrastruktuuria koskeva säännöstä on koettu sekavaksi, mutta duuma ei ole halunnut selkeyttää sääntelyä.[920] Avaruuden käytön osalta Venäjällä on myös ollut haasteita. Sen kyky tarjota Starlinkiä vastaavia datayhteyksiä suunnitellulla Skif-järjestelmällä omalla alueellaan on vuosien päässä ja Glonass-hankekin on vaikeuksissa.[921] Informaatioinfrastruktuurin resilienssiä on kuitenkin sääntelyn lisäksi pyritty kehittämään uusilla resursseilla ja hankkeilla. Valtiohallinnon oman RSNetin kehittämiseen on kohdennettu vuodelle 2024 4,8 miljardia ruplaa.[922] Venäjälle halutaan myös luoda oman CDN-verkko (Content Delivery Network) Googlen ja Akamain verkkojen rinnalle.[923] Rostelekom on myös esittänyt yhden, luotetun datavaraston luomista Venäjälle.[924] Esityksistä on pitkä matka toteutumiseen ja infrastruktuurin merkittäviä puutteita tuskin ehditään korjata Venäjän ja Ukrainan sodan aikana. Venäjä kuitenkin kerää arvokkaita havaintoja, joiden avulla se voi varautua paremmin seuraavaan kriisiin tai sotaan.

---

[915] Тельманов, Денис: "Антифрод" в действии. Почти за год Роскомнадзор проверил 69 млрд звонков. *Comnews*, 23.10.2023. [https://www.comnews.ru/content/229634/2023-10-23/2023-w43/1008/antifrod-deystvii-pochti-za-god-roskomnadzor-proveril-69-mlrd-zvonkov], luettu 6.2.2024.
[916] SecurityLab.ru: Россия вошла в топ-15 самых стабильных стран по отказоустойчивости интернета. *SecurityLab.ru*, 21.12.2023. [https://www.securitylab.ru/news/544765.php], luettu 6.2.2024.
[917] Ларина (2023a); 93.ru (2023a).
[918] Исакова, Татьяна: Данные эвакуируют за Урал. Растет спрос на услуги дата-центров подальше от Москвы. *Коммерсантъ*, 26.7.2023. [https://www.kommersant.ru/doc/6124141], luettu 6.2.2024.
[919] Roskomsvoboda: Минцифры готовит законопроект об определении перечня объектов КИИ. *Roskomsvoboda*, 18.5.2023. [https://roskomsvoboda.org/post/mincif-kii-obyekty/; https://tass.ru/ekonomika/19340569], luettu 5.1.2024.
[920] D-Russia: ФСТЭК сообщила об увеличении категории значимости для более чем 40 объектов КИИ в 2023 году. *D-Russia*, 11.10.2023. [https://d-russia.ru/fstjek-soobshhil-ob-uvelichenii-kategorii-znachimosti-dlja-bolee-chem-40-obektov-kii-v-2023-godu.html], luettu 6.2.2024.
[921] Einhorn, Bruce: Russia's Alternative to GPS Satellites Is Outdated and Outnumbered. *Bloomberg*, 21.9.2023. [https://www.bloomberg.com/news/articles/2023-09-20/russia-s-glonass-satellite-system-badly-needs-an-upgrade#xj4y7vzkg], luettu 6.2.2024; Dangwal, Ashish: Russia's 'Own' Starlink! Moscow Says Will Create A Satellite Constellation For High-Speed Internet In 2025. *The Eurasian Times*, 11.11.2022. [https://www.eurasiantimes.com/russias-own-starlink-moscow-to-create-a-satellite-constellation/], luettu 6.2.2024.
[922] Королев, Игорь: В России потратят 4,8 миллиарда на специальный «интернет для властей». *CNews*, 15.6.2023. [https://www.cnews.ru/news/top/2023-06-15_v_rossii_potratyat_48_milliarda], luettu 6.2.2024.
[923] Чебакова, Дарья & Пламенев, Илья: В Госдуме предложили создать национальную систему доставки контента. *РБК*, 20.12.2022. [https://www.rbc.ru/technology_and_media/20/12/2022/63a1d5809a7947ae36175bdb], luettu 6.2.2024.
[924] Roskomsvoboda: К 2030 году в России предлагают создать единое хранилище данных. *Roskomsvoboda*, 9.10.2023. [https://roskomsvoboda.org/post/edin-hran-dannyh/], luettu 6.2.2024.

Venäjä ei ole tyytynyt vain sisäisen kyber- ja informaatioturvallisuutensa kehittämiseen vaan on ajanut informaatioturvallisuuden valtiokeskeistä, kansainvälistä sopimusjärjestelmää olemassa olevien normien soveltamisen ja laaja-alaisen osallistumisen eli multistakeholder-mallin sijaan. Hankkeen perustana on ollut informaation sisällön turvallistaminen ja valtiosuvereniteetin kunnioittaminen informaatiotilassa, tosin uusimmissa versioissa on korostettu telekommunikaatioteknologian käsitettä. Vuoden 2021 lopulla Yhdysvallat ja Venäjä olivat löytämässä toisensa sopimusneuvotteluissa, mutta Ukrainan sota romutti haaveet yhteisymmärryksen löytymisestä. Syksystä 2022 prosessi jatkui OEWG:n (Open-ended Working Group) kehyksessä, mutta heinäkuussa 2023 pidetty OEWG:n kokous ajautui merkittäviin vaikeuksiin Venäjän kumppaniensa kanssa ajaessa aggressiivisesti oman konventioluonnoksensa hyväksymistä osaksi loppulauselmaa. Käytännössä Venäjän hanke ei siis ole hyökkäysoperaation aikana edennyt, mutta se on käyttänyt kiertotienä kahdenkeskisiä ja monenkeskisiä sopimuksia ja julkilausumia mm. Kiinan kanssa ja Shanghain yhteistyöjärjestön piirissä.[925] Joulukuussa 2023 Iranin parlamentti hyväksyi lakihankkeen informaatioturvallisuusyhteistyöstä Venäjän kanssa ja ITU:n WRC-23 konferenssissa Venäjä ajoi Starlink-järjestelmän käytön kieltämistä, koska se loukkasi valtioiden informaatiosuvereniteettia.[926] Vaikka sopimusjärjestelmän rakentamisen taustalla vaikuttaneekin edelleen Venäjän tarve suojautua teknologisesti kehittyneemmiltä vastustajilta, on hanke entistä enemmän tähdätty läntisen säätöpohjaisen maailmanjärjestyksen haastamiseen ja korvaamiseen.

Venäjä on ollut koko Ukrainan sodan ajan riippuvainen läntisestä ICT-teknologiasta ja ohjelmistoista. Sille ei myöskään yrityksistä huolimatta ole kehittynyt merkittävää kotimaista innovaatiopotentiaalia.[927] Suomen valtionhallinnon tilaaman raportin mukaan sota ja suurvalta-aseman ylläpitämisen tarve ovat ohjanneet Venäjän hankkeita entistä enemmän kohti valtiovallan säilyvyyden ja kansallisen turvallisuuden päämääriä taloudellisen kannattavuuden sijaan ja tehneet valmiiksi ylioptimistisista, digitaalisen suvereniteetin tavoittelun suunnitelmista mahdottomia toteuttaa. Valtion rooli informaatioteollisuuden ja -yhteiskunnan veturina on kasvanut entisestään ja Venäjä on pyrkinyt keskittymään kapeisiin, läpimurtoteknologioihin saadakseen edes hetkellisen asymmetrisen edun kilpailijoistaan. Valtion innovaatio-ohjelmat, kansainvälisten yritysten pakotettu lokalisaatio, tuonninkorvausohjelmat ja yhteistyö Kiinan kanssa, eivät kuitenkaan riitä teknologisen itsenäisyyden ja kansainvälisen kilpailukyvyn rakentami-

[925] Черненко, Елена: Третья пошла. Россия внесла на рассмотрение ООН новый проект Конвенции по международной информационной безопасности. *Коммерсантъ*, 21.5.2023. [https://www.kommersant.ru/doc/5999161], luettu 6.2.2024; Черненко, Елена: Манхэттенские проекты. Как Россия и западные страны продвигают в ООН конкурирующие резолюции по кибербезопасности. *Коммерсантъ*, 7.11.2022. https://www.kommersant.ru/doc/5651792], luettu 6.2.2024; Weber, Valentin: The Dangers of a New Russian Proposal for a UN Convention on International Information Security. Council on Foreign Relations, blogikirjoitus, 21.3.2023. [https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security], luettu 6.2.2024; Gavrilović, Andrijana, Grottola, Stefania, Ittelson, Pavlina, Kazakova, Anastasiya, Petit-Siemens, Salomé & Stadnik, Ilona: What's new with cybersecurity negotiations? OEWG 2021-2025 fourth substantive session. DiploFoundation, blogikirjoitus, 6.4.2023. [https://www.diplomacy.edu/blog/whats-new-with-cybersecurity-negotiations-oewg-2021-2025-fourth-substantive-session], luettu 6.2.2024; Hurel, Louise Marie: Avoiding Deadlock Ahead of Future UN Cyber Security Negotiations. RUSI, commentary, 31.8.2023. [https://www.rusi.org/explore-our-research/publications/commentary/avoiding-deadlock-ahead-future-un-cyber-security-negotiations], luettu 6.2.2024.

[926] SecurityLab.ru: МИД РФ призывает к ограничению деятельности спутниковых сетей вроде Starlink. *SecurtiyLab.ru*, 20.12.2023. [https://www.securitylab.ru/news/544750.php], luettu 6.2.2024; SecurityLab.ru: Иран решил объединить усилия с Россией для борьбы с киберугрозами. *SecurityLab.ru*, 11.12.2023.[https://www.securitylab.ru/news/544486.php], luettu 6.4.2024.

[927] Allinger, Barisitz & Timel (2022).

seen. [928] On siis kyseenalaista, missä määrin Venäjä kykenee kehittämään ja muuttamaan kansallisen informaatiotilan informaatiopotentiaalia. Tämä edellyttäisi innovatiivisen, kilpailukykyisen dataekosysteemin luomista Venäjän sisäisistä ongelmista ja geopoliittisesta kilpailusta huolimatta. Epäonnistuminen ei tarkoita välttämättä romahdusta, vaan Venäjän aseman jatkuvaa heikkenemistä suhteessa Yhdysvaltoihin ja Kiinaan. Suurvaltojen välisen informaatiokamppailun näkökulmasta heikkeneminenkin voi kuitenkin tuottaa eksistentiaaliseen uhan ja johtaa kriisiin, kun informaatiovoimaa ei ole tarvittaessa käytössä.

”Sotilaallisesta erikoisoperaatiosta” tuli Venäjän kansallisen informaatioturvallisuuden ja -puolustuksen testi aikaisemmin kuin oli kenties suunniteltu. Venäjään kohdistui välittömästi Ukrainan hyökkäysoperaation alettua massiivinen, kansainvälinen kyberhyökkäysten kampanja, joka on edelleen käynnissä. Kyberhyökkäyksillä on ollut merkittäviä taloudellisia ja informaatiovaikutuksia, mutta Venäjä ei kuitenkaan ole vielä päätynyt irrottamaan kansallista internetsegmenttiään globaaleista tietoverkoista, vaikka onkin tähän väitetysti varautunut. Venäjän informaatiotieteellinen ja -taloudellinen sektori, kriittinen informaatioinfrastruktuuri, yhteiskunnan eri valvonnan ja kontrollin keinot ja kyberpuolustuksen ja -turvallisuuden järjestelmät kävivät kahdessa vuodessa läpi merkittävän kriisin ja selviytymisprosessin. Lopputuloksena on ollut Kremlin ja turvallisuuspalveluiden informaatioylivoima Venäjän sisäisessä informaatiotilassa. Tätä ylivoimaa ei saavutettu vain ”puolustuksellisilla” toimilla. Venäjän ns. hyökkäykselliset kyberoperaatiot ja -tiedustelu kohdistuvat vähintään yhtä paljon oppositiota, separatisteja ja rikollisia vastaan kuin ulkomaailmaa kohtaan. Informaatioherruus, kansallisen informaatiotilan täydellinen hallinta, on jäänyt kuitenkin Venäjältä saavuttamatta. Ukraina ja sen liittolaiset kykenevät operoimaan, vaikkakin rajatusti, teknologisesti ja ajoittain psykologisesti Venäjän informaatiotilassa.[929] Tulevaisuudessa tilanne voi muuttua Venäjän kannalta huonompaan suuntaan. Voikin käydä niin, että Ukrainan sodan jatkuminen, Venäjän poliittisen järjestelmän luonne ja strategisen kulttuurin ideat ohjaavat Venäjän tavoittelemaan kansallista informaatioherruutta. Vain täydellinen hallinta tuo riittävää turvallisuutta.

Turvallisen internetin liigan johtajan mukaan Venäjä on vielä usean vuoden päässä suvereenin internetin rakentamisesta.[930] Tästä huolimatta Venäjän informaatiotila on yhä voimakkaammin vertikaalisti hallittu ja horisontaalisti integroitu. Vastustajien informaatiopsykologinen toiminnanvapaus on pitkälti kiistetty. Järjestelmä perustuu kuitenkin epävarmalle teknologiselle pohjalle, joka yhdessä Kiina-riippuvuuden kanssa uhkaa vesittää haaveet digitaalisesta ja teknologisesta suvereniteetista. Rakentaessaan kotimaiseen teknologiaan ja keskitettyihin hallintajärjestelmiin perustuvaa tilaa, Venäjä tuntuu ajautuvan kohti kriittisten haavoittuvuuksien miinakenttää. Tämä on Venäjälle hyväksyttävissä, koska kansallinen internetsegmentti on venäläisen informaatioturvallisuus ja -puolustusajattelun ilmentymä. Se on *ideologinen* keino globaalin informaatiotilan hallinnan rakenteiden muuttamiseksi ja näin voimatasapainoon vaikuttamiseksi, jonka kehitystä Ukrainan sota on vauhdittanut. Venäjän informaatioturvallisuuden ja -puolustuksen onnistumista tai epäonnistumista Ukrainan sodassa ei voikaan päätellä pelkästään kyberhyökkäysten torjunnan tai verkkosensuurin onnistu-

[928] Lehtinen, Saari, & Suominen (2022).
[929] Giles (2023), s. 33-40; Roskomsvoboda: Треть бизнесменов в России использует заблокированные западные соцсети. *Roskomsvoboda*, 15.11.2023. [https://roskomsvoboda.org/post/advertising-socialmedia-russia-2023/], luettu 6.2.2024.
[930] ТАСС: Эксперт: Россия пока крайне далека от создания суверенного Рунета. *ТАСС*, 12.12.2023. [https://tass.ru/ekonomika/19517217], luettu 6.2.2024.

misen perusteella. Niin pitkään kuin Putinin autoritaarinen hallinto pysyy vallassa, on laajempi strategisen deterrenssin järjestelmä. Vaikka teknisessä toteutuksessa olisikin puutteensa, eivät palvelunestohyökkäykset, tietovuodot tai verkkosivujen sotkemiset tuota riittävää vaikutusta, jos poliittinen toteutus on tarpeeksi toimiva.

8. JOHTOPÄÄTÖKSET

Venäjän kybertoimintaa 2000-luvulla tulee tarkastella yhtäältä venäläisen strategisen kulttuurin, toisaalta toimeenpanevien organisaatioiden ja käytössä olleiden resurssien ja kolmanneksi muuttuvien suurvaltasuhteiden kehyksessä. Valtioiden välisen jatkuvan kamppailun idea, informaatiokeinojen strategiset mahdollisuudet ja uhat, epäsuoruuden ja manipuloinnin lupaama asymmetria sekä suurvaltasuvereenisuuden reunaehdot ovat tehneet järkeenkäyväksi (reasonable) Venäjän kybertoiminnan käyttötavat ja sille asetetut tavoitteet. Informaatiokommunikaatioteknologialla voidaan lamauttaa suurvaltavastustaja, tukea vastustajan poliittisen järjestelmän manipulaatiota ja rakentaa keskitetysti johdettu autoritaarinen informaatioyhteiskunta ja mobilisoida tarvittaessa sen informaatiopotentiaali.

Strateginen kulttuuri ei kuitenkaan määrää toimintaa tai sen lopputulosta. Se mikä kaukaa tarkasteltuna voi näyttää eheältä, yhden toiminta-ajatuksen ja päämäärän mukaan ja selkeästi johdetulta, ei ole sitä käytännössä, ainakaan kaikilta osin. Kybertilan muuttuva luonne ja kybermenetelmien ominaispiirteet, kybertoimia toimeenpanevien turvallisuus-, sotilas- ja siviiliorganisaatioiden intressiristiriidat ja erilaiset toimintatavat, yleensäkin hajanainen toimijakenttä, valtiojohdon eli Kremlin ”käsiohjaus” tai ohjauksen puute, taloudelliset tekijät ml. korruptio, teknologian puutteet ja vastustajien toiminta vaikuttavat kaikki lopputulokseen. Sodan paineen alla käytännön kitkatekijöiden vaikutus saattaa kuitenkin heikentyä toiminnan kohdistuessa yhteisen päämäärän saavuttamiseen, jolloin holistinen teoria ja käytäntö saattavat todella kohdata. Carl von Clausewitz saattaisi tosin olla eri mieltä, sillä pitäisihän sodan päinvastoin lisätä kitkaa.

Suurvaltasuhteet ja niiden vaiheet rauhanomaisesta kilpailusta avoimeen sotaan määrittävät kybertoimien luonnetta, merkitystä ja tarkoitusta. Venäjän, Yhdysvaltojen ja Kiinan geopoliittinen kolmiosuhde, mukaan lukien alueellisten suurvaltojen pyrkimykset ja toiminta, ja vuorovaikutus vaikuttavat siihen, miten kybertoimet sijoittuvat sotilaallisten ja ei-sotilaallisten, aseellisten ja ei-aseellisten, väkivaltaisten ja ei-väkivaltaisten toimien jatkumolle. Venäläinen ja yhdysvaltalainen sekä kiinalainen ajattelu ovat olleet ja ovat edelleen kiinteässä vuorovaikutussuhteessa ja käynnissä on evoluutioprosessi suurvaltojen välillä.[931] Informaatiokamppailusta on tullut holismia kaikille. Kamppailujatkumosta (eng. competition coontinuum) on tullut hyväksytty suurvaltasuhteiden kuva ja se ohjannee kybertoiminnankin kehitystä tulevaisuudessa.[932] Suurvaltojen ”aktiivinen puolustus” tai ”eteen suunnattu puolustus” muuttavat globaalia kybertilaa jokaisen toimijan pyrkiessä informaatioylivoimaan tai jopa informaatioherruuteen jo rauhan aikana. Joskin vielä 2000-luvun alussa suurvallat ovat etsineet eri tapoja käyttää kyberkeinoja, voitaneen nyt todeta, että venäläisen ja läntisen informaatiosodankäynnin eroja määrittelevät enää lähinnä arvot – eli toiminnalle asetut omaehtoiset normatiiviset rajoitukset – jos nekään.

---

[931] U.S. Department of Defence: *2023 Cyber Strategy of The Department of Defense – Summary*. 12.9.2023. [https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF], luettu 6.2.2024; Puranen, Matti: *Informaatioherruus. Kiinan sotilasstrategia ja sodan kuva kylmän sodan jälkeisellä aikakaudella*. Maanpuolustuskorkeakoulu, Sotataidon laitos Julkaisusarja 2, Nro 21. Helsinki, 2022.
[932] NATO: *Allied Command Transformation Strategic Foresight Analysis 2023*. NATO ACT, 2023. [https://www.act.nato.int/wp-content/uploads/2024/01/SFA2023_Final.pdf], luettu 6.2.2024.

Venäjän ja Ukrainan välisen sodan erityisluonne, avoin, äärimmäinen mutta paikallinen aseellinen konflikti ilman varsinaisen sodan julistamista, on vaikuttanut kybersodankäynnin luonteeseen – etenkin Venäjän puolustukseen. Venäjän informaatioyhteiskunta joutui kriisitilaan Ukrainan ja kansainvälisten hakkereiden hyökkäysten seurauksena, mutta alkuhäiriöiden jälkeen se on osoittautunut kriisinsietoiseksi. Venäjän Ukrainaa vastaan toimeenpanevat kyberhyökkäykset vaikuttanevat yhtä paljon venäläisen kyberturvallisuus- ja -sodankäyntiajattelun kehittymiseen, kuin Ukrainan ja sen liittolaisten hyökkäykset Venäjää vastaan. Venäjä tuskin on valmis tulevaisuudessa turvautumaan Kiinan tai muiden valtioiden apuun kriittisen datansa suojelemisessa tai tietoliikennepalveluissa kuten Ukraina on tehnyt, sillä se olisi vastoin teknologisen suvereniteetin ja suurvalta-ajattelun perusteita. Ukrainan sodan perusteella dataa ja teollisuusohjausjärjestelmiä tuhoavat hyökkäykset, tietoliikennejärjestelmien elektroninen häirintä, massiiviset palvelunestohyökkäykset, mediapalveluiden häirintä ja verkkosivujen sotkemiset, tietovuodot, sosiaalisen median manipulaatio ja erilaiset väärennökset ovat varmasti venäläisten tulevaisuuden uhkalistalla. Venäjän valtiojohto on selvästi päätellyt, että informaatioläpimurtoteknologioiden kehittäminen, datan kotiuttaminen ja suojelu, kriittisen informaatioinfrastruktuurin valtiollinen hallinta, sensuuri ja anonymiteetin hävittäminen sekä kansallisten, valtiojohtoisten kyberturvallisuusjärjestelmien kehittäminen suojelevat Venäjää parhaalla tavalla. Informaation liikkuminen avaruudessakin on tuotava valtiolliseen hallintaan tai estettävä. Venäjä on presidentti Putinin johdolla uudistanut kaikki informaatioteknologiaa, -yhteiskuntaa ja -taloutta koskevat ohjelmansa ja strategiansa vuosian 2022–2023. Kehittymässä olleen kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmän puutteet on havaittu ja toimiin on ryhdytty niiden korjaamiseksi. Tulevaisuus näyttää, onko Venäjä tehnyt oikeat päätelmät ja onko sillä resursseja valitsemiensa hankkeiden toteuttamiseen ja informaatiopotentiaalin rakentamiseen.

Eräiden tutkijoiden mukaan Ukrainan sota näyttää todistaneen, että kybertoimet, käytettävissä olevan todistusaineiston valossa, eivät olleet ”game changer”,[933] niiden paikka on vakoilun ja informaatio-operaatioiden tukemisen välineinä,[934] ne enintään tukevat muita voimankäytön muotoja[935] tai ne eivät ole sodankäynnin välineitä laisinkaan.[936] Toiset tutkijat ovat pitäneet Venäjä toimintaa ennen näkemättömänä, käänteentekevänä ja ensimmäisenä aitona kybersotana.[937] Tällaiset väitteet tahallisesti tai tahattomasti ohittavat sen seikan, että Ukrainan ja Venäjän välinen sota vuodesta 2014 tähän päivään on erityistapaus etenkin kyberpuolustuksen näkökulmasta. Ukrainan monivuotinen kokemus Venäjän operaatioista, Lännen valtioiden ja etenkin yksityissektorin merkittävä tuki, Ukrainan informaatioinfrastruktuurin rakenne ja puolustukseen mobilisoitunut siviiliyhteiskunta, Venäjä vuoden 2022 hyökkäysoperaation itse aiheutettu epäonnistuminen, Venäjään ja Ukrainan liittolaisiin kohdistuneiden kyberhyökkäysten rajallisuus – sekä puolueettomien ja riittävien lähteiden puute! – teke-

[933] Hammes, T. X.: *Game-changers: Implications of the Russo-Ukraine War for the Future of Ground Warfare*. Atlantic Council, April 2023. [https://www.atlanticcouncil.org/wp-content/uploads/2023/04/Game-Changers-or-Little-Change-Lessons-for-Land-War-in-Ukraine-.pdf], luettu 6.2.2024.
[934] Bateman (2022).
[935] Mueller et al. (2023).
[936] Zilincik, Samuel & Duyvesteyn, Isabelle: Strategic Studies and Cyber Warfare. *Journal of Strategic Studies*, 2023. [DOI: 10.1080/01402390.2023.2174106].
[937] Näistä näkemyksistä ks. Kerr (2023), s. 1–2; Nilsson (2023).

vät kybersodankäyntiin liittyvistä yleistyksistä epäluotettavia.[938] Tämänkin tutkimuksen havainnot tullevat vanhenemaan tiedon lisääntyessä.

Erityisyydestään huolimatta Ukrainan sota on todennäköisesti murroskohta niin läntisessä kuin venäläisessä kybersodankäyntiin liittyvässä ajattelussa. Yhtäältä Venäjän operaatioiden epäonnistuminen ja Ukrainan onnistuminen, toisaalta Lännen ja Venäjän välinen kyberdeterrenssiviestintä, ja kolmanneksi, vielä osittain tuntematon, Ukrainan ja läntinen kybervaikuttaminen Venäjään tulevat muokkaamaan kybersodankäynnin kuvaa. Lisäksi informaatioteknologisten ja psykologisten menetelmien ja keinojen suhde kehittyy jatkuvasti aggressiivinen informaatiovaikuttamisen jatkuessa.

Venäjän sotataidon kehittymisen näkökulmasta olennaista ovat venäläisten, eivät läntisten tarkkailijoiden, tekemät päätelmät kyberoperaatioiden strategisen ja operatiivisen vaikutuksen puutteesta. Venäjän näkökulmasta luonnollisin selitys on se, että Yhdysvalloilla on kyky käyttää hyväkseen yhdysvaltalaisten ja läntisten yritysten ohjelmistoissa olevia haavoittuvuuksia niin puolustus- kuin hyökkäystoimintaan. Yhdysvaltojen kyky auttaa Ukrainaa Venäjän kyberhyökkäysten torjunnassa kevättalvella 2022 tukee tätä näkemystä. Tämän takia on Venäjän näkökulmasta rationaalista pyrkiä rakentamaan kotimaista ohjelmisto- ja laitteistotuotantoa. Ainakin se laimentaa Yhdysvaltojen asymmetrista etua kybertilassa – huolimatta ratkaisun mukanaan tuomista kyberturvallisuuteen liittyvistä ongelmista. Väliaikainen riippuvuus Kiinasta on pienempi paha kuin riippuvuus Yhdysvalloista. Samaan aikaan on strategisen tasapainon säilyttämisen kannalta oleellista viestittää Yhdysvalloille, että sen kriittinen informaatioinfrastruktuuri on jatkuvan uhan alla. Hyökkäysmenetelmiä on kehitettävä ja niiden suorituskyky on todistettava, jotta rapautuneen tavanomaisen deterrenssin jättämää tyhjiötä kyetään täyttämään – absoluuttisen strategisen ydinasedeterrenssiviestinnän tukena.[939]

Vahva usko teknologian suomaan asymmetriaan ja näkemys läntisten yhteiskuntien heikkoudesta tuskin saa Venäjän asevoimia luopumaan kyberaseista, kun ne ovat niihin nyt tarttuneet. On hyvin todennäköistä, että Venäjä katsoo onnistuneensa kyberdeterrenssiviestinnässä vuosina 2022–2023 ja tulee toistamaan ja kehittämään vastaavaa toimintaa tulevaisuudessa. Tämä tarkoittaa kyberoperaatioiden, olivat ne sitten huliganismia, vakoilua tai voimannäyttöjä, käyttöä Venäjän vastustajia vastaan, olivat ne sitten yksittäisiä maita tai liittoumia. Vaikka hyökkäyksellisten tuhoavien kybertoimien vaikutus on jäänyt vaillinaiseksi, ne tulevat varmasti olemaan osa Venäjän tulevaisuuden sotataitoa. Informaatioteknologisen sodankäynnin eri osa alueiden vaikutusten synkronoinnista on saatua oppia ja kyberhyökkäyksillä on Ukrainan tapahtumien perusteella potentiaalia niin yllätyksellisen hyökkäyksen kuin pitempi aikaisen yhteiskunnan eheyden ja talouden rapauttamisessa. Modernissa asemasotavaiheessa ja kulutussodankäynnissä kyberoperaatiot ulottuvat vastustajan tukialueelle siinä missä ohjukset ja lennokitkin. Venäjällä ei ole myöskään mitään syytä luopua kyberavusteisten informaatio-operaatioiden käytöstä vastustajien tahdon ja kilpailevien liittokuntien rapauttamiseksi. Kamppailu informaatiotilan hallinnasta on jatkuvaa ja ydinasedete-

[938] Venäjän epäonnistumisen ja Ukrainan onnistumisen syiksi on esitetty mm. puutteellista valmistelua, huonoa suorituskykyä, Ukrainan hyvää puolustusta ja sen saamaa ulkomaista tukea, Venäjän omaehtoista pidättäytymistä, kyberhyökkäys-puolustustasapainon muutosta, kybertilan vakoilua ja infovaikuttamista korostavaa luonnetta, kybertoiminnan haastavaa yhteensovittamista operaatioihin, vaikutusten aikaansaamisen vaikeutta tai niiden jäämistä näkymättömiksi. (Kerr (2023); Giles (2023); Nilsson (2023)).

[939] Venäjän deterrenssin rapautumisesta ks. Forsström, Pentti: *Russia's War on Ukraine. Strategic and Operational Designs and Implementation*. National Defence University, Department of Warfare, Series 2 nro 29. Helsinki, 2023.

rrenssin alla tulevaisuuden informaatiovaikuttaminen voi saada entistä radikaalimpiakin muotoja. Muutosta voi myös tapahtua siinä, miten kybertilasta tai -tilaan kohdistetaan strategiseen deterrenssiin liittyvää toimintaa eli miten kineettinen, digitaalinen ja psykologinen nivoutuvat toisiinsa sodankäynnin toimintaympäristöjen läpi.

Venäjän tulevaisuuden kyberoperaatioiden ja kybermenetelmien käytön arviointia vaikeuttaa se, että vaikka Venäjän operaation alkuvaiheen kyberoperaatiot olivat ennen näkemättömiä ja huolellisesti suunniteltuja, niiden epäonnistumista on vaikea erottaa koko kaappaushyökkäyksen epäonnistumisesta, jolla oli omat moninaiset syynsä. Arviointia vaikeuttaa myös se, että Venäjän toiminta on sodan tapahtumien takia muuttunut useaan otteeseen. Kybertoiminnasta voidaan jälkikäteen erottaa vaiheita, mutta nämä ovat helposti mielivaltaisia ja perustuvat asioiden selittämiseen nykyhetkestä käsin. Selvää on, että hyökkäyksen alkuvaihe, sitä seurannut improvisoitu jatko, kevään perääntymisvaihe, kesän hiljaisempi kausi ja syksyn sekä talven uudet hyökkäykset muodostavat jonkinlaisen vaiheistuksen vuodelle 2022.

Vuoden 2023 vastaavaa vaiheistusta on paljon vaikeampi muodostaa. Yksi kuvaus lienee jatkuva kyberavusteinen kulutussodankäynti, jossa vakoilu, satunnaiset tuhoavat hyökkäykset ja informaatiovaikuttamisen tukeminen ovat olleet pääosassa. Tällaisesta sodankäynnistä on vaikea erottaa venäläisteoreetikkojen informaatioiskuoperaatioita ja strategisia iskuja kriittiseen infrastruktuuriin vaan kyse on pikemminkin jatkuvasta operoinnista, jonka tavoitteen on heikentää Ukrainaa, kunnes se romahtaa tai on lyötävissä. Kuluttaminen ei tässä viittaa välttämättä merkittäviin taloudellisiin menetyksiin tai tuotannon pysyvään alenemiseen. Kyberhyökkäykset eivät tuota itsenäisesti sellaisia vaikutuksia pitkällä aikavälillä. Se ei viittaa myöskään infrastruktuurin rapautumiseen tai asevoimien kulumiseen. Pikemminkin kyberhyökkäysten rooli on, sotilaallisten ja väkivaltaisten toimien lisäksi, pitää vastustaja jatkuvan sekasorron, epävarmuuden ja epätietoisuuden tilassa. Kun sodankäynnin luonne muuttuu jälleen tuhoavaksi, kyberoperaatiot voivat, hyvin valmisteltuina, siirtyä tukemaan tällaista sodankäyntiä.

Venäjän toimintaa vuonna 2023 voidaan tarkastella myös toimintojen kautta. Pistemäiset tuhoavat hyökkäykset, joskus kostamistarkoituksessa joskus kineettisten operaatioiden tukena, massamaiset ja kohdennetut palvelunestohyökkäykset Ukrainan ja Nato-maiden eri valtiollisia ja yhteiskunnallisia sektoreita vastaan, tietovuodot ja verkkosivujen sekä muiden medialähetysten sotkemiset, asevoimien järjestelmien häirintä ja lamauttaminen, tunkeutuminen tietoverkkoihin suorituskyvyn osoittamiseksi sekä kaikkinainen vakoilu voidaan erotella omiksi muodoikseen ja menetelmikseen. Tällöin on selvemmin nähtävissä, kuinka eri venäläistoimijoiden operaatiot ovat käynnissä rinnakkain palvellen kenties sodan päämäärää, mutta keskittyen omiin kohteisiinsa ja tavoitteisiinsa. Vaiheistuksen etsiminen tällaisesta prosessista tai kaiken kybertoiminnan sijoittaminen kulutussodankäynnin kehykseen ei tällöin tarjoa parasta mahdollista ymmärrystä Venäjän toiminnasta. Tuloksellisempi tapa voisi olla Sandwormin, APT28:n, Gamaredonin tai XakNetin operaatioiden tarkastelu rinnakkain ja ajassa – jotain mihin tämä tutkimus tarjoaa perusteet. Etsittiin kybersodankäynnistä sitten vaiheita, sotatoimen tapoja tai toimintoja on kybertilan jatkuva muutos huomioitava analyysissä. Muutos ei synny ainoastaan toiminnasta ja vastatoiminnasta vaan myös sotatoimen tilan ominaisuuksien muutoksesta.

Olisi väärin vetää ulkopuolelta muodostetuista vaiheista tai prosesseista johtopäätöksiä venäläisen kybersotataidon kehittymisestä. Operaation alun epäonnistuminen ja

nykytilanne ovat varmasti asioita, joita venäläiset haluavat tulevaisuudessa välttää. Toisaalta on vaikea osoittaa, mistä syystä venäläiset katsovat epäonnistuneensa ja mitä he katsovat vaihtoehtojen olleen. Helppoa on kuitenkin liioitella Venäjän saamaa oppia ja rakentaa pelon ilmapiirissä yhtäläisyysmerkit kokemusten ja tulevaisuuden ylivoimaisen suorituskyvyn välille.[940] Olemassa olevan tiedon perusteella voitaneen väittää, että Venäjän operaatiot kybertilassa eivät olleet toteutukseltaan holistisia, yhtenäisiä tai keskeytymättömiä hyökkäyksen ensivaiheen jälkeen. Ne eivät sellaisinaan johtaneet strategisten tavoitteiden saavuttamiseen, kuten eivät Venäjän kyberoperaatiot Ukrainaa vastaan ennen erikoisoperaation alkuakaan.[941] FSB, GRU, SVR ja monimuotoiset haktivistiryhmät todennäköisesti toimeenpanivat operaatioita omin tavoittein ja kyvyin osittain opportunistisesti. Sodan toisena vuonna toiminnasta on tullut järjestelmällisempää ja todennäköisesti ohjatumpaa. Menetelmät ovat sopeutuneet sodan luonteeseen ja sotatoimen päämääriin.[942] Näin ollen venäläinen kybersodankäynnin doktriini tulee varmasti kehittymään seuraavien vuosien aikana kohti kohdattujen ongelmien ratkaisuja. Mikäli läntiset attribuutiot ovat olleet oikeassa, Sandwormin ja Gamaredonin riveistä nousevat tulevaisuuden venäläisen kybersodankäyntitaidon kehittäjät. Ja jos väite siitä, että sotilaat valmistautuvat sotimaan edellistä sotaa pitää paikkansa[943], niin nämä kehittäjät pyrkivät löytämään vastauksen siihen, miten vuoden helmi-maaliskuun 2022 hyökkäykset olisivat tuottaneet strategisia vaikutuksia.

Muutama Ukrainan sodan kokemus ja erityispiirre tulee todennäköisesti vaikuttamaan Venäjän ja muidenkin valtioiden kybertoiminnan kehitykseen tulevaisuudessa. Ei olisi lainkaan yllättävää, jos informaatioiskuoperaatiot nousisivat uudelleen venäläisen sotatieteellisen keskustelun aiheeksi. Aikaisemmin esitetyt näkemykset olivat teoreettisia pohdintoja, mutta nyt informaatioiskujen, -operaatioiden ja -taisteluiden toteuttamisesta on käytännön kokemuksia. Kyber- ja kineettisten operaatioiden koordinointi voi onnistua, jos aikautus on hyvissä ajoin tiedossa ja tiedustelulla ja valmistelulla on näin ollen riittävästi aikaa ja tilanne on vakaa eli kybertila ei muutu operaation ”jalkojen alla.” Muussa tapauksessa vain palvelujen ja talouden yksinkertainen häirintä ja informaatiovaikuttamisen tukeminen on riittävän luotettavaa ja kustannustehokasta ollakseen vaikuttavaa. Kyber- ja kineettisten iskujen yhteisvaikutusten ketjuttaminen vastustajan järjestelmissä vaikuttaa olevan vaativaa, eivätkä keskinäisriippuvuuksien haitalliset vaikutukset välttämättä toteudu helposti. Kyberpuolustus tai paremmin ehkä resilienssi, yhdistettynä määrättyyn yhteiskunta- ja talousrakenteeseen, näyttää sittenkin tarjoavan toimivia vastauksia, kun hyökkäyksiä pidettiin pitkän aikaa ylivoimaisina.

Ukrainan sota on osoittanut, että kybertilassa yksityisillä toimijoilla ja ruohonjuuritason aktivismilla voi olla merkittäviä vaikutuksia tulevaisuuden sodissa.[944] Venäjällä on ollut käytössään ainakin neljä erilaista sijaistoimijaryhmää: Turvallisuuspalveluiden peiteorganisaatioita, niiden johtamia aktivistiryhmiä, ostettuja rikollisia ja kevyesti ohjattuja patrioottisia ryhmiä. Lisäksi Venäjä on käyttänyt muiden valtioiden kyberorganisaatioiden infrastruktuuria hämärtääkseen toimijuutensa. Venäjä on myös mobi-

[940] Esim. Giles (2023), s. 53–54.
[941] Maschmeyer, Lennart: The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. *International Security*, 46(2) 2021, s. 51–90.
[942] GRU kehityksestä ks. Black & Roncone (2023).
[943] Dana, Mike: Future War: Not Back to the Future. *War on the Rocks*, 6.3.2019. [https://warontherocks.com/2019/03/future-war-not-back-to-the-future/], luettu 6.2.2024.
[944] Franke, Ulrike & Söderström, Jenny: Star tech enterprise: Emerging technologies in Russia's war on Ukraine. European Council on Foreign Relations, 5.9.2023. [https://ecfr.eu/publication/star-tech-enterprise-emerging-technologies-in-russias-war-on-ukraine/], luettu 6.2.2024.

lisoinut yksityiset kyberturvallisuusalan yritykset sekä palkkasotilasyritysten kybersuorituskyvyt osaksi taistelutoimia. Näiden kaikkien rinnalla ovat toimineet aidosti patrioottiset hakkeriyhteisöt.

Venäjä pyrkinee häivyttämään attribuoidut APT-toimijansa uusien organisaatioiden, yhteisöjen ja toimintatapojen taakse, jotta niiden valtiosidonnaisuutta ei voitaisi käyttää sitä vastaan oikeustoimissa tai informaatiovaikuttamisen välineenä. Myös Ukraina ja sen liittolaiset ovat mobilisoineet tuhansia aktivisteja ja yrityksiä tuekseen toteuttamaan operaatioita, joiden suhde sotatoimiin on sodan lakien näkökulmasta epämääräinen. Tulevaisuuden kybertaistelukenttä tulee hämärtymään ja sodan lakien soveltamisesta tulee entistä hankalampaa. Ukrainan sota ja syksyllä 2023 alkanut Israelin ja Hamasin välinen sota ovat osoittaneet, että tulevaisuuden sotiin kuuluvat niin valtiosidonnaiset kuin ideologiset haktivistiryhmät sekä rahalla ostettavat tai oikeustoimilla painostettavat rikollisryhmät. Tämä kehitys voi omalla, kierolla tavallaan palvella Venäjän pyrkimyksiä kansainvälisen, valtiokeskeisen informaatioturvallisuussopimuksen solmimiseksi. Anarkian edistäminen on yksi tapa osoittaa, että anarkia on uhka ja sitä pitää hallita.

Teleliikenneinfrastruktuurin kaappaaminen ja informaatiotilan rajojen siirtäminen aluevalloitusten mukana ei ole varsinaisesti uusi ilmiö, mutta Venäjän ja Ukrainan sodassa se on saanut informaatioyhteiskuntien ja -talouden kehittymisen myötä uudenlaista merkitystä. Kyky toteuttaa vallatun tilan informaatioteknologista ja -psykologista hallintaa on edellytys väestön hallinnalle ja uuden järjestyksen rakentamiselle sekä tietenkin jatkuvien sotatoimien tukemiselle. Tämän hallinnan on huomioitava niin vapaa tila, sähköiset järjestelmät kuin tietosisällöt ja ihmiset. Informaatiotilan valtaaminen ja hallinta on osa tulevaisuuden sotatoimien tapoja ja keinoja. Ukrainan sota on myös osoittanut, että ainakin Venäjä on tarvittaessa ollut valmis tuhoamaan informaatioinfrastruktuuria kyberhyökkäyksillä ja samalla paljastamaan pitkäaikaiset vakoiluoperaationsa, vaikka operatiivinen tilanne ei ole sitä vaatinut. Tällaiset tapaukset ovat toki olleet poikkeuksia ja tapahtuneet pääosin hyökkäysoperaation toisena vuonna. Ne kuitenkin osoittavat, että tiedonhankinnan tarpeet eivät ole aina ohittaneet muita intressejä. Joskus nämä intressit tosin ovat vaikuttaneet enemmänkin kustonhalulta tai pyrkimykseltä osoittaa kybertoiminnan relevanttiutta kuin todellisen operatiiviseen tai strategiseen tarpeeseen perustuneilta toimilta.

Maailman autoritaariset valtiot tarkkailevat Venäjän digitaalisen suvereniteetin ja kansallisen internetsegmentin hanketta. Jos se osoittautuu riittävän hyväksi tavaksi turvata valtion informaatioturvallisuus, saattaa Venäjän ratkaisu saada seuraajia. Venäjä ei ole toki ainut maa, joka pyrkii kontrolloimaan informaatiotilaansa, mutta se on ainut, jonka mallin kestävyyttä on koeteltu Lännen väitettyä informaatioylivoimaa vastaan. Mikäli valloitussodat tulevat tulevaisuudessa lisääntymään, tarjoaa Venäjä mallin myös informaatioinfrastruktuurisodankäynnille. Fyysisten yhteyspisteiden ja valokaapeliyhteyksien kaappaaminen ja tuhoaminen, verkkoliikenteen uudelleen reitittäminen ja valvonta, vastustajan mobiiliyhteyksien hyväksikäyttö, satelliitti- ja mobiiliyhteyksien häirintä, taajuusalueiden käytön häirintä tai estäminen ja kotimaisten teleoperaattoreiden käyttö informaatiotilan valtaamisessa kuuluvat todennäköisesti erottamattomasti tulevaisuuden sodankäyntiin. Kybertoiminnassa tulee kiinnittää aikaisempaa suurempaa huomiota siihen, mitä uhkia ja mahdollisuuksia liikkuvat maantieteelliset rintamalinjat ja pitkään jatkuvat taistelutoimet synnyttävät.

Lopuksi on hyvä tuoda esiin se, mitä Venäjän hyökkäysoperaatiossa ei tähän mennessä ole nähty: Hallitsemattomasti leviäviä tai laaja-alaisesti eri kohteisiin käytettyjä tuhoavia kyberhyökkäyksiä, jotka aiheuttavat miljardiluokan tappioita teollisuudelle tai kuolonuhreja. NotPetya osoitti, että tällaiset hyökkäykset ovat mahdollisia ja VIASAT:n modeemeja vastaan tehty hyökkäys osoitti, että Venäjällä oli valmius ja tahto toteuttaa tällaisia hyökkäyksiä. VIASAT operaatio jäi kuitenkin ainutkertaiseksi. Talous-, finanssi-, energia- ja teollisuuskohteisiin tehdyt hyökkäykset ovat kuitenkin olleet jatkuva osa Venäjän operaatiota. Niiden yhteisvaikutuksen vakavuutta on vaikea todistusaineiston puutteessa todentaa. Ne ovat silti todennäköisesti madaltaneet suorituskyvyllistä ja moraalista kynnystä laajamittaisiin hyökkäyksiin tulevissa konflikteissa. Vähintäänkin tuhoavat kyberhyökkäykset ovat muodostuneet osaksi vastustajan talouteen kohdistuvaa kulutussodankäynnin keinovalikoimaa. On mahdollista, että ilman Ukrainan sodan deterrenssiasetelmaa Yhdysvaltojen ja Naton sekä Venäjän välillä tuhoavat kyberhyökkäykset olisivat saaneet toisenlaisen luonteen.

Venäjän epäonnistumista Ukrainan hyökkäysoperaatiossa on pidetty todisteena sekä kybersodankäynnin tutkimuksen että Venäjään kohdistuva sotatieteellisen tutkimuksen epäonnistumisesta.[945] Läntistä itsetutkiskelua ja -kritiikkiä tärkeämpää on kuitenkin se, mitä oppeja kaikki Ukrainan sodan osapuolet ja ulkopuoliset tarkkailijat operaatiosta johtavat. Venäjän näkemykset kyberpuolustuksesta ja -turvallisuudesta sekä hyökkäysoperaatioiden käytettävyydestä muuttuvat varmasti. Koska nämä toiminnot kuuluvat eri organisaatioiden toimintakenttään, joista jokaisella on oma kulttuurinsa ja intressinsä, voivat näkemykset olla ristiriitaisia. Suurvaltasuhteiden näyttäessä kehittyvän keskipitkällä aikavälillä kohti entistä tiukempaa vastakkainasettelua on perusteltua olettaa, että Venäjän näkemysten kehitystä ohjaa alueellisen tai jopa suursodan mahdollisuus tulevaisuudessa. Venäläisen sotataidollisen ajattelun mukaan tällaisissa sodissa kaikki kansakunnan voimavarat sekä keinot ovat käytössä ja sotaa edeltävällä ja sodan alkuvaiheella on ratkaiseva merkitys. Näissä vaiheissa tuhoavilla kyberhyökkäyksillä ja niiltä puolustautumisella on venäläisen strategisen kulttuurin mukaan paikkansa todennäköisesti myös tulevaisuudessa.

[945] Keskustelusta ks. Kostyuk & Gartzke (2022); Renz (2023).

Maanpuolustuskorkeakoulu
Sotataidon laitos
PL 7, 00861 HELSINKI

Puh. +358 299 800

www.mpkk.fi

ISBN 978-951-25-3436-4 (nid.)
ISBN 978-951-25-3437-1 (PDF)
ISSN 2343-5275 (painettu)
ISSN 2343-5283 (verkkojulkaisu)

SOTATAIDON YTIMESSÄ

Puolustusvoimat
The Finnish Defence Forces