Puolustusvoimien tutkimuslaitos
Julkaisuja 13

Rakenteellisen kyberasymmetrian strategiset vaikutukset:

Venäjän kansallinen internetsegmentti sotilasstrategisena ilmiönä

Juha Kukkola

Puolustusvoimien tutkimuslaitoksen julkaisuja numero 13

RAKENTEELLISEN KYBERASYMMETRIAN STRATEGISET VAIKUTUKSET:
VENÄJÄN KANSALLINEN INTERNETSEGMENTTI SOTILASSTRATEGISENA ILMIÖNÄ

Juha Kukkola

PUOLUSTUSVOIMIEN TUTKIMUSLAITOS
FINNISH DEFENCE RESEARCH AGENCY

RIIHIMÄKI 2021

Kannen layout: Valtteri Vanhatalo

ISBN 978-951-25-3211-7 (painettu)
ISBN 978-951-25-3212-4 (verkkojulkaisu)
ISSN 2342-3129 (painettu)
ISSN 2342-3137 (verkkojulkaisu)

Puolustusvoimien tutkimuslaitos
Finnish Defence Research Agency

PunaMusta
Tampere 2021

Esipuhe

Venäjä ei useinkaan vastaa odotuksia, vaan onnistuu yllättämään. Venäjää voi kuitenkin järjellä ymmärtää, jos sitä tarkastelee sen omista lähtökohdista. Tämä yleisesikuntaupseerikurssi 60:n diplomityöstä muokattu julkaisu päättää Venäjän kyber/informaatiotoimintaympäristön käsittelevän julkisen tutkimuskokonaisuuden, jota Maanpuolustus-korkeakoulun (MPKK) ja Puolustusvoimien tutkimuslaitoksen (PVTUKL) tutkijat ovat yhdessä työstäneet vuodesta 2016 asti.

Tutkimuksen keskiössä on ollut Venäjän tavoite saavuttaa "digitaalinen suvereniteetti" ja rakentaa suljettu riippumaton kansallinen internetsegmentti. Tutkijat tarkastelivat prosessia ennakkoluulottomasti Venäjän näkökulmasta ja tunnistivat sen sisäisen johdonmukaisuuden. Tutkijat osoittivat, ensimmäisten joukossa, että Venäjä on aloittanut kansallisen internetsegmentiin sulkemisprosessin jo vuosia sitten ja toteuttanut useita toimenpiteitä "digitaalisen suvereniteetin" saavuttamiseksi lainsäädännössä, kansallisten ohjelmistojen ja verkkohallintaratkaisujen kehityksessä ja käyttöönotossa sekä uusien liittolaisten hankinnassa. Tutkimuksessa osoitettiin myös mahdollisesti syntyvä voimaepätasapaino, johon vastaaminen vaatii laaja-alaista, monitieteellistä tutkimusta teknis-matemaattiselta strategiselle ja poliittiselle tasolle ilmiön vaikutusten ja sen taustalla olevien toimien ymmärtämiseksi. Tästä aihepiiristä on MPKK:n ja PVTUTKL:n tutkijoiden yhteistyöllä tuotettu merkittävä määrä monitieteellisiä kansainvälisesti vertaisarvioituja julkaisuja ja opinnäytetöitä.

Venäjän kansallinen internetsegmentti vaikuttaa toteutuessaan globaalin kybertoimintaympäristön voimasuhteisiin ja toimintaperiaatteisiin. Jo pelkästään verkon sulkemisen suunnittelu pakottaa muut reagoimaan. Nyt käsissä oleva julkaisu selvittää Venäjän kansallisen internetsegmentin potentiaalisia strategisia vaikutuksia ja vertailee avoimien ja suljettujen verkkojen rakenteellisia eroja mahdollisen konfliktin eri vaiheissa.

Helmikuussa 2021 Venäjän turvallisuusneuvoston varapuheenjohtaja Dmitri Medvedev ilmoitti Venäjän olevan halutessaan valmis irrottautumaan globaalista internetistä. Mahdollista tai ei - ilman MPKK:n ja PVTUTKL:n tutkijoiden avarakatseista työtä tämä olisi saattanut tulla yllätyksenä. Tutkimuksen kautta Venäjän toimet ja niiden seurauksen tulevat ymmärrettäviksi. Kenties jopa paremmin kuin kansallisen internetsegmentin rakentajille itselleen.

Tutkimme, ymmärrämme, valmistaudumme - emme tule yllätetyksi.

Rauno Kuusisto
Professori, FT
Osastonjohtaja
Informaatiotekniikkaosasto
Puolustusvoimien tutkimuslaitos

Tiivistelmä

Tämän tutkimuksen tavoitteena on kehittää käsite- ja teoriapohjaa rakenteellisen kyberasymmetrian tutkimiseksi ja tarkastella Venäjän kansallisen internetsegmentin strategisia vaikutuksia. Aihe on tärkeä, koska kybertila on yksi sodankäynnin ulottuvuuksista, joiden läpi tai jonne voimaa voidaan suunnata poliittisten päämäärien saavuttamiseksi. Menetelmällisesti työ on tapaustutkimus, joka perustuu teoriasidonnaiseen ja käsitepohjaiseen ymmärtämiseen pyrkivään laadulliseen analyysiin.

Työ osoittaa, että kybervoiman tarkastelu kybertilan ja -toimintaympäristön muokkaamisen välineenä tarjoaa uuden näkökulman valtioiden kyberstrategioiden vaikutusten ja valtioiden asymmetristen voimasuhteiden tutkimiseen. Toiminnan vapaus, yhteinen tilannekuva, johtaminen ja resilienssi ovat käyttökelpoisia käsitteitä tutkittaessa suljettujen ja avoimien kansallisten verkkojen suhdetta. Käsitteiden yhdistäminen informaatioturvallisuuden ja -puolustuksen järjestelmän malliin mahdollistaa kansallisten verkkojen hallinnan tarkastelun ja vertailun uudella ja kybertoimintaympäristön muutoksen huomioivalla tavalla.

Työn perusteella voidaan väittää, että kansallisen internetsegmentin tuottama rakenteellinen kyberasymmetria asettaa merkittäviä reunaehtoja valtioiden voimankäytölle ja muokkaa sen vaikutuksia. Kansallisen internetsegmentin rakentamista voidaan verrata taistelukentän strategiseen muokkaamiseen ja valmisteluun. Venäjän kansallinen internetsegmentti voi toteutuessaan muuttaa globaalin kybertoimintaympäristön voimatasapainoa. Kansallisessa internetsegmentissä on kuitenkin merkittäviä haavoittuvuuksia. Lisäksi sen rakentaminen lisää toimintaympäristöjen välistä keskinäisriippuvuutta, suurvaltakilpailua, eskalaatioriskejä ja taipumusta ennaltaehkäisevään iskuun. Kansallinen internetsegmentti edistää kybertilan fragmentaatiota ja kybersuvereniteetin normin vahvistumista.

Asiasanat: Kyber, Venäjä, asymmetria, deterrenssi, eskalaatio, sotilasstrategia

Summary

The aim of this study is to develop a theoretical and conceptual basis for studying structural cyber asymmetry and to examine the strategic effects of the Russian national segment of the Internet. Methodologically this study is a theory-driven qualitative case study based on content analysis and abduction.

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

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

Keywords: Cyber, Russia, Asymmetry, Deterrence, Escalation, Military Strategy

Sisällys

Tiivistelmä **5**

Summary **6**

1 Johdanto **13**

1.1 Aikaisempi tutkimus 14

1.2 Tutkimusongelma ja -kysymykset 23

1.3 Teoreettinen viitekehys ja näkökulma 25

1.4 Tutkimusmenetelmät ja lähteet 30

1.5 Luotettavuudesta ja rajoituksista 35

2 Kybervoima ja rakenteellinen kyberasymmetria **40**

2.1 Kybertila, kybervoima ja kyberstrategia 41

2.2 Voimankäyttö, konfliktin vaiheet, ennaltaehkäisy, deterrenssi ja eskalaatio 51

2.3 Asymmetrian käsite 74

2.4 Rakenteellinen kyberasymmetria 91

2.5 Rakenteellisen kyberasymmetrian analyysikäsitteet 97

2.5.1 Toiminnan vapaus 101

2.5.2 Yhteinen tilannekuva 106

2.5.3 Johtaminen 111

2.5.4 Resilienssi 120

3 Venäjän kansallinen internetsegmentti **124**

3.1 Systeemi analyysikehikkona 124

3.2 Venäjän valtion ominaispiirteet 136

3.3 Kansallisen internetsegmentin käsitteet ja tausta 141

3.4 Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä 153

3.5 Teoreettisen avoimen kansallisen verkon rakenne ja ominaispiirteet 159

4 Asymmetrian analyysi **168**

4.1 Suljetun ja avoimen kansallisen verkon väliset hyökkäysvektorit 169

4.2 Suljetun ja avoimen kansallisen verkon sisäiset rakenteelliset erot 174

4.3 Suljetun ja avoimen kansallisen verkon erot valtiosuhteiden jatkumolla 181

4.4 Analyysin yhteenveto 188

5 Strategiset vaikutukset 192
5.1 Konfliktin ennaltaehkäisy 193
5.2 Deterrenssin toimivuus 200
5.3 Konfliktin eskalaation hallinta 214
5.4 Asymmetrian sotilaallinen hyväksikäyttö 224

6 Päätäntä 240
6.1 Vastaukset 240
6.2 Pohdinta 256
6.3 Kritiikki ja jatko 265

KESKEISET KÄSITTEET

Luku, jossa käsite on esitelty, johdettu aikaisemmasta tutkimuksesta tai määritelty on merkitty käsitemääritelmä perään. Mikäli käsitteen määrittely on ainutkertainen, se on viitteistetty.

Informaatio: Kontekstiin asetettuja ja rakenteen ja näin merkityksen saaneitä erillisiä, itsessään järjestäytymättömiä faktoja (dataa).[1]

Informaatioturvallisuus: Informaatioturvallisuus liitetään useimmin tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen. Tässä työssä se ymmärretään venäläisittäin ja valtiokeskeisittäin eli valtion suojaksi ulkoisilta ja sisäisiltä informaatiouhilta, mikä turvaa valtion suvereniteetin, alueellisen eheyden, taloudellisen kehityksen, puolustuksen ja turvallisuuden. Informaatiouhat voivat olla luonteeltaan niin psykologisia eli mieleen kohdistuvia kuin teknologisia eli järjestelmiin, laitteisiin ja niissä sijaitsevaan informaatioon kohdistuvia (ks. kyberoperaatio). (Luku 3.1)

Informaatiovaikuttaminen: ”Toiminta[a], jossa informaatiota tuottamalla, muokkaamalla tai sen saatavuutta rajoittamalla muutetaan kohteen käsityksiä tai toimintaa informaatio- ja mielipideympäristön kautta.”[2] Informaatiovaikuttamista voidaan toteuttaa kybertoimintaympäristön kautta ja sitä voidaan tukea kyberoperaatioilla. (Luku 2.2)

Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä: Valtion informaatioturvallisuutta tuottavaa järjestelmien järjestelmä. Yhtenäinen kokoelma valtiojohdon välineitä ja keinoja kansallisen internetsegmentin rajaamiseksi, rakentamiseksi ja turvaamiseksi kybertilassa. Järjestelmä suojelee valtiota ulkoisilta ja sisäisiltä kyber- ja informaatiouhilta, turvaa osiltaan sen suvereniteettia ja toimii sen voimanlähteenä. Järjestelmän rakenne, toiminta ja päämäärä saavat tarkemman muotonsa valtion ominaispiirteistä. Tässä työssä järjestelmä on

---

[1] Rowley, Jennifer: The Wisdom Hierarchy: Representations of the DIKW Hierarchy. *Journal of Information Science*, Vol. 33, No. 2 (2007), s. 163–180; Zins, Chaim: Conceptual Approaches for Defining Data, Information, and Knowledge. *Journal of the American Society for Information Science and Technology*, Vol. 58, No. 4 (2007), s. 479–493.

[2] Sanastokeskus TSK: Kyberturvallisuuden sanasto TSK 52. Sanastokeskus TSK, Helsinki, 2018, s.29.

johdettu Venäjän kansallisen internetsegmentin hankkeen tavoitetilasta ja Venäjän valtion ominaispiirteistä. (Luku 3.3)

Kansallinen internetsegmentti: Kansallinen internetsegmentti on suljetun kansallisen verkon venäläinen käytännön ilmenemismuoto. Se koostuu valtion alueella sijaitsevasta ja sen suvereenin määräämisvallan alla olevasta Internetin infrastruktuurista ja palveluista sekä muista tietoverkoista- ja järjestelmistä. Se määrittelee valtion rajat kybertilassa. (Luku 3.3)

Konfliktin ennaltaehkäisy: Osana valtion turvallisuuspolitiikkaa potentiaalisen uhan neutralointi kaikilla käytettävissä olevilla toimilla niin, että suoraa aseellisen voiman käyttöä tai sillä uhkaamista ei tarvita. (Luku 2.2)

Konfliktin eskalaation hallinta: Käynnistyneen konfliktin intensiteetin säätely voimankäytöllä tai sillä uhkaaminen kybertilassa tai sen kautta, jonka tavoitteena on saada vastustaja lopettamaan voimankäyttö itselle hyödyllisellä ja poliittisten päämäärien tavoittelua palvelevalla tavalla sekä samalla estää tahaton ja vahingossa tapahtuva eskalaatio. (Luku 2.2)

Kyberdeterrenssi: Pyrkimys taivutella potentiaalinen vastustaja pidättäytymään voimankäytöstä kybertilassa, kybertilasta tai muussa tilassa uhkaamalla sietämättömällä rangaistuksella, kiistämällä potentiaaliset hyödyt tai muutoin vaikuttamalla vastustajan hyötykustannuslaskelmiin kybertilaan liittyvillä suorituskyvyillä. (Luku 2.2)

Kyberoperaatio: Kyberoperaatiot voidaan jakaa hyökkäyksellisiin, puolustuksellisiin ja kybervakoiluun. Kyberhyökkäys määritellään tässä työssä kybertoimintaympäristössä tai sen avulla tapahtuvaksi toiminnaksi, jolla pyritään vahingoittamaan eli häiritsemään, kiistämään, rapauttamaa tai tuhoamaan informaatiojärjestelmiä tai niissä olevan informaation luottamuksellisuutta, eheyttä tai saatavuutta. Kyberpuolustus on valtion ja yhteiskunnan kriittisten tietoverkkojen, tietojärjestelmien ja niiden sisältämän tiedon aktiivista ja passiivista suojaamista valtioiden voimankäyttöön liittyvältä vihamieliseltä vaikuttamiselta. Kybervakoilulla hankitaan tietoa tai mahdollistetaan tiedon hankkiminen, muttei pyritä aiheuttamaan välitöntä vahinkoa kohdejärjestelmille. (Luku 2.2)

Kyberstrategia: Kyberstrategia on kybervoiman jatkuvaa käytön suunnittelua, sen käyttöön valmistautumista ja sen käyttämistä sotilaallisin

ja ei-sotilaallisin keinoin kybertoimintaympäristössä valtion turvallisuuspäämäärien saavuttamiseksi. (Luku 2.2)

Kybertaistelutila: Sotilaallinen toimintaympäristö, joka voidaan jakaa kybertaistelukenttiin taktisten, operatiivisten ja strategisten tavoitteiden saavuttamiseksi. Jako noudattaa toiminnan muotoa, tavoitteita ja päämäärää, eikä ole ennalta säädetty. (Luku 2.1)

Kybertila: 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. (Luku 2.1)

Kybervoima: Valtion kyky vaikuttaa toisiin valtioihin kybertilassa tai sen kautta ja muokata ja kontrolloida kybertilaa omaksi edukseen preferenssiensä mukaan. (Luku 2.1)

Kybervoimaresurssit: Kybervoimaresurssit tai potentiaali ovat luonteeltaan pääasiassa teknologisia, tieteellisiä, taloudellisia, normatiivisia, doktrinaalisia, organisatorisia ja inhimillisiä (ammatillisia). Ne saavat luonteensa käyttötapansa, ympäristönsä ja tavoitteensa kautta. (Luku 2.1)

Länsi: ”Länsi” viittaa englanninkieliseen käsitteeseen ”*the West*.” Se tarkoittaa Amerikan Yhdysvaltoja ja sen poliittisia ja sotilaallisia liittolaisia, jotka vastustivat kommunistista Neuvostoliittoa ja sen liittolaisia kylmän sodan aikana 1940-luvun loppupuolelta vuoteen 1989/1991 asti ideologisista, taloudellisista ja sotilasstrategisista syistä. Kylmän sodan jälkeiseen aikakauteen liittyen Lännellä tai läntisellä tarkoitetaan Yhdysvaltoja, Kanadaa, Länsi-Eurooppaa erityisesti NATO ja Euroopan Unioni jäsenmaineen sekä Japania, Etelä-Koreaa, Australiaa ja Uutta-Seelantia. Länsi voidaan tulkita Yhdysvaltojen liittolaisjärjestelmänä, liberaalidemokraattisena arvoyhteisönä tai suhteessa määrätyn poliittisen yhteisön vihollisiin, joita ovat Venäjä, Kiina ja radikaali poliittinen islam. Se voidaan myös tulkita joukoksi valtioita, jotka jakavat määrätyn ymmärryksen sodan luonteesta ja sodankäyntitavan. Termillä viitataan myös akateemisiin piireihin, jotka

kirjoittavat englanniksi tieteellisissä journaaleissa, ja joita julkaistaan edellä mainituissa maissa.[3]

Rakenteellinen kyberasymmetria: Kybertilan ominaisuus, joka syntyy kahden tai useamman toimijan välille, kun kybertilan rakennetta ja sääntöjä muokataan niin, että yksi toimijoista saa epäsuhtaisen ja hyväksikäytettävän puolustuksellinen ja hyökkäyksellisen edun toisiin toimijoihin nähden. (Luku 2.4)

Rakenteellisen kyberasymmetrian sotilaallinen hyväksikäyttö: Pakottamisen ja raa'an voiman käyttö kybertilassa ja kyky aiheuttaa sellaista vaikutusta kybertilassa tai sen kautta, joka pakottaa vastustajan lopettamaan vastarinnan vastoin omaa tahtoaan tai kiistää vastaavan vaikutuksen omiin järjestelmiin konfliktissa tai sodassa. (Luku 2.2)

Strateginen taso: Valtion kansallisten turvallisuuspäämäärien tavoitteluun liittyvä valtiojohdon päätöksenteon taso. Sotilasstrateginen taso on mahdollisen tai aktuaalisen sodan päämäärien tavoitteluun liittyvä sotilasjohdon päätöksenteon taso. (Luku 1)

Strateginen vaikutus: Strateginen vaikutus muuttaa valtioiden toimintaympäristöä niin, että niiden turvallisuusjärjestelmien välinen voimasuhde muuttuu potentiaalisen tulevan konfliktin osalta. Strateginen vaikutus liittyy yhtäältä voimankäytön edellytysten muuttumiseen ja toisaalta voimankäytön päämäärän tavoittamiseen liittyvään muutokseen kohdejärjestelmässä strategisella tasolla. (Luku 2.2)

Suljettu kansallinen verkko: Valtion kontrolloima osa kybertilaa, joka voidaan teknisesti kytkeä irti globaalista Internetistä, mutta kykenee silti toimimaan kansallisten kriittisten palvelujen osalta normaalisti. Sen vastakohtana on avoin kansallinen verkko, joka ei ole valtion suoraan kontrolloima, eikä sitä voida lähtökohtaisesti kytkeä irti globaalista kybertilasta ilman erityisiä valmisteluja tai yhteiskunnan kriittisen toimintojen ja talouselämän vakavia häiriöitä. (Luku 2.4)

---

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

1 Johdanto

"The best kind of fortresses are those that forbid access to one's country while at the same time giving an opportunity to attack the enemy in his own territory."
M. Maigret: Treatise on Preserving the Security of States by Means of Fortresses, Paris, 1725[4]

"Informaatiotilasta on tullut yksi sotatoimien näyttämöistä."
Venäjän puolustusministeri Sergei Šoigu, 25.3.2020[5]

Venäjän federaatio kehittää kansallista internetsegmenttiä (*rossijskij segment seti Interneta*)[6], joka voidaan irrottaa globaalista Internetistä määrättyjen uhkien realisoituessa.[7] Projekti on sisällytetty vuonna 2017 hyväksyttyyn Venäjän Digitaalisen talouden kansalliseen ohjelmaan, jonka tavoitteena on saavuttaa niin kutsuttu digitaalinen suvereniteetti vuoteen 2024 mennessä.[8] Ohjelmaa toimeenpannaan pääsääntöisesti lainsäädäntöön perustuvan kontrollin ja valtionyhtiöiden hankintojen avulla, joiden tuloksena kansalaisyhteiskunnan ja liike-elämän kehittämä Venäjän Internet on siirtymässä yhä tiukemman valtion kontrollin alle.[9] Venäjän kansallisella internetsegmentillä voi toteutuessaan olla merkittäviä poliittisia, taloudellisia ja kulttuurisia vaikutuksia. Strategian

---

[4] Lainattu ja viitattu teoksessa Guerlac, H.: Vauban: The Impact of Science of War. Teoksessa Paret, Peter (ed.): *Makers of Modern Strategy from Machiavelli to the Nuclear Age*. Clarendon Press, Oxford, 1990, s. 64–90, 87.

[5] 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.

[6] Tässä työssä noudatetaan venäläisten termien ja erisnimien translitteroinnin osalta: Suomen Standardisoimisliitto, Kyrillisten kirjainten translitterointi. Slaavilaiset kielet. SFS 4900 -standardi, 2. painos, vahvistettu 17. elokuuta 1998. Pääsääntöisesti venäläiset termit ja erisnimet ilmaistaan viitteissä kyrillisessä kirjoitusasussa lähdeaineiston jäljittämisen helpottamiseksi.

[7] ФЗ-90: Федеральный закон от 01.05.2019 № 90-ФЗ *"О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации"*. [http://www.consultant.ru/document/cons_doc_LAW_323815/], luettu 8.5.2019.

[8] РП-1632: Распоряжение Правительства РФ от 28.07.2017 N 1632-р *"Об утверждении программы "Цифровая экономика Российской Федерации"*. [http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf], luettu 23.01.2018.

[9] Kukkola, Juha: *Civilian and Military Information Infrastructure and the Control of the Russian Segment of Internet*. Esitetty The International Conference on Military Communications and Information Systems (ICMCIS) Varsova, Puola, Toukokuu 22.-23., 2018.

tutkimuksen näkökulmasta kansallisen internetsegmentin rakentaminen muodostaa mielenkiintoisen tutkimuskohteen. Sen sotilasstrategiset vaikutukset ovat vielä pitkälti tutkimatta ja tuntemattomia.

1.1 Aikaisempi tutkimus

Venäjän hanke kansallisen internetsegmentin rakentamiseksi on yhteydessä kybertilan fragmentaatioon, josta on käytetty myös termejä balkanisaatio tai sirpaloituminen. Fragmentaatiota on tutkittu kybertilan hallinnan (*governance*) piirissä on 2010-luvulta alkaen. Laura DeNardisin mukaan hallinnalla tarkoitetaan ”niiden teknologioiden suunnittelua ja hallinnointia, jotka ovat välttämättömiä Internetin toiminnalle sekä näihin teknologioihin liittyvän politiikan [*policy*]” toteuttamista.[10] Tutkimuksen kohteena ovat olleet sellaiset asiat kuten ei-valtiollisten ja valtiollisten toimijoiden valtasuhteet, valtioiden pyrkimykset säännellä Internettiä, standardeihin liittyvät valtapoliittiset kysymykset sekä Internetin fragmentaatio.[11] Fragmentaatiokeskustelussa näkökulmat ovat olleet pääosin poliittisia, ihmisoikeudellisia, teknologisia tai hallinnollisia.[12] Venäjän tapauksessa Internetin kontrolli on nähty poliittisena kysymyksenä.[13] Esimerkiksi Andrei Soldatov ja Irina Borogan ovat

---

[10] DeNardis, Laura: *The Global War for Internet Governance*. Yale University Press, New Haven, 2014, s. 6.

[11] DeNardis (2014); Mueller, Milton: *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace.* Polity, Cambridge, UK, 2017; Musiani, Francesca, Cogburn, Derrick L., DeNardis, Laura & Levinson, Nanette S. (Eds.): *The Turn to Infrastructure in Internet Governance*. Palgrave Macmillan, New York, 2016; Choucri, Nazli: *Cyberpolitics in International Relations*. The MIT Press, Cambridge, 2012.

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

[13] Freedom House: *Freedom on the Net 2017: Russia, 2017*. [https://freedomhouse.org/report/freedom-net/2017/russia], luettu 11.1.2018; Роскомсвобода: «Китаизация» Рунета входит в активную фазу и начнётся с точек обмена трафиком. *Роскомсвобода*, 18.8.2017. [https://roskomsvoboda.org/31224/], luettu 17.5.2019; Агора: *Свобода интернета 2018: делегирование репрессий.* [https://meduza.io/static/0001/Свобода-интернета-2018.pdf], luettu 1.3.2019; Агора: *Свобода интернета 2019: план «Крепость».* [https://2019.runet.report/assets/files/Internet_Freedom%202019_The_Fortress.pdf], luettu 17.3.2020; Deibert, Ronald, Palfrey, John, Rohozinski, Rafal & Zittrain, Jonathan (eds.): *Access Controlled The Shaping of Power, Rights, and Rule in Cyberspace*. The MIT Press, Cambridge, Massachusetts, 2010; Musiani et al. (2016); Nocetti, Julian: Contest and conquest: Russia and Global Internet Governance. *International Affairs*, Vol.

väittäneet Venäjän valtion toiminnan heijasteleva sisäpoliittisia tekijöitä ja ”KGB-mentaliteettia.”[14]

Venäjän hanketta internetsegmentin rakentamiseksi on pääsääntöisesti kommentoitu mediassa, mutta akateeminen tutkimus on lisääntymässä. Julian Nocetti on liittänyt hankkeen suvereenisuuden rakentamiseen kyberavaruudessa.[15] Myös Margarita Jaitner ja Jari Rantapelkonen ovat väittäneet Venäjän toiminnan kybertilassa liittyvän valtiosuvereniteetin rakentamiseen ja ylläpitämiseen.[16] Carolina Vendil Pallin on tarkastellut sitä, kuinka Venäjän valtion on hankkinut suoraan ja epäsuoraan hallintaansa maan Internet-yhtiöt voidakseen ulottaa autoritaarisen hallinnan kybertilaan. Hän on myös tarkastellut Internetin hallintaan liittyviä valtion ohjelmia.[17] Katri Pynnöniemikin on tutkinut Venäjän kriittisen infrastruktuurin (objektien) sääntelyyn liittyvää kehitystä.[18] Eneken Tikk ja Mika Kerttunen ovat taas lähestyneet Venäjän toimintaa kansainvälisten normien rakentamisesta käsin.[19] Eva Claessen on vertaillut Venäjän kansallisen Internetsegmentin suhdetta Euroopan unionin hankkeisiin ja Venäjän digitalisaation on herättänyt laajempaakin monitieteellistä kiinnostusta.[20] Sotatieteiden ulkopuolella Venäjän kansallinen internetsegmentti onkin alkanut kiinnostaa niin poliittisena, sosiaalisena kuin kulttuurisena ilmiönä.

91, No. 1 (2015), s. 111–130; Vendil Pallin, Carolina: Internet Control Through Ownership: The Case of Russia. *Post-Soviet Affairs*, Vol. 33, No. 1 (2017), s. 16–33.

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

[15] Nocetti (2015).

[16] Jaitner, Margarita & Rantapelkonen, Jari: Russian Struggle for Sovereignty in Cyberspace. *Tiede ja Ase*, Vol. 71 (2013), s. 64–89, 83.

[17] Vendil Pallin (2017); Vendil Pallin, Carolina: Russian information security and warfare. Teoksessa Kanet, Roger E.: *Routledge Handbook of Russian Security*. Routledge, London and New York, 2019, s. 203–213.

[18] Pynnöniemi, Katri (toim.): *Russia´s Critical Infrastructures - Vulnerabilities and Possibilities*. FIIA Report 35, Helsinki, 2012.

[19] Tikk, Eneken & Kerttunen, Mika: *Parabasis. Cyber-diplomacy in Stalemate*. Norwegian Institute of International Affairs, 2018. [https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2569401/NUPI_Report_5_18_Tikk_Kerttunen.pdf?sequence=1&isAllowed=y], luettu 6.5.2019.

[20] Claessen, Eva: Reshaping the Internet – The Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU. *Journal of Cyber Policy*, Vol.5, No.1 (2020), s. 140–157; Gritsenko, Daria, Wijermars, Mariëlle & Kopotev, Mikhail (Eds.): *The Palgrave Handbook of Digital Russia Studies*. Palgrave Macmillan, London, 2021.

Poikkeuksena edellä mainittuun fragmentaatiokeskusteluun Chris Demchak ja Peter Dombrovski ovat lähestyneet fragmentaatiota sotilaallisesta näkökulmasta ja kutsuneet sen lopputulosta ”kyberoituneeksi westfaaliseksi aikakaudeksi” (*Cybered Westpahalian Age*). Heidän mukaansa valtiot reagoivat kybertilasta kumpuaviin uhkiin rakentamalla valtioiden maantieteellisiä rajoja noudattavat rajat kybertilaan sekä perustamalla sotilaallisia suorituskykyjä siellä toimimiseksi.[21] Demchak ja Dombrovski eivät kuitenkaan ole tarkastelleet sitä, miten tämä kehitys käytännössä etenisi. Allison Lawlor Russell on sen sijaan tarkastellut fragmentaatiota toiminnan eli saarrostuksen ja toiminnan vapauden kiistämisen kautta. Hänen analyysinsa tarkastelee aihetta kuitenkin lähinnä hyökkääjän eli eristäjän näkökulmasta.[22]

Aivan viime aikoina läntisessä tutkimuskentässä on herätty ajatukseen siitä, että Venäjän internetsegmenttihankkeella voi olla laajempia sotilasstrategisia merkityksiä. Esimerkiksi Rod Thornton ja Marina Miron ovat väittäneet, että Venäjä pyrkii kehittämään kyberresilienssiään Lännen tekoälyllä vahvistettuja kyberhyökkäyksiä vastaan.[23] Kiinan ”mahtavan palomuurin” sotilaallista merkitystä on myös tarkasteltu, mutta analyysi on keskittynyt pikemminkin ilmiöön kuin sen merkityksiin ja vaikutuksiin.[24] Globaalin kybertilan fragmentaation tarkastelu strategisella tasolla on jäänyt tutkimuksen marginaaliin. Strategisella tasolla tarkoitetaan valtion kansallisten turvallisuuspäämäärien tavoitteluun liittyvää valtiojohdon päätöksenteon tasoa ja sotilasstrategisella tasolla mahdollisen tai aktuaalisen sodan päämäärien tavoitteluun liittyvää sotilasjohdon päätöksenteon tasoa.

---

[21] Demchak, Chris & Dombrowski, Peter: Rise of the Cybered Westphalian Age. *Strategic Studies Quarterly*, Vol. 5, No. 1 (Spring 2011), s. 32–61; Demchak, C. & Dombrowski, P.: Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Affairs*, Volume International Engagement on Cyber III, 2013, s. 29–38.

[22] Russell, A. L.: *Cyber Blockades*. Georgetown University Press, Washington DC, 2014; Lawlor Russell, Alison: Strategic Anti-Access/Area Denial in Cyberspace. Teoksessa Maybaum, M., Osula, A. & Lindström, L. (Eds.): *7th International Conference on Cyber Conflict: Architectures in Cyberspace*. NATO CCD COE Publications, Tallinn, 2015, s. 153–168.

[23] Thornton, Rod & Miron, Marina: Towards the ‘Third Revolution in Military Affairs’. *The RUSI Journal*, Vol. 165, No. 3 (2020), s. 12–21.

[24] Inkster, Nigel: *China´s Cyber Power*. IISS. Routledge, New York, 2016; Lindsay, Jon R., Cheung, Tai Ming & Reveron, Derek S.: *China and Cybersecurity. Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press, Oxford, 2015; Kolton, Michael: Interpreting China’s Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence. *The Cyber Defense Review*, Vol. 2, No. 1 (Winter 2017), s. 119–154.

Kybersodankäyntiin liittyvä aikaisempi julkinen strategisen tason tutkimus keskittyy pääsääntöisesti kybertapahtumien sotilaallisen luonteen arviointiin, hyökkäyksellisten operaatioiden tarkasteluun tai hyökkäyksen ja puolustuksen välisen suhteen arviointiin.[25] Suomalainen julkinen tutkimus rajoittuu pitkälti Puolustusvoimien piirissä toimitettuihin julkaisuihin, joissa päätavoitteena on ollut kybersodankäynnin ilmiön kansallinen ymmärtäminen ja käsitteellistäminen tai laajemman informaatiosodankäynnin ilmiön tarkastelu.[26] Kybertilan rakenteen muuttumista tai muokkaamista sotilasstrategisesta näkökulmasta ei ole tarkasteltu aiemmassa läntisessä tutkimuksessa lukuun ottamatta Puolustusvoimien Tutkimuslaitoksen (PVTUTKL) tutkimuksia. Näihin palataan alempana. Itse asiassa kybersodankäynnin ja mahdollisen kyberkonfliktin luonne ja olemassaolo ovat kiistanalaisia käsitteitä.

---

[25] Katso tarkemmin kansainvälisestä kybersodankäynnin tutkimuksesta luku 2.

[26] Saarelainen, Jorma: *Näkemyksiä Venäjän Informaatiosodankäynnistä*. Maanpuolustuskorkeakoulu Taktiikan laitos, Julkaisusarja 1 Taktiikan tutkimuksia, N:o1/1999. Hakapaino, Helsinki, 1999; Huhtinen, Aki Mauri & Rantapelkonen, Jari: *Imagewars: Beyond the mask of information warfare*. Gummerus, Saarijärvi, 2002; Piiroinen, Mika (toim.): *Verkkotaistelu 2020: Taustatutkimus Maavoimien Taistelun kuvat 2020 tutkimukseen*. Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2, No. 2/2003, Edita Prima Oy, Helsinki, 2003; Candolin, Catharina: *Securing Military Decision Making in a Netwok-Centric Enviroment*. Helsingin Teknillinen korkeakoulu, väitöskirja, Picaset Oy, Helsinki, 2005; Berger, Heidi: *Venäjän informaatio-psykologinen sodankäyntitapa terrorismin torjunnassa ja viiden päivän sodassa*. Maanpuolustuskorkeakoulu, Johtamisen ja sotilaspedagokiikan laitos, Julkaisusarja 1. Nro 5/2010, Edita Prima Oy, Helsinki, 2010; Sirén, Torsti (toim.): *Strateginen kommunikaatio ja informaatio-operaatiot 2030*. Maanpuolustuskorkeakoulu, Johtamisen ja sotilaspedagogiikan laitos, Juvenes Print Oy, Helsinki, 2011; Jantunen, Saara: *Strategic Communication: practise, communication and dissonance*. Maanpuolustuskorkeakoulu, Johtamisen ja sotilaspedagogiikan laitos, Julkaisusarja 1, No. 11, Juvenes, Helsinki, 2013; Kosola, Jyri & Solante, Tero: *Digitaalinen taistelukenttä: Informaatioajan sotakoneen tekniikka*. Maanpuolustuskorkeakoulu, Sotatekniikan laitos, Julkaisusarja 4, No. 35, Helsinki, 2013; Kuusisto, Tuija (toim.): *Kybertaistelu 2020*. Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2 No. 1/2014, Juvenes, Tampere, 2014; Rantapelkonen, Jari & Salminen Mirva (Eds.): *The Fog of Cyber Defence*. Maanpuolustuskorkeakoulu, Johtamisen ja pedagogiikan laitos, Julkaisusarja 2, No: 10, Juvenes Print Oy, Tampere, 2013; Limnéll, Jarno: Kyber rantautui Suomeen. *Aalto-yliopiston julkaisusarja Tiede + Teknologia* 12/2014; Lehto, Martti: *Kybermaailman ilmiöitä ja määrittelyjä*. Jyväskylän yliopisto, Informaatioteknologian tiedekunta, 2019. [https://www.jyu.fi/it/fi/hae-opiskelemaan/hakukohteet/kyberturvallisuuden-seka-turvallisuus-ja-strateginen-analyysi-maisteriohjelmien-yhteisvalinta/kybermaailma_v10-0.pdf], luettu 16.3.2020; Laari, Tommi (toim.): *#kyberpuolustus. Kyberkäsikirja Puolustusvoimien henkilöstölle*. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 3: Työpapereita nro. 12, Helsinki 2019.

Samoin perinteisen sodankäynnin käsitteiden soveltaminen kybertilaan.[27] Suurvaltojen nykyisten puolustusdoktriinien valossa on kuitenkin selvää, että kybertilaa pidetään sodankäynnin toimintaympäristönä.[28]

Venäjän hyökkäyksellisiä kyberoperaatioita on viime vuosina tutkittu paljon.[29] Myös Venäjän näkemykset informaatiosodankäynnistä ovat olleet laajan huomion kohteena. Alan kiistämätön auktoriteetti on Timothy Thomas, joka on kirjoittanut aiheesta 1990-luvulta alkaen.[30] Myös mm. Mary Fitzgerald, Jakob W. Kipp, Roger N. Dermott, Dima Adamsky, Kier Giles, Oscar Jonsson ja Benjamin Jensen, Brandon Valeriano sekä Ryan Maness ovat kirjoittaneet aiheesta.[31] Venäjän puolustuksellinen

---

[27] Rid, Thomas: *Cyber War Will Not Take Place*. Oxford University Press, Oxford, 2017; Stone, John: Cyber War Will Take Place! *Journal of Strategic Studies*, Vol. 36, No. 1 (2013), s. 101–108; Libicki, Martin C.: *Cyberspace in Peace and War*. Naval Institute Press, Annapolis, Maryland, 2016; Schmitt, Michael N. (ed.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, Cambridge, 2017, s. 452–453.

[28] The United States Department of Defense (U.S. DoD): *Cyber Strategy – Summary, 2018.* [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF], luettu 5.5.2020; The State Council Information Office of the People's Republic of China: *China's National Defense in the New Era*. Foreign Languages Press Co. Ltd., Beijing, 2019; Указ-646: Указ Президента РФ от 05.12.2016 N 646 *"Об утверждении Доктрины информационной безопасности Российской Федерации*". [http://www.consultant.ru/document/cons_doc_LAW_208191/], luettu 5.5.2020.

[29] Suhteellisen tuore eri tutkimuksia ja raportteja kokoava artikkeli ks. Lilly, Bilyana & Cheravitch, Joe: The Past, Present, and Future of Russia's Cyber Strategy and Forces. Teoksessa 2020 *12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade*. T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, G. Visky (Eds.) NATO CCDCOE Publications, Tallinn, 2020, s. 129–155.

[30] Thomasin ensimmäinen aiheeseen liittyvä artikkeli on vuodelta 1996 (Thomas, Timothy L.: Russian Views on Information-Based Warfare. *Airpower Journal* – Special Edition 1996, s. 26–35.)

[31] Adamsky, Dmitry (Dima): From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture. *Journal of Strategic Studies*, Vol. 41, No. 1-2 (2018), s. 33–60; Giles, Keir: *Handbook of Russian Information Warfare*. Fellowship monograph 9. Rome: NATO Defence College, 2016; Fitzgerald, Mary: Russian Views on IW, EW, and Command and Control: Implications for the 21st Century. *Command & Control Research & Technology Symposium, 1999. U.S. Naval War College, Rhode Island. June 29 - July 1, 1999.* [http://www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/089fitzg.pdf], luettu 5.8.2018; McDermott, Roger N.: *Russian Perspective on Network-Centric Warfare: The Key Aim of Serdyukov's Reform*. FMSO, Fort Leavenworth, Kansas, 2011; Kipp, Jacob W.: 'Smart' Defense From New Threats: Future War From a Russian Perspective: Back to the Future After the War on Terror. *The Journal of Slavic Military Studies*, Vol. 27, No. 1 (2014), s. 36–62; Jonsson, Oscar: *The Understanding of War. Blurring the Lines between War and Peace*. Georgetown University Press, Washington, D.C., 2019; Jensen,

kyberstrategia on kiinnostanut harvoja. Ilmari Susiluoto, Slava Gerovich ja Benjamin Peters ovat tarkastelleet historiantutkimuksen keinoin Venäjän Internetin kehitystä (tai kehittymättömyyttä). Heidän tutkimuksensa kuuluvat kuitenkin enemmän historian ja kulttuurin tutkimuksen kuin sotatieteiden alaan.[32] Venäjän nykyiset teknologiahankkeet ovat myös herättäneet jonkin verran mielenkiintoa. Näitä tarkasteluja tosin hallitsee määrätty potentiaalisen vihollisen suorituskykyjen arviointiin ja raportoitiin perustuva näkökulma.[33] Yleisesti voidaan todeta, että pääosaa Venäjän sotilaalliseen kybertoimintaan liittyvää tutkimusta on ohjannut Venäjän toimien tarkastelu läntisestä näkökulmasta, jossa Venäjä nimetään suoraan viholliseksi (*adversary*).[34]

Poikkeuksen muodostaa Martti Kari, joka on väitöskirjassaan tutkinut Venäjän kybertoimintaympäristöön liittyviä strategiseen kulttuuriin liittyviä uhkakuvia ja niiden vaikutusta Venäjän toimintaan.[35] Maija Turunen ja Martti Kari ovat myös tarkastelleet Venäjän ”aktiivista kyberdeterrenssiä”. Heidän mukaansa se perustuu puolustettavan kybertilan luomiseen, hyökkäyksellisten kykyjen kehittämiseen sekä käyttämiseen viestimistarkoituksessa sekä muiden maiden sitouttamiseen omaan ratkaisuunsa.[36] Samoja havaintoja ovat jo 2017 esittäneet Kukkola, Ristolainen ja Nikkarila.[37] Turunen ja Kari perustelevat väitteitään Venäjän strategisen kulttuurin sisältämillä uhkakuvilla, haavoittuvuuden tunteella,

---

Benjamin, Valeriano, Brandon & Maness, Ryan: Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies*, Vol. 42, No. 2 (2019), s. 212–234.

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

[33] Dear, Keith: Will Russia Rule the World Through AI? *The RUSI Journal*, Vol. 164, No. 5-6 (2019), s. 36–60; Thornton & Miron (2020).

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

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

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

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

narratiivilla Venäjästä ”piiritettynä linnakkeena” sekä käsityksellä jatkuvasta valtioiden välisestä sotatilasta.

Olen omassa väitöskirjassani *Digital Soviet Union: The Russian national segment of the Internet as a closed national network shaped by strategic cultural ideas* esittänyt neoklassiseen realismiin ja strategiseen kulttuuriin perustuvan näkökulman Venäjän kyberstrategian taustoihin.[38] Uhkakuvien sijaan työ tarkastelee usean historiallisesti pysyvän idean vaikutusta Neuvostoliiton ja Venäjän näkemykseen voimasta ja sen käytöstä informaatio- ja kybertoimintaympäristössä. Kybersodankäynnin tutkimuksen näkökulmasta väitöskirjassa on puutteensa. Siinä rakennetaan pohja venäläisen kyber- ja informaatiotilaan liittyvän sotilasstrategisen ajattelun ymmärtämiselle ja kuvataan Venäjän kansallinen internetsegmentti perinpohjaisesti. Siinä ei kuitenkaan tarjota ymmärrystä tutkittavan ilmiön laajemmista, teoreettisista ja käytännöllisistä vaikutuksista.

PVTUTKL:n julkinen tutkimusprojekti sen sijaan on tarkastellut Venäjän hankkeen mahdollisia seurauksia. Tutkimuksessa on osoitettu, että Venäjän kansallinen internetsegmentti ei ole vain poliittisen kontrollin tai valtiojohtoisen talouspolitiikan väline tai uhkakuvien tuottama reaktio.[39] Juha Kukkolan, Mari Ristolaisen ja Juha-Pekka Nikkarilan mukaan suljettua kansallista verkkoa, eli valtion kontrolloimaa osaa Internetistä, joka voidaan kytkeä teknisesti irti globaalista Internetistä, voidaan käyttää strategisen edun saavuttamiseksi kybertilassa. Tämä tarkoittaa sitä, että valtiot kykenevät käyttämään kybervoimaa muokatakseen ja kontrolloidakseen muuttuvaa, teknologiaperusteista ja ihmisen luomaa kybertilaa haluamaansa suuntaan muuttaen sen rakennetta tavalla, joka tuottaa rakenteellista kyberasymmetriaa. Yksinkertaistetusti rakenteellinen kyberasymmetria on kybertilan rakenteesta johtuva epäsuhtainen etu kahden tai useamman osapuolen välillä. Kukkolan, Ristolaisen ja Nikkarilan mukaan Venäjä voi siis muokata strategista kybertaistelutilaa jo

[38] Kukkola, Juha: *Digital Soviet Union. The Russian national segment of Internet as a closed national network shaped by strategic cultural ideas*. National Defence University Series 1: Research Publications No. 40. National Defence University, Helsinki, 2020a.
[39] Kukkola, Ristolainen & Nikkarila (2017); Kukkola, Juha, Ristolainen, Mari & Nikkarila, Juha-Pekka: *Game Player. Facing the structural transformation of cyberspace*. Finnish Defence Research Agency Publications 11. Finnish Defence Research Agency, Riihimäki, 2019.

rauhan aikana saavuttaakseen merkittävän edun konfliktin alkuvaiheessa ja sen aikana.[40]

Asymmetrian käsitettä on tutkittu varsin laajasti länsimaisessa sotatieteellisessä kirjallisuudessa, mutta vähemmän toimintatilan strategisen tason muokkaamisen näkökulmasta.[41] Havaintoja kansallisten verkkojen tai suorituskykyjen vaikutuksista kybertilaan ei ole kehitetty teoreettiselle tasolle.[42] Rakenteellisen kyberasymmetrian luonnetta ja sen strategisia vaikutuksia ei ole riittävästi tutkittu. Strategisilla vaikutuksilla tarkoitetaan tässä suppeasti sellaisia tarkoituksellisia muutoksia sotilaallisen voiman käytön ehdoissa, joilla on suora suhde valtion poliittisten päämäärien tavoitteluun.[43] Voimankäytön eri muodot valtioiden välisten suhteiden eri vaiheissa vaativat lisää tutkimusta.[44] Etenkin kyky estää sotilaallisen konfliktin syntyminen, deterrenssin toimivuus, eskaloituvan konfliktin hallinta ja kyky hyväksikäyttää rakenteellista asymmetriaa sotilaallisesti konfliktin aikana muodostavat kiinnostavan tarkastelukohteen. Niitä on aikaisemmin tarkasteltu kybertoimintaympäristöön liittyen, muttei rakenteellisen kyberasymmetrian kehyksessä.[45] Ilmiöt muodostavat loogisen jatkumon

---

[40] Ks. Kukkola, Ristolainen & Nikkarila (2017); Kukkola, Ristolainen & Nikkarila (2019).
[41] Ks. Luku 2.3.
[42] Betz, David & Stevens, Tim: Cyberspace and the State: Toward a Strategy for Cyberpower. *Adelphi Series* Vol. 51, No. 424 (2011), s. 93; Libicki (2016), s. 201–209.
[43] Tämä määritelmä poikkeaa yleisesti hyväksytyistä määritelmistä. Ks. Gray, Colin S.: *Modern Strategy*. Oxford University Press, Oxford, 1999, s. 296; Strachan, Hew: *The Direction of War: Contemporary Strategy in Historical Perspective*. Cambridge University Press, New York, 2013, s. 191–192; Valeriano, Brandon & Maness, Ryan C.: *Cyber War versus Cyber Realities Cyber Conflict in the International System*. Oxford University Press, New York, 2015, s. 60.
[44] Voimankäytöstä ks. Esim. Schelling, T. C.: *Arms and Influence*. Yale University Press, New Haven, 2008.
[45] Yleisesti kybertilan osalta näitä ilmiöitä ovat yleisesti tarkastelleet mm. Nye, Joseph: Deterrence and Dissuasion in Cyberspace. *International Security*, Vol. 41, No. 3 (2016/2017), s. 44–71; Harknett, Richard J. & Nye, Joseph S. Jr.: Correspondence – Is Deterrence Possible in Cyberspace. *International Security*, Vol. 42, No. 2 (2017), s. 196–199; Cimbala, Stephen J.: Nuclear Deterrence and Cyber Warfare: Coexistence or Competition? *Defense & Security Analysis*, Vol. 33, No. 3 (2017), s. 193–208; Chen, Jim: Cyberdeterrence by Engagement and Surprise. *PRIMS*, Vol. 7, No. 2 (2017), s. 100–107; Libicki, M. C.: *Conquest in Cyberspace. National Security and Information Warfare*. Cambridge University Press, Cambridge, 2007; Rivera, J.: Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk. Teoksessa *7th International Conference on Cyber Conflict: Architectures in Cyberspace*. M. Maybaum, O. &. A.-M. & L. Lindström (eds.) NATO CCD COE Publications, Tallinn, 2015, s. 7–24; Rid, T. & Buchanan, B.: Attributing Cyber Attacks. *Journal of Strategic Studies*, Vol. 35, No. 1

suhteessa valtioiden välisiin suhteisiin rauhasta sotaan. Lisäksi niiden kautta voidaan tarkastella sotilaallisen ja ei-sotilaallisen voimankäytön suhteen kehittymistä valtiosuhteiden jatkumolla.[46] Koska kybertila tulee tavalla tai toisella olemaan osa tämän päivän ja tulevaisuuden valtioiden välisiä konflikteja, on oleellista tarkastella toimintaympäristön muutoksen vaikutusta voimankäyttöön. Lisäksi uhkien ennalta ehkäisy, deterrenssi, konfliktin hallinta ja sotilaallisen ja ei-sotilaallisen voiman käyttö muodostavat luonnollisen jatkumon niin läntisessä kuin venäläisessä ajattelussa tarkasteltaessa valtion sotilaspoliittisia päämääriä.[47]

Aikaisemmassa PVTUTKL:n tutkimuksessa kyberasymmetrian syntymistä on tarkasteltu vertaamalla tilannetietoisuutta (*situation awareness*), päätöksentekoa (*decision-making*) ja toiminnan vapautta (*freedom of action*) hyökkäyksellisessä ja puolustuksellisessa toiminnassa verkkonsa sulkevan (*closed network nation*) ja auki pitävän valtion (*open network nation*) välillä.[48] Analyysi perustui hyökkäysvektoreiden

---

(2015), s. 4–37; Gartzke, Erik & Lindsay, John: *Cybersecurity and Cross-Domain Deterrence: The Consequences of Complexity* [http://deterrence.ucsd.edu/_files/LindsayGartzke_ConsequencesofComplexity_Draft.pdf], luettu 16.8.2018; Stevens, Tim: A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy*, Vol. 33, No. 1 (2012), s. 148–170; Forrest E. Morgan, Karl P. Mueller, Evan S. Medeiros, Kevin L. Pollpeter & Roger Cliff: *Dangerous Thresholds: Managing Escalation in the 21st Century*. RAND, Santa Monica, 2008; Maness, R. C. & Valeriano, B. *Conflict in Cyber Space: Theoretical, strategic and legal perspectives*. Routledge, New York, 2016; Valeriano, Brandon, Jensen, Benjamin & Maness, Ryan C.: *Cyber Strategy: The Evolving Chracter of Power and Coercion*. Oxford University Press, New York, 2018; Kello, Lucas: The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, Vol. 38, No. 2 (Fall 2013), s. 7–40; Maurer, Tim: *Cyber Mercenaries. The State, Hackers, and Power*. Cambridge University Press, Cambridge, 2018; Rattray, Gregory J.: *Strategic Warfare in Cyberspace*. MIT Press, Cambridge, 2001; Geers, Kenneth: The Cyber Threat to National Critical Infrastructures: Beyond Theory. *Information Security Journal*: A Global Perspective, Vol. 18, No. 1 (2009), s. 1–7; Clarke, R. A. & Knake, R. K.: *Cyber War: The Next Threat to National Security and What to Do About It*. Harper Collins, New York, 2010; Liff, Adam: Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*, Vol. 35, No. 3 (2012) s. 401–428.

[46] Ks. Luku 2.2 näistä käsitteistä tarkemmin.

[47] Forsström, Pentti: *Venäjän sotilasstrategia muutoksessa: tulkintoja Venäjän sotilasstrategian perusteiden kehityksestä Neuvostoliiton hajoamisen jälkeen*. Akateeminen väitöskirja, Maanpuolustuskorkeakoulu, Julkaisusarja 1 Nro 32, Helsinki, 2019; Kukkola (2020a); Kofman, Michael, Fink, Anya & Edmonds, Jeffrey: *Russian Strategy for Escalation Management: Evolution of Key Concepts*. CNA, Washington, D. C., 2020.

[48] Ks. käsitteistä ja analyysistä luku 2.5.

tarkasteluun. Suljettuja ja avoimia verkkoja tulisi kuitenkin tarkastella ominaisuuksien erojen, eikä pelkästään hyökkäysvektoreiden kautta. Lisäksi analyysissä käytetyt käsitteet edellyttävät tarkentamista ja jatkotutkimusta. Olen väitöskirjassani esittänyt, että Venäjän kansallista internetsegmenttiä, teoreettisen suljetun kansallisen verkon ilmentymänä, voidaan tarkastella kansallisena informaatioturvallisuuden ja -puolustuksen järjestelmänä.[49] Esittämässäni mallissa kansallinen segmentti jaetaan osajärjestelmiin, joiden toimintaa tarkastellaan valtioiden välisten suhteiden eri vaiheissa erilaisten uhkakuvien ilmetessä. Jaottelu mahdollistaa suljetun kansallisen verkon toiminnan tarkastelun käytännössä ja sen vertaamisen avoimiin kansallisiin verkkoihin. Malli perustuu venäläiseen ajatteluun sellaisena kuin se on tulkittu venäläisen strategisen kulttuurin ideoiden kautta. Mallilla syvennetään tässä työssä ymmärrystä kansallisten verkkojen rakenteesta ja toiminnasta.

Koska aiemmat tutkimukset ovat olleet joko varsin teoreettisia ja uutta ilmiötä kuvaavia ja toisaalta keskittyneet Venäjän strategiseen ajatteluun, politiikkaan ja teknologisiin ratkaisuihin, on kansallisten internetsegmenttien strategisten vaikutusten tutkiminen vasta alussa. Tarvitaan syvempää tapaustutkimusta, käsitteiden ja menetelmien kehittämistä kansallisten segmenttien luonteen ja vaikutusten tarkastelemiseksi, mikäli aikaisempien tutkimusten esittämiä teoreettisia oletuksia halutaan todentaa ja varautua niiden synnyttämiin sotilasstrategisiin uhkiin ja mahdollisuuksiin kybertoimintaympäristössä. Tämä työ rakentaa siltaa aikaisempien tutkimusten välille tulevaa tutkimusta varten.

1.2 Tutkimusongelma ja -kysymykset

Tämän tutkimuksen tavoitteena on kehittää käsite- ja teoriapohjaa rakenteellisen kyberasymmetrian tutkimiseksi ja tarkastella Venäjän kansallisen internetsegmentin strategisia vaikutuksia. Tämä on tärkeää, sillä kybertila on yksi sodankäynnin ulottuvuuksista, joiden läpi tai jonne voimaa voidaan suunnata poliittisten päämäärien saavuttamiseksi. Menetelmällisesti työ on tapaustutkimus, joka perustuu teoriasidonnaiseen ja käsitepohjaiseen ymmärtämiseen pyrkivään laadulliseen analyysiin.[50]

[49] Kukkola (2020a).
[50] Ks. Hollis, Martin and Smith, Steve: *Explaining and Understanding International Relations*. Clarendon Press, Oxford, 1990; Lamont, Christopher: *Research Methods in International Relations*. SAGE Publications Ltd., London, 2015.

Työ perustuu aikaisempaan tutkimukseen, väitöskirjaani *Digital Soviet Union* ja PVTUTKL:n julkiseen tutkimukseen, kehittää sitä edelleen ja avaa uusia polkuja. Tutkimuksessa täydennän PVTUTKL:n tutkimusten kyberasymmetrian analyysiä resilienssillä, joka ilmentää kansallisten verkkojen passiivista puolustuskykyä. Edelleen korvaan tilannetietoisuuden ja päätöksenteon yhteisellä tilannekuvalla ja johtamisella, koska edellisten analyysi strategisella tasolla on mahdotonta ilman päätöksentekijöiden ajatusmaailman tuntemusta. Olen valinnut toiminnan vapauden, yhteisen tilannekuvan, johtamisen ja resilienssin analyysin käsitteiksi, koska ne mahdollistavat rakenteellisen kyberasymmetrian tarkastelun teknologisten rakenteiden, toimintojen ja organisaatioiden kautta vaikeammin havainnoitavien päätöksentekijöiden subjektiivisten tulkintojen ja ajatusmallien sijaan. Hyökkäysvektoreiden lisäksi laajennan analyysiä koskemaan suljettujen ja avoimien kansallisten verkkojen ominaisuuksia, jotta verkkojen eroavaisuuksia voidaan tarkastella perusteellisemmin. Lisäksi syvennän väitöskirjani analyysiä tarkastelemalla rakenteellisen kyberasymmetrian luonnetta ja strategisia vaikutuksia.

Tutkimuksen tutkimusongelma on, tuottaako Venäjän kansallinen internetsegmentti rakenteellista kyberasymmetriaa, miten se ilmenee ja mitkä ovat sen strategiset vaikutukset? Tähän ongelmaan vastataan alatutkimuskysymysten kautta, jotka myös muodostavat työn rakenteen.

1. Mitä on rakenteellinen kyberasymmetria, miten sen olemassaoloa voidaan tarkastella ja mitä tarkoitetaan strategisilla vaikutuksilla?

2. Mikä on Venäjän kansallinen internetsegmentti ja sen suhde informaatioturvallisuuden ja -puolustuksen järjestelmän ja suljetun kansallisen verkon käsitteisiin?

3. Miten Venäjän kansallinen internetsegmentti vertautuu avoimiin kansallisiin verkkoihin toiminnan vapauden, yhteisen tilannekuvan, johtamisen ja resilienssin osalta ja muodostuuko suhteesta rakenteellista kyberasymmetriaa?

4. Miten rakenteellinen kyberasymmetria vaikuttaa voimankäyttöön tai sillä uhkaamiseen poliittisten tavoitteiden saavuttamiseksi valtioiden välisten suhteiden eri vaiheissa?

1.3 Teoreettinen viitekehys ja näkökulma

Tämä tutkimus kuuluu kansainvälisen politiikan tutkimuksen ja sen alahaaran strategian tutkimuksen piiriin.[51] Tieteenfilosofiselta perustaltaan työ ammentaa niin tieteellisen realismin ja kuin pragmatismin premisseistä lähtökohtanaan materiaalisen ja sosiaalisen todellisuuden olemassaolo. Tuosta todellisuudesta on mahdollista saada tietoa havaintojen ja järkemme avulla ja siitä on mahdollista rakentaa saadun tiedon piirissä *mahdollisimman* tosia teorioita perustuen ihmisjärkeen. Pragmatismiin liittyvän analyyttisen eklektismin mukaisesti jokainen tutkittava ongelma ja tapaus on ainutkertainen. Teoriat ja metodit on laadittava sitä silmällä pitäen ja tulokset ovat yleistettävissä rajoitetusti, ja vain mikäli tieteellinen yhteisö hyväksyy tulokset.[52]

Työn ongelmanasettelun keskiössä ovat valtioiden väliset voimankäyttöön perustuvat suhteet. Työn viitekehys muodostuu hyvin löyhästi uusklassisen realismin ja konstruktivismin teorioista ja aikaisemmassa tutkimuksessa johdetuista käsitteistä.[53] Uusklassista realismia tai konstruktivismia ei tässä

---

[51] Kansainvälisen politiikan tutkimuksesta (*International Relations*) ks. Dunne, T., Kurki, M. & Smith, S.: *International Relations Theories: Discipline and Diversity* (4th ed.) Oxford University Press, Oxford, 2013. Strategian tutkimuksesta ks. Sivonen, Pekka: *Suomalaisia näkökulmia strategian tutkimukseen*, Maanpuolustuskorkeakoulu, Julkaisusarja 1: Strategian tutkimuksia No. 33. Juvenes Print, Tampere, 2013; Baylis, J., Wirtz, J. J. & Gray, C. S.: *Strategy in the Contemporary World* (4th ed.) Oxford University Press, New York, 2013; Mahnken, Thomas G.: The Future of Strategic Studies. *The Journal of Strategic Studies*, Vol. 26, No. 1 (2003), s. x–xviii.

[52] Joseph, Jonathan & Wight, Colin (eds.): *Scientific Realism and International Relations*. Palgrave, Basingstoke, 2010; Adler, Emmanuel: Seizing the Middle Ground: Constructivism in World Politics. *European Journal of International Relations*, Vol. 3, No. 3 (1997), s. 319–363; Hellmann, Gunther (ed.): Pragmatism and International Relations: Beliefs as Rules for Action: Pragmatism as a Theory of Thought and Action. *International Studies Review* (2009) 11, s. 638–662; Pratt, S.: Pragmatism as Ontology, Not (Just) Epistemology: Exploring the Full Horizon of Pragmatism as an Approach to IR Theory. *International Studies Review* (2016) 18, s. 508–527.

[53] Rose, Gideon: Neoclassical Realism and Theories of Foreign Policy. *World Politics*, Vol. 51, No. 1 (1998), s. 144–172, s. 146). Uusklassisesta realismista lisää: Rathbun, Brian: A Rose by Any Other Name: Neoclassical Realism as the Logical and Necessary Extension of Structural Realism. *Security Studies*, Vol. 17, No. 2 (2008), s. 294–321; Lobell, S. E., Ripsman, N. M. & Taliaferro, J. W.: *Neoclassical Realism, the State, and Foreign Policy*. Cambridge University Press, Cambridge, 2009; Ripsman, Norrin M., Taliaferro, Jeffrey W. & Lobell, Steven E.: *Neoclassical Realist Theory of International Relations*. Oxford University Press, New York, 2016; Legro, Jeffrey & Moravcsik, Andrew: A. Is Anybody Still a Realist. *International Security*, Vol. 24, No. 2 (1999), s. 5–55.

työssä käsitellä tilan säästämiseksi tarkemmin vaan ne on esitelty väitöskirjassani, jossa aloitettua teoreettista kehitystyötä tämä työ jatkaa. Lähtökohtana on, että valtiot ovat kansainvälisen järjestelmän ja sen yhden toimintaympäristön, kybertoimintaympäristön, merkittävimpiä toimijoita. Järjestelmä, jossa valtiot toimivat, on sekä materiaalinen että sosiaalinen samoin kuin voima, jota valtiot käyttävät ja joiden kohteena ne ovat. Valtioiden strateginen toimintaympäristö ja voimankäyttö saavat merkityksensä toimijoiden, tarkemmin valtion ulko- ja turvallisuuspoliittisten päätöksentekijöiden uskomusten pohjalta. Päätöksentekijät ovat henkilöitä, jotka päättävät valtion voimankäytöstä ja havaittuihin uhkiin vastaamisesta. Heidän uskomuksensa määrittelevät, mikä on järkevää ja toivottavaa, mutta eivät rajoita vaan ainoastaan ohjaavat päätöksentekijöiden instrumentaalista rationaalisuutta.[54]

Tässä työssä uskomuksilla tarkoitetaan strategiskulttuurisia ideoita, jotka ovat kausaalisia tai periaatteellisia uskomuksia voimankäytöstä ja sillä uhkaamisesta poliittisten päämäärien saavuttamiseksi.[55] Nämä ideat muodostavat osan valtion strategisesta kulttuurista, niillä on ajallista pysyvyyttä ja ne ohjaavat valtioiden toimintaa antaen perustelut järkeväksi katsotulle toiminnalle. Strateginen kulttuuri voidaan määritellä keskenään sidoksissa oleviksi uskomuksiksi, normeiksi, oletuksiksi tai kollektiivisiksi odotuksiksi, jotka määrittelevät ymmärrystä strategisesta ympäristöstä ja hyväksyttävistä ja ei hyväksyttävistä strategisista valinnoista.[56] Tässä työssä strateginen kulttuuri itsessään ei ole tutkimuksen keskiössä. Kohteena on Venäjän kansallinen internetsegmentti, jonka rakentamisen strategisen kulttuurin ideat tekevät järkeväksi (*give reason*).[57] Näitä ideoita tarkastellaan lyhyesti luvussa 3.1.

---

[54] Tämä teoreettinen viitekehys perustuu Kukkola (2020a). Instrumentaalisesta rationaalisuudesta ks. March, James G. & Olsen, Johan P.: The Institutional Dynamics of International Political Orders. *International Organization*, Vol. 52, No. 4 (Autumn 1998), s. 943–969.

[55] Kukkola (2020a).

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

[57] Banerjee, Sanjoy: Rules, Agency, and International Structuration. *International Studies Review*, Vol. 17, No. 2 (June 2015), s. 274–297; Barkin, Samuel J.: *Realist constructivism: Rethinking International Relations Theory*. Cambridge University Press, Cambridge, 2010, s. 66–71; Hamati-Ataya, Inanna: Beyond (Post)Positivism: The Missed Promises of Systemic Pragmatism. *International Studies Quarterly*, Vol. 56, No. 2 (June 2012), s. 291–305; Barnett, Michael: Culture, Strategy and Foreign Policy Change: Israel's Road to Oslo. *European Journal of International Relations*, Vol. 5, No. 1 (1999), s. 5–36.

Työssä käytettävät voimankäytön käsitteet perustuvat yhdysvaltalaiseen ns. *bargaining model of war* malliin, jossa merkitseviä tekijöitä ovat kiistanalaisen resurssin jakautuminen, toimijoiden suhteellinen sotilaallinen voima, sotaan valmistautumisen ja sen käymisen kustannukset sekä edellä mainittuihin tekijöihin liittyvä epävarmuus.[58] Nämä instrumentaaliseen rationaalisuuteen, materialismiin ja peliteorioihin pohjaavat käsitteet nivoutuvat osaksi neoklassisen realismin kehystä strategian laatimisen ja toimeenpanon kautta, johon strategiskulttuuriset ideat vaikuttavat. Tähän viitekehykseen perustuen olen väitöskirjassani määritellyt kybervoiman valtion kyvyksi vaikuttaa toisiin valtioihin kybertilassa tai sen kautta ja muokata ja kontrolloida kybertilaa omaksi edukseen preferenssiensä mukaan.[59] Kybervoima ei ole pelkästään sotilaallista vaan se pohjaa teknologiseen, inhimilliseen, organisatoriseen ja normatiiviseen potentiaaliin, jotka saavat sotilaallisen luonteensa vasta käyttötapansa ja tavoitteensa kautta. Valtiot käyttävät kybervoimaa strategian ohjaamana.[60] Tämä kyberstrategia on jatkuva tilanteenarvion, päätöksenteon ja toimeenpanon epälineaarinen prosessi.[61] Yhtenä kybertilan muokkaamisen tuloksena voi olla rakenteellinen kyberasymmetria.[62] Valtiot voivat siis muokata kybertoimintaympäristön rakennetta ja sääntöjä ja nämä muutokset vaikuttavat takaisin valtioihin päätöksentekijöiden tulkintojen kautta. Konstruktivistisesta näkökulmasta Venäjän projekti kansallisen internetsegmentin rakentamiseksi, eli kybervoiman käyttö, ymmärretään siten strategian laatimisen ja toimeenpanon prosessina ja rakenteellinen kyberasymmetria sen teoreettisena ja todellisuudessa monimuotoisena lopputuloksena.

Kansallista internetsegmenttiä käsitellään tässä työssä järjestelmäteorian kehyksessä informaatioturvallisuuden järjestelmien järjestelmänä.[63] Tässä työssä se saa sisältönsä Venäjän kansallisen internetsegmentin hankkeen tavoitetilasta ja Venäjä valtion ominaispiirteistä. Kyseessä on heuristinen malli, jonka on tarkoitus tuottaa ymmärrystä adaptiivisesta ja

---

[58] Lindsay, Jon R. & Gartzke, Erik: Politics by Many Other Means: The Comparative Strategic Advantages of Operational Domains. *Journal of Strategic Studies*, 2020 DOI: 10.1080/01402390.2020.1768372.
[59] Kukkola (2020a), s. 78.
[60] Kukkola (2020a), s. 93.
[61] Adler (1997); Joseph & Wight (2010). Ajatusta on soveltanut strategian käsitteeseen mm. Popescu, Ionut C.: Grand Strategy vs. Emergent Strategy in the conduct of foreign policy. *The Journal of Strategic Studies*, Vol. 41, No. 3, (2018), s. 438–460.
[62] Kukkola, Ristolainen & Nikkarila (2017).
[63] Tästä ja muista järjestelmäteoriaan liittyvistä käsitteistä ks. Luku 3.1.

kompleksisesta järjestelmästä. Lähestymistapa resonoi venäläisen järjestelmäteoreettisen ajattelun kanssa, keskittää huomion tutkimuksen näkökulman mukaisesti kansallisen turvallisuuden tarkasteluun ja mahdollistaa Venäjän tapauksesta tehtävien havaintojen yleistämisen suljettujen kansallisten verkkojen ja rakenteellisen kyberasymmetrian teoreettisiin ilmiöihin. Kansallisen segmentin mallintaminen järjestelmänä mahdollistaa suljetun kansallisen verkon ominaisuuksien ja muutoksen tarkastelun käsitteellisellä tasolla. Lähestymistapa mahdollistaa uuden tiedon hankkimisen kybersodankäyntiin liittyvistä strategisen tason tekijöistä. Kansallisiin verkkoihin liittyvät käsitteet on esitelty luvussa 3.3.

Rakenteellista asymmetriaa tarkastellaan vertaamalla Venäjän kansallisen internetsegmentin eli suljetun kansallisena verkon ja teoreettisen avoimen kansallisen verkon suhdetta toiminnan vapauden, yhteisen tilannekuvan, johtamisen ja resilienssi kautta. Käyttämällä näitä käsitteitä analyysin välineinä voidaan tutkia niin teoreettisten kuin tosimaailman avoimien ja suljettujen verkkojen suhdetta. Samalla työ kiinnittyy käsitteiden kautta tiiviimmin läntiseen sotatieteelliseen kenttään. Työssä käytettävät käsitteet ohjaavat huomion järjestelmien suhteellisiin ominaisuuksiin ja rakenteisiin, eivät niinkään toimijoihin tai toimintojen vuorovaikutukseen tai vaikutuksiin. Käsitteet avataan tarkemmin luvussa 2.5.

Työ rajataan koskemaan Venäjän kansallista internetsegmenttiä sellaisena kuin se näyttäytyy julkisten lähteiden kautta tarkasteluna aikajaksolla 2017–2021. Kyseessä on siis tapaustutkimus, jossa yhden tapauksen (Venäjän kansallinen internetsegmentti) kautta pyritään ymmärtämään laajempaa teoreettista ilmiötä (rakenteellinen kyberasymmetria).[64] Työn tuloksena syntyvä tieto on näin ollen kontekstisidonnaista, eikä tavoitteena ole tuottaa kaikki tapaukset kattavia eli peittäviä (deduktiivis-nomologisia) testattavia selityksiä tai ennustuksia.[65] Venäjän kansallista internetsegmenttiä voidaan pitää suljetun kansallisen verkon esimerkkitapauksena, jonka pohjalta rakennetaan tieteellistä tietoa uudesta

[64] Laine, Markus, Bamberg, Jarkko & Jokinen, Pekka (toim.): *Tapaustutkimuksen taito*. Gaudeamus Helsinki University Press, Helsinki, 2007; Bennett, Andrew & Elman, Colin: Case Study Methods in the International Relations Subfield. *Comparative Political Science*, Vol. 40, No. 2 (February 2007), s. 170–195.

[65] Sosiaalitieteiden kentässä tämä on tapaustutkimuksen osalta tieteenfilosofisesti mahdotonta ja eräiden mielestä jopa ei-toivottavaa (Flyvbjerg, Bent: Five Misunderstandings About Case-Study Research. *Qualitative Inquiry* Vol. 12, No. 2 (April 2006), s. 219–245).

ilmiöstä.[66] Eräät muut maat kuten Kiina, Iran (*National Information Network*) ja Pohjois-Korea (*Kwangmyong*) ovat myös kehittäneet kansallisen Internetverkon hallintaa.[67] Niiden toimenpiteet ovat vaihtelevalla voimakkuudella tähdänneet kahdennetun, eristettävän, keskitetysti hallitun, vaihtoehtoiselle kansallisen teknologialle ja palveluille perustuvan omavaraisen kyber- ja informaatiotilan rakentamiseen. Venäjän erityispiirteenä on se, että se pyrkii suurvallan resursseilla saattamaan alun perin vapaasti kehittyneen Internetin valtiolliseen kontrolliin. Lisäksi sen hankkeella on pitkät historialliset juuret.[68] Tällaisen hankkeen tarkastelun voi olettaa tuovan hyvin esiin kaikki kansallisen internetsegmentin rakentamiseen ja hallintaan liittyvät elementit.

Avoin kansallinen verkko perustuu lähtökohdiltaan Yhdysvalloissa ja Läntisessä Euroopassa vallitsevaan tapaan järjestää Internetin hallinta 2010-luvun puolivälissä. Perusteena aikarajauksella on se, että Venäjän kansallinen segmentti oli vaste oman aikansa tilanteelle. Käyttämällä teoreettista vertailukohtaa saadaan analyysi terävöitettyä Venäjän tapaukseen ja estetään työn laajeneminen yleiseksi Internetin hallinnan tutkimukseksi. Lännessä käynnissä oleva muutos kybertilan saattamiseksi valtioiden suvereeniin hallintaan tiedostetaan ja sen seurauksiin palataan myöhemmissä luvuissa.

Työssä edetään suljettujen ja avoimien verkkojen suhteellisesta tarkastelusta rakenteellisen asymmetrian strategisten vaikutusten tarkasteluun voimankäytön muotojen ja valtioiden välisten suhteiden jatkumon kehyksessä. Kyseistä suhdetta voitaisiin tarkastella matemaattisesti, muodollisesti mallintaen, simuloiden tai peliteoreettisesti. Tässä työssä näkökulma on laadullinen, periaatteellinen ja käsitteellinen. Näin kehitetään edelleen teoreettista ja käsitteellistä ymmärrystä suljetuista

---

[66] Flyvbjerg (2006), s. 233–234.
[67] Williams, Martyn: How the Internet Works in North Korea. *Slate*, November 28, 2016. [https://slate.com/technology/2016/11/how-the-internet-works-in-north-korea.html], luettu 28.1.2021; Article 19: Iran: *Tightening the Net 2020: After Blood and Shutdowns*. Article 19, London, 2020 [https://www.article19.org/wp-content/uploads/2020/09/TTN-report-2020.pdf], luettu 28.1.2021; Nagelhus Schia, Niels & Gjesvik, Lars: The Chinese Cyber Sovereignty Concept (Part 1). *The University of Nottingham's Asia Research Institute*, September 7, 2018. [https://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-1/], luettu 28.1.2021.
[68] Kukkola (2020a).

verkoista, rakenteellisesta kyberasymmetriasta ja strategisista vaikutuksista muodollisempia analyysimenetelmiä varten.[69]

Tarkasteltaessa strategisia vaikutuksia keskitytään sotilaallisen konfliktin syntymisen välttämiseen ja ennaltaehkäisyyn, deterrenssin toimivuuteen, eskaloituvan konfliktin hallintaan ja kykyyn hyväksikäyttää asymmetriaa konfliktin puhjetessa lähitulevaisuudessa eli 2030-luvulle asti nähtävissä olevien teknologisten kehityskulkujen kehyksessä. Sodankäyntiin liittyvät operatiiviset ja taktiset kysymykset rajataan työn ulkopuolelle. Työssä ei erityisesti käsitellä venäläisen tai läntisen sotataidollisen tai strategisen ajattelun perusteita. Näitä on käsitelty aikaisemmassa tutkimuksessa.[70] Sen sijaan työssä pyritään ajoittain vertailemaan läntistä, venäläistä ja kiinalaista ajattelua eräiden keskeisten käsitteiden osalta läntisen kyber- ja strategian tutkimuksen käsitteiden kulttuurisidonnaisuuksien paljastamiseksi ja toisaalta työssä käytettävien käsitteiden täydentämiseksi. Samalla saavutetaan parempi ymmärrys Venäjän strategisen ympäristön toimijoista, joilla on suora vaikutus kansallisen internetsegmentin hankkeeseen ja sen vaikutuksiin.

1.4 Tutkimusmenetelmät ja lähteet

Tämä työ on tutkimusstrategisesti ja metodologisesti teoriasidonnainen selvittävä ja kuvaileva laadullinen tapaustutkimus.[71] Venäjän kansallinen internetsegmentti tulkitaan esimerkinomaisena ja mahdollisesti tulevaisuuden kehityksestä kertovana suljettujen kansallisten verkkojen tapauksena.[72] Se nähdään tyyppiesimerkkinä uudesta ilmiöstä, jota tarkastelemalla kyetään luomaan käsitteitä toisten vastaavien ilmiöiden tutkimiseksi sekä rakenteellisen kyberasymmetrian ymmärtämiseksi.[73] Tapauksen teoreettisena kehyksenä ovat neoklassisen realismin teoria, myöhemmin esiteltävät kyberjohdannaiset käsitteet ja järjestelmäteoria. Tapauksen empiirisenä kehyksenä toimii Venäjän strateginen ympäristö (*strategic environment*) mukaan lukien kybertila. Ripsmanin, Taliaferron ja Lobellin mukaan strateginen ympäristö koostuu kansainvälisen

---

[69] Laadullisen tutkimuksen suuntauksista ks. Tuomi, Jouni & Sarajärvi, Anneli: *Laadullinen tutkimus ja sisällönanalyysi*. Tammi, Helsinki, 2018.
[70] Ks. esim. Kukkola (2020a).
[71] Yin, Robert K.: *Case Study Research: Design and Methods*, 4th ed. CA Sage Publications, Newbury Park, California, 2009.
[72] Laine, Bamberg & Jokinen (2007), s. 32–33.
[73] Tapaustutkimuksesta ks. Gerring, John: What Is a Case Study and What Is It Good for? *The American Political Science Review*, Vol. 98, No. 2 (May, 2004), s. 341–354, s. 342.

järjestelmän voimajakaumaan perustuvasta rakenteesta, maantieteestä, teknologian diffuusiosta, hyökkäys-puolustustasapainosta, uhkien luonteesta, aikatekijöistä, optimaalisista toimintavaihtoehdoista sekä turvallisuuspoliittisten eliittien tulkinnoista.[74] Analyysiyksikkönä on ensimmäisessä vaiheessa Venäjän kansallisen internetsegmentin luonne ja rakenne. Toisessa vaiheessa se on kansallisen internetsegmentin, informaatioturvallisuuden ja -puolustuksen järjestelmän, ja teoreettisen avoimen kansallisen verkon suhde. Kolmannessa vaiheessa se on rakenteellisen kyberasymmetrian vaikutus voimankäyttöön.[75]

Työn rakenne muodostuu alatutkimuskysymyksiin vastaamalla. Ensimmäinen luku on johdanto. Toinen luku koostuu tulkitsevasta käsitteellisestä analyysistä yhdistettynä teoreettiseen kirjallisuuskatsaukseen. Nämä pohjautuvat suurilta osin aikaisempaan väitöskirjatyöhöni. Tavoitteena on asettaa tutkittava ilmiö aikaisemman tutkimuksen kehykseen ja muodostaa käsiteanalyysin edellyttämä tietopohja sekä mahdollistaa kriittinen lähestyminen aikaisempaan tietämykseen. Tässä kontekstissa määritellään, ymmärretään ja selitetään ilmiötä käsitteenmuodostuksen kautta. Käsitteet ovat sidoksissa tutkimusongelmaan, eikä työssä pyritä rakentamaan yleispätevää terminologista systeemiä.[76] Luvussa esitellään keskeisimmät käsitteet, kuten kybertila, -voima ja -strategia. Niiden kautta perustellaan ja tehdään ymmärrettäväksi kybertilan muokkaamisen strateginen merkitys. Käsiteanalyysiä jatketaan (kyber)konfliktin ja sodan, konfliktin ennaltaehkäisyn, deterrenssin, eskalaation ja voimankäytön käsitteiden tarkastelulla. Ne on valittu työn keskeisiksi käsitteiksi, koska niiden avulla rakenteellinen kyberasymmetria saa ajallisen ulottuvuuden ja tulee sidotuksi osaksi strategista ja sotilasstrategista toiminnan tasoa.[77] Ne

---

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

[75] Ks. Laine, Bamberg, & Jokinen (2007), s. 94–95.

[76] Nuopponen, Anita: *Käsiteanalyysia käsiteanalyysista – kohti systemaattista käsiteanalyysia. Käännösteoria, ammattikielet ja monikielisyys*. VAKKI:n julkaisut, N:o 36. Vaasa, 2009, s. 308–319; Näsi, Antti: *Ajatuksia käsiteanalyysista ja sen käytöstä yrityksen taloustieteessä*. Yrityksen taloustieteen ja yksityisoikeuden laitoksen julkaisuja. Sarja A2: Tutkielmia ja raportteja 11. Tampere, 1980; Takala, Tuomo & Lämsä, Anna-Maija: Tulkitseva käsitetutkimus organisaatio- ja johtamistutkimuksen tutkimusmetodologisena vaihtoehtona. *Liiketaloudellinen aikakauskirja* 50, 3 (2001), s. 371–390; Salminen, Ari: *Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin*. Vaasan yliopiston julkaisusarja opetusjulkaisuja 62, julkisjohtaminen 4, Vaasa, 2011.

[77] Strategisesta tasosta ks. Huttunen, Mika: *Monimutkainen taktiikka*. Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 1, Nro 1/2010, s. 52. Ks. Myös

muodostavat ei-sotilaallisen ja sotilaallisen voimankäytön loogisen jatkumon kybertilassa ja sen ulkopuolella. Jatkumon vaiheita ja toimintoja voidaan näin analysoida toisistaan erillään. Käsitteitä käytetään luvussa viisi strategisten vaikutusten tarkasteluun.

Uutena käsitteenä toisessa luvussa rakennetaan rakenteellisen kyberasymmetrian käsite. Tämä tapahtuu analysoimalla asymmetrian käsitettä strategian tutkimuksen käsitteistön kehyksessä ja sijoittamalla se muiden keskeisten käsitteiden yhteyteen. Lisäksi tarkastellaan teoreettisten avoimien ja suljettujen kansallisten verkkojen[78] suhdetta ja rakennetaan toiminnan vapauden, yhteisen tilannekuvan, johtamisen ja resilienssin analyysikäsitteet ja -tekijät rakenteellisen kyberasymmetrian tutkimiseksi. Kolme ensimmäistä tekijää on valittu aikaisempaan tutkimukseen perustuen. Niitä kehitetään edelleen aikaisemmassa tutkimuksessa esiintyneiden puutteiden korjaamiseksi. Näitä ovat esimerkiksi puutteellinen käsitteellistäminen ja operationalisointi, kybertilan muokkaamisen käytettyjen välineiden sekä kybertilan luonteen tarkastelu sekä muokkaamisen vaikutuksen tarkastelu tilan lisäksi suhteessa aikaan ja informaatioon. Resilienssi on otettu mukaan verkkojen passiivisen puolustuksen ja infrastruktuurin vaikutuksen lisäämiseksi analyysiin. Käsitteiden valinnan perustana on se, että niillä kyetään tarkastelemaan rakenteellisen kyberasymmetrian vaikutuksia toiminnan ja tilanteen vaatiman tilannetiedon, sen käsittelyn, arvioinnin ja ymmärtämisen, päätöksenteon ja toimeenpanon, toimeenpanon aktiivisen hyökkäyksellisen ja puolustuksellisen toteuttamisen sekä passiivisen puolustuksen eli resilienssin kautta. Käsitteet sitovat työn läntisen sotataidollisen tutkimuksen kenttään. Niitä käytetään luvun neljä analyysissä. Luvun päälähteinä ovat aikaisempi länsimainen ja englanninkielinen sotataidon ja strategian sekä kybersodankäynnin ja turvallisuuden tutkimus.

Kolmas luku tarkastelee systeemiteoriaa, Venäjän strategiskulttuurisia ideoita, Venäjän valtion ominaispiirteitä, Venäjän kansallista

---

Gray, Colin S.: *War, Peace and International Relations: An Introduction to Strategic History*. Routledge, New York, 2007; Smith, Rupert: *The Utility of Force: The Art of War I the Modern World*. Vintage Books, New York, 2008; Strachan (2013); Angström, Jan & Widen J. J.: *Contemporary Military Theory: The Dynamics of War*. Routledge, New York, 2015; Milevski, Lucas: *The Evolution of Modern Grand Strategic Thought*. Oxford University Press, Oxford, 2016; Vego, Milan: On Operational Art. *Strategos*, Vol. 1 No. 2 (2017), s. 15–39.

[78] Suljetun verkon käsitteestä ks. Luku 3.3.

internetsegmenttiä kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmänä ja esittelee teoreettisen avoimen kansallisen verkon mallin. Luku perustuu aikaisempaan tutkimukseen täydentäen sekä päivittäen sitä laadullisen asiakirja-analyysin[79] kautta. Laadullisella asiakirja-analyysillä tarkoitetaan tässä yksinkertaisesti valittujen kirjallisten ja sähköisten lähteiden (asiakirjat, raportit, uutiset ja muut kirjoitukset) teoria- ja käsiteohjautuvaa tulkitsevaa lukemista asetettuihin tutkimuskysymyksiin vastaamiseksi. Kyseessä ei siis ole muodollinen sisällönanalyysi tai temaattinen analyysi. Luvussa kuvataan lyhyesti järjestelmäajattelua ja -teorioita sekä venäläistä kyberneettistä ajattelua väitöskirjani pohjalta. Nämä antavat perusteet kansallisen segmentin ymmärtämiseksi järjestelmien järjestelmänä.[80] Päälähteinä ovat väitöskirjani lisäksi venäläisten uutistoimistojen uutiset, Venäjän johdon viralliset lausunnot ja asiakirjat sekä Venäjän federaation lait ja järjestelmäteoreettinen kirjallisuus.

Neljännessä luvussa käytetään toiminnan vapauden, yhteisen tilannekuvan, johtamisen ja resilienssin käsitteitä Venäjän kansallisen internetsegmentin ja teoreettisen avoimen kansallisen verkon välisen rakenteellisen kyberasymmetrian analysointiin. Analyysi on kolmivaiheinen. Ensimmäinen vaihe täydentää aikaisemman tutkimuksen hyökkäysvektoreihin perustuvaa tarkastelua. Toinen vaihe vertailee suljettua ja teoreettista avointa verkkoa kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmien järjestelmän alajärjestelmien kautta. Kolmas vaihe perustuu suljetun ja avoimen kansallisen verkon vertaamiselle konfliktin eri vaiheissa verkkorakenteiden muutoksen vaikutusten tarkastelemiseksi. Analyysi on muodoltaan laadullinen ja perustuu abduktiiviseen päättelyyn yhtäältä Venäjän kansallisen segmentin kuvauksen ja toisaalta rakenteelliseen kyberasymmetriaan liittyvän teorian rajapinnassa. Luvun päälähteinä ovat aikaisempien lukujen esittelemät havainnot, käsitteet ja teoriat.

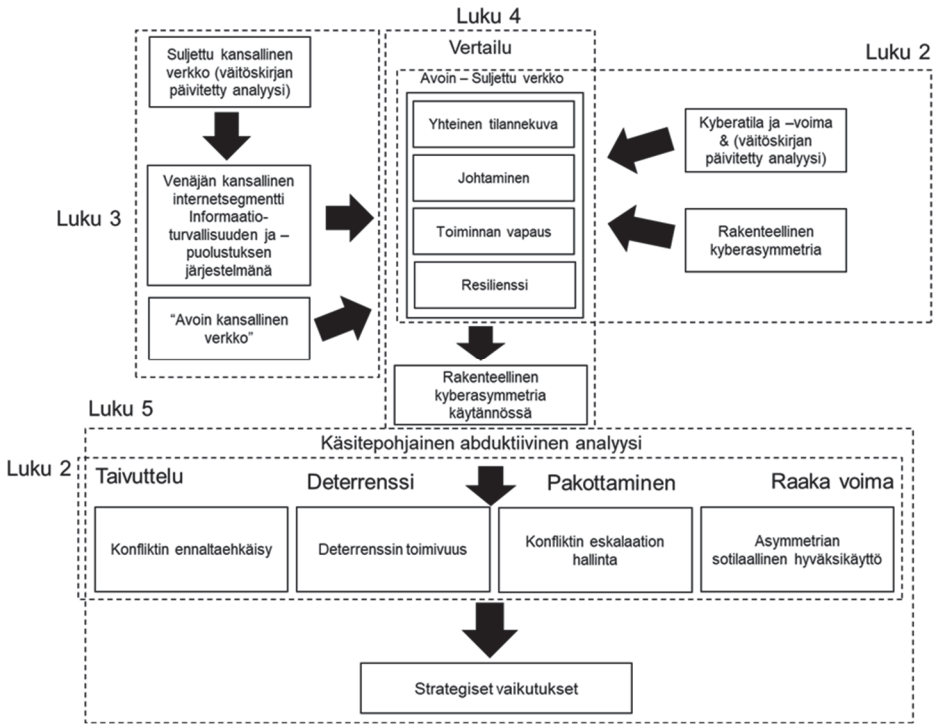
Viidennessä luvussa edellisen luvun tuloksia tarkastellaan voimankäytön muotojen eli taivuttelun, deterrenssin, pakottamisen ja raa'an voiman kautta. Analyysissa keskitytään rakenteellisen kyberasymmetrian vaikutukseen uhkien ennaltaehkäisyyn, deterrenssin toimivuuteen, eskaloituvan konfliktin hallintaan ja rakenteellisen kyberasymmetrian

---

[79] Bowen, Glenn: Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, Vol. 9, No. 2 (2009), s. 27–40.
[80] Järjestelmän käsitteestä ks. Luku 3.1.

sotilaalliseen hyväksikäyttöön. Strategisia vaikutuksia lähestytään luvussa 2 tehdyn määrittelyn mukaan voimankäytön edellytysten muokkaamisen ja sotilaallisen päämäärän saavuttamiseen tähtäävän toiminnan tarkastelun kautta. Luku jatkaa abduktiivista päättelyä, jossa aikaisemman luvun tulokset asetetaan vastakkain teoreettiskäsitteellisen näkökulman kanssa. Viidennen luvun lähteet koostuvat strategian tutkimuksen teoriakirjallisuudesta ja aikaisempien lukujen tuloksista.

Kuudes luku koostuu yhteenvedosta ja päätelmistä. Lisäksi luvussa pohditaan avoimien verkkojen viimeaikaista muutosta ja kybertilan sekä -toimintaympäristön kehitystä lähitulevaisuudessa sekä Venäjä- ja kybertutkimukseen liittyvien käsitteiden käyttöön liittyviä haasteita. Lopuksi esitellään jatkotutkimusaiheita. Työn teoreettinen ja menetelmällinen viitekehys on esitetty kuvassa 1.



Kuva 1: Työn teoreettinen ja menetelmällinen viitekehys

Venäjän kansallisen internetsegmentin kuvaamiseen käytetään lähtökohtaisesti venäjänkielisiä lähteitä. Päälähteitä ovat uutistoimistot kuten *TASS, Izvestija, RBK, Vedomosti* ja *Kommersant*, oppositio- ja kansalaisyhteiskuntanäkökulmaa edustavat Internet -sivut kuten *Roskomsvoboda*, *Meduza* ja *Novaja Gazeta* sekä Venäjän hallinnon

viralliset verkkosivut, joissa julkaistaan turvallisuus- ja puolustuspoliittisen eliitin lausuntoja sekä virallisia asiakirjoja sekä verkossa toimivat lakitekstipalvelut kuten *KonsultantPljus* sekä *Garant.ru*. Asevoimien verkkojen ja järjestelmien suhteen lähteinä toimivat EastView tietokannan kautta käytettävissä olevat sotilasaikakausilehdet kuten *Voennaja mysl*, *Vestnik akademii vojennyh nauk* ja *Vojenno-promyšlennyi kurjer,* jotka ovat alan johtavia julkaisuja sekä asevoimien verkkosivut ja puolustushaarojen sekä aselajien vuosikirjat ja vastaavat julkaisut. Työssä käytetään myös venäläisten kyberalan asiantuntijoiden blogikirjoituksia, Venäjällä järjestetyissä kyberturvallisuustapahtumissa esitettyä materiaalia sekä kyberturvallisuuteen keskittyvien Internet-julkaisujen tekstejä. Läntisiä ja englanninkielisiä lähteitä käytetään Venäjän tarkastelun osalta lähinnä tukemaan ja varmentamaan venäläisiä lähteitä sekä taustoittamaan Internetin ja kybertilan laajempia kehityskulkuja. Lähteitä on kerätty aina keväälle 2021 saakka. Lähteiden keräämisen perusteena on saturaatio eli tapaustutkimuksen strategian mukaisesti Venäjän internetsegmentistä pyritään muodostamaan mahdollisimman kattava (*in depth*) kuva perustuen laajaan joukkoon lähteitä.[81]

Työssä käytettävä teoriakirjallisuus on lähtökohtaisesti läntistä ja englanninkielistä. Kirjallisuus on kerätty kansainvälisistä sähköisistä artikkelitietokannoista (EBSCO, JSTOR, SAGE ja Taylor & Francis). Sitä on täydennetty joukolla viimeaikaisia merkittäviä monografioita. Viimeisimmät julkaisut ovat työn valmistumisaikatauluun liittyvistä syistä keväältä 2021. Luvuissa 2 ja 3 yhtenä päälähteenä käytetään väitöskirjaani. Näin ollen keskeisten käsitteiden taustalla olevaa teoriaa ja analyysia avataan vain välttämättömiltä osin ja Venäjän kansallisesta internetsegmentistä esitetään vain tiivistetty kuvaus.

1.5 Luotettavuudesta ja rajoituksista

Työn tulkinnallisen lähestymistavan takia absoluuttisia tosiväittämiä ei ole tarkoituksen mukaista tehdä. Venäjän kansallista internetsegmenttiä lähestytään sellaisena, kuin se valituissa lähteissä esiintyy. Segmentti kuuluu Venäjän kansallisen turvallisuuden piiriin ja osa sen kehittämiseen liittyvästä tiedosta on todennäköisesti salaista. Näin ollen työssä ei voida olettaa, että kansallisen internetsegmentin kaikki teknologiset toimintatavat ja -rakenteet olisivat tiedossa. Aihe on kuitenkin siinä määrin yhteiskunnallisesti merkittävä, että teknologisen toteutuksen periaatteiden

[81] Yin (2009), s. 18.

salaamisen ei voida olettaa olevan tarkoituksen mukaista. Työssä ei myöskään oteta kantaa yksittäisten järjestelmien suorituskykyyn tai käyttöperiaatteisiin. Informaatioteknologia kehittyy jatkuvasti ja tutkimuksen näkökulma on strategisten periaatteiden tasolla. Näidenkin periaatteiden pohja toki todennäköisesti muuttuu 2030-luvulle tultaessa.

Koska internetsegmentin luonteen kuvaus perustuu avoimiin laadullisiin lähteisiin, työssä ei pyritä erityisesti arvioimaan lähteiden reliabiliteettia. Lähteiden luotettavuuden arviointi perustuu niiden julkaisijan viralliseen asemaan tai vakiintuneeseen asemaan mediakentässä. Mahdollisuuksien mukaan pyritään tiedot varmistamaan useasta eri lähteestä. Tämä ei kuitenkaan poista sitä seikkaa, että uutisten ja raporttien takana on usein yksi ja sama lähde ja venäläiset uutispalvelut tyytyvät usein viittaamaan toistensa uutisiin sen syvemmin niiden väitteitä täydentämättä tai esittämällä uusia lähteitä. Työssä tehtävissä tulkinnoissa lähteiden väittämiä arvioidaan kriittisesti suhteessa aikaisempaan pohjatietoon.

Monet työn käsitteistä on alun perin määritelty väitöskirjassani. Teoria ja käsitteet on tässä työssä esitelty ja määritelty niin, että niiden pohjalta tehty analyysi on läpinäkyvä ja tiedeyhteisön arvioitavissa. Työn tieteenfilosofinen perusta on esitelty väitöskirjassani, jossa olen todennut sen olevan luonteeltaan ”realistisanalyyttispragmaattinen.”[82] Tämä tarkoittaa, että on mahdollista tehdä tosiväittämiä objektiivisesta sosiaalisesta todellisuudesta, rakentaa teoria ja metodologia abduktion, ongelmalähtöisyyden ja anlyyttisen ekletismin (teorioiden ja metodien käyttö ongelmalähtöisesti) pohjalle ja tuottaa tapaustutkimuksella yleistettävää tietoa, mikäli tutkimus ja sen tulokset läpäisevät tieteellisen yhteisön tarkastelun. Työn tulosten validiteetin tarkastelu jää siis pragmatistisen tieteenfilosofisen lähestymistavan pohjalta tiedeyhteisön arvioitavaksi. Totuus on olemassa, mutta se on kontekstisidonnaista ja teoriaa pitää soveltaa siihen todellisuuteen, jonka kuvaamiseen sitä käytetään. Teorian pitää olla avoin kohteesta kumpuaville muutoksille.[83] Tuon oman näkemykseni asioiden tilasta ja tulevaisuudesta esiin luvussa 6.

---

[82] Kukkola (2020a), s. 31.

[83] Jackson, Patrick Thaddeus & Nexon, Daniel H.: Paradigmatic Faults in International-Relations Theory. *International Studies Quarterly* Vol. 53, No. 4, (December 2009), s. 907–930; Jackson, Patrick Thaddeus: Situated Creativity, or, the Cash Value of a Pragmatist Wager for IR. *International Studies Review*, Vol. 11, No. 3 (September 2009), s. 638–662, s. 656–659; Friedrichs, J. and Kratochwil, F.: On Acting and Knowing: How Pragmatism Can Advance International Relations Research and Methodology. *International Organization*, Vol. 63, No. 4 (Fall, 2009), s. 701–731.

Suljettujen kansallisten verkkojen ja rakenteellisen kyberasymmetrian tarkastelu yhden tapauksen kautta on luonnollisesti rajoittunutta. Venäjän valintaa tutkimuskohteeksi puoltaa se, että sen hankkeesta kansallisen internetsegmentin rakentamiseksi on saatavilla runsaasti tietoa. Lisäksi tapa, jolla Venäjä pyrkii saamaan vapaasti kehittyneen Internetin kansalliseen hallintaansa, antaa mahdollisuuden tarkastella laajasti suljetun kansallisen verkon rakentamiseen liittyviä tekijöitä. Vertailevan tutkimuksen tarve on kuitenkin ilmeinen, ennen kuin suljettujen verkkojen tai rakenteellisen kyberasymmetrian osalta voidaan tehdä yleistettäviä päätelmiä. Esimerkiksi Kiina, Iran ja Pohjois-Korea tarjoavat hyvän vertailukohteen. Tässä suhteessa tämä työ on vasta keskustelun avaus.

On syytä mainita, että suhtaudun kriittisesti osaan läntisten tutkijoiden ja median esittämiin näkemyksiin. Venäjän toimia kybertoimintaympäristössä on etenkin vuoden 2014 jälkeen tarkasteltu varsin rajatusta näkökulmasta. Huomio on kiinnitetty Venäjän suorittamiin kybertiedustelu- ja hyökkäysoperaatioihin ja tutkimuskohteeseen on suhtauduttu kuin viholliseen. Venäjän toimintaa on tulkittu Lännen näkökulmasta Länteen kohdistuvana. Venäjän toimet kyber- ja informaatiotoimintaympäristössä on esitetty aggressiivisina ja lähes kaikkivoipina. Vertailua Lännen toimiin tai vastavuoroisuuden tarkastelua on vältetty ja syyt Venäjän toimille etsitään siitä itsestään.[84] Yhtenä syynä voi olla pelko ”*whataboutismin*”[85] leimasta. Toiminnan vertailu nähdään toiminnan vähättelynä. Toisena syynä voi olla aluetutkijoiden keskittyminen omaan kohteeseensa ja sen erityispiirteiden korostaminen. Kolmantena syynä ovat voineet olla tiedepoliittiset intressit.

[84] Ks. esim. Giles, Keir: *The Russian Information Warfare Construct. Contract Report*. Defence Research and Development Canada, 2020; Thornton & Miron (2020); Lucas, Edward & Pomeranzev, Peter: *Winning the Information War Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe*. CEPA, 2016. [https://li.com/wp-content/uploads/2016/08/winning-the-information-war-full-report-pdf.pdf], luettu 28.1.2021; Lilly & Cheravitch (2020); Blank, Stephen: Cyber War and Information War à la Russe. Teoksessa *Understanding Cyber Conflict: Fourteen Analogies*. Perkovich, George & Levite, Ariel E. (Eds.) Georgetown University Press, Washington, D.C., 2017, s. 81–98; Flynn, Matthew J.: Strategic Cyber: Responding to Russian Online Information Warfare. *Cyber Defence Review*, Special Edition 2019, s. 193–207; Freudenstein, Roland: Facing up to the Bear: Confronting Putin’s Russia. *European View*, Vol. 13 (2014) s. 225–232; Thomas, Timothy L: Information Weapons: Russia’s Nonnuclear Strategic Weapons of Choice. *The Cyber Defense Review*, Vol. 5, No. 2, (Summer 2020), s. 125–144.

[85] Lucas, Edward: Trump Has Become Putin’s Ally in Russia’s War on the West. *CNN*, February 7, 2017. [https://www.cnn.com/2017/02/07/opinions/trumps-moral-relativism-lucas-opinion/index.html], luettu 28.1.2021.

Poikkeuksiakin on onneksi esiintynyt.[86] Venäjän toiminnalle on yritetty myös löytää kaiken kattavia selityksiä, kuten ”hybridisodankäynti” tai sitten tulkinnan välineeksi on nostettu yksittäinen idea kuten ”Gerasimovin doktriini.”[87]

Niin kutsutulla poliittisella, taloudellisella ja psykologisella sodankäynnillä on juurensa niin Neuvostoliiton kuin Lännen kylmän sodan aikaisessa toiminnassa.[88] Tämän seikan sivuuttaminen johtaa Venäjän toimien tulkintaan vääristyneestä näkökulmasta. Raymond Garthoff on osoittanut, miten kylmän sodan aikana tällainen ajattelu johti toisen osapuolen puolustuksellisten toimien näkemiseen hyökkäyksellisinä ja tulkintoja vastaavaan vihamieliseen politiikkaan.[89] Ongelmaa pahentaa Venäjän asevoimien tutkijakentän ja median samankaltainen yksipuolinen suhtautuminen Länttä kohtaan.[90] Edellä mainituista syistä Venäjän toimintaan tai kansallisen internetsegmentin rakentamiseen ei tässä työssä

---

[86] Chernobrov, Dmitry & Briant, Emma L.: Competing Propagandas: How the United States and Russia Represent Mutual Propaganda Activities. *Politics*, 2020, s. 1–17. [https://doi-org.mp-envoy.csc.fi/10.1177/0263395720966171], luettu 29.1.2021; Baumann, Mario: ‘Propaganda Fights’ and ‘Disinformation Campaigns’: The Discourse on Information Warfare in Russia-West relations. *Contemporary Politics*, Vol. 26, No. 3 (2020), s. 288–307.

[87] Johnson, Robert: Hybrid War and Its Countermeasures: A Critique of the Literature. *Small Wars & Insurgencies*, Vol. 29, No. 1 (2018), s. 141–163; Galeotti, Mark: *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right*. Mayak Intelligence, Prague, 2016.

[88] Rid, Thomas: *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux, London, 2020, s. 68–73; O´Rourke, Lindsay: *Covert Regime Change: America´s Secret Cold War*. Cornell University Press, Ithaca, 2018, s. 101–103; Schoen, Fletcher & Lamb, Christopher J.: *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*. Center for Strategic Research Institute for National Strategic Studies National Defense University, Washington D.C., 2012; Gioe, David V., Lovering, Richard & Pachesny, Tyler: The Soviet Legacy of Russian Active Measures: New Vodka from Old Stills? *International Journal of Intelligence and CounterIntelligence*, Vol. 33, No. 3 (2020), s. 514–539.

[89] Garthoff, Raymond L.: *Deterrence and the Revolution in Soviet Military Doctrine*. The Brookings Institution, Washington, D.C., 1990, s. 64; Garthoff, Raymond L.: *Soviet Leaders and Intelligence: Assessing the American Adversary during the Cold War*. Georgetown University Press, Washington, D.C., 2015, s. 98. Ks. myös Gray, Colin S.: What Rand Hath Wrought. *Foreign Policy* No. 4 (Autumn, 1971), s. 111–129,

[90] Esimerkiksi venäläisestä hybridsotakeskustelusta ks. Kukkola (2020a); 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.

lähtökohtaisesti suhtauduta hyökkäyksellisenä tai puolustuksellisena vaan suurvallan voimankäyttönä.

Toinen huomioitava seikka on, että kybertutkimuksen käsitekenttä on vakiintumaton ja läntisen tutkijakentän kehittämä. Läntisen teorian soveltamista työssä voitaneen kritisoida. Työ on kuitenkin liitettävä johonkin tieteelliseen kenttään kommunikaation mahdollistamiseksi. Lisäksi niin amerikkalaisen, suomalaisen kuin venäläisen (ja kiinalaisen) sotilastieteellisen yhteisön ja päätöksentekijöiden viime aikoina omaksuttua samat strategiset peruskäsitteet, toki kansallisilla vivahteilla muokattuna, voidaan deterrenssin, eskalaation ja voimankäytön käsitteitä määrätyin varauksin käyttää voimankäytön vaikutusten tulkintaan.[91] Erityistä huomiota on toki kiinnitettävä siihen, että kansainvälisen politiikan ja strategian tutkimuksen käsitteet vaativat muokkaamista ja kehittämistä sopiakseen kybertoimintaympäristön tarkasteluun.[92] Siihen on tässä työssä pyritty.

[91] The President of the United States: *National Security Strategy of the United States of America*, December 2017. White House, Washington, DC., 2017; Suomen Valtioneuvosto: *Valtioneuvoston puolustusselonteko*. Valtioneuvoston kansalian julkaisusarja 5/2017, Helsinki, 2017; Указ-2976: Указ Президента РФ 25 декабря 2014 г., № Пр-2976. *Военная доктрина Российской Федерации.* [http://base.garant.ru/70830556/], luettu: 21.3.2019; The State Council Information Office of the People's Republic of China (2019). Erityisesti venäläisestä pidäke -käsitteen (*сдерживание*) käytöstä ks. Forsström (2019), s. 152.

[92] Whyte, Christopher: Dissecting the Digital World: A Review of the Construction and Constitution of Cyber Conflict Research. *International Studies Review*, Vol. 20, No. 3 (2018), s. 520–532.

2 Kybervoima ja rakenteellinen kyberasymmetria

Tässä luvussa esitellään työn keskeiset käsitteet, joista osa perustuu aikaisempaan väitöskirjatyöhöni. Tavoitteena on määritellä työn keskeisimmät käsitteet ja rakentaa perusteet niiden käytölle myöhempien lukujen analyysissä. *Kaikki esiteltävät käsitteet määritelmineen on rakennettu tätä työtä varten, eivätkä noudata vakiintuneita tai aikaisemmin esitettyjä muotoiluja, ellei niin ole erikseen todettu*. Ensimmäinen alaluku esittelee kybertilan ja -toimintaympäristön, kybervoiman ja kyberstrategian peruskäsitteet. Tavoitteena on asemoida työ käsitteellisesti strategian ja kybersodankäynnin tutkimuksen kenttään. Toisessa alaluvussa esitellään strategian tutkimuksen alaan kuuluvia valtioiden voimankäyttöön liittyviä käsitteitä kybertoimintaympäristöön sitoen. Tavoitteena on osoittaa, että ei-sotilaallisen ja sotilaallisen voimankäytön eri muodot kybertilassa ja sen ulkopuolella muodostavat loogisen jatkumon, jonka vaiheita ja toimintoja voidaan kuitenkin analysoida toisistaan erillään. Kolmas alaluku esittelee asymmetrian käsitteen taustaa sotilaallisessa kontekstissa. Tavoitteena on osoittaa aikaisempien asymmetriakäsitteiden puutteet tämän työn tutkimusongelman kontekstissa. Neljännessä ja viidennessä alaluvussa muodostetaan rakenteellisen kyberasymmetrian käsite ja sen analyysin käytettävät toiminnan vapauden, yhteisen tilannekuvan, johtamisen ja resilienssin käsitteet.

Tässä luvussa käsitteille annettujen merkitysten taustalla vaikuttaa realistinen analyyttinen pragmatismi, joka tarkoittaa, että käsitteet on muodostettu työssä tarkasteltavan ongelman (ja todellisen ilmiön) tutkimista varten. Lähtökohtaisesti käsitteiden oletetaan viittaavan tosimaailman ilmiöihin, mutta niillä ei oleteta olevan yleistettävää vastaavuutta tapauksen kontekstin ulkopuolella – ennen kuin vertaileva jatkotutkimus lisää todistusaineistoa. Käsitteiden taustalla on myös konstruktivistisilla vaikutteilla muokattu uusklassisen realismin teoria, joka on tarkemmin esitelty väitöskirjassani.

Vaikka tässä luvussa esiteltävillä käsitteillä katsotaankin kuvattavan yhteisesti jaettuja materiaalisen ja sosiaalisen todellisuuden ilmiöitä, eri maiden ulko- ja turvallisuuspoliittisella johdolla voi strategisen ympäristön ja kulttuurin johdosta olla niistä ajassa ja paikassa toisistaan poikkeavia tulkintoja. Tästä syystä luvussa esitellään myös venäläisiä ja kiinalaisia näkemyksiä määriteltävistä ilmiöistä. Käsittelyn avulla lisätään käytettyjen käsitteiden yleistettävyyttä, osoitetaan niiden kulttuurisidonnaisuuksia ja

pragmatismin mukaisesti tuodaan sopivuutta työn kohteena olevan ilmiön käsittelyyn.

2.1 Kybertila, kybervoima ja kyberstrategia

Kybertila (*cyberspace*) määritellään tässä työssä Daniel T. Kuehlin määritelmää mukaillen seuraavasti: *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*.[93] Määritelmä korostaa kybertilan luonnetta plastisena eli muuttuvana. Kybertila jakautuu fyysiseen, syntaktiseen ja semanttiseen tasoon, joilla kaikilla on omat sääntönsä. Tasot ovat keskinäisriippuvaisia, mutta ne eivät ole täysin hallittavissa toistensa kautta ja niiden vuorovaikutus tuottaa vaikeasti ennustettavia seurauksia. Huomioitavaa määritelmässä on, että ihmiset kuuluvat tähän tilaan vain subjekteina, eivät objekteina.

Kybertila on siis itsessään kompleksinen järjestelmä.[94] Ihmiset voivat muokata kybertilaa kontrolloimalla sen infrastruktuuria, ohjelmia ja palveluita ja sitä sääteleviä teknisiä standardeja, lakeja ja säädöksiä. Kybertilan olennainen suhde informaation käsittelyyn (ihmisten toimesta koneiden kautta) ja tämän informaation vaikutus ihmisten olemiseen tekee siitä toimintaympäristön.[95] Korostettaessa kybertilan luonnetta nimenomaan *toiminnan* ympäristönä voidaan käyttää käsitettä kybertoimintaympäristö. Tällöin huomio ei ole pelkästään tilassa, sen luonteessa tai ominaisuuksissa vaan myös prosesseissa, tiedonhallinnassa

---

[93] Kukkola (2020a), s. 72. Kuehlin alkuperäinen ks. Kuehl, Daniel T.: *From Cyberspace to Cyberpower - Defining the Problem*. Teoksessa *Cyberpower and National Security*. Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K., National Defence University Press, Washington, D.C., 2009, s. 24–42, s. 28.

[94] Kompleksisuudesta ks. Luku 3.1.

[95] Tilan ja toiminnan suhteesta ks. Sanastokeskus TSK (2018), s. 21; Kuusisto, Tuija: Tiedonhallinta päätöksenteossa kybertoimintaympäristössä. Teoksessa *Kybertaistelu 2020*. Kuusisto, Tuija (toim.) Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2, No. 1/2014, Juvenes Print, Helsinki 2014, s. 33–61; Lehto, Martti: *Kybermaailman ilmiöitä ja määrittelyjä*. Jyväskylän yliopisto, Informaatioteknologian tiedekunta, 2019 [https://www.jyu.fi/it/fi/hae-opiskelemaan/hakukohteet/kyberturvallisuuden-seka-turvallisuus-ja-strateginen-analyysi-maisteriohjelmien-yhteisvalinta/kybermaailma_v10-0.pdf], luettu 16.3.2020; Laari (2019).

ja subjektien vuorovaikutuksessa.[96] Kybertila vertautuu mereen, maahan, ilmaan ja avaruuteen – se on toiminnan kehys ja rakenne. Kybertilan ja toimintaympäristön leikkauspisteessä on kybertaistelutila tai -ulottuvuus (*domain*).[97] Sillä tarkoitetaan tässä työssä sotilaallista toimintaympäristöä, joka voidaan jakaa kybertaistelukenttiin taktisten, operatiivisten ja strategisten tavoitteiden toteuttamiseksi.[98] Jako noudattaa toiminnan muotoa, tavoitteita ja päämäärää, eikä ole ennalta säädetty. Koska informaatiota, tietoteknisiä järjestelmiä ja elektromagneettista säteilyä on käytännössä mahdoton erottaa toisistaan, on kybertaistelutila nähtävä lähinnä funktionaalisena ja/tai toimintaa organisoivana käsitteenä.[99] Hierarkkisesti kybertoimintaympäristö on informaatiotoimintaympäristön osa. Jälkimmäinen on ”informaatiota keräävien, käsittelevien, jakavien tai sen mukaan toimivien yksilöiden, organisaatioiden ja järjestelmien kokonaisuus”[100] tai fyysisen, informaatio- ja kognitiivisen ulottuvuuden kokonaisuus, joiden sisällä yksilöt, organisaatiot ja järjestelmät ovat vuorovaikutuksessa.[101] Informaatioympäristössä ihmisten mielet ovat läsnä objekteina ja subjekteina. Kybertoimintaympäristön ja informaatiotoimintaympäristön suhde on esitetty kuvassa 2.

---

[96] Erilaisten kybertilakäsitteiden suhteesta ks. Lehto (2019), s. 8; Magd, Noora: Kybertaistelutila kybertoimintaympäristön sotilaallisena ulottuvuutena. Teoksessa *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, s.84–93.

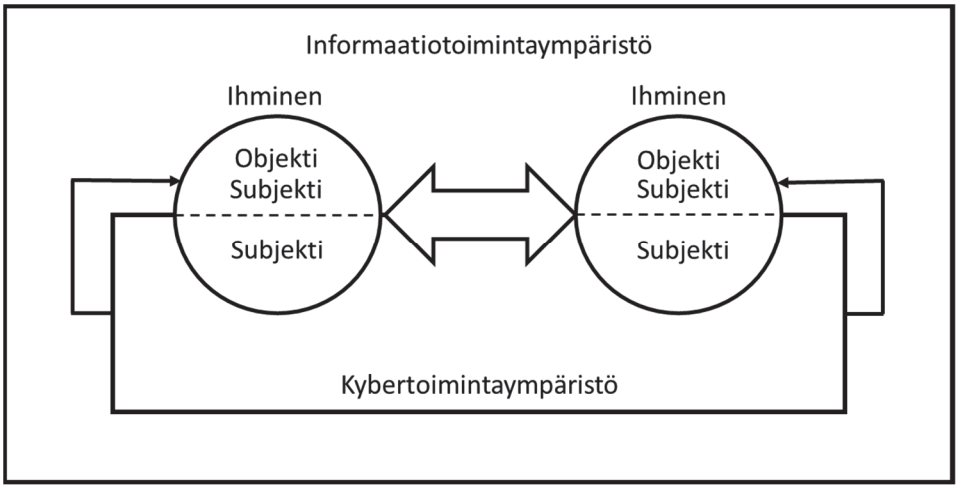
[97] Magd (2018), s. 90–91.

[98] Ks. Magd (2018), s. 90–91; Kukkola, Ristolainen & Nikkarila (2017), s. ix.

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

[100] The United State Department of Defence (U.S. DoD): *Joint Publications 3-12: Cyberspace Operations, 8th June 2018*, s. viii. [https://fas.org/irp/doddir/dod/jp3_12.pdf], luettu 17.10.2019.

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



Kuva 2: Kyber- ja informaatiotoimintaympäristön suhde

Kybertila ei ole yhteiskäyttöinen tila (*commons*) siinä mielessä kuin valtioiden määräysvallan ulkopuolella oleva maa-, meri- tai ilmatila.[102] Kybertilan infrastruktuurin omistavat suurilta osin yksityiset ja julkiset tahot. Valtioiden suvereniteetti suhteessa informaatioon ja informaatioinfrastruktuuriin vahvistuu vuosi vuodelta.[103] Kybertilan osia voivat yksipuolisesti muokata tahot, joilla on tarvittavat resurssit, suorituskyvyt ja toimivalta. Toisaalta muut toimijat ja kybertilan oma logiikka voivat haastaa muokkaamisen. Kybertilaa ei voi tuhota tai sen käyttöä kiistää kuin rajoitetusti (tai totaalisesti kaikilta osapuolilta). Se voidaan palauttaa ja sen yhteydet reitittää uudelleen uusilla tavoilla. Näin esimerkiksi kyberhyökkäys muuttaa kybertilaa puolustajan toimien ja hyökkääjän vaikutusten kautta.

Kybertila on kuitenkin haavoittuvainen niin tahallisille kuin tahattomille vaikutuksille. Sen rakenne ei ole homogeeninen vaan se koostuu useista verkoista, jotka eivät kaikki ole yhteydessä toisiinsa, joiden väliset yhteydet ovat erilaatuisia ja joiden rakenteissa on fyysiseen ja loogiseen rakenteeseen perustuvia pisteitä, joiden kautta informaation kulkua

[102] Raymond, Mark: Puncturing the Myth of the Internet as a Commons. *Georgetown Journal of International Affairs, International Engagement on Cyber III: State Building on a New Frontier*, 2013, s. 57–68.
[103] Demchak & Dombrowski (2011).

voidaan hallita.[104] Tiivistetysti kybertila on keinotekoinen, perustaltaan fyysinen, sääntöpohjainen, verkottunut, epähomogeeninen, plastinen, uudelleen syntyvä ja rakennettavissa, helppopääsyinen kaikille toimijoille ja näin ollen useiden, vaikeasti attribuutioitavissa olevien toimijoiden kenttä, jossa voima on jakautunut ja jossa maantieteellinen etäisyys on menettänyt merkityksensä ja ajankäsitys perustuu koneaikaan.[105]

Edellä esitetystä määrittelystä huolimatta tai siitä johtuen Myriam Dunn Cavealtyn ja Andreas Wengerin mukaan kybertilan, -turvallisuuden ja -puolustuksen käsitteiden käyttöön liittyy paljon politiikkaa ja ne ovat vielä vakiintumattomia.[106] Läntisessä käytössä kyberturvallisuus viittaa tietokonejärjestelmien, tietoverkkojen ja informaation suojaamiseen tahalliselta tai tahattomalta vahingolta. Se koostuu esimerkiksi uhkien estämisestä, monitoroinnista, havainnoinnista, analysoinnista, niihin vastaamisesta ja palautumisesta niiden vaikutuksesta. Kyberpuolustus viittaa suojajärjestelmiin tai funktioihin, jotka on tarkoitettu sotilaallisen puolustuksen toteuttamiseksi kybertoimintaympäristössä.[107] Informaatioturvallisuus (*information security*) liitetään useimmin tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen.[108] Kybertilalla, turvallisuudella- ja puolustuksella on kuitenkin osittain ilmiön uutuudesta ja siihen liittyvistä poliittisista intohimoista johtuen useita erilaisia kansallisia määritelmiä ja käytännön sovelluksia, jopa valtioiden virastojen välillä.[109]

---

[104] Rattray, Gregory J.: An Environmental Approach to Understanding Cyberpower. Teoksessa *Cyberpower and National Security*. Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K. (Eds.) National Defence University Press, Washington, D.C., 2009, s. 253–274; Nye, Joseph: *Cyber Power*. Harvard Kennedy School, Cambridge, 2010, s. 5; Choucri (2012).

[105] Kybertilan ominaisuuksien listauksista ks. esim Schreier, Fred: *On Cyberwarfare*. DCAF Horizon 2015 Working Paper No. 7. [https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf], luettu 27.4.2020.

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

[107] Rantapelkonen & Salminen (2013); ENISA: *Definition of Cybersecurity: Gaps and overlaps in standardisation Version 1.0, December 2015.* [https://www.enisa.europa.eu/publications/definition-of-cybersecurity], luettu 28.4.2020.

[108] Fall, Kevin R. & Stevens, Richard W.: *TCP/IP Illustrated, Volume 1: The Protocols (2nd ed.)* Addison-Wesley, Upper Saddle River NJ, 2012, s. 806–807.

[109] Ks. Godwin III, J. B., Kulpim, A., Rauscher, K. F. & Yaschenko, V. (eds.): *Critical Terminology Foundations 2. Russia-U.S. Bilateral on Cybersecurity*. Policy Report 2/2014. EastWest Institute and the Information Security Institute of Moscow State

Läntisestä näkökulmasta on erikoista, että Venäjän viralliset asiakirjat eivät tunnista kybertilan käsitettä. Sen sijaan informaatiotila (*informatsionnoe prostranstvo*) määritellään "kokoelmaksi informaatioresursseja, jotka informaatiotoimintaympäristön subjektit ovat luoneet, sekä näiden subjektien vuorovaikutuksen keinot, niiden informaatiojärjestelmät ja niille tarpeellinen informaatioinfrastruktuuri."[110] Painotus on siis informaatiossa, informaation käytössä ja sen päämäärässä ja substanssissa – informaatiopsykologinen ja teknologinen tila kuuluvat yhteen. Venäjällä informaatioturvallisuus liittyy virallisissa asiakirjoissa niin psykologisiin kuin teknologisiin informaatiouhkiin.[111] Epävirallisissa venäläisissä määritelmissä kyberturvallisuus toki esiintyy ja virallisissa asiakirjoissa kriittisen informaatioinfrastruktuurin turvaamisesta on tullut kyberturvallisuuden venäläinen vastine.[112]

Kiina on Venäjän tavoin käyttänyt informaatiotilan käsitettä julkisessa viestinnässään. Se on liittänyt käsitteen informaatioturvallisuuteen. Vuonna 2015 Kiina kuitenkin määritteli kybertilan kansallisen turvallisuuden toimintaympäristöksi (*domain*) ja on ollut Venäjää selvästi halukkaampi käyttämään kybertilan ja -turvallisuuden käsitteitä.[113] Kiinan osalta kyberturvallisuuden käsite näyttää vuoden 2014 tienoilla eronneen informaatioturvallisuuden käsitteestä edellisen lähestyessä läntistä teknisempää näkökulmaa ja jälkimmäisen pysyttäytyessä informaation sisällössä ja hallinnassa. Molemmat ovat sidoksissa valtion intresseihin,

---

University, 2014, s. 17: Valtioneuvosto: *Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta*. Lausuntopyynnön diaarinumero: VN/ 797/2021.
[https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=e09805fc-83a1-4207-8f16-55a991363d0d], luettu, 12.3.2021.

[110] Указ-203: Указ Президента РФ от 09.05.2017 N 203 "*О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы*". [https://www.garant.ru/products/ipo/prime/doc/71570570/], luettu 15.5.2019.

[111] Указ-646 (2016).

[112] Kukkola (2020a).

[113] РП-788: Распоряжение Правительства Российской Федерации от 30 апреля 2015 г. N 788-р "*О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности*". [http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=620700#046323 5836450268], luettu 27.4.2020; The State Council Information Office of the People's Republic of China. *China's Military Strategy*. Beijing, May 2015. [http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm], luettu 27.4.2020. Kiinasta ks. Kolton (2017); Inkster (2016); Lindsay, Cheung, Ming & Reveron (2015).

etenkin vakauteen.[114] Vuoden 2017 kyberturvallisuuslaki yhdistää tiedon sisältöön ja järjestelmien turvallisuuteen liittyvät tekijät korostaen samalla kriittisen informaatioinfrastruktuurin merkitystä.[115]

Läntisten, venäläisten ja kiinalaisten käsitemääritelmien erot pohjaavat poliittisten järjestelmien arvoihin ja intresseihin ja strategisen kulttuurin eroihin. Venäjä ja Kiina esimerkiksi ajavat informaatiosuvereniteetin hyväksymistä kansainväliseksi normiksi. Niiden tulkinnassa suvereniteetista korostuu valtion informaation sisältöön ja välittämiseen liittyvä hallinta.[116] Joissain tulkinnoissa venäläisiä ja kiinalaisiakin tulkintoja on kutsuttu ”holistisiksi.”[117] Tulkinnat häivyttävät näkyvistä sen tosiasian, että läntiset, venäläiset ja kiinalaiset sotilasmääritelmät informaatio- ja kybertilasta ovat lähestyneet toisiaan systeemiteoreettisen ymmärryksen kautta.[118] Näiden tulkintojen haasteisiin palataan luvussa 6. Kybertilan käsite on siis osittain politisoitu, kiistetty ja muuttuva, mutta kansakunnat ylittävä sotatiede on havainnut siinä määrättyjä, omaan alaansa kuuluvia yhdenmukaisuuksia.

Voiman käsite on kiistelty, monimuotoinen, sekä konteksti- ja kulttuurisidonnainen.[119] Täten kybervoimallekaan ei ole olemassa

---

[114] Cuihong, Cai: Cybersecurity in the Chinese Context. Changing Concepts, Vital interests, and Prospects for Cooperation. *China Quarterly of International Strategic Studies*, Vol. 1, No. 3 (2015), s. 471–496.

[115] Jones Day: Implementing China’s Cybersecurity Law, August 2017. [https://www.jonesday.com/files/upload/Implementing%20Chinas%20Cybersecurity%20Law.pdf], luettu 28.4.2020.

[116] Kukkola (2020a); Nocetti, Julian: Cyber Power. Teoksessa *Routledge Handbook of Russian Foreign Policy*. Tsygankov, Andrei P. (Ed.) Routledge, London and New York, 2018, s. 182–198, s. 192.

[117] Adamsky (2018); Giles (2016); Nocetti (2018); Jonsson (2019), s. 33–34.

[118] Kukkola (2020a); Libicki (2016), s. 190–191; U.S. DoD JP 3-0 (2018), s. IV-1–IV-2; Engström, Jeffrey: *Systems Confrontation and System Destruction Warfare. How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*. RAND, Santa Monica, 2018; Lin, Herbert: Doctrinal Confusion and Cultural Dysfunction. *The Cyber Defense Review*, Vol. 5, No. 2 (2020), s. 89–108.

[119] Nye, Joseph S. Jr.: *The Future of Power*. PublicAffairs, New York, 2011; Barnett, M. & Duvall, R.: Power in International Politics. *International Organization*, Vol. 59, No. 1 (2005), s. 39–75; Digiser, Peter: Fourth Face of Power. *The Journal of Politics*, Vol. 54, No. 4 (1992), s. 977–1007; Guzzini, Stefano: The Limits of Neorealist Power Analysis. *International Organization*, Vol. 47, No. 3 (1993), s. 443–478; Lukes, Steven: Power: *A Radical View* (2nd ed.) Palgrave Macmillan, Basingstoke, 2005; Guzzini, Stefano: *Power, Realism and Constructivism*. Routledge, London and New York, 2013; Art, Robert J.: Force and Fungibility Reconsidered. *Security Studies*, Vol. 8, No. 4 (1999), s. 183–189.

vakiintunutta määritelmää.[120] Tässä työssä käytetään määritelmää, jonka olen esittänyt väitöskirjassani. Se sopii myös pragmatismin perusteiden mukaisesti tämän tutkimuksen tutkimusongelmaan. Kybervoiman määritelmä on "*kyky, joka mahdollistaa toimijan vaikutuksen muihin kybertilassa tai sen kautta ja kybertilan hallinnan ja muokkaamisen toimijan preferenssien mukaisesti*."[121] Kybervoimaa käytetään kybertilassa tai sen kautta. Määritelmä korostaa voiman toimintaympäristön infrastruktuuria ja normeja eli rakennetta muokkaavaa luonnetta. Kybervoiman käytöllä voi olla suhteellisen pysyviä vaikutuksia ja täten kybertilaa voidaan hallita ja muokata. Pysyvyys on suhteellista, koska muut toimijat pyrkivät myös jatkuvasti muokkaamaan kybertilaa. Voiman resurssit ja menetelmät eivät välttämättä ole itsessään sotilaallisia tai väkivaltaisia, vaikka tarkoitusperät ja tulokset sellaisia olisivatkin. Kybervoimaresurssit tai potentiaali ovat luonteeltaan pääasiassa teknologisia, tieteellisiä, taloudellisia, normatiivisia, doktrinaalisia, organisatorisia ja inhimillisiä (ammatillisia).[122] Periaatteellisella tasolla kybervoiman käyttö voi tuottaa lisää voimaa, koska kybertilan

---

[120] Aikaisemmista käsitemuotoiluista ks. Sheldon, John B.: The Rise of Cyberpower. Teoksessa *Strategy in the Contemporary World* (4th ed.) Baylis, John, Wirtz, James J. & Gray, Colin S. (Eds.) Oxford University Press, Oxford, 2013, s. 282–298; Schreier (2015); Kuehl (2009); Nye (2011); Rattray (2009); Kern, Sean & Gaines, Charles: Expanding Combat Power Through Military Cyber Power Theory. *Joint Forces Quarterly*, Vol. 79, No. 4 (Quartet 2015), s. 88–95; Valeriano & Maness (2015); Valeriano, Jensen & Maness (2018); Demchak, Chris: Cybered Conflict, Cyber Power, and Security Resilience as Strategy. Teoksessa *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Reveron, Derek (ed.) Georgetown University Press, Washington, D.C., 2012, s. 121–136; Klimburg, Alexander: Mobilising Cyber Power. *Survival*, Vol. 53, No. 1 (2011), s. 41–60, s. 43, s. 56; Bebber, Robert: Cyber Power and Cyber Effectiveness: An Analytic Framework. *Comparative Strategy*, Vol. 36, No. 5 (2017), s. 426–436; Slayton, R.: What is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment. *International Security*, Vol. 41, No. 3 (2017), s. 72–109; Whyte, Christopher & Mazanec, Brian: *Understanding Cyber Warfare. Politics, Policy and Strategy*. Routledge, London and New York, 2019, s. 150–154.

[121] Kukkola (2020a), 78. Tämä määritelmä on muokattu R. S. Endresenin käsitteestä (ks. Endresen, R. S.: Hard Power in Cyberspace: CNA as a Political Means. Teoksessa *Cyber Power*. Pissanidis, N., Rõigas, H., Veenendaal, M. (Eds.) NATO CCD COE, Tallinn, 2016, s. 23–36, s. 25).

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

ominaisuuksien hallinta itsessään voi olla voiman lähde.[123] Valtioiden ja ei-valtiollisten toimijoiden jakama tila mahdollistaa poliittisen, sosiaalisen, taloudellisen ja sotilaallisen vallan käyttämisen.

Kybervoimaa voidaan käyttää niin sodan kuin rauhan aikana ja sen käytölle antavat merkityksen mm. strategiskulttuuriset ideat. Kybervoiman käyttö on suunniteltua, tarkoituksellista ja strategista ja se on riippuvainen siitä, miten käyttäjä käsittää ja kokee kybertilan ja -voiman. Kybervoimaa ei voi mitata sen suhteen ja/tai kontekstin ulkopuolella, missä sitä käytetään, vaikkakin resursseja ja potentiaalia voidaan tarkastella erikseen. Olennaista on, että kybervoima ei ole lähtökohtaisesti hyökkäyksellistä tai puolustuksellista – tai edes sotilaallista. Määritelmä korostaa voiman luovaa luonnetta ja muodostaa perustan sen ymmärtämiseksi, miten suljettuja kansallisia verkkoja tai kansallisia internetsegmenttejä rakennetaan ja hallitaan. Tässä työssä käytettävä voiman määritelmä poikkeaa siis oleellisesti historiallisista, sotilaallisista maa-, meri- ja ilmavoimien määritelmistä.[124] Ne pyrkivät selittämään kyseisen voiman lajin erityispiirteitä sotilasstrategian ja sodan voittamisen kontekstissa usein omaa ratkaisevuuttaan korostaen. Voima ja sen käyttö ymmärretään usein suhteessa tilan käytön hallintaan tai vastustajan voimaan vaikuttamiseen.[125] Itse asiassa Whyte ja Mazanec väittävät, että kybervoimaakin tulisi tarkastella vain pakottavina (*coercive*) suorituskykyinä, koska kybervoiman merkitykset ovat usein strategisten

---

[123] Ajatus voiman tuottamisesta voimalla strategian välineenä on Lawrence Freedmanin (Freedman, Lawrence: *Strategy: A History*. Oxford University Press, New York, 2013, s. xi–xii).

[124] Ks. Wylie, J. C.: *Military Strategy: A General Theory of Power Control*. Naval Institute Press, Annapolis Maryland, 2014; Mahan, Alfred T.: *The Influence of Sea Power upon History 1660-1783*. Dover edition. Little, Brown and Company, Boston, 1890; Mets, David R.: *The Air Campaign. John Warden and the Classical Airpower Theorists*. Air University Press, Maxwell Air Force Base, Alabama, 1999; Pape, Robert A.: *Bombing to Win: Air Power and Coercion in War*. Cornell University Press, Ithica and London, 1996; Olsen, John Andreas: *Routledge Handbook of Air Power*. Routledge, Abingdon, Oxon, 2018; Liddell Hart, B. H.: *Strategy* (2nd rev. ed.) Meridian, New York, 1991; Fuller, J. F. C.: *The Foundations of the Science of War*. A Military Classic Reprint (org. 1925). U.S. Army Command and General Staff College Press, Fort Leavenworth, Kansas, 1993; Corbett, Julian: *Some Principles of Maritime Strategy*. Longmans, Green and Company, London, 1911 [http://onlinebooks.library.upenn.edu/webbin/gutbook/lookup?num=15076], luettu 27.4.2020.

[125] Gray (1999); Sloan, Elinor C.: *Modern Military Strategy: An introduction.* Routledge, New York, 2012; Angström & Widen (2015).

intressien ja ympäristön muokkaamia.[126] Tämä voi olla ymmärrettävä lähestymistapa kyberturvallisuuden tutkimuksen näkökulmasta. Kansainvälisen politiikan ja strategian tutkimuksen näkökulmasta se kuitenkin tarkoittaisi kybervoiman ja sen käytön erityispiirteiden tarkastelua erittäin rajoittuneesta näkökulmasta.

Kybervoiman käyttö perustuu strategiaan. Sotilasstrategia voidaan ymmärtää suunnitelmana sotilaallisen päämäärän saavuttamiseksi, voimankäyttönä ja sillä uhkaamisena poliittisten päämäärien saavuttamiseksi, kahden vastakkaisen tahdon dialektiikan taitona ratkaista ristiriitansa voimakeinoin, tulevan sodan luonteen ymmärtämisenä, valmistautumisena siihen ja sen johtamisena, välineiden ja keinojen yhteensovittamisena päämäärien saavuttamiseksi, tai Aleksandr Svetšinin sanoin, taitona yhdistää sotaan valmistautuminen ja operaatioiden ryhmittäminen sodan asevoimille asettaman päämäärän saavuttamiseksi.[127] Koska strategia on kiinteästi yhteydessä tekijöidensä strategiseen kulttuuriin ja ympäristöön, eri kansakunnilla ja asevoimilla on omat käsityksensä strategiasta.[128] Analyyttisestä näkökulmasta sotilasstrategialla voidaan nähdä kuusi eri tulkintaa. Se voi olla teoria sodan käymisestä korkeimmalla tasolla, kirjattu ja suhteellisen pysyvä suunnitelma kansakunnan kovien turvallisuuspäämäärien saavuttamiseksi, jatkuvasti muuttuva suunnitelma sodan käymiseksi määrätyssä uhkatilanteessa, suunnitelmien laatimisen prosessi tai sodan käyminen asevoimien ja valtiojohdon tasolla. Kuudes tulkinta näkee strategian ”tekemisenä” (*continuous process / practice*), emergenttinä toimintana, joka muotoutuu käytännön ja oppimisen kautta.[129] Kaaos- ja kompleksisuusteorian näkökulmasta strategia onkin kaoottiselta vaikuttavan turvallisuusympäristön ohjailua ja muokkaamista, koska täysi

[126] Whyte & Mazanec (2019), s. 142.
[127] Määritelmistä ks. Wylie (2014), s. 14; Gray (1999), s. 17; Kolodziej, E. A.: French Strategy Emergent: General Andre Beaufre: A Critique. *World Politics*, Vol. 19, No. 3 (1967), s. 417–444; Handel, M.: *Masters of War: Classical Strategic Thought*. Frank Cass, London, 1996, s. 36; Gray (1999), s. 24; Strachan (2013), s. 118; Lykke, Arthur F.: Toward an Understanding of Military Strategy. *Military Review* Vol. LXIX, No. 5, (May 1989), s. 2–8; Svechin, Aleksandr A.: *Strategy*. East View Information Services, Minneapolis, Minnesota, 1992.
[128] Gray (1999), s. 141–150. Timothy Thomasin mukaan esimerkiksi Kiinalla ja Venäjällä on omat, kansalliset sotilasstrategian käsitteensä ja ymmärryksensä. (Thomas, Timothy: Nation-state Cyber Strategies: Examples from China and Russia. Teoksessa *Cyberpower and National Security*. Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K. (Eds.) National Defence University Press, Washington, D.C., 2009, s. 465–488).
[129] Popescu (2018).

hallinta on mahdotonta.[130] Tämä strategia on jatkuva tilanteenarvion, suunnittelun, päätöksenteon ja toimeenpanon epälineaarinen prosessi, jolla on emergenttejä, eli inkrementaalisia, ennalta-arvaamattomia, lähtötilanteeseen redusoimattomia ja käytännön kautta itsensä tuottavia, ominaisuuksia.[131] Hew Strachanin mukaan strategian käytäntöön kuuluukin muutoksen ja ennalta-arvaamattomuuden hyväksyminen sodan luonteen (*character*) ja politikan muutoksen ristipaineessa.[132] Tiivistäen, strategian laatiminen ja toimeenpano ovat siis kaksi eri asiaa.

Kybertilan kontekstissa strategia on yleensä ymmärretty suunnitelmana tai konseptina, joissa määritellään valtiota kohtaavia uhkia, mahdollisuuksia, vastauksia, vastuita, resursseja ja visioita tulevaisuudesta.[133] Tämän työn ongelmanasettelun näkökulmasta tällainen määritelmä on liian kapea. Kyberstrategian määritelmän tulisi huomioida strategian laatimisen ja toimeenpanon prosessi ja se, että strategiaa tehdään aina ympäristöä ja muita toimijoita kohden. Nämä muut toimijat ovat sotilasstrategian eli kansallisen turvallisuuden avainkysymysten yhteydessä valtioita.[134] Strategiaan liittyy neuvottelua, painostusta, voimankäyttöä ja ympäristön muokkaamista.[135] Strategiaa siis ”tehdään” rauhan aikana, valmistautuessa sotaan ja sodan aikana. Siihen liittyvällä voimankäytöllä on omat muotonsa eri toimintaympäristöissä.[136] Strategia on kulttuurisidonnaista ja liittyy vahvasti turvallisuus- ja puolustuspoliittisten eliittien maailmankatsomukseen. Kyberstrategia on hyödyllistä määritellä taitoon (*art*) ja kokemukseen perustuvana käytäntönä ja tietoon pohjautuvana kykynä, joka mahdollistaa moninaisten resurssien, välineiden ja keinojen

---

[130] Yarger, Harry R.: *Strategic Theory for the 21st Century: The Little Book on Big Strategy*. Strategic Studies Institute, U.S. Army War College, Carlisle, PA, 2006, s. 21–23.

[131] Adler (1997); Joseph & Wight (2010). Ajatusta on soveltanut strategian käsitteeseen mm. Ionut Popescu (Popescu (2018)).

[132] Strachan, Hew: Strategy in Theory, Strategy in Practice. *Journal of Strategic Studies*, Vol. 42, No. 2 (2019), s. 171–190.

[133] Valerian, Jensen & Maness (2018), s. 9–10.

[134] Neoklassinen realismi ohjaa tässä kiinnittämään käsitteen muodostamisen valtioihin kansainvälisen järjestelmän päätoimijoina (Ripsman, Taliaferro & Lobell (2016)).

[135] Freedman (2013), s. xi–xii; International Telecommunications Union (ITU): *Global Cybersecurity Index (CGI) 2017.* [https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf], luettu 28.4.2020; Greiman, Virginia: Cyber Security and Global Governance. Teoksessa *Proceedings of the 14th European Conference on Cyber Warfare & Security*. Abouzakher, Nasser (ed.) University of Hertfordshire, Hattfield, 2015, s. 71–78.

[136] Gray (1999).

käytön vaikutuksen aikaan saamiseksi.[137] Näin ollen kyberstrategia voi pitää sisällään sotilaallisen voimankäytön ulottuvuuden, mutta mahdollistaa ei-sotilaallisten välineiden ja keinojen käytön. Kyberstrategia voidaan siis määritellä *kybervoiman jatkuvaksi käytön suunnitteluksi, sen käyttöön valmistautumiseksi ja sen käyttämiseksi sotilaallisin ja ei-sotilaallisin keinoin kybertoimintaympäristössä valtion turvallisuuspäämäärien saavuttamiseksi*. Käsite on näin sidoksissa voimankäytön menetelmiin (*ways*) määrätyssä ympäristössä ja selittää, miksi strategian tulokset ovat harvoin pysyviä ja joskus odottamattomia. Strategiaa tekevät muutkin ja sen ympäristöllä on oma vaikeasti hallittava, ajassa muuttuva luonteensa.[138] Suppeampana muotoiluna voidaan käyttää Timothy Thomasin ehdottamaa ”kyberteknologian ja siihen liittyvän osaamisen käyttöä suhteellisen voimaedun ja kontrollin (niin hyökkäyksellisen kuin puolustuksellisen) hankkimiseksi tai ylläpitämiseksi kilpailuympäristöässä.”[139]

2.2 Voimankäyttö, konfliktin vaiheet, ennaltaehkäisy, deterrenssi ja eskalaatio

Kyberstrategiaan ja -sodankäyntiin liittyvä tutkimus on ollut osiltaan spekulatiivista, koska empiiristä lähdeaineistoa on vielä tarjolla suhteellisen vähän. Yhtäkään kybersotaa ei ole vielä käyty, eikä yksikään yksittäinen kyberhyökkäys ole ylittänyt kansainvälisen yhteisön silmissä aseellisen voimankäytön kynnystä. Pääosa käsitteistä on lainattu aikaisemmista ilma-, meri ja ydinsodankäynnin teorioista. Tämä on kokemuksen karttuessa herättänyt yhä enemmän arvostelua.[140] Esimerkiksi Janeen Klingerin mukaan deterrenssiteoria on nauttinut hyväksyntää

[137] Ajatus seurailee Joseph Nyen pohdintoja voiman luonteesta (Nye 2011, s. 40–41).

[138] Tämä näkemys on peräisin Edward Luttwakin strategian paradoksaalisen logiikan käsitteestä. (Luttwak, Edward N. Strategy: *The Logic of War and Peace*. The Belknap Press of Harvard University Press, Cambridge, Massachusetts, 2001).

[139] Thomas, Timothy: Creating Cyber Strategists: Escaping the ‘DIME’ Mnemonic. *Defence Studies*, Vol. 14, No. 4 (2014), s. 370–393, s. 373.

[140] Aiheesta tarkemmin Libicki (2016); Lewis, James Andrew: *Rethinking Cybersecurity*. A Report of the CSIS Technology Policy Program. Rowman & Littlefield, New York, London, 2018; Whyte & Mazanec (2019); Sanger, David, E.: *The Perfect Weapon. War, Sabotage, and Fear in the Cyber Age*. Scribe, London, 2019; Clarke, Richard A. & Knake, Robert K.: *The Fifth Domain. Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Penguin Press, New York, 2019; Cimbala, Stephen J.: *The New Nuclear Disorder: Challenges to Deterrence and Strategy*. Routledge, London & New York, 2015, s. 109–110.

tieteellisenä teoriana ja näin sen ydinase-, kulttuuri- ja aikasidonnaisuus on jäänyt huomiotta myöhemmin sovelluksissa.[141]

Voimankäyttö on sidoksissa kontekstiinsa. Tässä työssä konteksti muodostuu valtioiden strategisesta ympäristöstä, jonka ajallista ulottuvuutta määrittelevät valtioiden väliset suhteet. *Valtioiden suhteet jaetaan rauhanomaiseen kilpailuun, kiristyneeseen kilpailuun, konfliktiin mukaan lukien sodan alkuvaihe ja sotaan*. Jaottelu perustuu yhdysvaltalaisen ja venäläisen ajattelun synteesiin.[142] Vaiheisiin liittyy määrättyjä uhkia kuten vakoilu ja sabotaasi, paikalliset konfliktit ja sisäiset levottomuudet, alueelliset sodat ja kansannousut sekä suurvaltojen välinen sota.[143] Rauhanomaisen kilpailun aikana valtiot ajavat kansallisia etujaan avoimesti yleisesti hyväksytyillä keinoilla hyväksyen yhteisen turvallisuuden (*common security*) toimintansa lähtökohdaksi. Kiristyneessä kilpailussa kansalliset intressit ovat osittain vastakkaisia, keinot usein ei-sotilaallisia ja päämäärät rajoitettuja. Konflikti voidaan määritellä voimankäytöksi tai sillä uhkaamiseksi, joka ei ylitä avoimen, julistetun sodan kynnystä. Konflikti voi ilmetä valtioiden tai valtioiden ja ei-valtiollisten toimijoiden välillä, joiden intressi ovat vastakkaiset. Konflikti on rajoittunut käytettävien keinojen ja välineiden sekä niiden mittakaavan osalta verrattuna sotaan. Sodan alkuvaihe viittaa rauhan ajan suorituskyvyillä suoritettaviin ensimmäisiin hyökkäys- ja puolustustoimiin. Sen aikana vastapuolet taistelevat rauhanaikana perustetuilla ja ryhmitetyillä joukoilla ennen lisävoimien perustamista ja ryhmittämistä. Sodan alkuvaiheen pääongelma on, miten muodostaa uskottava deterrenssi, sen pettäessä välttää yllätetyksi tuleminen ja miten mobilisoida lisävoima vastahyökkäystä ja vastustajan lyömistä varten.[144] Koska sodan alkuvaihe varjostaa voimakkaasti konfliktia, liitetään se sodan alkuvaiheeseen varsinaisen sodan sijaan. Sota on valtioiden välinen tila, jossa poliittisten päämäärien tavoittelemiseksi käytetään avointa sotilaallista voimaa.[145]

---

[141] Klinger, Janeen M.: *Social Science and National Security Policy. Deterrence, Coercion, and Modernization Theories*. Palgrave Macmillan, Cham, Switzerland, 2019.
[142] Kukkola (2020a); U.S. DoD JP 3-0 (2018); Kofman, Fink & Edmonds (2020).
[143] Kukkola (2020a), s. 361.
[144] Sodan alkuvaiheella on erityinen rooli venäläisessä sotataidollisessa ajattelussa. Ks. tarkemmin Kukkola (2020a), s. 111.
[145] Ks. valtiosuhteiden vaiheista ja sodasta Valeriano & Maness (2015), s. 31–33; Libicki (2016); Valeriano, Jensen & Maness (2018); Gray (1999); Gray (2007); Jordan, D., Kiras, James D. Lonsdale, David J., Speller, Ian, Tuck, Christopher & Dale, Walton: *Understanding Modern War. Cambridge University Press*. Cambridge University Press, Cambridge, 2008; Kaldor, Mary: *New and Old Wars: Organized Violence in a Global Era*

Kybersota määritellään, eittämättä teoreettiseksi, sodan muodoksi, joka käydään vain kybertilassa tai sen kautta.[146] Kybersodankäynti on tarkoituksellisten ja vahinkoa tuottavien tietoverkkohyökkäyksien käyttämistä vastustajan siviili- tai sotilasinfrastruktuuria ja joukkoja vastaan voimapolitiikan osana.[147] Kyberkonflikti on laaja-alainen ja poliittinenkin käsite. Eräiden teoreetikkojen mukaan maailma elää jo jatkuvan kyberkonfliktin vaihetta.[148] Käsite muuttuu digitaalisen toimintaympäristön, sodan kuvan ja suurvaltojen strategisen kilpailun muutoksen mukana.[149]

Edelleen on huomioitava, että valtioiden lisäksi kybertoimintaympäristössä on muitakin toimijoita. Ne ymmärretään tässä työssä joko valtioiden työkaluiksi (*proxy*) tai valtiovaltaa vastustaviksi valtion sisäisiksi toimijoiksi, jotka voivat toiminnallaan heikentää valtiota suhteessa muihin valtioihin.[150] Näin siksi, että työn keskiössä ovat valtioiden väliset suhteet ja kybertilaan liittyvät strategiset vaikutukset.
Vaikkakin termi kyberase on osittain vanhahtava ja harhaanjohtava, käytetään sitä tässä työssä synonyyminä kyberhyökkäykselle tarkoitettaessa aseena (välineenä) ymmärrettävää koodia ja/tai tietoteknistä järjestelmää, joka on tarkoitettu aiheuttamaan vahinkoa osana valtioiden voimapolitiikkaa.[151] Kyberhyökkäys (*Computer Network Attack*) on myös monitulkintainen käsite. Yksinkertaistaen se määritellään tässä työssä *kybertoimintaympäristössä tai sen avulla tapahtuvaksi toiminnaksi, jolla*

(3rd edition). Stanford University Press, Stanford, 2012; Kane, Thomas M. & Lonsdale, David J.: *Understanding Contemporary Strategy*. Routledge, New York, 2012; Sloan (2012); Strachan (2013).

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

[147] Liff (2012), s. 401–428.

[148] Libicki (2016); Whyte & Mazanec (2019).

[149] Taillat, Stéphane: Disrupt and Restraint: The Evolution of Cyber Conflict and the Implications for Collective Security. *Contemporary Security Policy*, Vol. 40, No. 3 (2019), s. 368–381, s. 369.

[150] Whyte ja Mazanec jaottelevat toimijat tarkemmin hakkereihin, skriptipentuihin, kyberterroristeihin, sijaistoimijoihin, haktivisteihin, viidenteen kolonnaan (*subversives*), rikollisiin ja kaunaisiin työntekijöihin. (Whyte & Mazanec (2019), s. 170–171). Maurer (2018); Sanger (2018).

[151] Rid, T. & McBurney, P.: Cyber-Weapons. *The RUSI Journal*, Vol. 157, No. 1 (2012), s. 6–13, s. 7; Schmitt (2017), s. 452–453, s. 564; Libicki, Martin C.: *Cyberdeterrence and Cyberwar*. RAND, Santa Monica, 2009; Slayton (2017); Rid (2017); Fischerkeller, Michael: Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies. *Survival*, Vol.59, No.1 (February-March 2017), s. 103–134, s. 114–115.

pyritään vahingoittamaan eli häiritsemään, kiistämään, rapauttamaa tai tuhoamaan informaatiojärjestelmiä tai niissä olevan informaation luottamuksellisuutta, eheyttä tai saatavuutta.[152] Tietoverkko- tai tietojärjestelmävakoilu (*Computer Network Exploitation*) ei ole kyberhyökkäys. Sillä ei pyritä aikaansaamaan välitöntä vahinkoa järjestelmille tai tiedolle vaan hankkimaan tietoa tai mahdollistamaan sen hankkiminen.[153] Tietoverkkovakoilu tukee kyberstrategiaa valtioiden välisten suhteiden kaikissa vaiheissa.

Kyberpuolustus (*Computer Network Defence*) viittaa kotimaisittain maanpuolustukselliseen kyberturvallisuuden, eli kybertoimintaympäristön luottamuksen ja toiminnan turvaamisen, osa-alueeseen, joka pitää sisällään tiedustelun, vaikuttamisen ja suojautumisen.[154] Tässä työssä kyberpuolustus ja siihen liittyvä toimintaa ymmärretään *valtion ja yhteiskunnan kriittisten tietoverkkojen, tietojärjestelmien ja niiden sisältämän tiedon aktiivisena ja passiivisen suojaamisena valtioiden voimankäyttöön liittyvältä vihamieliseltä vaikuttamiselta*. Näin ollen kyberpuolustus ei koske vain asevoimien verkkoja tai ole vain asevoimien toteuttamaa toimintaa.[155] Martti Lehdon ja Jarno Limnéllin kybersuoja -käsitettä mukaillen kyberpuolustus on toimintojatkumo, joka koostuu tiedon, palvelujen ja järjestelmien suojaamisesta, niiden ja niissä tapahtuvan toiminnan valvonnasta, vihamielisen toiminnan havaitsemisesta, omissa verkoissa ja ulkopuolissa verkoissa tapahtuvasta reagoinnista, haitallisten vaikutusten minimoinnista sekä palautumisesta.[156] Kyberpuolustus on jossain muodossa toiminnassa kaikissa valtiosuhteiden vaiheissa ja osa ennaltaehkäisyä, deterrenssiä,

---

[152] Kyberaseen määritelmästä ks. Brangetto, Pascal, Veenendaal, Matthijs A.: Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. Teoksessa *8th International Conference on Cyber Conflict: Cyber Power*. Pissanidis N., Rõigas H. ja Veenendaal, M. (Eds.) CCD COE, Tallinn, 2016, s. 113–126; Libicki (2009), s. 23; McGraw, Gary & Fick, Nathaniel: Separating Threat from the Hype: What Washington Needs to Know about Cyber Security. Teoksessa *America's Cyber Future Security and Prosperity in the Information Age volume II*. Lord, Kristin M. & Sharp, Travis (ed.) Center for New American Security, 2011, s. 43–53, s. 46; Friis, Karsten & Ringsmose, Jens: *Conflict in Cyber Space. Theoretical, strategic and legal perspectives*. Routledge, New York, 2016; Sanastokeskus TSK (2018); Laari (2019).

[153] Andress, Jason & Winterfeld, Steve: *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners. (*2nd ed*.)* Syngress, Waltham. 2014, s. 169–171.

[154] Sanastokeskus TSK (2018); Laari (2019).

[155] Andress & Winterfeld (2014), s. 196; Liff (2012), s. 404.

[156] Lehto, Martti & Limnéll, Jarno: Kybersodankäynnin kehityksestä ja tulevaisuudesta. *Tiede- ja Ase*, Vol. 75 (2017), s. 179–212, s. 196; U.S. DoD JP 3-12, s. viii, s. II-4.

pakottamista ja raa'an voiman käyttöä ja siihen vastaamista. Samoin valtion kyky kyberhyökkäykseen on osa voimankäyttöä ja sillä uhkaamista. Tässä esitetyt kyberhyökkäyksen ja -puolustuksen käsitteet eivät ota kantaa niiden toteuttajaan.

Kyberhyökkäys ja - puolustus ovat voimankäytön operatiivisia ja taktisia muotoja. Strategisella tasolla voimankäytön eri muodot ovat sidoksissa konfliktin vaiheisiin, mutta niillä on myös itsenäinen luonteensa. Voimankäytön muodoista lievin on konfliktin ennalta ehkäisy. *Konfliktin ennaltaehkäisyllä osana valtion turvallisuuspolitiikkaa tarkoitetaan tässä työssä potentiaalisen uhan neutralointia kaikilla käytettävissä olevilla toimilla niin, että suoraa aseellisen voiman käyttöä tai sillä uhkaamista ei tarvita*.[157] Määritelmä perustuu osiltaan siihen, että aseellinen voima kuuluu puolustuspolitiikan ja strategian alaan. Puolustuspolitiikka määritellään tässä työssä siksi osaksi valtion politiikkaa, joka käsittelee voiman käyttöä tai sillä uhkaamista, mukaan lukien uhkien arvioinnin, suunnittelun ja valmistautumisen ja voimankäytön tai sillä uhkaamisen toimeenpanon. Sotilasstrategia on näin ollen alisteinen puolustuspolitiikalle. Konfliktin ennaltaehkäisy on siis laajasti valtion politiikan alaan kuuluva muoto, vaikkakin se on oleellisesti kiinnittynyt voimankäyttöön. Sen kontekstina on rauha tai kiristynyt kilpailutilanne, jossa uhka ei ole vielä konkretisoitunut.

Konfliktin ennaltaehkäisy liittyy tiedusteluun potentiaalisten uhkien havaitsemiseksi, viestintään, suostutteluun, sitouttamiseen, liittolaispolitiikkaan, diplomatiaan ja ei-sotilaalliseen painostukseen ja sillä uhkaamiseen. Näitä kutsutaan tässä työssä taivutteluksi (*persuasion*).[158] Taivuttelu ymmärretään laajemmin kuin "positiivisena vetovoimana." Se sisältää painostamisen ilman suoraa voimankäyttöä tai sillä uhkaamista.

Yhdysvaltojen, Venäjän ja Kiinan turvallisuuspoliittiset doktriinit erottavat konfliktien ennaltaehkäisyn deterrenssistä ja sodankäynnistä erillisenä toimintona, vaikkakin jokaisella on selvästi oma tulkintansa ennaltaehkäisyn muodoista, toimijoista, tavoitteista ja päämääristä.[159]

---

[157] Ks. turvallisuuden takaamisesta Miller, Benjamin: The Concept of Security: Should it be Redefined? *The Journal of Strategic Studies*, Vol. 24, No. 2 (2001), s. 13–42; Jervis, R.: Dilemmas About Security Dilemmas. *Security Studies*, Vol. 20, No. 3 (2011), s. 416–423.Venäläisistä näkemyksistä Forsström (2019).

[158] Taivuttelusta ks. Nye (2011).

[159] Garthoff, Raymond L.: *Deterrence and the Revolution in Soviet Military Doctrine*. The Brookings Institution, Washington, D.C., 1990; Adamsky (2018); Thomas, Timothy:

Ennaltaehkäisy, deterrenssi ja pakottaminen ovat siis toiminnassa yhtä aikaa, vaikkakin deterrenssi ja pakottaminen perustuvat sotilaallisen voimakäytön uhkaan, jossa väkivallan uhalla pyritään vaikuttamaan potentiaalisen vastustajan käytökseen.[160] Kybertoiminnan osalta konfliktien ennaltaehkäisyn voi ajatella liittyvän tiedusteluun, ennakkovaroituksen hankkimiseen, taivutteluun, kansainvälisten normien rakentamiseen sekä toimintaympäristön muokkaamiseen potentiaalisten uhkien ehkäisemiseksi.[161]

Azar Gatin mukaan deterrenssi eli kostaminen tai sillä uhkaaminen on ollut ihmisen selviytymiskeino läpi historia.[162] Tavoitteiden saavuttamisen kiistämisellä tai rankaisulla uhkaaminen on järjestyneen ihmiskunnan ikäinen ilmiö.[163] Deterrenssi- ja pakoteteoria sen sijaan syntyi 1940–1950-luvuilla Yhdysvalloissa. Se keskittyi kylmän sodan aikana alun perin

---

Russian Military Thought: Concepts and Elements. MITRE Corporation, McLean VA, 2019. [https://www.mitre.org/publications/technical-papers/russian-military-thought-concepts-and-elements], luettu 4.5.2020; Forsström (2019); Kukkola (2020a); Lindsay, Cheung & Reveron (2015); Ministry of Foreign Affairs of the People's Republic of China: *China's Policies on Asia-Pacific Security Cooperation, January 2017.* [https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1429771.shtml], luettu 4.5.2020; The White House: *National Security Strategy of the United States of America, December 2017.* [https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf], luettu 4.5.2020.

[160] Näiden käsitteiden erottelu ei ole ongelmatonta ks. Joseph Nyen ja Richard Harknettin kirjeenvaihto (Harknett, & Nye (2017)).

[161] Libicki (2009) & (2016); Nye (2016/2017); Lewis (2018); Barrinha, André & Renard, Thomas: Cyber-diplomacy: The Making of an International Society in the Digital Age. *Global Affairs*, Vol.3, No.4-5 (2017), s. 353–364; Klimburg, Alexander: Mixed Signals: A Flawed Approach to Cyber Deterrence. *Survival*, Vol.62, No.1 (2020), s. 107–130; Rudner, Martin: Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge. *International Journal of Intelligence and CounterIntelligence*, Vol.26, No.3 (2013), s. 453–481; Brantly, Aaron Franklin: *The Decision to Attack. Military and Intelligence Cyber Decision-Making*. University of Georgia Press, Athens, Georgia, 2016; Robinson, Linda, Helmus, Todd C., Cohen, Raphael S., Nader, Alizera, Radin, Andrew, Magnuson, Madeline & Migacheva, Katya: *Modern Political Warfare: Current Practices and Possible Responses*. RAND, Santa Monica, Calif., 2018; Libicki, Martin C.: The Conversion of Information Warfare. *Strategic Studies Quarterly*, Vol. 11, No. 1, (Spring 2017), s. 49–65.

[162] Gat, Azar: War in Human Civilization. Oxford University Press, Oxford, 2006, s. 92–93.

[163] Gat, Azar: So Why Do People Fight? Evolutionary Theory and the Causes of War. *European Journal of International Relations*, Vol. 15, No. 4 (2009), s. 571–599; Cioffi-Revilla, Claudio: Origins and Age of Deterrence: Comparative Research on Old World and New World Systems. *Cross-Cultural Research*, Vol. 33 No. 3 (August 1999), s. 239–264.

ydinaseiden käytettävyyteen ja suurvaltasuhteisiin, mutta laajeni käsittämään myös tavanomaisen sotilaallisen voiman.[164] 1990-luvulta lähtien alettiin tutkia deterrenssin toimivuutta terroristeja, ei-valtiollisia ja sijaistoimijoita vastaan. 2000-luvulla teorian toimivuutta on tarkasteltu informaatio- ja kybertilan uhkien kontekstissa. Koettu sodan ja rauhan välisen rajan hämärtyminen valtioiden välisissä suhteissa on synnyttänyt pyrkimyksiä laajentaa deterrenssiteoriaa ei-sotilaallisten toimien piiriin. Samalla on syntynyt räätälöidyn deterrenssin (*tailored deterrence*) käsite, joka perustuu näkemykseen siitä, että pelote pitää rakentaa määrättyä tilannetta, toimijaa tai uhkaa varten. Toisaalta uhkakuvien laajentuminen on tuottanut toimintaympäristöjen rajat ylittävän deterrenssin (*cross-domain deterrence*) käsiteen. Se liittyy toisistaan poikkeavien menetelmien ja ympäristöjen vuorovaikutukseen.[165]

Neuvostoliitto ei tuottanut kylmän sodan aikana deterrenssiteoriaa vastaavaa käsitekokonaisuutta.[166] Sen sijaan Venäjällä on 1990-luvun lopulta alkaen omaksuttu ja muokattu läntisestä teoriasta strategisen deterrenssin (*strategitšeskoe sderživanie*) käsite. Käsite on saavuttanut keskeisen aseman Venäjän kansallisessa turvallisuusajattelussa. Se perustuu ajatukseen uhkien ennaltaehkäisemisestä, sodan välttämisestä ja konfliktin kulun ohjaamisesta sotilaallisin ja ei-sotilaallisin keinoin. Käsite sisältää turvallisuusympäristön muokkaamisen poikkihallinnollisin toimenpitein, kiistämis- ja rankaisudeterrenssin ylläpitämisen sekä sotaan varautumisen ja voimankäytön. [167] Myös Kiina on omaksunut deterrenssin käsitteen, vaikkakin se poikkeaa läntisistä näkemyksistä ja on lähempänä venäläistä strategisen deterrenssin käsitettä eli sisältää ei-sotilaallisia elementtejä ja pakottamista eri keinoin.[168] Lisäksi niin Venäjän kuin

---

[164] Ks. Biddle, Tami Davis: Coercion Theory: A Basic Introduction for Practitioners. *The Strategist*, Vol. 3, No. 2 (Spring 2020). [https://tnsr.org/2020/02/coercion-theory-a-basic-introduction-for-practitioners/], luettu 1.5.2020.

[165] Michel, Leo & Pesu, Matti: *Strategic Deterrence Redux. Nuclear Weapons and European Security*. FIIA Report, September 2019/60, Helsinki, 2019, s. 136; Schelling (2008); Knopf, Jeffrey W.: The Fourth Wave in Deterrence Research. *Contemporary Security Policy*, Vol. 31, No. 1 (2010), s. 1–33; Garthoff (1990); Kaplan, Fred: *The Wizards of Armageddon*. Stanford University Press, Stanford, California, 1983; Gartzke, Eric & Lindsay, Jon R.: *Cross-Domain Deterrence: Strategy in an Era of Complexity*. Oxford University Press, New York, 2019.

[166] Garthoff (1990), s. 151.

[167] Forsström (2019); Kukkola (2020a); Kofman, Fink & Edmonds (2020).

[168] Heath, Timothy R.: An Overview of China's National Military Strategy. Teoksessa *China's Evolving Military Strategy*. McReynolds, Joe (ed.) The Jamestown Foundation, Washington, D.C., 2016, s. 12–45; Babiarz, Renny: The People's Nuclear Weapon:

Kiinankin voimassa olevaa sotilasstrategiaa kutsutaan ”aktiiviseksi puolustukseksi”, joka molempien tapauksessa perustuu todennettujen uhkien sotilaalliseen ennaltaehkäisyyn.[169] Deterrenssi on siis kulttuuri- ja aikasidonnainen käsite. Se on myös tulkinnallinen käsite. Yhdysvaltojen, Venäjän ja Kiinan tulkinnat toistensa deterrenssistrategioista ohjaavat niiden omaa teoriaa ja toimintaa.

Englannin kielen sana *deterrence* on käännetty suomeksi joko pidäkkeeksi tai pelotteeksi. Pentti Forsströmin mukaan edellisessä korostuu vaikutusfunktio ja jälkimmäisessä tavoite eli vastustajassa aiheutettu tila.[170] Puhuttaessa suurvaltojen ydinasestrategiasta käyttöön on vakiintunut pelotteen käsite, mutta puhuttaessa Suomen puolustuspolitiikasta on käytetty pidäkkeen käsitettä kuvattaessa uskottavaa puolustusta.[171] Jan Hanska esittää pidäkkeen termin käyttöä viitattaessa suomalaiseen deterrenssin eri muotoja yhdistelevään malliin.[172] Koska sekä termit pidäke että pelote voidaan käsittää deterrenssin erityisiksi muodoiksi, käytetään tässä tutkimuksessa termiä deterrenssi yleisen ilmiön kuvaamiseksi. Termiä pakottaa tai pakote käytetään englanninkielisen termin *compellence* tilalla. Voimapolitiikka viittaa englanninkieliseen termiin *coercion*, joka ymmärretään deterrenssin ja pakottamisen yläkäsitteeksi.[173]

Thomas Schelling mukaan voimapolitiikka poikkeaa raa'asta voimasta (*brute force*), joka perustuu yksipuoliseen tuhoamiseen tai haltuun ottamiseen sotilaallisella voimankäytöllä. Voimapolitiikassa on aina

---

Strategic Culture and the Development of China's Nuclear Weapons Program. *Comparative Strategy*, Vol. 34, No. 5 (2015), s. 422–446; Adamsky, Dima: *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the USA, and Israel*. Stanford University Press, Stanford, 2010; Герасимов, Валерий: Развитие военной стратегии в современных условиях. Задачи военной науки. *Вестник Академии военных наук*, № 2 (67) 2019, с. 6–1.

[169] Blasko, Dennis J.: China’s Evolving Approach to Strategic Deterrence. Teoksessa *China’s Evolving Military Strategy*. McReynolds, Joe (ed.) The Jamestown Foundation, Washington, D.C., 2016, s. 279–297.

[170] Forsström (2019), s. 86.

[171] Ks. Esim. Blombergs, Fred (toim.): *Suomen turvallisuuspoliittisen ratkaisun lähtökohtia*. Maanpuolustuskorkeakoulu, Julkaisusarja 1, No. 4. Maanpuolustuskorkeakoulu, Helsinki, 2016; Valtioneuvoston kanslia: *Valtioneuvoston puolustusselonteko*. VNS 3/2017 vp. Valtioneuvoston kanslia, Helsinki 2017.

[172] Hanska, Jan: Pelotetta vai pidäkettä? Deterrenssiteorian käytäntöä pienen valtion näkökulmasta. *Tiede ja Ase*, Vol 2019, No. 1, s. 42–70, s. 58–59.

[173] Schelling (2008); Michel & Pesu (2019); Hanska (2019).

mukana neuvottelun elementti.[174] Kohde pyritään kustannusten (kivun) määrää ja todennäköisyyttä (pelkoa) manipuloimalla joko saamaan pidättäytymään jostain toiminnasta, keskeyttämään toiminta tai ryhtymään siihen. Pakottaminen viittaa pyrkimykseen saada kohde tekemään jotain, mitä se ei muuten tekisi. Deterrenssi eli potentiaalisen vastustajan toiminnasta pidättäytyminen voidaan saada aikaiseksi joko uhkaamalla rangaistuksella (*deterrence by punishment*) tai antamalla kohteen ymmärtää, että se ei hyödy toiminnastaan (*deterrence by denial*). Oleellista deterrenssissä on kyvykkyys, uskottavuus, määrätty epävarmuus ja viestintä. Kohteen on tiedettävä ja ymmärrettävä uhan olemassaolo ja luonne. Deterrenssin perusidea on vaikuttaa vastustajan hyötykustannuslaskelmiin, joten lopullinen päätös deterrenssiin reagoimisessa on kohteella. Taustaoletuksena on kohteen rationaalisuus ja osapuolten jakama intressi välttää sota, jos mahdollista. Ongelmana on, että nykyisen käsityksen mukaan kohteen eli valtiojohdon ajatteluprosessia ei voida täydellisesti ennustaa.[175] Yleisesti sekä deterrenssi että pakottaminen perustuvat siihen, että kohde uskoo välttyvänsä seurauksilta, jos toimii tai jättää toimimatta halutulla tavalla. Uskottavuutta voidaan tehostaa osoittamalla, että uhkaaja on valmis tekemään uhrauksia jo ennen kohteen reagointia tai se sitoutuu julkisesti ”punaisiin viivoihin” eli sitoo kätensä. Koska deterrenssi voi kärsiä liian selkeistä kynnyksistä, joiden alla vastustaja voi toimia vapaasti, voidaan kynnyksiin liittää määrittelemättömyyttä eli epävarmuutta.[176]

Schellingin teoria pyrkii kuvaamaan kovan, sotilaallisen voiman käytön muotoja, ei varsinaisesti strategioita. Myöhemmin näitä muotoja on kuitenkin täydennetty strategioilla, jotka liittyvät voiman osoittamiseen (pelottelu tai esittely) tai tarkempiin käyttömuotoihin (vakoilu, häiritseminen, kuluttaminen, kiistäminen, kiristäminen ja kontrolli), riskin manipulointiin, ja määrättyihin kohteisiin, esimerkiksi johtamiseen, vaikuttamiseen (*decapitation*).[177] Deterrenssiteoria eri käsitteineen on

---

[174] Schelling (2008), s. 2–5.
[175] Schelling (2008); Kaplan (1983); Snyder, Glenn: *Deterrence and Defence*. Princeton University Press, Princeton, 1961; Pape (1996); Freedman (2013), s. 159; Libicki (2016); Freedman, Lawrence: *The Evolution of Nuclear Strategy* (3rd ed.) Palgrave Macmillian, New York, 2003, s. 303; Jervis, Robert: Review: Deterrence Theory Revisited. *World Politics*, Vol. 31, No. 2 (January 1979), s. 289–324; Knopf (2010).
[176] Borghard, Erica D. & Lonergan, Shawn W.: The Logic of Coercion in Cyberspace. *Security Studies*, Vol. 26, No. 3 (2017), s. 452–481.
[177] Pape (1996); Nye (2011), s. 21; Nye (2016/2017), s. 44–71; Borghard & Lonergan (2017); Valeriano, Jensen & Maness (2018), s. 33-35.

tarkoitettu strategispoliittisen tason ilmiöiden ymmärtämiseen. Taktisella tasolla vaikuttaa pelkästään kova voima.[178] Vaikka deterrenssiteorian logiikka on yleisesti tunnustettu pitäväksi, sen käytännön vaatimukset ja toteuttaminen jakavat voimakkaasti näkemyksiä.[179]

Kyberdeterrenssin sisältö ja toimivuus on pitkään ollut kiistanalainen aihe.[180] Deterrenssiteoria kehitettiin alun perin ydinaseiden nopean, massiivisen ja peruuttamattoman tuhovoiman ymmärtämiseksi ja hallitsemiseksi. Tästä se on laajentunut koskemaan tavanomaisen aseellisen voiman hallintaa fyysisissä toimintaympäristöissä ja viime aikoina kyber- ja informaatioympäristöihin.[181] Yleisimmät argumentit kyberdeterrenssin toimimattomuudesta ovat seuraavat. Kyberaseet (vast.) eivät vertaudu vaikutuksiltaan ydinaseisiin, joihin deterrenssiteoria alun perin perustuu. Kyberhyökkäyksiä on vaikeaa ja aikaa vievää attribuoida, joten rankaisupelotteen toimeenpano sen poliittisen legitimiteetin vaatimassa aikaraamissa voi olla vaikeaa. Valtiot ja ei-valtiolliset toimijat todennäköisesti reagoivat deterrenssiin eri tavoin. Suorituskykyjen salaaminen heikentää pelotteen uskottavuutta, koska kyberaseilla on vaikea uhata paljastamatta todellisia suorituskykyjä. Kyberaseita on vaikea valmistaa varastoon, ne eivät säily hyvin ja niiden vaikutusta on vaikea toistaa, koska kohteen on suhteellisen helppo korjata haavoittuvuutensa ja muuttaa järjestelmiään. Uhkaamisen merkitys siis heikkenee ja viestittäminen vaikeutuu. Deterrenssin suhteellisuutta on vaikea mitata, koska potentiaalisista kohteista on vaikea saada riittävästi tietoa. Tämä voi johtaa tahattomaan tai vahingossa tapahtuvaan eskalaatioon. Kyberhyökkäysten osalta puuttuu yhteisymmärrystä ja läpinäkyvyyttä lisäävä kansainvälinen normisto, joka edes auttaisi deterrenssiviestintää. Lisäksi kyberhyökkäyksellä uhkaaminen edellyttää valmistelua, joka saatetaan tulkita varsinaiseksi hyökkäykseksi. Kyberdeterrenssi ei myöskään voi rakentua uhan tasapainon (*deterrence stability*) varaan. Molemminpuolista varmaa tuhoa (tai sekasortoa *disruption*) ei voida taata tai pelotetta rakentaa niin, ettei se muodostaisi toiselle osapuolelle

[178] Schelling (2008), s. 5.
[179] Glaser, Charles L.: Why do Strategists Disagree about the Requirements of Strategic Deterrence? Teoksessa *Nuclear Arguments: Understanding the Strategic Nuclear Arms and Arms Control Debates*. Eden, Lynn & Miller, Steven E. (Eds.) Cornell University Press, Ithica, NY, 1989, s. 109–171.
[180] Ks. Libicki (2009); Geist, Edward: Deterrence Stability in the Cyber Age. *Strategic Studies Quarterly*, Vol. 9, No. 4 (Winter 2015), s. 44–61; Valeriano, Jensen & Maness (2018).
[181] Hanska (2019), s. 53.

turvallisuusdilemmaa[182]. Vastapuolen ”kyberaseita” on mahdoton arvioida tai laskea ja niiden vaikutusta kohteessa tai sen ympäristössä riittävällä luotettavuudella ennustaa.[183] Näin ollen deterrenssin perustekijöitä eli kyvykkyyttä, uskottavuutta ja viestittämistä on hankala saada toimimaan tehokkaasti.

Rankaisuun perustuva kyberdeterrenssi vaikuttaa nykykäsityksen mukaan vaikealta toteuttaa. Sen sijaan kiistämiseen perustuva deterrenssi vaikuttaa lupaavammalta. Teknologian ja attribuutiomenetelmien kehitys, saadut kokemukset todellisista kyberoperaatioista ja kyberturvallisuuden tekniikoiden ja periaatteiden kehittyminen ovat tasoittaneet ”aina läpi pääsevän” hyökkäyksen ja puolustuksen eroa.[184] Todellista tuhoa aikaansaavien kyberaseiden kehittämisen on ymmärretty vaativan valtiotason resursseja sekä pitkää valmistelua, mikä rajoittaa ei-valtiollisten toimijoiden suorituskykyä. Kyberaseiden on katsottu soveltuvan lähinnä ensi-iskuaseiksi ja menettävän nopeasti käyttökelpoisuutensa konfliktin käynnistyttyä. Niiden strategisia vaikutuksia on alettua kyseenalaistaa 2010-luvulta alkaen.[185] Puolustuksen

---

[182] Turvallisuusdilemmasta ks. Van Evera, Stephen: Offense, Defense, and the Causes of War. *International Security*, Vol. 22, No. 4 (Spring 1998), s. 5–43; Jervis (2011); Slayton (2017); Lantis, Jeffrey S.: Strategic Culture and Tailored Deterrence: Bridging the Gap between Theory and Practice. *Contemporary Security Policy*, Vol. 30, No. 3 (2009), s. 467–485.

[183] Kyberdeterrenssin kritiikistä ks. Meakins, Joss: *Living in (Digital) Denial: Russia's Approach to Cyber Deterrence*. Euro-Atlantic Security Report. European Leadership Network, 2018. [https://www.europeanleadershipnetwork.org/report/living-in-digital-denial-russias-approach-to-cyber-deterrence/], luettu 29.4.2020; Leuprecht, Christian, Szeman, Joseph & Skillicorn, David B.: The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity. *Contemporary Security Policy*, Vol. 40, No. 3 (2019), s. 382–407; Geist (2015); Lantis (2009); Libicki (2009), s. xiv–xix; Liff (2012), s. 417–422; Andress & Winterfeld (2014), s. 92–96; Hare, F.: The Significance of Attribution to Cyberspace Coercion: A Political Perspective. In *4th International Conference on Cyber Conflict*. C. Czosseck, R. Ottis & K. Ziolkowski (eds.) NATO CCD COE Publications, Tallinn, 2012, s. 125–140; Valeriano, Jensen & Maness (2018); Brantly, Aaron F.: The Cyber Deterrence Problem. Teoksessa *10th International Conference on Cyber Conflict CyCon X: Maximising Effects*. Minárik, T., Jakschis, R. & Lindström, L. (eds.) NATO CCD COE, Tallinn, 2018, s. 31–53; Chen (2017).

[184] Libicki (2017); Lewis (2018); Sharp, Travis: Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony. *The Journal of Strategic Studies*, Vol. 40, No. 7 (2017), s. 898–926.

[185] Gartzke, Erik J. & Lindsay, Jon R.: Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace. *Security Studies*, Vol. 24, No. 2 (2015), s. 316–348; Libicki (2016); Rid (2017), s. 167-179; Gartzke, Erik: Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth. *International Security*, Vol. 38, No. 2 (Fall 2013), s. 41–

on katsottu hyötyneen muun muassa uhkatiedon lisääntymisestä ja jakamisesta, turvallisuusasenteiden muutoksesta, tekoäly[186]- ja pilviteknologian kehityksestä, valvonta- ja torjuntajärjestelmien kehityksestä salauksen käytön yleistymisestä, ja kehittyneistä harhautusmenetelmistä.[187] Kaikki nämä seikat lisäävät hyökkääjän kustannuksia ja tavoitteiden saavuttamisen epävarmuutta. Eräät ovat jopa esittäneet kybertilan hallinnan ja käytön kiistämisen olevan mahdollista.[188] Äärimmäisenä keinona voisi olla koko Internetin uudelleen rakentaminen attribuution mahdollistavien protokollien varaan.[189] Koska puolustus on kuitenkin edelleen haavoittuvainen ja hyökkääjän uskoa hyökkäyskykyyn vaikea ehkäistä, kiistämiseen perustuva deterrenssi on alkanut rakentua resilienssin eli vaikutusten kiistämisen varaan.[190]

Kyberresilienssi tai kybersietoisuus on määritelty ”*kyvyksi ennakoida, sietää, palautua, ja sopeutua haitallisiin olosuhteisiin, stressiin, hyökkäyksiin tai muutoksiin järjestelmissä, joihin kuuluu*

73; Liff (2012); Nye (2016/2017), s. 51; Rid & Buchanan (2015); Lin (2016); Lewis (2018); Lindsay, Jon R: Stuxnet and the Limits of Cyber Warfare. *Security Studies*, Vol.22, No.3 (2013), s. 365–404; Valeriano, Jensen & Maness (2018), s. 87; Rattray (2001); Geers, Kenneth: Strategic Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, 2011; Clark & Knake (2010); Sharp (2017); Hodgson, Quentin E.: Understanding and Countering Cyber Coercion. Teoksessa *10th International Conference on Cyber Conflict CyCon X: Maximising Effects*. Minárik, T., Jakschis, R. and Lindström, L. (eds.) NATO CCD COE, Tallinn, 2018, s. 73–88; Chen, Jim: Effectively Exercising Deterrence in the Cyber Domain. Teoksessa *Proceedings of the 13th International Conference on Cyber Warfare and Security 8-9 March 2018*. Chen, Jim Q. & Hurley, John S. (ed.) National Defense University, Washington D.C., 2018, s. 120–125; Rid (2017); Stone (2013); Valeríano & Maness (2018); Smeets, Max: A matter of time: On the transitory nature of cyberweapons. *Journal of Strategic Studies*, Vol.41, No.1-2 (2018), s. 6–32; Taillat (2019); Green, James A (ed.): *Cyber Warfare: A multidisciplinary analysis*. Routledge, New York, 2015; Stevens (2012); Lin, Herbert: Attribution of Malicious Cyber Incidents: From Soup to Nuts. *Journal of International Affairs*, Vol. 70, No. 1 (Winter 2016), s. 75–137.

[186] Tekoäly nykyisessä tilassaan on edelleen kokoelma teknologiaa, laskentatekniikoita ja algoritmeja, joka kykenee oppimaan ohjattuna. Yksi määritelmä tekoälytoimijalle (AGI): “*artificially intelligent actors that have the ability to imitate, and outperform, human intelligence, act upon their own, distinct from and without further human intervention*.” (Van Rijmenam, Mark & Logue, Danielle: Revising the ‘Science of the Organisation’: Theorising AI Agency and Actorhood. *Innovation*, 2020 DOI: 10.1080/14479338.2020.1816833, s. 3).

[187] Geist (2015); Libicki (2016); Clarke & Knake (2019).

[188] Lawlor Russell (2015), s. 156.

[189] Stevens (2012).

[190] Tästä ajatuskulusta ks. Libicki (2016), s. 269–272.

kyberresursseja."[191] Käsitteen perusideana on, että järjestelmät kykenevät palautumaan nopeasti tai jatkamaan rajoitetusti toimintaansa huolimatta onnistuneista hyökkäyksistä. Näin vaikutukset (riski) minimoidaan ja vastustajan kulut maksimoidaan. Hyökkäyksen onnistumisen todennäköisyys pysyy ennallaan, mutta vaikutukset minimoidaan. Gratzken ja Lindsayn mukaan resilienssiin kuuluu myös hyökkääjän harhauttaminen.[192] Kyberresilienssi siis muuttaa melkoisesti kiistämiseen perustuvan deterrenssin käsitettä. Sen heikkoudeksi on esitetty passiivisuutta eli hyökkääjän toiminnan vapautta.[193] Vaikka kyberresilienssin käsite esiintyy puhtaimmillaan läntisissä teksteissä, on sillä vastaavuutensa venäläisessä ja kiinalaisessa ajattelussa. Ilmiöllä on siis kulttuurien rajat ylittävää objektiivista sisältöä.[194] Kyberresilienssiä käsitellään tarkemmin luvussa 2.5.4.

Läntiseen kyberdeterrenssiajatteluun on viime vuosina liitetty nk. aktiivinen tai etupainotteinen puolustus.[195] Se tarkoittaa vastustajan verkkoihin tunkeutumista, tiedustelutiedon keräämistä ja valmistautumista toteuttamaan ennaltaehkäisevä (*preventive*) tai puolustuksellinen ensi-isku (*preemptive*).[196] Ensimmäinen iskutyyppi perustuu ajatukselle aloittaa sota

---

[191] Ross, Ron, Graubart, Richard, Bodeau, Deborah & Rosalie Mcquaid: *Systems Security Engineering Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems*. Draft NIST Special Publication 800-160 Volume 2, 2018. [https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf], luettu 1.5.2020. Ks. myös Vlacheas, Panagiotis T., Stavroulaki, Vera, Demestichas, Panagiotis, Cadzow, Scott & Slawomir Gorniak: *Ontology and taxonomies of resilience*. ENISA, 2011. [https://www.enisa.europa.eu/publications/ontology_taxonomies/at_download/fullReport], luettu 1.5.2020; European Commission: *Building Resilience: The EU's approach – Factsheet, 2018.* [http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/resilience_en.pdf], luettu 1.5.2020; Björck, Fredrik, Henkel, Martin, Stirna, Janis & Jelena Zdravkovic: Cyber Resilience - Fundamentals for a Definition. *Advances in Intelligent Systems and Computing*, Vol. 353 (2015), s. 311–316.

[192] Gartzke & Lindsay (2015).

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

[194] Kukkola (2020a), s. 375; Cyberspace Administration of China: *National Cyberspace Security Strategy*, 27.12.2016. [https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/], luettu 23.12.2020.

[195] Tästä konseptista ja sen kritiikistä ks. Klimburg (2020).

[196] Käsitteiden suomennoksista ks. Kerttunen, Mika: Ydinaseet 2000-luvun maailmanjärjestyksessä. Teoksessa *Sota – Teoria ja todellisuus. Näkökulmia sodan muutokseen*. Raitasalo, Jyri & Sipilä, Joonas (toim.) Maanpuolustuskorkeakoulu,

itselle sopivalla hetkellä ennen vastustajan vahvistumista. Jälkimmäinen tyyppi perustuu halulle olla mieluummin hyökkääjä kuin puolustaja väistämättömässä sodassa.[197] Etenkin puolustuksellisella ensi-iskulla ajatellaan olevan deterrenssivaikutus, koska potentiaaliselle hyökkääjälle viestitetään sen kohteiden olevan alttiina aloitteen tempaavalle iskulle.[198] Lännessä on lisäksi pohdittu mahdollisuutta rakentaa deterrenssiä muiden toimintaympäristöjen kautta. Kyberhyökkäykset eivät välttämättä vaatisi kybervastetta tai vastamitallisuutta vastustajan laskelmiin vaikuttamiseksi.[199]

Koska kyberhyökkäykset eivät ole muotoutuneet vaikutuksiltaan ydinaseita vastaaviksi, on Lännessä katsottu voitavan luopua deterrenssikynnyksen absoluuttisuuden ja äärimmäisen rankaisun vaatimuksesta. Deterrenssin ei siis tarvitsisi perustua kertaluontoiseen rankaisuun vaan toistuviin, kevyempiin, mutta silti haitallisiin vastatoimiin. Niiden vaikutus voisi olla ajan suhteen kumulatiivinen ja täten hitaasti hyökkääjän käytöstä muokkaava.[200] Yhdysvallat ja Iso-Britannia ovat 2010-luvun jälkipuoliskolla harjoittaneet kyberhyökkääjien henkilöllisyyksien julkaisua ja sanktioiden asettamista henkilöille ja instituutioille. Tätä voidaan pitää eräänlaisena ”henkilöön kohdistuvan deterrenssin” muotona, jolla pyritään vaikuttamaan kansainvälisen normiston syntymiseen.[201] Lännessä deterrenssikäsitteen laventamista on oikeutettu Venäjän ja Kiinan viimeaikaisilla teoilla ja teksteillä.[202]

Strategian laitos, Julkaisusarja 1, No. 24. Maanpuolustuskorkeakoulu, Helsinki, 2008, s. 11–41, s. 24–25.

[197] Cimbala (2015), s. 54–55; Mueller, Karl P., Castillo, Jasen J. & Morgan, Forrest E. (et al.): *Striking First: Preemptive and Preventive Attack in U.S. National Security Policy*. RAND, Santa Monica, 2006.

[198] Libicki (2016), s. 84; Goldsmith, Jack: *Living Inside Adversary Networks*. Lawfare blog, 16th March 2018. [https://www.lawfareblog.com/living-inside-adversary-networks], luettu 5.5.2020; U.S. DoD Cyber Strategy (2018); Harknett & Nye 2017.

[199] Tor, Uri: ’Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence. *The Journal of Strategic Studies*, Vol. 40, No. 1-2 (2017), s. 92–117; Gartzke & Lindsay (2018); Chen (2018).

[200] Wilner (2020).

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

[202] Ks. esim. Sweijs, Tim & Zilincik, Samo: *Cross Domain Deterrence and Hybrid Conflict*. The Hague Centre for Strategic Studies, Hague, 2019. [https://hcss.nl/sites/default/files/files/reports/Cross%20Domain%20Deterrence%20-%20Final_0.pdf], luettu 11.1.2021.

Kyberdeterrenssillä ei ole jaettua, yleisesti hyväksyttyä määritelmää. Alex S. Wilner onkin todennut käytännön ohjanneen deterssikäsityksen muodostumista teoriaa enemmän.[203] Tässä työssä kyberdeterrenssi määritellään pragmaattisista syistä *pyrkimykseksi taivutella potentiaalinen vastustaja pidättäytymään voimankäytöstä kybertilassa, kybertilasta tai muussa tilassa uhkaamalla sietämättömällä rangaistuksella, kiistämällä potentiaaliset hyödyt tai muutoin vaikuttamalla vastustajan hyötykustannuslaskelmiin kybertilaan liittyvillä suorituskyvyillä*. Kyberdeterrenssi muodostaa osan valtion yleisestä deterrenssistrategiasta, jossa toimintaympäristöjen rajat ovat häilyvät. Kyberdeterrenssi liittyy valtion suojaamiseen uhilta myös laajemmassa informaatio(psykologisessa)ympäristössä ja se on vuorovaikutuksessa muihin toimintaympäristöihin ja keinoihin. Kyberdeterrenssi voi siis olla osa toimintaympäristöjen rajat ylittävää deterrenssiä.[204] Käsitteen puitteissa hyväksytään uhkaamisen lisäksi sotilaallisen ja ei-sotilaallisen voiman käyttö aseellisen voimankäytön rajan alapuolella hyötykustannuslaskelmiin ehkäisevästi vaikuttamiseksi.

Voimankäyttöön liittyy eskalaation käsite. RAND:in eskalaatioteoriaa käsittelevä tutkimus määrittelee sen ”konfliktin intensiteetin tai alan lisääntymiseksi, joka ylittää kynnyksen(t), jota yksi tai useampi osapuoli pitää merkittävänä.”[205] Eskalaatio perustuu siis osapuolten tulkintaan tilanteesta. Se voi tapahtua vertikaalisti (toimien intensiteetti), horisontaalisti (toimien laajentuminen) tai poliittisesti (päämäärien tai konfliktin reunaehtojen muuttaminen). Eskalaatio voi tapahtua tarkoituksellisesti, tahattomasti tai vahingossa. Tahaton eskalaatio tapahtuu, koska vastapuoli tulkitsee toisen ei-eskaloivaksi tarkoitetut toimet eskaloiviksi. Vahinkoon perustuva eskalaatio perustuu tahattomiin toimiin.[206] Tarkoituksellisuus liittyy eskalaatiokontrollin käsitteeseen. Se perustuu siihen, että yksi osapuolista pyrkii saavuttamaan edun toisiin nähden. Etu perustuu joko konkreettiseen hyötyyn tai vastustajan vakuuttamiseen omasta päättäväisyydestä.[207]

---

[203] Wilner (2020).
[204] Lindsay & Gartzke (2019).
[205] Morgan et al. (2008), s. xi.
[206] Ibid. s. 24-26.
[207] Ibid. s. 31–33; Byman, Daniel & Waxman, Matthew: *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might*. Cambridge University Press, Cambridge, 2002, s. 18.

Eskalaatiohallinnan tavoitteena on eskalaatioherruus (*dominance*). Se tarkoittaa tilaa, jossa yksi osapuoli kykenee eskaloimaan tilannetta itselleen hyödyllisellä tavalla, johon muut eivät voi vastata tai voivat vastata, mutta vastaaminen heikentäisi niiden asemaa tai kustannukset olisivat liian korkeat. Kyseessä on suorituskyvyn tai tahdon asymmetria osapuolten välillä.[208] Johtuen eskalaatioon liittyvistä epävarmuustekijöistä konfliktin osapuolten katsotaan ainakin periaatteessa pyrkivän eskalaatiokontrolliin. Konfliktin eskalaation hallinnassa voimankäyttö perustuu neuvotteluun pakottamisen kautta. Oletuksena on, että osapuolet edelleen suorittavat rationaalisia hyötykustannus- ja todennäköisyyslaskelmia. Tavoitteena voi olla edun saaminen, uhan ehkäiseminen, tappion välttäminen tai tavoitteita ja kynnyksiä koskeva viestintä. Eskalaation hallinta liitetään yleensä rajoitettuun sotaan (*limited war*), jossa osapuolten katsotaan pyrkivän rajoitettuihin tavoitteisiin rajoitetuin keinoin ja olevan avoimia neuvottelulle.[209]

Eskalaatio liittyy deterrenssin käsitteeseen, koska deterrenssi perustuu usein pyrkimykseen estää tilanteen kehittyminen epäsuotuisaan suuntaan. Deterrenssiä ja eskalaatiokontrollia ei kuitenkaan pidä sekoittaa keskenään, kuten esimerkiksi Glenn Snyder tekee ydinaserankaisudeterrenssin osalta.[210] Hänen ajatuksensa sodan aikaisesta deterrenssistä perustuu ydinaseiden käyttökynnykseen kylmän sodan kehyksessä. Jos deterrenssi sidotaan määrättyjen teknologioiden tai menetelmien käyttöön, sen suhde sotaan ja voimankäyttöön hämärtyy. Jos deterrenssi jatkuu sodan aikana, se tarkoittaa, että sota on neuvottelua, politiikkaa samoin keinoin, eikä sillä ole erityistä clausewitzilaista luonnetta. Sodasta tulee rationaalinen, hallittava neuvotteluprosessi. Edes Herman Kahn ei täysin uskonut tähän.[211] Myöskään sotien historia ei tue tätä näkemystä.[212] Deterrenssi ei määritelmällisesti voi liittyä sodan aikaan, koska avoimeen sotilaalliseen voimankäyttöön on jo päädytty. Deterrenssikäsitteen venyttäminen rauhasta ja sotaan hävittää sen analyyttisen arvon ja tekee kaikesta poliittisesta toiminnasta alisteista ”deterrenssille.” Deterrenssi liittyy voimankäytön potentiaaliin ja konfliktia edeltävään tilanteeseen,

[208] Forrest et al. (2008), s. 15–16; Freedman (2003), s. 205.
[209] Schelling (2008), s. 135.
[210] Hanska (2019), s. 53.
[211] Freedman (2003), s. 203–205; McDermott, Basil W.: Thinking about Herman Kahn. *The Journal of Conflict Resolution* , 1971, Vol. 15, No. 1 (Mar., 1971), s. 55–70.
[212] Keegan, J. A.: *History of Warfare* (2nd ed.) Pimlico, London, 2004; Terrill, Andrew W.: *Escalation And Intrawar Deterrence During Limited Wars In The Middle East*. Strategic Studies Institute, U.S. Army War College, Carlisle, PA, 2009.

eskalaatiokontrolli taas voimankäyttöön, pakottamiseen ja konfliktin tilanteeseen. Deterrenssiä ei pidä myöskään sekoittaa konfliktien ja uhkien ennaltaehkäisyyn. Tällöin taivuttelu, vetovoima ja pehmeä voima sekoittuvat pakottamiseen ja rationaaliseen nollasummapeliin perustuviin hinta-hyötylaskelmiin. Edellä esitetty huomioiden voidaan kysyä, onko koko deterrenssin käsitteestä hyötyä ydinasetematiikan ulkopuolella.

Huolimatta eskalaatioteorian yhdysvaltalaisista juurista, venäläiset ovat omaksuneet sen deterrenssin tavoin omien strategisten pohdintojensa osaksi.[213] Sama pätee jossain määrin myös kiinalaisiin.[214] Eskalaatioteorioita, kuten deterrenssiteorioitakin sovellettaessa on huomioitava niiden historialliset ja kulttuuriset juuret. Eskalaatioteoriat perustuvat ajatukseen totaalisesta, osapuolet tuhoavasta sodasta sodan äärimmäisenä ilmenemismuotona. Herman Kahnin eskalaatioportaikot ovat ääriesimerkki mekanistisesta eskalaatiokontrollista.[215] Teorioiden heikkouksiksi on nähty mekanistinen maailmankuva, joka ei huomioi laadullista ympäristöä, julkilausuttujen propagandististen doktriinien käyttö käytöksen ennustamisessa ja vastapuolen luonnetta vääristävien mallien käyttö tai ajatusvinoumat.[216]

Kybersodankäynnin tutkimuksessa eskalaatio on liitetty eskalaatioherruuden käsitteeseen tai toimintaympäristöjen rajat ylittävään eskalaatioon, minkä on katsottu tarkoittavan konfliktin hallitsematonta ja vahingossa tapahtuvaa laajentumista (*spill-over*) kybertilasta tavanomaisen tai ydinasesodankäynnin puolelle.[217] Eskalaationhallinnan on katsottu olevan vaikeaa kybertoimintaympäristössä johtuen sen ominaispiirteistä.[218] Erityisesti huomiota on kohdistettu strategisten ennakkovaroitusjärjestelmien sekä strategisten ydinaseiden johtamisjärjestelmien kyberhaavoittuvuuksiin. Pelkona on, että toinen potentiaalisen konfliktin osapuolista voisi turvautua ennaltaehkäisevään ydinaseiskuun pelätessään strategisten ydinaseidensa

[213] Forsström (2019); Kofman, Fink & Edmons (2020).
[214] Fravel, M. Taylor.: China's "World-Class Military" Ambitions: Origins and Implications. *The Washington Quarterly*, Vol.43, No.1 (2020), s. 85–99.
[215] McDermott (1971).
[216] Davis, Paul K. & Stan, Peter J.: *Concepts and Models of Escalation*. RAND, Santa Monica CA, 1984.
[217] Valeriano & Maness (2015), s. 102–105; Maness, R. C. & Valeriano, B.: Cyber spillover conflicts: Transition from cyber conflict to conventional foreign policy disputes. Teoksessa *Conflict in Cyber Space: Theoretical, strategic and legal perspectives*. Routledge, New York, 2016, s. 45–64; Libicki (2016), s. 280–28; Kello (2013).
[218] Libicki (2016), s. 276. S. 288–290.

johtamisjärjestelmien joutuvan kyberhyökkäyksen kohteeksi hyökkääjän pyrkiessä estämään vastaiskun.[219] Kyberhyökkäyksien eskalaatioherkkyyttä on perusteltu muun muassa sillä, että kriittiseen infrastruktuuriin kohdistuva iskujenvaihto ja sen seuraukset voi laajeta hallitsemattomasti. Kolmansien osapuolten tekemät harhauttavat hyökkäykset, jotka on tarkoitettu saattamaan suurvallat konfliktiin tai jopa sotaan, on nähty myös eskalaation lähteenä. Lisäksi on pelätty suurvaltojen kybersodankäyntidoktriinin ennaltaehkäisyyn ja hyökkäyksellisyyden painottumisen nostavan eskalaatioriskiä.[220] Toisaalta Borghard ja Lonergan kiistävät kyberoperaatioiden eskalaatioherkkyyden kybertilassa. Heidän mukaansa valtioilta puuttuu kybersuorituskykyjä, jotka voisivat aiheuttaa eskalaation edellyttämää vahinkoa, ja vaikka kyky olisikin olemassa, sitä pyritään varjelemaan tiedustelukyvyn säilyttämiseksi.[221] Fischerkeller ja Harknett ovat taas väittäneet, että valtioiden jatkuva kilpailu ja vihamielinen kanssakäyminen kybertilassa eivät noudata samaa eskalaatiomallia kuin potentiaaliset ja jaksottaiset konfliktitilanteet.[222]

Kysymys siitä, kykeneekö yksi konfliktin osapuoli eskaloimaan tilannetta itselleen hyödyllisellä tavalla, johon muut eivät voi vastata tai voivat vastata kyberkeinoin tai kybertilassa tai voiko kyberkeinojen käyttö johtaa tahattomaan tai vahingossa tapahtuvaan eskalaatioon on siis empiirisesti avoin. Näin ollen konfliktin eskalaation hallinnalla viitataan tässä tutkimuksessa *rajatusti jo käynnistyneen konfliktin intensiteetin säätelyyn voimankäytöllä tai sillä uhkaamalla kybertilassa tai sen kautta, jonka tavoitteena on saada vastustaja lopettamaan voimankäyttö itselle*

---

[219] Gompert, David C. & Libicki, Martin: Cyber War and Nuclear Peace. *Survival*, Vol.61, No.4 (2019), s. 45–62; Cimbala, S. J.: Accidental/Inadvertent Nuclear War and Information Warfare. *Armed Forces & Society*, Vol. 25, No.4 (1999), s. 653–675; Cimbala (2017); Acton, James M.: Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War. *International Security*, Vol. 43, No. 1 (Summer 2018), s. 56–99.

[220] Klare, Michael T.: Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation. *Arms Control Today*, November 2019. [https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation], luettu 30.4.2020.

[221] Borghard, Erica D. & Lonergan, Shawn W.: Cyber Operations as Imperfect Tools of Escalation. *Strategic Studies Quarterly*, Vol. 13, No. 3 (Fall 2019), s. 122–145. Ks. myös Valeriano, Jensen & Maness (2018), s. 88.

[222] Fischerkeller, Michael P. & Harknett, Richard J.: Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation. *The Cyber Defense Review*, Special Edition: International Conference on Cyber Conflict (CYCON U.S.), November 14-15, 2018: Cyber Conflict During Competition (2019), s. 267–287.

hyödyllisellä ja poliittisten päämäärien tavoittelua palvelevalla tavalla sekä samalla estää tahaton ja vahingossa tapahtuva eskalaatio.

Kybervoiman pakottavaan käyttöön on liittynyt pitkälti samoja teoreettisia ja käytännöllisiä haasteita kuin deterrenssiin. Martin C. Libicki on väittänyt, että kyberhyökkäyksillä ei ole samanlaista pysyvää ja mittakaavaltaan yhtäläistä vaikutusta kuin tavanomaisilla tai ydinaseilla.[223] Whyten ja Mazanecin mukaan kyberpakottamiselta puuttuu strategisella tasolla selvä vaikutuksen ja pakottajan välinen yhteys, välittömyyden tunne sekä kyky selvästi osoittaa taipumattomuuden kustannukset.[224] Thomas Ridin mukaan kyberhyökkäysten vaikutukset ovat hitaita, välillisiä, eivätkä ole tähän mennessä yltäneet vakoilua, sabotaasia tai kansankiihottamista vakavammalle eli tappamisen tasolle.[225] Thomas Mahnken mukaan kyberaseet tulee liittää muiden aseiden käytön yhteyteen, jotta niillä olisi pakottavaa vaikutusta.[226] Gartzke ja Lindsay väittävät, että kyberoperaatiot ovat hyödyllisiä vain tiedustelun tai erikoisoperaatioiden osana.[227] Valeriano, Jensen ja Maness ovat väittäneet omaan tilastolliseen tutkimukseensa perustuen, että kyberoperaatioilla on saavutettu haluttu tulos vain 5,7% tapauksista.[228] Skeptisyys kybervoiman pakottavaa käyttöä kohtaan on siis vahvaa.

Vastakkaisia näkemyksiäkin on toki esitetty. Kyberhyökkäyksillä katsotaan voivan vaikuttaa kriittiseen informaatioinfrastruktuuriin, yhteiskunnan elintärkeisiin toimintoihin, asevoimien johtamisjärjestelmiin tai poliittisen johdon toimintakykyyn niin, että vastustajan kyky ja tahto tehdä vastarintaa ehtyy.[229] Kyberhyökkäyksillä voidaan valvoa tai kaapata tietoliikennesatelliittien liikennettä, manipuloida dataa ja kaapata hallintaan itse satelliitit, joista esimerkiksi Yhdysvaltojen sotilasmahti on

---

[223] Libicki (2009), s. xiv-xv; Libicki (2016), s. 201.
[224] Whyte & Mazanec (2019), s. 131.
[225] Rid (2012); Rid (2017).
[226] Mahnken (2011), s. 61–62.
[227] Gartzke & Lindsay (2015), s. 347.
[228] Valeriano, Jensen & Maness (2018), s. 17.
[229] Geers (2011); Clark & Knake (2010); Rattray (2001); Smeets, Max & Lin, Herbert S.: Offensive Cyber Capabilities: To What Ends? Teoksessa *10th International Conference on Cyber Conflict CyCon X: Maximising Effects*. Minárik, T., Jakschis, R. and Lindström, L. (eds.) NATO CCD COE, Tallinn, 2018, s. 55–72; Wirtz, J. J.: Life in the "Gray Zone": Observations for contemporary strategists. *Defense & Security Analysis*, Vol. 33, No. 2 (2017), s. 106–114.

riippuvainen.[230] Kybervoimaan uskovat perustelevat argumenttinsa yhteiskunnan ja asevoimien perustavan laatuisella riippuvuudella informaatioteknologiasta.

Koska suora tuhoaminen, kybervoimalla tappamisesta puhumattakaan, on jäänyt teoreettiseksi ilmiöksi ja koska kybertilassa on käytännössä mahdoton saavuttaa pysyvää herruutta eli tilan omistajuutta, raa'an voiman käyttö ei ole näytellyt aikaisemmassa tutkimuksessa merkittävää osaa strategisen tason voimankäyttöä pohdittaessa. Raa'an voiman käyttöön liittyy myös Martin Libickin huomio siitä, että kybertilaan ei voi pakolla tunkeutua, koska kaikkien toimijoiden on noudatettava sen sääntöjä ja vain sääntöjen noudattaminen takaa pääsyn tilaan. Libicki on myös korostanut, että "voiman korrelaatio" ei voi olla perusta ylivoimalle kybertilassa, koska hyökkäykselliset kyberjoukot eivät asetu toisiaan vastaa kybertilassa.[231] Raakaa voimaa on käytännössä mahdotonta käyttää kybertoimintaympäristössä niin kauan kuin kohteella on edes teoreettinen mahdollisuus estää toimintaympäristön käyttö hyökkääjältä tai puolustaja tulee toimeen ilman kybertoimintaympäristöä. Tällöin hyökkääjä ei voi saavuttua kykyä kontrolloida tai tuhota vastustaa.

Tutkittaessa *rakenteellisen kyberasymmetrian sotilaallista hyväksikäyttöä tarkastellaan tässä tutkimuksessa pakottamisen ja raa'an voiman käyttöä kybertilassa ja kykyä aiheuttaa sellaista vaikutusta kybertilassa tai sen kautta, joka pakottaa vastustajan lopettamaan vastarinnan vastoin omaa tahtoaan tai kiistää vastaavan vaikutuksen omiin järjestelmiin*. Tällainen voimankäyttö liittyy avoimeen sotatilaan valtiotoimijoiden välillä. Sillä voi olla useita strategioita kuten kuluttaminen (*attrition*), tuhoaminen (*destroy*), lamauttaminen (*disrupt*) tai dekapitaatio (*decapitation*).[232] Ensimmäinen perustuu vastustajan voiman kuluttamiseen sarjalla vastustajan taisteluvoimaan ja/tai yhteiskunnan kriittisiin toimintoihin ja taisteluvoiman tukitoimiin kohdistuvia taistelutoimia (operaatioilla). Toinen vastustajan taistelukyvyn tuhoamiseen yhdellä iskulla nopean ratkaisun aikaan saamiseksi. Kolmas vastustajan sotilaallisten suorituskykyjen ja tahdon lamauttamiseen iskemällä niiden heikkouksiin ja horjuttamalla koheesiota. Neljäs strategia perustuu sotilas- ja siviilijohdon tuhoamiseen.

---

[230] Harrison, Todd, Johnson, Kaitlyn, Roberts, Thomas G., Way, Tyler & Young, Makena: *Space Threat Assessment 2020*. Center for Strategic & International Studies, Washington, D.C., 2020.
[231] Libicki (2016).
[232] Valeriano, Jensen & Maness (2018); Sloan (2012).

Teoreettinen kädenvääntö kybervoiman käytön seurauksista ja mahdollisuuksista liittyy empiirisen datan puutteen lisäksi strategisten vaikutusten käsitteeseen. Colin S. Grayn mukaan sillä voidaan tarkoittaa määrätyn käytöksen konfliktin päämäärien saavuttamiseen liittyviä vaikutuksia. Se ei siis ole välineen tai käytöksen ominaisuus vaan seuraus. Yleensä vaikutus kohdistuu vastustajan kykyyn, tahtoon tai resursseihin.[233] Vaikutus viittaa koko joukkoon lopputuloksia, tapahtumia ja seurauksia, jotka johtuvat määrätystä toiminnasta.[234] Vaikutukset voivat olla esimerkiksi suoria, epäsuoria, sarjamaisia (*cascading*) tai kollateraalisia.[235] Edelleen vaikutukset voivat olla fyysisiä, funktionaalisia, systeemivaikutteisia tai psykologisia.[236] Moninaisuudesta johtuen vaikutusten etukäteen määrittely ja ennustaminen kompleksisissa ja adaptiivisissa järjestelmissä on haastavaa.[237] Vaikutus voi olla usean eri keinon käytön tulos.[238]

Strateginen vaikutus on sidoksissa kohteeseen ja kontekstiin, sillä kohteen reaktio vaikutukseen on ratkaiseva.[239] Esimerkiksi ilmavoiman väitetty itsenäinen strateginen vaikutus strategisten pommitusten kautta on kiistanalainen, koska vastustaja päättää reaktiostaan.[240] Pakottaminen ei myöskään ole yksisuuntainen suhde vaan pakotettava voi yrittää muuttaa suhdetta esim. suojaamalla heikkouksiaan. Tilanne voi myös muuttua tai pakottamiseen yhdistyä muita tekijöitä, joilla on ratkaiseva vaikutus.[241]

---

[233] Gray (2009), s. 19.
[234] Mann, Edward C., Endersby, Gary & Searle, Thomas R.: *Thinking Effects: Effects-Based Methodology for Joint Operations*. Air University Press, Alabama, 2002, s. 46.
[235] Mann, Endersby & Searle (2002), s. 53.
[236] Mann, Endersby & Searle (2002), s. 37–38; Snodgrass, Anthony W., Gallagher, Mark A. & Gregory A. McIntyre: Modeling Military Strategic Effects with an Input-Output Metamodel. *Military Operations Research*, Vol. 9, No. 1 (2004), s. 19–32.
[237] Ks. Luku 3.1.
[238] Pape 1996; Warden, John A. III: Success in Modern War: A Response to Robert Pape's Bombing to Win. *Security Studies*, Vol. 7, No. 2 (1997), s. 172–190; Bratton, Patrick: A Coherent Theory of Coercion? The Writings of Robert Pape. *Comparative Strategy*, Vol. 22, No. 4 (2003), s. 355–372; Biddle, Tami Davis: *Air Power And Warfare: A Century Of Theory And History*. Strategic Studies Institute, US Army War College, 2019.
[239] Vego, Milan: Effects-Based Operations: A Critique. *Joint Forces Quarterly,* Vol. 41, No. 2 (2006), s. 51–57; Carpenter, Paul & Andrews, William F.: Effect-based Operations: Combat Proven. *Joint Forces Quarterly*, Vol. 52, No. 1, s. 78–81; Correll, John T.: The Assault on EBO. The cardinal sin of Effects-Based Operations was that it threatened the traditional way of war. *Air Force Magazine*, Vol. 96, No. 1 (January 2013), s. 50–53.
[240] Pape (1996); Warden (1997); Bratton (2003); Sloan (2012).
[241] Byman, Daniel L. Ja Waxman, Matthew C.: Kosovo and the Great Air Power Debate. *International Security*, Vol. 24, No. 4 (Spring 2000), s. 145–171.

Vaikutus siis nähdään hyökkäyksellisen, yksilöitävän, toiminnan tuloksena vastustajassa – tai jossain järjestelmässä – ei neuvottelun tuloksena.[242] Kuitenkin kyberhyökkäysten strategisten vaikutusten osalta Harknett ja Smeets ovat vastikään esittäneet, että kyberkampanjat voivat saavuttaa strategisia vaikutuksia ilman sotilaallista voimankäyttöä perustuen yksittäisten, aseellisen voiman käytön tason alle jäävien operaatioiden kumulatiiviseen vaikutukseen.[243] Myös Libicki ja Lewis väittävät, että kyberoperaatioiden strateginen vaikutus ilmenee lähinnä tietojärjestelmiin kohdistuvan epävarmuuden synnyttämisen ja luottamuksen rapauttamisen kautta.[244] Harknettin, Smeetsin, Libickin ja Lewisin näkemyksissä heijastuvat Yhdysvaltojen vuoden 2016 presidentinvaalien kokemukset, mutta ajatus kumulatiivisista strategisista vaikutuksista on pätevä. Kyseessä on pakottaminen toisin, ei-sotilaallisin, keinoin.

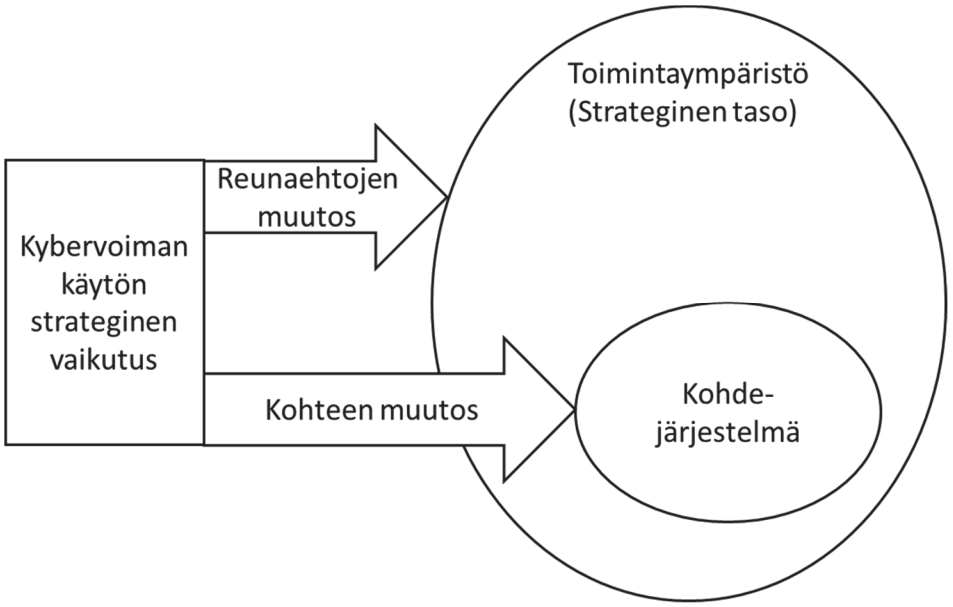
Strateginen vaikutus voi kuitenkin olla myös potentiaalinen. Se voi liittyä tulevaisuuteen tähtäävään puolustuspolitiikkaan tai sotilasstrategiaan tai koko puolustusjärjestelmän toimintaan. Esimerkiksi ydinaseilla on pelkällä olemassaolollaan strateginen vaikutus, samoin kuin Maginot-linjalla ajateltiin olevan 1930-luvulla tai linnoituksilla 1600- ja 1700-luvuilla.[245] Ottaen huomioon aikaisempi kybervoiman määrittely ja sen strategisiin vaikutuksiin liittyvä keskustelu on strategisen vaikutuksen määritelmää perustelua laajentaa koskemaan myös toimijoiden jakamaa toimintaympäristöä. Ben Buchanan on esimerkiksi esittänyt, että kybervoiman todellinen käyttö perustuu pikemminkin signalointiin ja toimintaympäristön muokkaamiseen, kuin pakottamiseen ja deterrenssiin. Buchanan ymmärtää ”muokkaamisen” (*shaping*) tiedon hankintana ja hyväksi käyttämisenä edun hankkimiseksi sodan kynnyksen alapuolella.[246] Tässä työssä toimintaympäristön muutos ymmärretään huomattavasti konkreettisemmin.

Toimintaympäristön muutos vaikuttaa valtioihin, kun valtiot ja niiden turvallisuuskoneistot ymmärretään järjestelminä.[247] Tästä näkökulmasta

---

[242] Klinger (2019).
[243] Harknett, Richard J. & Smeets, Max: Cyber Campaigns and Strategic Outcomes. *Journal of Strategic Studies*, 2020 DOI: 10.1080/01402390.2020.1732354.
[244] Lewis (2018); Libicki (2016).
[245] Gibson, Irving M.: The Maginot Line. *The Journal of Modern History*, Vol. 17, No. 2 (Jun., 1945), s. 130–146; Guerlac (1990), s. 87.
[246] Buchanan, Ben: *The Hacker and The State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press, Cambridge, 2020.
[247] Ks. Luku 3.1.

strateginen vaikutus muuttaa valtioiden toimintaympäristöä niin, että niiden turvallisuusjärjestelmien välinen voimasuhde muuttuu potentiaalisen tulevan konfliktin osalta. Strateginen vaikutus liittyy yhtäältä voimankäytön edellytysten muuttumiseen ja toisaalta voimankäytön päämäärän tavoittamiseen liittyvään muutokseen kohdejärjestelmässä strategisella tasolla. Kybervoiman strategisen vaikutuksen kaksijakoinen luonne on esitetty kuvassa 3.



Kuva 3: Strategisten vaikutusten luonne

Toimintaympäristön tai taistelukentän muokkaaminen ei kuulu Schelling alkuperäiseen voimapolitiikan jaotteluun, mutta kybertilan osalta, jossa valtioiden välisen voimankäytöllisen vuorovaikutuksen kehys on muokattavissa, se on perusteltu lisäys. Strategisia vaikutuksia voidaan näin ollen väittää esiintyvän kaikissa valtioiden välisten suhteiden vaiheissa konfliktin ennaltaehkäisyyn, deterrenssiin, eskalaation hallintaan ja asymmetrian sotilaalliseen hyväksikäyttöön liittyen. Voimankäytön muodot eivät ole täysin sidottu konfliktin vaiheisiin. Strategiset vaikutukset, ymmärrettynä reunaehtoina tai edellytyksinä, ovat nekin tulkintakysymyksiä.

2.3 Asymmetrian käsite[248]

Asymmetria ei ole pelkästään sotilaallinen käsite. Sitä voitaisiin kyberkysymysten piirissä tarkastella esimerkiksi taloudellisesta tai puhtaasti teknologisesta näkökulmasta.[249] Toisaalta asymmetrian käsitettä on käytetty strategian tutkimuksen ja valtionhallinnon piirissä merkitsemään eri asioita eri aikakausina.[250] Tässä työssä asymmetrian käsitettä lähestytään voimankäytön näkökulmasta työn keskittyessä tarkastelemaan kybervoiman käyttöä sotilaallisessa kontekstissa.

Hew Starchanin mukaan jokaisella konfliktilla on asymmetrisiä piirteitä. Konfliktien osapuolten voimassa esiintyy vahvuuksia, haavoittuvuuksia ja eroja.[251] Lisäksi sotilaallisiin konflikteihin oleellisesti liittyvä strategian käsite perustuu vastustajan heikkouksien hyväksi käyttämiseen.[252] Itse asiassa Edward Luttwakin mukaan toiminta, joka ei haasta vastustajan suunnitelmia, ei ansaitse strategian nimeä.[253] Itsestään selvyyksistä huolimatta asymmetrisesta sodankäynnistä on kehittynyt osa sotatieteiden käsitteistöä. Yleensä se liitetään osapuolten epäsuhtaisiin resursseihin ja vihollisen haavoittuvuuksien hyödyntämiseen epätavanomaisia menetelmiä käyttäen.

Lawrence Freedmanin mukaan asymmetrisen konfliktin käsite ilmaantui läntiseen sotilasajatteluun 1970-luvulla.[254] Esimerkiksi Yhdysvaltojen puolustusstrategian kontekstissa *offset* -käsitettä on käytetty kuvaamaan

---

[248] Tämä luku perustuu ja osiltaan päivittää aikaisemmin julkaistua tekstiä: Kukkola, Juha: Cyber asymmetry
– Towards new strategic thinking? Teoksessa *Game Changer: Structural Transformation of Cyberspace*. Kukkola, Juha, Ristolainen, Mari & Nikkarila, Juha-Pekka. Finnish Defence Research Agency, Riihimäki, 2017, s. 131–188.

[249] Google hakukone tuotti 221 000 000 osumaa sanalle ‘asymmetric’ 14.4.2020.

[250] Asymmetria käsitteen historiasta ks. Mahnken (2003), s. x–xviii; Blank, Stephen: Rethinking the Concept of Asymmetric Threats in U.S. Strategy. *Comparative Strategy*, Vol. 23, No. 4-5 (2004), s. 343–367; Lambakis, Steven, Kiras, James & Kolet, Kristin: Understanding "Asymmetric" Threats to the United States. *Comparative Strategy*, Vol. 21, No. 4 (2002), s. 241–277.

[251] Strachan (2013), s. 22.

[252] Nye, Joseph: Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly*, Vol. 5, No. 4 (Winter 2011), s. 18–38; Freedman (2013), s. 227; Strachan (2013), s. 22; Milevski, Lucas: Asymmetry is Strategy, Strategy is Asymmetry. *JFQ*, Vol. 75, No. 4 (2014), s. 77–83, s. 78; Smith (2008), s. 6.

[253] Luttwak (2001).

[254] Freedman (2013), s. 52.

suurvallan pyrkimyksiä säilyttää tai hankkia teknologinen ylivoima (*superiority*) vastustajistaan 1950-, 1970–1980 ja 2010-luvuilla.[255] Asymmetria on ollut implisiittisesti läsnä yhdysvaltalaisessa operaatiotaidollisessa ajattelussa vastustajan voimanlähteen ja sen neutraloinnin kautta1980-luvulta alkaen. Ajattelulla on yhtymäkohtia mm. Liddell Hartin epäsuoran strategian ja rajoitettujen sotien (*limited wars*) käsitteisiin.[256]

Asymmetrian käsite ilmestyi 1990-luvulla läntisiin doktriineihin ja strategioihin, joissa se ensin ymmärrettiin suurvallan etuna, mutta pian haavoittuvuutena Yhdysvaltojen kohdatessa kumouksellisia joukkoja kansainvälisissä operaatioissa.[257] 1990- ja 2000-lukujen aikana asymmetrisen sodankäynnin käsite kietoutui sodankäynnin vallankumouksesta (*Revolution of Military Affairs, RMA*), verkostokeskeisestä sodankäynnistä (*Network Centric Warfare, NCW*) ja uuden sukupolven sodankäynnistä (*Next Generation Warfare, NGW*) käytyihin keskusteluihin.[258] Keskustelut saivat käyttövoimansa havaitusta

---

[255] Cimbala (2015). Ks. myös Grier, Peter: The First Offset. *Air Force Magazine*, Vol. 99, No. 6 (June 2016), s. 56–60; Tomes, Robert: The Cold War Offset Strategy: Assault Breaker And The Beginning Of The RSTA Revolution. *War on the Rocks*, November 20, 2014. [https://warontherocks.com/2014/11/the-cold-war-offset-strategy-assault-breaker-and-the-beginning-of-the-rsta-revolution/], luettu 14.4.2020; Hagel, Chuck: *Secretary of Defense Speech: Reagan National Defense Forum Keynote*, November 15th 2014. [https://www.defense.gov/Newsroom/Speeches/Speech/Article/606635/], luettu 14.4.2020.

[256] "More often than not, the enemy recognizing his center of gravity will take steps to protect it, and *indirect means* will be required to force him to expose it to attack." Kursivointi tekijän (The United States Army Combined Arms Doctrine Directorate: *FM 100-5 Operations*, May 1986, s.180. [http://cgsc.cdmhost.com/utils/getdownloaditem/collection/p4013coll9/id/893/filename/894.pdf/mapsto/pdf/type/singleitem], luettu 14.4.2020). Ks. myös Strange, Joe: *Centres of Gravity & Critical Vulnerabilities*. Marine Corps University Perspectives on Warflghting Number Four Second Edition [https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/3B_COG_and_Critical_Vulnerabilities.pdf], luettu 14.4.2020.

[257] Metz, S. & Johnson, D. I.: *Asymmetry and U.S. Military Strategy L Definition, Background, and Strategic Concepts*. U. S. Army Strategic Studies Institute: Carlisle, 2001, s. 3–4 [https://apps.dtic.mil/sti/pdfs/ADA387381.pdf], luettu 20.8.2017.

[258] Arquilla, John and Ronfeldt, David: *In Athena's Camp.* RAND, Santa Monica, 1997; Cebrowski, A. K. & Garstka, J. J.: Network-Centric Warfare: Its Origin and Future. *Proceedings Magazine*, Vol. 124, No. 1 (1998), s. 28–35; Owens, Bill: *Lifting the Fog of War*. The Johns Hopkins University Press, Baltimore, 2001; Hammes, T. X.: *The Sling and the Stone: On War in the 21st Century*. Zenith Press, St Paul, 2006; Chase, Jesse: Defining Asymmetric Warfare: A Losing Proposition. *Joint Forces Quarterly*, Volume 61

muutoksesta sodankäynnin luonteessa, johon kuuluivat valtioiden heikkeneminen, ei-valtiollisten toimijoiden vahvistuminen, informaatioyhteiskunnan synty ja kulttuuristen tekijöiden merkityksen kasvu – tai niiden merkityksen uudelleen löytäminen.[259] Paul Mitchellin mukaan verkostokeskeisen sodankäynnin idea perustui informaation jakamiseen verkoston sisällä, jonka nähtiin johtavan vastustajaa nopeampaan ja tehokkaampaan päätöksentekoon. Asymmetria on läsnä tässä ideassa siten, että kontrolloimalla informaatiota ja sen käsittelyyn liittyviä prosesseja, toisin sanoen informaatioympäristöä, konfliktin osapuoli voi päästä vastustajansa päätöksentekosyklin sisään, horjuttaa tätä ja tuhota tai taivuttaa tämä tahtoonsa.[260]

Asymmetrinen sodankäynti sai 2000-luvulla muunkinlaisia merkityksiä. Esimerkiksi Ison-Britannian yhteisoperaatiodoktriinissa asymmetria yhdistettiin vuoden 2004 doktriinissa liikesodankäyntiin ja epäsuhtaisen voiman käyttöön vastustajan heikkouksia vastaa.[261] Terrorismin vastaisen taistelun kehyksessä asymmetria alettiin ymmärtää ei-valtiollisten toimijoiden ja suurvallan tai liittouman välisenä sodankäyntinä. Siinä vahvempi osapuoli käytti tavanomaisia korkean teknologian asejärjestelmiä, mutta sen toimintaa rajoittivat omien tappioiden ja sivullisten uhrien (*collateral damage*) pelko. Heikompi osapuoli käytti tekniikoita ja menetelmiä, joiden käyttöön valtiotoimijalla ei ollut poliittista halua tai kykyä.[262] Samaan aikaan kulttuurista ymmärrystä painottaneet ns. neljännen sukupolven sodankäynnin (4GW) teoreetikot katsoivat, ettei asymmetria ollut niinkään resurssierojen kuin käyttäytymistä säätelevien tahdon, päämäärien, organisoitumisen ja

(2nd Quarter 2011), s. 115–120; Mitchell, P.: Network Centric Warfare: Coalition Operations in the Age of US Military Primacy. IISS, *The Alelphi Papers* Vol. 6, No. 385 (2006), s. 31; Cebrowski & Garstka (1998); The United States Department of Defense (U.S. DoD): *Network Centric Warfare, Report to Congress*, 27 July 2001. [http://www.dodccrp.org/files/ncw_report/report/ncw_appendix.pdf], luettu 14.4.2020.

[259] Creveld Van, M.: *The Transformation of War*. The Free Press, New York, 1991; Keegan (2004); Kaldor (2012).

[260] Mitchell (2006).

[261] Ministry of Defence of the Great Britain: *Joint Operations Execution. Joint Warfare Publication 3-00*. (2nd ed.) The Joint Doctrine & Concepts Centre, Shrivenham 1-11, 2004. [https://dokumen.tips/documents/jwp-3-00-jt-ops-execution-2004.html], luettu 11.1.2021.

[262] Evans, M.: Elegant Irrelevance Revisited: A Critique of Fourth-Generation Warfare. *Contemporary Security Policy*, Vol. 26, No. 2 (2005), s. 242–249; Hammes (2006); Smith (2008).

normien epäsuhdan tulos.[263] Kritiikki ei ole estänyt asymmetrisia tekniikoita ja taktiikoita käyttävien ei-valtiollisten hyökkääjien käsitettä juurtumasta esimerkiksi Yhdysvaltojen asevoimien doktriineihin.[264]

Asymmetrisen sodankäynnin käsitteen ilmaantuminen virallisiin asiakirjoihin on ruokkinut tutkijoiden ajatuksenvaihtoa aiheesta.[265] Asymmetria siirtyi myös oppikirjoihin ”epätavanomaisen sodankäynnin” (*irregular warfare*)[266] käsitteen kautta, joka heijasteli etenkin Yhdysvalloille ja sen liittolaisille tärkeää nk. sotaa terrorismia vastaan (*War on Terror*).[267] Esimerkiksi Lawrence Freedman ja Colin Gray ovat eksplisiittisesti liittäneet asymmetrisen sodankäynnin kumouksellisen sodankäyntiin.[268] Tässä yhteydessä Freedman liitti käsitteeseen sellaisia tekijöitä kuin maantiede, parempi kyky kestää tappioita, kärsivällisyys, piittaamattomuus tappioista ja narratiivin hallinta.

Asymmetrian olemus on kehittynyt sodankäynnin ulottuvuuksien lisääntyessä. Yhdysvaltojen asevoimien puolustushaarojen yhteisoperaatiodoktriiniin on kirjattu sellaiset käsitteet kuin kokonaisvaltainen toimintaympäristöylivoima (*full-spectrum superiority*)

---

[263] Tästä keskustelusta ks. Evans (2005); Hammes (2006); Benbow, Tim: Talking ‘Bout Our Generation? Assessing the Concept of “Fourth-Generation Warfare”. *Comparative Strategy*, Vol. 27, No. 3 (2008), s. 148–163; Junio, Timothy J.: Military History and Fourth Generation Warfare. *Journal of Strategic Studies*, Vol. 32, No. 2 (2009), s. 243–269; Freedman (2013), s. 225–227; Biddle, Stephen: *Military Power - Explaining Victory and Defeat in Modern Battle.* Princeton University Press, Princeton, 2004; Biddle, Stephen: Military Power: A Reply. *Journal of Strategic Studies*, Vol. 28, No. 3 (2005), s. 453–469; Echevarria, Antulio J.: *Operational Concepts and Military Strength, 2017 Index of U.S. Military Strength*. [https://www.heritage.org/military-strength-topical-essays/2017-essays/operational-concepts-and-military-strength], luettu 14.4.2020; Echevarria, Antulio J.: Deconstructing the Theory of Fourth-Generation War. *Contemporary Security Policy*, Vol. 26, No. 2 (2005), s. 233–241.

[264] U.S. DoD JP 3-0, s. I-4.

[265] Tästä todistaa esimerkiksi akateemisten journaalien perustaminen aiheen käsittelemiseksi (Ryan, Maria: Full Spectrum Dominance: Donald Rumsfeld, the Department of Defense, and US Irregular Warfare Strategy, 2001–2008. *Small Wars & Insurgencies*, Vol. 25, No. 1 (2014), s. 41–68). Ks. Ivan Arreguín-Toft asymmetriaa koskevien teorioiden kehittymisestä 2000-luvulla (Arreguín-Toft, Ivan: Contemporary Asymmetric Conflict Theory in Historical Perspective. *Terrorism and Political Violence*, Vol. 24, No. 4 (2012), s.635–657).

[266] Elinor Sloanin mukaan epätavanomainen sodankäynti sisältää kumouksellisen ja sissisodankäynnin sekä terrorismin (Sloan (2012), s. 65–66).

[267] Jordan et al. (2008), s. 232.

[268] Freedman, Lawrence: Asymmetric War. *The Adelphi Papers*, Vol. 45, No. 379 (2006), s. 49–60; Gray (2007), s. 245.

ja toimintaympäristörajat ylittävä toiminta (*cross-domain action*), jotka ovat edelleen vaikuttaneet käsitykseen asymmetriasta.[269] Asymmetrian näkökulmasta nämä käsitteet tarkoittavat, että missä tahansa sodankäynnin toimintaympäristöistä (*domain*) – maa, meri, ilma, avaruus, informaation ja kyber – saattaa olla kriittisiä heikkouksia, joita vastustaja kykenee käyttämään muiden toimintaympäristöjen vahvuuksien kiertämiseksi. Toisaalta kaikkien toimintaympäristöjen hallinta tarkoittaisi Yhdysvaltojen ja sen liittolaisten äärimmäistä ylivoimaa.[270]

Kriittisempi ja moninaisempi näkökulma asymmetriaan kehittyi 2010-luvulla virallisten doktriinien ulkopuolella. Jesse Chace esimerkiksi kritisoi asymmetrisen sodankäynnin oppikirjamaisuutta, kun sen ytimen piti hänen mukaansa olla mielikuvituksen käytössä.[271] Lawrence Freedman kritisoi niin 4GW:tä kuin teknologisiakin visioita sodankäynnistä ja korosti erästä asymmetrian tärkeää puolta: Asymmetriaa on ilmeisen hankala neutraloida, kun se on kerran saavutettu.[272] Hew Strachan on taas väittänyt, että asymmetrisessä sodankäynnissä, joka ymmärretään pieninä sotina (*small wars*) tai kapinoina, ei ole mitään uutta.[273] Lucas Milevski on väittänyt, että ”strategia voidaan tulkita asymmetrian tuottamiseksi ja hyväksikäyttämiseksi sodan päämääriä varten.”[274] Hän erottaa tavanomaisen asymmetrian epätavanomaisesta ja väittää edellisen viittaavan kahden tasavahvan toimijan väliseen konfliktiin ja jälkimmäisen kumoukselliseen sodankäyntiin, jossa voimasuhde on epätasainen.[275] Toisaalta Jan Angström ja J. Widen ovat kritisoineet tapaa jaotella sotia niissä käytettävien keinojen mukaan. Keinoja voidaan käyttää taktisella tasolla tai strategisen vaikutuksen saavuttamiseksi. Heidän mielestään asymmetriasta pitäisi puhua voiman jakautumisen sekä organisaatioiden,

---

[269] Echevarria II, Antulio J.: Strategic Culture Is Not a Silver Bullet. *Naval War College Review*, Vol. 70, No. 4, (Autumn 2017), s. 121–124.
[270] The United States Department of Defense (U.S. DoD): *Joint Vision 2020*, printed in Joint Force Quarterly, Summer 2000. [http://www.dtic.mil/dtic/tr/fulltext/u2/a526044.pdf], luettu 14.4.2020; The United States Department of Defense (U.S. DoD), Joint Staff Force Development (J7): *Cross-Domain Synergy in Joint Operations: Planner's Guide*, 14 January 2016. [http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/cross_domain_planning_guide.pdf?ver=2017-12-28-161956-230], luettu 14.4.2020.
[271] Chace (2011).
[272] Freedman (2013), s. 220–236.
[273] Strachan (2013), s. 21–22.
[274] Milevski (2014).
[275] Ibid., 80-81.

keinojen ja normien laadun ja tyyppien yhteydessä – ei sodan tyypeistä keskusteltaessa.[276]

Yhdysvaltojen asevoimien kiinnostuttua 2010-luvulla uudelleen suurvaltakilpailijoista syntyi A2/AD:n (*anti-access and area denial*) käsite.[277] Asymmetria esiintyy A2/AD käsitteessä toisen osapuolen kykynä kiistää vastustajan toiminta määrätyllä alueella perustuen sotilaallisten suorituskykyjen yhteiskäyttöön. A2/AD uhkakuva on osa yhdysvaltalaista AirSea Battle doktriinikehitystyötä ja osoittaa, kuinka asymmetria on siirtynyt terrorismin vastaisen sodan aikakaudelta suurvaltojen ja vertaisvastustajien (*near-peer*) aikakaudelle.[278]

Asymmetrian viimeisin ilmentymä liittyy hybridisodankäynnin käsitteeseen.[279] Hybridisodankäynti tai -vaikuttaminen voidaan määritellä sotilaallisten ja ei-sotilaallisten, avoimien ja salaisen keinojen käyttämiseksi poliittisten tavoitteiden saavuttamiseksi.[280]

---

[276] Angström & Widen (2015).

[277] Lasconjarias, Guillaume & Marrone, Alessandro: *How to Respond to Anti-Access/Area Denial (A2/AD)? Towards a NATO Counter-A2/AD Strategy*. Research Division - NATO Defense College, Rome, 2016; Simon, Luis: A European Perspective on Anti-Access/Area Denial and the Third Offset Strategy. *War on the Rocks*, May 3rd 2016. [https://warontherocks.com/2016/05/a-european-perspective-on-anti-accessarea-denial-and-the-third-offset-strategy/], luettu 14.4.2020; Tangredi, Sam J. CNO vs A2AD: Why Admiral Richardson is Right about Deconstructing the A2/AD Term. *The Navalist,* January 2017. [https://thenavalist.com/home/2017/1/8/dissecting-the-buzz-words-that-control-the-defense-debates], luettu 15.4.2020.

[278] Echevarria (2017); Biddle, Stephen & Oelrich, Ivan: Future Warfare in the Western Pacific: Chinese Antiaccess / Area Denial, U.S. AirSea Battle, and Command of the Commons in East Asia. *International Security*, Vol. 41, No. 1 (2016), s. 7–48; Simon, Luis: Demystifying the A2/AD Buzz. *War on the Rocks*, 2017. [https://warontherocks.com/2017/01/demystifying-the-a2ad-buzz/], luettu 15.4.2020; Hutchens, Michael E., Dries, William D., Perdew, Jason C., Bryant, Vincent D. & Kerry E. Moores: Joint Concept for Access and Maneuver in the Global Commons: A New Joint Operational Concept. *Joint Forces Quarterly*, Vol. 84 (Jan. 27, 2017), s. 134–139.

[279] Ks. Hoffman, Frank G.: *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies, Arlington, Virginia, 2007. [http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf], luettu 14.4.2020; Renz, Bettina & Smith, Hanna: *Russia and Hybrid Warfare: Going Beyond the Label*. Aleksanteri Papers 1/2016. Aleksanteri Institute, Helsinki, 2016; Galeotti (2016).

[280] Lalu, Petteri & Puistola, Juha: *On the concept of hybrid warfare*. Finnish Defence Research Agency, Research Bulletin 01 – 2015. [https://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+TUTKIMUSKATSAUS+2015_1+engl.pdf/12fd458c-aa76-4ed6-a402-

Hybridisodankäynnin tai operaatioiden yhteydessä asymmetriaa ei määritellä niinkään konfliktityypiksi tai voimaeroksi vaan menetelmiksi ja välineiksi.[281] Luovuus, joustavuus, epäsuoruus, mukautuvuus ja aloitteellisuus ovat tällöin asymmetrian elementtejä.[282] Hybridikeskustelun tuloksena läntiseen keskusteluun on ilmaantunut uudelleen ”harmaan alueen” tai ”harmaan vaiheen” (*gray zone*) konfliktin käsite.[283] Asymmetria irrotetaan tässä ajattelussa ei-valtiollisista toimijoista ja avoimesta sodasta tai konfliktista. Se liitetään strategisen edun hankkimiseen käyttämällä avoimesta aseellisesta voimasta poikkeavia keinoja. Keinot valitaan tarkoituksella niin, ettei niihin kyetä reagoimaan deterrenssistrategian puitteissa. Harmaan alueen toiminnalla voidaan myös tarkoittaa sodan alkuvaihetta edeltävää taistelukentän muokkaamista.[284]

Eräänlainen käsitehistoriallinen ympyrä on sulkeutunut poliittisen sodankäynnin käsitteen ilmestyttyä uudelleen läntiseen kielenkäyttöön. Sen kylmän sodan aikaiset määritelmät ovat hyvin lähellä hybridisodankäynnin määritelmiä.[285] Viimeaikaisen kansainvälispoliittisen tilanteen johdosta traditionaalisempia näkemyksiä asymmetriasta on myös esiintynyt, kun mitattavia suorituskykyjä on tarkasteltu ohjuspuolustusta ja uusia hypersoonisia ja ydinkäyttöisiä ohjustyyppejä vertailtaessa. Näiden tarkastelujen mukana peliteoreettiset ja systeemianalyyttiset mallit ovat

---

b19c13fb18c3/PVTUTKL+TUTKIMUSKATSAUS+2015_1+engl.pdf.pdf], luettu 14.4.2020.

[281] Ks. Hoffman, Frank G.: Hybrid Warfare and Challenges. Teoksessa *Strategic Studies: A Reader*. Mahnken, Thomas G. & Maiolo, Joseph A. (eds.) Routledge, New York, 2014, s. 329–337; Galeotti (2016); Thomas, Timothy: The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking. *The Journal of Slavic Military Studies*, Vol. 29, No. 4 (2016), s. 554–575; Jonsson, Oscar and & Seely, Robert: Russian Full-Spectrum Conflict: An Appraisal After Ukraine. *Journal of Slavic Military Studies*, Vol. 28, No. 1 (2015), s. 1–22.

[282] Johnson (2018).

[283] Votel, Joseph, Cleveland, Charles, Connett, Charles & Irwin, Will: Unconventional Warfare in the Gray Zone. *Joint Forces Quarterly*, Vol. 80 (1st Quarter) 2016, s. 101–109.

[284] Operaation vaiheista yhdysvaltalaisessa ajattelussa ks. U.S. DoD JP 3-0 (2018), s. V-13; Wirtz (2017).

[285] Ks. Esim. Robinson et al. (2018); Kennan, George: *George F. Kennan on Organizing Political Warfare*, April 30th 1948. [https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=941dc9ee5c6e51333ea9ebbbc9104e8c], luettu 15.4.2020.

tekemässä paluuta läntiseen ajatteluun, jos ovat koskaan siitä väistyneetkään.[286]

Edellä käsiteltyyn doktrinaaliseen kehityksen perustuen voidaan väittää, että asymmetria voidaan nykyisellään läntisessä sotilasajattelussa ymmärtää niin laadullisesti kuin määrällisesti. Lawrence Freedman on itse asiassa eritellyt kolme erilaista asymmetrian tyyppiä eli voiman, keinot ja intressit.[287] Ensimmäinen tyyppi liittyy osapuolten sotilaallisen voiman eroihin, toinen toisen osapuolen käyttämiin menetelmiin, jotka antavat sille edun, ja kolmas intressien eroon, joka liittyy toisen osapuolen vahvempaan tahtoon tai erilaiseen näkemykseen käytävän sodan luonteesta. Viimeinen tyyppi tuottaa asymmetrisiä strategioita, joiden Freedman väittää keskittyvä kivun tuottamiseen voiton sijaan. Ne pelaavat aikaa vastustajan arvoja vastaan. Kotimaisittain Jyri Kosola on esittänyt, että asymmetriaa on pyritty hakemaan hyödyntämällä tekniikkaa uusissa suorituskykykonsepteissa, lukumäärän tai toimintatavan kautta tai siirtämällä taistelu ympäristöön, jossa vastustajan vahvuuksista ei ole hyötyä.[288] Jälkimmäinen asymmetrian muoto on sikäli kiinnostava, että se kiinnittää huomion ympäristöön asymmetrian mahdollistajana ja lähteenä.

Asymmetrian muodoista ja seurauksista on käyty vilkasta keskustelua. Huomio on siirtynyt materiaalisista ja toiminnallisista tekijöistä kohti toimijoiden luonnetta. Ivan Arreguin-Toftin mukaan asymmetrian lähteenä on haavoittuvuuksien, voimaerojen ja metodien sijaan erilainen ymmärrys sodasta, tämän ymmärryksen ohjaama joukkorakenne ja sisäpoliittiset tekijät.[289] Myös Stephen Biddle on päätynyt siihen tulokseen, että voitto ja tappio ovat riippuvaisia doktriinista eli siitä, miten voimaa käytetään.[290] Voiman käyttämistä ohjaa strateginen kulttuuri, joten kulttuurista tulee

---

[286] Aihe liittyy vahvasti hyökkäyspuolustus teoriaan (*offense – defence theory*) (Biddle (2004)). Ks. Esim. Shlapak, D. A. and Johnson, M. W.: *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of Baltics*. RAND, Santa Monica, 2016; Heginbotham, E. (ed.): *The U.S. - China Military Scorecard: Forces, Geography, and the Evolution of Balance of Power 1996-2017*. RAND, Santa Monica, 2017.

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

[288] Kosola, Jyri: Teknologia 2030+. Vaikutukset tulevaisuuden sodankäyntiin. Teoksessa *Tuleva sota. Tulevaisuuden sodan tulevaisuus*. Rantapelkonen, Jari (toim.) Edita, Helsinki, 2018, s. 44–83, s. 78.

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

[290] Biddle (2004), s. 194–196; Posen, B.: *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars*. Cornell University Press, Ithica, 1984.

asymmetrian lähde. Emily Goldman ja Leslie Eliason ovat väittäneet, että valtioiden pyrkiessä kompensoimaan (*offset*) voimakkaampien valtioiden etuasemaa, ne kehittävät erityisiä suorituskykyjä ja käsitteellisiä innovaatioita. Näin syntyvä asymmetria perustuu siis teknologiaan ja ideoihin ja etenkin toimijan suhteeseen sotataidon innovaatioiden kulloiseenkin johtovaltioon.[291]

Asymmetriakeskustelu on koskettanut myös kybersodankäyntiin liittyvää teoretisointia. Ei-valtiolliset toimijat ovat olleet kybertilaa koskevan turvallisuustutkimuksen keskiössä. Kyberterrorismia ja rikollisuutta koskeva diskurssi on 1990-luvulla vaikuttanut Yhdysvaltojen ja useimpien Euroopan maiden kyberstrategioihin.[292] Nämä uhat on tulkittu luonteeltaan asymmetrisiksi suhteessa valtiovaltaan. Myös kriittisen infrastruktuurin käsite, joka on keskeinen informaatioyhteiskunnan toiminnan ja kybersodankäynnin ymmärtämiselle, on luonteeltaan asymmetrinen. Se perustuu näkemykselle modernien, kehittyneiden valtioiden haavoittuvuudesta ei-valtiollisten ja valtiollisten toimijoiden suhteellisin pienin resurssein tekemille hyökkäyksille. Narratiivit "kyber-Pearl Harbourista" tai vastaavista yllättävistä katastrofeista perustuvat ajatukselle siitä, että pahantahtoiset tahot voivat aiheuttaa suhteetonta vahinkoa kyberhyökkäyksin, joita vastaan valtiot eivät kykene luomaa deterrenssiä.[293] Kybersodankäyntiä itsessään on kutsuttu epätavanomaiseksi ja asymmetriseksi.[294] NATO:n kyberdoktriinin mukaan kybertilan ominaisuuksiin kuuluvat asymmetriset vaikutukset, joilla viitataan vastustajien kokoon, voimaan ja vaikutusten epäsuhtaan.[295]

---

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

[292] Kaplan (2016). Potomac Institute on tuottanut raportteja kansallisista kyberstrategioista ks. esim. Potomac Institute for Policy Studies: *Netherlands Cyber Readiness at a Glance*, 2017. [http://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf], luettu 15.4.2020; Lewis, James A.: National Perceptions of Cyber Threats. *Strategic Analysis*, Vol. 38, No. 4 (2014), s. 566–578; Guitton, Clement: Cyber insecurity as a national threat: overreaction from Germany, France and the UK? *European Security*, Vol. 22, No. 1 (2013), s. 21–35; Lewis (2014).

[293] Kyber-Pearl Harbourista ks. Clarke & Knake (2010); Clarke & Knake (2019).

[294] Ks. Geers (2011); Choucri (2012), s. 223–224; Nye (2010), s. 5.

[295] NATO: *Allied Joint Doctrine For Cyberspace Operations, AJP-3.20, Edition A Version 1, January 2020*. NATO Standardization Office (NSO), 2020. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf], luettu 13.7.2020.

Eräiden mielestä kyberhyökkäysten asymmetrisyys on liioiteltua. Vaikka valtiot eivät kykenisikään torjumaan kaikkia hyökkäyksiä, ne voivat käyttää resurssejaan kasvattaakseen strategisiin vaikutuksiin pyrkivien hyökkäysten kustannuksia. Attribuution ongelma on ratkaistavissa ajan kanssa ja deterrenssiin liittyvä rankaiseminen voidaan toteuttaa jokin toisen toimintaympäristön kautta.[296] Näkemyksiä kyberhyökkäyksen paremmuudesta suhteessa puolustukseen sekä kyberaseiden alhaisista kustannuksista, nopeudesta ja tehokkuudesta verrattuna tavanomaisiin tai ydinaseisiin on viime aikoina alettu myös haastaa.[297]

Toiset ovat kiinnittäneet huomionsa kybertoimintaympäristön tuottamaan asymmetriaan. Martin Libicki on väittänyt, että USA on digitalisaation takia varsin riippuvainen Internetistä ja näin ollen haavoittuvainen, mutta on toisaalta myös vahvoilla, sillä suurin osa maailmassa käytettävistä ohjelmistoista tulee Yhdysvalloista. Kilpailevien suurvaltojen vaihtoehtoiset ratkaisut eivät toisi suojaa, koska niiden pieni käyttäjäkunta heikentää koodin laatua. Libicki toteaa myös, että valtiot ovat varsin riippuvaisia ”kolmansien tahojen” osaamisesta eli kansainvälisistä tietoturvayrityksistä.[298] David Betz ja Tim Stevens ovat tarkastelleet keskustelua, jossa avoimien (Länsi) ja valvottujen (Kiina) kansallisten verkkojen välillä esitetään olevan asymmetriaa, joka hyödyttäisi jälkimmäistä kyberkonfliktin aikana. He suhtautuvat kuitenkin ajatukseen kriittisesti, sillä heidän mukaansa yksikään suursota ei pysyisi pelkästään kybertilan puolella. Tästä johtuen asymmetriaa kompensoitaisiin muilla voimavaroilla ja käytön muodoilla.[299]

Asymmetrian merkitys kybersodankäynnin kontekstissa on muuttunut etenkin 2010-luvulla. Se johtuu kahden erillisen käsitteen kehittymisestä: resilienssin (kybersietoisuuden) ja kyber-A2/AD:n. Resilienssin näkökulmasta kyberhyökkäyksiä tapahtuu jatkuvasti ja päämääränä on minimoida niiden vaikutus eli riskit ja maksimoida hyökkääjän investointikustannukset. Asymmetrian näkökulmasta kyseessä on hyökkäyksestä saatavan edun kiistäminen minimoimalla sen vaikutukset.

---

[296] Libicki (2009); Gartzke & Lindsay (2015); Mahnken (2011), s. 61–62.
[297] Ks. Slayton (2017); Liff (2012); Rid & McBurney (2012). Tämä keskustelu liittyy hyökkäyspuolustusteoriaan ja todistaa kylmän sodan ajan käsitteiden vaikutuksesta kyberilmiöiden tulkinnassa. Ks. Robert Jervis hyökkäyspuolustusteoriasta ja Charles L. Glaser sen kritiikistä (Jervis (1978), s. 187–190; Glaser, Charles L.: The Security Dilemma Revisited. *World Politics*, Vol. 50, No. 1 (1997), s. 171–201, s. 194–199).
[298] Libicki (2016), s. 201-209.
[299] Betz & Stevens (2011), s. 93.

Alison Lawlor Russell on siirtänyt A2/AD konseptin kybertilaan. Hän määrittelee kyber-A2/AD:n toimiksi, joiden on tarkoitus kiistää valtion pääsy kybertilaan ja/tai heikentää sen kykyä operoida siellä vapaasti.[300] Hänen mukaansa kybertila on haavoittuvainen voimankäytölle, vaikkakin haavoittuvuuden hyödyntäminen vaatii merkittävää voimankäyttöä niin fyysisellä kuin syntaktisella tasolla. Kyber-A2/AD ja resilienssin käsiteet osoittavat, kuinka kybertila nähdään yhä suuremmassa määrin valtiollisesta ja territoriaalisesta näkökulmasta. Kyberasymmetriaa tarkasteltaessa siihen siis liittyvät entistä tiiviimmin kysymykset esimerkiksi ympäristöstä, paikasta, rajoista, liikkeestä ja väylistä.

Asymmetrian käsitteen määrittely on ollut huomattavasti haastavampaa kuin sen muotojen tai seurausten tarkastelu. Vuonna 2001 Steven Metz ja Douglas Johnson väittivät, että ”strateginen asymmetria oli jonkin eron käyttämistä edun hankkimiseksi vastustajasta.”[301] Heidän mukaansa asymmetria on: ”Sotilaallisten suhteiden ja kansallisen turvallisuuden kehyksessä […] toimimista, organisoitumista ja ajattelemista eri tavalla kuin vastustajat omien etujen maksimoimiseksi, vastustajan heikkouksien hyväksi käyttämiseksi, aloitteen tempaamiseksi tai suuremman toiminnan vapauden saavuttamiseksi.”[302] Vaikka Metzin ja Johnsonin määritelmä on varsin lavea, sen mielenkiintoisin piirre on vastustajasta poikkeavan ajattelun korostaminen ja aktiivisuus. Metzille ja Johnsonille asymmetria on selvästi tulosta määrätystä käyttäytymisestä, ei konfliktin luonteesta.[303]

Morgan Forrest et al. ovat esittäneet seuraavan asymmetrian määritelmän: ”Asymmetrinen vahvuus tai heikkous on yksinkertaisesti sellainen toisen osapuolen ominaisuus, joka toiselta merkittävissä määrin puuttuu. Asymmetrinen hyökkäys hyväksi käyttää tätä epäsuhtaa suorituskyvyissä tai jotain muut heikkoutta, jota ei kyetä puolustamaan, riippumatta käytettävän aseen tai taktiikan luonteesta.”[304] Asymmetriaksi ei kelpaa

---

[300] Lawlor Russell (2015), s. 154.
[301] Metz & Johnson (2001), s.1.
[302] Ibid., s. 5–6.
[303] Ks. Huttunen (2010); Lalu, Petteri: *Syvää vai pelkästään tiheää: neuvostoliittolaisen ja venäläisen sotataidollisen ajattelun lähtökoh-dat, kehittyminen, soveltaminen käytäntöön ja nykytilanne. Näkökulmana 1920- ja 1930-luvun syvän taistelun ja operaation opit*. Akateeminen väitöskirja, Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 1 Nro 3/2014, Helsinki, 2014. Taktiikan, operaatiotaidon ja strategian käsitteistä ks. Vego (2017).
[304] Morgan, Forrest E., Mueller, Karl P., Medeiros, Evan S., Pollpeter, Kevin L. & Cliff, Roger: *Dangerous Thresholds. Managing Escalation in the 21st Century*. RAND, Santa Monica, 2008, s. xv.

pieni tai rajallinen etu. Tämä viittaa siihen, että asymmetria voidaan jotenkin mitata ja että se liittyy osapuolten ominaisuuksiin tai piirteisiin.

Yksi viimeisimmistä ja mielenkiintoisimmista asymmetrian määritelmistä kybertilan kontekstissa on Oehmen et al. esittämä.[305] He määrittelevät asymmetrian: ”suhteettomaksi, hyväksikäytettävissä olevaksi epätasapainoksi toimijoiden välillä, joka liittyy, muttei rajoitu, resursseihin, toiminnan intensiteettiin (*level of effort*), riskiin ja seurauksiin.” Määritelmä on muodostettu tukemaan kyberresilienssin ja puolustuksen kvantitatiivista vertailua toimijoiden välisen suhteen kautta, eikä se ole sidoksessa määrättyyn toimijaan, käytökseen tai menetelmään. Oehmen et al. jakavat asymmetrian määrällisiin ja kyvykkyyseroihin. Molemmat ovat suhteellisia, mutta edellinen on yhteismitallinen kun taas jälkimmäinen on fundamentaalinen, suhteeton ja monikertainen etu. Oehmen et al. liittävät kyvykkyyseroihin kyvyn muokata maastoa suosimaan suhteettomasti puolustajaa.

Huolimatta siitä, että Oehmen et al. ja eräät muuta aikaisemmin mainitut ovat laajentaneet asymmetrian käsitettä koskemaan kybertilan muokkaamista, läntinen näkökulma on edelleen varsin yksipuolinen. Se kärsii kulttuurisesta vinoumasta, jossa ”muiden” toimet nähdään hyökkäyksellisiksi ja omat puolustuksellisiksi. Se rakentaa keinotekoisen dikotomian hyökkäyksen ja puolustuksen välille ja sivuuttaa ”voimankäytön dialektiikan.” Ja se on edelleen suurimmassa määrin sidoksissa ei-valtiollisiin toimijoihin ja ajatukseen kybertilasta ”yhteiskäyttöalueena” (*commons*), jossa valtiorajoilla ei pitäisi olla merkitystä. Näin ollen asymmetria on läntisessä diskurssissa lähtökohtaisesti jotain uhkaavaa, hyökkäävää ja kybertilan ominaispiirteistä, ei rakenteista tai voimasuhteista, riippuvaa.[306]

---

[305] Oehmen, Christopher & Multari, Nicholas: *AiR: Asymmetry in Resilience: Report on the First Meeting on Asymmetry in Resilience for Complex Cyber Systems*, U.S. Department of Energy, 2014. [https://cybersecurity.pnnl.gov/documents/AiR_1.0_Final_Report.pdf], luettu 15.4.2020; Oehmen, Christopher & Multari, Nicholas: *AiR2: Second Meeting on Asymmetry in Resilience Report on the Second Meeting on Asymmetry in Resilience for Complex Cyber Systems*, U.S. Department of Energy, 2016. [https://cybersecurity.pnnl.gov/documents/AiR_2.0_Final_Report.pdf], luettu 15.4.2020.

[306] Läntistä asymmetrian käsitettä jo vuonna 2005 arvostellut vastaavilla perusteilla Timothy Thomas (Thomas, Timothy: *Cyber Silhouettes. Shadows Over Information Operations*. Foreign Military Studies Office, Fort Leavenworth, KS, 2005).

Asymmetrian pohdinta ei ole läntisen sotatieteen yksinoikeus. Myös venäläiset sotatieteilijät ovat pyrkineet määrittelemään asymmetriaa.[307] Esimerkiksi A. Selivanov ja S. Tšvarkov ovat tarkastelleet ”asymmetristen toimien strategiaa ja konseptia” vahvan ja heikon valtion suhteen kautta. Heidän mukaansa molemmat voivat toimia asymmetrisesti pyrkiessään maksimaaliseen menestykseen minimaalisin kuluin. Valitut keinot riippuvat osapuolten voimasuhteesta.[308] Selivanovin ja Tšvarkovin ajatusten taustalla on venäläinen näkemys suurvaltasuhteista jatkuvana suurvaltojen kamppailuna tai vastakamppailuna (*protivoborstvo*).[309] Sen kulkua määrittelevät poliittisella, sotilasstrategisella, operatiivisella ja taktisella tasolla vaikuttavat määrälliset ja laadulliset symmetrisiin ominaisuuksiin perustuvat voimasuhdelaskelmat (*sootnošenie sil i sredstv*), joiden juuret ovat neuvostoliittolaisessa sotatieteellisessä ajattelussa.[310] Nykyisessä venäläisessä ajattelussa asymmetriset toimet tarjoavat mahdollisuuden kiertää epäedullisia voimasuhteita. Esimerkiksi johtavien sotilasteoreetikkojen S. G. Tšekinovin ja A. Bogdanovin mukaan asymmetrinen lähestymistapa (*asimmetrinyi podhod*) perustuu ei-identtisiin toimintamahdollisuuksiin pohjautuviin toimintatapoihin ja suorituskykyihin, jotka mahdollistavat suoran yhteenoton välttämisen vastustaja (poliittisesti) voittaen.[311] Asymmetriset toimet neutraloivat tai kompensoivat (*nivelirovat'*) vastustajan teknologisen ylivoiman.[312]

Venäjän nykyinen sotilasjohto on useaan otteeseen osoittanut mielenkiintonsa asymmetrian käsitettä kohtaan. Venäjä nähdään heikompana osapuolena, jonka tulee käyttää laajaa sotilaallisten ja ei-sotilaallisten keinojen valikoimaa joustavasti tapauskohtaisesti, poikkihallinnollisesti ja kustannukset minimoiden. Yleisesikunnan päällikkö kenraali Valeri Gerasimov on käskenyt luoda asymmetristen

---

[307] Kokonaisvaltaisin ja tuorein esitys tästä ajattelusta on Thomas (2019).

[308] Селиванов, А.А. & Чварков, С.В.: О стратегии и концепции ассиметричных действий. *Вестник академии военных наук*, № 3 (72) 2020, с. 57–63.

[309] *Protivoborstvo* käsitteestä ks. Kukkola (2020a).

[310] Lider, Julian: The Correlation of World Forces: The Soviet Concept. *Journal of Peace Research*, Vol. 17, No. 2 (1980), s. 151–171; Reach, Clint, Kilambi, Vikram & Cozad, Mark: *Russian Assessments and Applications of the Correlation of Forces and Means*. RAND, Santa Monica, 2020.

[311] Чекинов, С. Г. & Богданов, С. А.: Асимметричные действия по обеспечению военной безопасности России. *Военная Мысль*, № 3 2010, с. 13–22.

[312] Фадеев, А. С. & Ничипор, В. И.: Военные конфликты современности, перспективы развития способов их ведения. прямые и непрямые действия в вооруженных конфликтах XXI века. *Военная Мысль*, № 9 2019, с. 33–41.

toimien kattavan (*comprehensive*)[313] tai holistisen (*holistic*)[314] teorian, käännöksestä riippuen (alkup. *tslostnyi*).[315]

Katri Pynnöniemen mukaan venäläinen asymmetrinen lähestymistapa (*assymmetric approach*) koostuu käytännössä kolmesta konseptista: organisaatioaseesta (*organizational weapon*), refleksiivisestä kontrollista (*reflexive control*)[316] ja aktiivisista toimenpiteistä (*active measures*). Hän liittää käsitteen venäläisiin informaatio- ja vaikuttamisoperaatioihin, jotka ovat osa Venäjän ulko- ja turvallisuuspolitiikkaa.[317] Toinen käytännön lähestymistapa liittyy asymmetriseen vasteeseen (*otvet*), joka on strategisen tason konsepti. Sitä voi kuvata pyrkimykseksi kiistää vastustajan hyökkäyksellinen ylivoima ja puolustuskyky samaan aikaan omat järjestelmät suojaten halvalla ja innovatiivisesti. Järjestelmät voidaan tässä tapauksessa ymmärtää kapeasti asejärjestelminä tai laveasti valtionhallintona, yhteiskuntana ja taloutena.[318]

Venäläisen asymmetria-ajattelun taustalla vaikuttaa informaatiosodankäynnin merkityksen kasvu sekä Lännen ”hybridisodankäyntidiskurssi”, joka on pyritty omaksumaan ja tulkitsemaan venäläisittäin.[319] Niin Venäjän kuin Lännen sotilasajattelijat

---

[313] Gerasimov, Valery: The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. Originally published in Military-Industrial Kurier, 27 February 2013.1 Translated from Russian 21 June 2014 by Robert Coalson, editor, Central News, Radio Free Europe/Radio Liberty. *Military review*, January-February 2016, s. 23–29.

[314] Thomas (2019).

[315] Герасимова, В.В.: Основные тенденции развития форм и способов применения вооруженных сил, актуальные задачи военной науки по их совершенствованию. *Вестник Академии военных наук*, № 1 (42) 2013, с. 24-29; Картаполов, А.В.: Уроки военных конфликтов, перспективы развития средств и способов их ведения. Прямые и непрямые действия в современных международных конфликтах. *Вестник Академии военных наук*, № 2 (51) 2015, с. 26–36; Герасимов, В.В.: Организация обороны Российской Федерации в условиях применения противником «традиционных» и «гибридных» методов ведения войны. *Вестник Академии военных наук*, № 2 (55) 2016, с. 19–23, с. 20.

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

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

[318] Kukkola (2020a).

[319] Thomas (2015); Kukkola (2020a); Renz, Bettina: Russia and ‘Hybrid Warfare’. *Contemporary Politics*, Vol. 22, No. 3 (2016), s. 283–300; Pynnöniemi & Jokela (2020);

ovat olleet 2000–2010-luvuilla entistä kiinnostuneempia informaatiosta aseena ja huolestuneempia siitä haavoittuvuutena. Näissä pohdinnoissa kybertilalla ymmärrettynä informaation teknisenä alarakenteena (infrastruktuurina) on ollut merkittävä rooli.[320] Läpimurtoteknologioista tulee informaatiosodankäynnissä asymmetrian lähde. Hybridikeskustelussa, joka on vahvasti politisoitunut, asymmetria muuntuu niin Venäjällä kuin Lännessä helposti joksikin, mitä ”ne” tekevät ”meille” aseellisen voiman käytön kynnyksen alapuolella. Viime aikoina hybridisodankäynnin käsitettä on Lännessä syystäkin arvostelu hysteeriseksi, epähistorialliseksi ja analyyttisesti tyhjäksi.[321]

Kiinalaiseen sotataitoon historiallisesti liittyvä sotajuonien (*stratagem*) käsite on hyvin lähellä asymmetrialle annettuja läntisiä ja venäläisiä merkityksiä.[322] 2000-luvun alusta alkaen asymmetrian käsite on kiinalaisessa keskustelussa liittynyt sodankäynnin ”informatisaatioon.” Yleisellä tasolla asymmetrian nähdään syntyvän osapuolten erilaisista kyvyistä ja ominaisuuksista, tavoista käydä sotaa ja ympäristötekijöistä.[323] Käytännön tasolla asymmetriaa voidaan soveltaa kehittämällä yllättävän edun tarjoavia teknologisia suorituskykyjä (*assassins mace*) tai vaikuttamalla informaation kautta vastustajan kykyyn ja haluun taistella.[324] Läntisissä tulkinnoissa Kiinan pyrkimykset kehittää sotavoimiaan ja doktriiniaan on säännönmukaisesti tulkittu ”asymmetrisiksi.”[325]

NATO: *Brussels Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018.* [https://www.nato.int/cps/en/natohq/official_texts_156624.htm], luettu 24.8.2020.

[320] Freedman (2006); Libicki (2009); Geers (2011); Inkster (2016); Kaplan, Fred: *Dark Territory. The Secret History of Cyber War*. Simon & Schuster, New York, 2016.

[321] Kukkola (2020a); Pynnöniemi & Jokela (2020); Wither, James K.: Making Sense of Hybrid Warfare. *Connections*, Vol. 15, No. 2 (Spring 2016), s. 73–87; Johnson (2018); Mälksoo, Maria: Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO. *European Security*, Vol. 27, No. 3 (2018), s. 374–392.

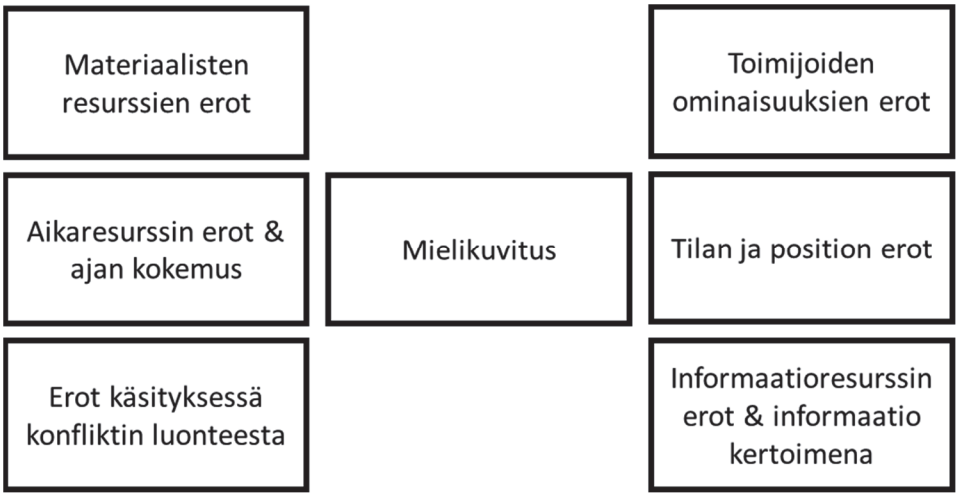
[322] Stone, Christopher: The Implications of Chinese Strategic Culture and Counter-intervention upon Department of Defense Space Deterrence Operations. *Comparative Strategy*, Vol. 35, No. 5 (2016), s. 331–346.

[323] Thomas, Timothy: *The Chinese Way of War: How Has it Changed*? MITRE, McLean, VA, 2020, s. 70.

[324] Dossi, Simone: On the Asymmetric Advantages of Cyberwarfare. Western Literature and the Chinese Journal Guofang Keji. *Journal of Strategic Studies*, Vol. 43, No. 2 (2020), s. 281–308.

[325] Johnson, James S.: China’s Vision of the Future Network-centric Battlefield: Cyber, Space and Electromagnetic Asymmetric Challenges to the United States. *Comparative Strategy*, Vol. 37, No. 5 (2018), s. 373–390.

Perustuen edellä esitettyihin asymmetrian sotilaallisiin ja kybersodankäyntiin liittyviin määritelmiin voidaan asymmetrialla väittää olevan vähintään seitsemän eri merkitystä (Kuva 4).



Kuva 4: Asymmetrian seitsemän eri merkitystä

Ensinnäkin asymmetria voi perustua materiaalisten resurssien suhteelliseen epätasapainoon. Se ilmenee esimerkiksi heikkojen ja vahvojen valtioiden sekä valtioiden ja ei-valtiollisten toimijoiden materiaalisissa voimavara- eli resurssieroissa. Toiseksi asymmetria voi perustua suhteellisiin perusluontoisiin eroihin ominaisuuksissa. Nämä voidaan ymmärtää suorituskykyinä, keinoina, informaationa (ks. alas), doktriineina, organisaatioina, normeina ja kulttuureina. Tämä asymmetria pohjaa olennaisiin laadullisiin vahvuuksiin ja heikkouksiin tai peräti puutteisiin. Kolmas asymmetria muoto on myös suhteellinen, mutta perustuu konfliktin luonteeseen ja osapuolten käsitykseen siitä. Se koostuu tahdosta, intresseistä ja päämääristä. Nämä ovat ei-materiaalisia tekijöitä, jotka vaikuttavat kustannus-hyötylaskelmiin.

Asymmetrian neljäs muoto liittyy tilaan. Se on rakenteellinen, koska se on toiminnan kontekstin ominaisuus, joka sotilasstrategian tapauksessa on taistelukenttä ja vaikuttaa kaikkiin toimijoihin riippuen näiden positiosta. Se mahdollistaa tai rajoittaa toimijan kykyä havainnoida ympäristöään, projisoida voimaa ja suojella resurssejaan. Viidenneksi asymmetria voi perustua aikaan. Aika voidaan ymmärtää toimijan ominaisuutena eli

ajantajuna. Toiset kokevat ajan lineaariseksi ja toiset sykliseksi.[326] Aika voidaan ymmärtää myös resurssina, koska toimijalla voi olla joko enemmän tai vähemmän aikaa tavoitteidensa saavuttamiseen kuin vastustajalla (tai johonkin tulevaan tapahtumaan nähden). Tämä näkemys vastaa erityisesti verkostokeskeisen sodankäynnin teorian premissejä.[327] Aika liittyy myös tilaan. Sotilaallisessa toimintaympäristössä etäisyys on vaihdantasuhteessa aikaan, missä liike tilan läpi kuluttaa aikaa. ”Ajan hinta” viittaa siihen, että aikaa voidaan käyttää johonkin. Itseasiassa, tila ja aika ovat niin sidoksissa toisiinsa, että niiden erottaminen on lähes toivotonta.

Informaatio voidaan ymmärtää osaksi kaikkia tässä esitettyjä ymmärryksiä asymmetriasta. Se esimerkiksi läpäisee kybertoimintaympäristön rakenteena, prosessina ja sisältönä. Läntisessä ja venäläisessä ajattelussa informaatio nähdään joksikin, jota voidaan kontrolloida ja jonka suhteen voidaan hankkia ylivoima suhteessa vastustajaan.[328] Informaatio voidaan siis nähdä resurssina, mutta se ei ole verrattavissa materiaan tai energiaan.[329] Informaatio voidaan itse asiassa nähdä perusluonteeltaan asymmetrisenä, koska se muuttuu ja saa uusia muotoja jatkuvasti, on ennustamaton ja saa merkityksensä ympäristönsä muuttuessa.[330] Informaation piirteet, ajankohtaisuus, täydellisyys tai eheys, voivat toimia resurssien tai ominaisuuksien kertoimina. Näin ollen informaatio on yhtäältä asymmetrian tekijä ja toisaalta sen kuudes ilmenemismuoto.

Asymmetrian seitsemäs muoto on mielikuvitus. Se on äärimmäinen mahdollistaja ja luo asymmetriaa perustuen puhtaaseen luovuuteen. Sen

---

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

[327] Arquilla & Ronfeldt (1997); Alberts, David S., Gartska, John J. & Stein, Frederick P.: *Network Centric Warfare: Developing and Leveraging Information Superiority* (2nd ed.). CCRP Publications, 2000.

[328] The United State Department of Defence (U.S. DoD): *Joint Publication 3-13: Information Operations*; 27 November 2012 Incorporating Change 1 20 November 2014. [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf], luettu 11.1.2021; Kolton (2017); Kukkola (2020a).

[329] Mingers, John & Standing, Craig: What is Information? Toward a Theory of Information as Objective and Veridical. *Journal of Information Technology*, Vol. 33 (2018), s. 85–104.

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

vaikutus perustuu subjektin tahdon kykyyn vaikuttaa todellisuuteen tuntemalla ja manipuloimalla sitä ohjaavia lakeja.[331]

2.4 Rakenteellinen kyberasymmetria

Perustuen edellä esitettyyn voidaan väittää, että sellainen käsitys asymmetriasta, joka liittyy ajatukseen heikommasta, mahdollisesti attribuutiota välttelevästä, ei-valtiollisesta toimijasta, joka käyttää epätavanomaisia keinoja, on liian rajallinen näkemys kybertilan kontekstissa. Ensiksikin voiman diffuusio tekee valtiollisten ja ei-valtiollisten toimijoiden erosta vähemmän merkittävää.[332] Kybertila ei ole ympäristö, jossa vastustajat piilottelevat koodin seassa, kuten kumoukselliset kansan seassa.[333] Lisäksi, koska jopa kehittyneet haittaohjelmat ovat yleisesti saatavilla ja kyberkeinojen jatkuva yleistyminen ja kehittyminen rapauttaa niiden ”epätavanomaisuutta”, menetelmät eivät määrittele asymmetriaa kybertilassa.[334]

Toiseksi. Vallalla oleva läntinen näkemys koskien sotilaallista asymmetriaa perustuu määrättyjen keinojen tai ei-valtiollisten toimijoiden kohteena olemiseen. Valtioiden välisissä suhteissa esiintyvät puolustuksellisen ja hyökkäyksellisen asymmetrian muodot jätettiin huomiotta, kunnes Venäjän ja Kiinan suorituskyvyistä alkoi muodostua uhka 2010-luvulla. Herännyt kiinnostus on kuitenkin kiinnittynyt liiaksi määrättyjen suurvaltojen toimiin. Voimaepätasapainon kehitystä ja sen vaikutusta valtioiden toimintaan tulisi tutkia erillään määrättyjen suurvaltojen strategisista intresseistä ja poliittisista asetelmista.

Kolmanneksi. Asymmetrian hyväksikäyttö on mahdollista, koska asymmetria kuuluu kahden tai useamman osapuolen suhteeseen ja on riippumatta merkityksestään havaittavissa ja arvioitavissa. Mikäli asymmetrian olemassaolo on tiedossa rauhan, kiristyneen kilpailun,

---

[331] Тюшкевич, С. А.: *О законах войны вопросы военной теории и методологии*. Проспект, Москва, 2017, s. 45–47.
[332] Nye (2010); Libicki (2016), s. 202–209; Gartzke (2013); Maurer (2018), s. 149–150.
[333] Smith (2008), s. 19.
[334] Sanger (2018), s. 227–230. Kyberuhkien ja hyökkäysten jatkuvasta yleistymisestä ks. Centre for Strategic and International Studies: *Significant Cyber Incidents, September 2018.* [https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity], luettu 7.5.2020; Council on Foreign Relations: *Cyber Operations Tracker, September 2018.* [https://www.cfr.org/interactive/cyber-operations], luettu 7.5.2020.

syttyvän konfliktin tai sodan aikana, sitä voidaan hyödyntää ennalta ehkäisyn, deterrenssin, eskalaation hallinnan ja avoimen sotilaallisen voimankäytön osana. Suhteeton etu, on se sitten sotilaallinen tai muunlainen, on vähintään merkittävä suorituskyvyn kerroin. Asymmetrialla on siis kiistämättä strategista vaikutusta.

Neljänneksi. Poiketen muista toimintaympäristöistä, joiden kontekstissa asymmetriaa voi muodostua, kybertila on keinotekoinen ja sitä voidaan muokata perustuen voimakkaiden toimijoiden turvallisuusintresseihin. Täten osia kybertilasta voidaan muokata tuottamaan etu valtiotason kyberkonfliktissa, luomaan perusta valtiosuvereniteetin ulottamiselle kybertilaan tai ehkäisemään kybertilasta nousevia uusia uhkia ja haavoittuvuuksia.[335] Kybertilan muokkaaminen voi näin ollen luoda potentiaalista asymmetriaa, jota tässä työssä kutsutaan rakenteelliseksi kyberasymmetriaksi.

Rakenteellisen kyberasymmetrian käsitettä tarvitaan Venäjän ja eräiden muiden valtioiden strategioiden ymmärtämiseksi. Niiden tavoitteena on muokata ja kontrolloida kansallisia digitaalisesti ja fyysisesti määrittyneitä maantieteellisiä osia Internetistä. Kyberasymmetrian käsite auttaa kiinnittämään huomion valtioiden Internetin kontrollipyrkimysten sotilasstrategiseen luonteeseen. Kyseessä on taistelutilan muokkaaminen, ei pelkästään hallinnollinen (*governance*) tai ihmisoikeuskysymys. Teoreettisesta näkökulmasta katsoen Venäjä, tai mikä tahansa valtio, kykenee käyttämään kybervoimapotentiaaliaan muokatakseen ja kontrolloidakseen muuttuvaa, teknologiaperusteista ja ihmisen luomaa kybertilaa haluamaansa suuntaan. Näin se muuttaa tilan rakennetta tavalla, joka tuottaa rakenteellista kyberasymmetriaa, mikäli mahdolliset vastustajat pidättäytyvät vastatoimista. *Rakenteellinen kyberasymmetria on siis kybertilan ominaisuus, joka syntyy kahden tai useamman toimijan välille, kun kybertilan rakennetta ja sääntöjä muokataan, niin että yksi toimijoista saa epäsuhtaisen ja hyväksikäytettävän puolustuksellinen ja hyökkäyksellisen edun toisiin toimijoihin nähden*.

Rakenteellisen kyberasymmetrian teoreettisena ilmenemismuotona on suljettu kansallinen verkko. Se on valtion kontrolloima osa kybertilaa, joka

---

[335] Kiinan ja Venäjän pyrkimyksistä rakentaa ‘digitaalista’ tai ‘kybersuvereniteettia’ ks. Inkster (2016); Kolton (2017); Ristolainen, Mari: Should “RuNet 2020” be Taken Seriously? Contradictory Views about Cybersecurity between Russia and the West. *Journal of Information Warfare*, Vol. 16, No. 4 (2017), s. 113–131; Kari (2019); Kukkola (2020a).

voidaan teknisesti kytkeä irti globaalista Internetistä, mutta kykenee silti toimimaan kansallisten kriittisten palvelujen osalta normaalisti.[336] Sen vastakohtana on avoin kansallinen verkko, joka ei ole valtion suoraan kontrolloima, eikä sitä voida lähtökohtaisesti kytkeä irti globaalista kybertilasta ilman erityisiä valmisteluja tai yhteiskunnan kriittisen toimintojen ja talouselämän vakavia häiriöitä. Kansallisella verkolla yleisesti viitataan useiden eri järjestelmien ja verkkojen kokonaisuuteen, joka sijaitsee määrätyllä maantieteellisellä alueella ja jota operoivat määrätyn valtion oikeudellisen määräysvallan olevat yksityiset ja julkiset toimijat.

Rakenteellista kyberasymmetriaa kutsuttiin alun perin kyberasymmetriaksi tai asymmetrisiksi rintamalinjoiksi Juha Kukkolan, Mari Ristolaisen ja Juha-Pekka Nikkarilan kirjoittamassa konferenssipaperissa.[337] Käsitteen juuret ovat Nikkarilan ja Ristolaisen konferenssipaperissa, jossa he käyttivät taistelun elementtejä eli liikettä, tulta ja suojaa tarkastellakseen, mitä vaikutuksia voisi olla Venäjän pyrkimyksellä eristää kansallinen verkkonsa.[338] Heidän perusväitteensä oli, että paremman suojan lisäksi Venäjä voisi saavuttaa suhteellisen edun tulessa ja liikkeessä verkkonsa avoimina pitäviä valtioita kohtaan.[339] Kukkola, Ristolainen ja Nikkarila kehittivät suhteellisen edun ajatuksen asymmetristen rintamalinjojen analyyttiseksi kehykseksi. He käyttivät taistelun elementtien sijaan tietoverkkohyökkäys- ja tietojärjestelmätiedusteluoperaatioiden

---

[336] Kukkola (2020a), s. 94–95.

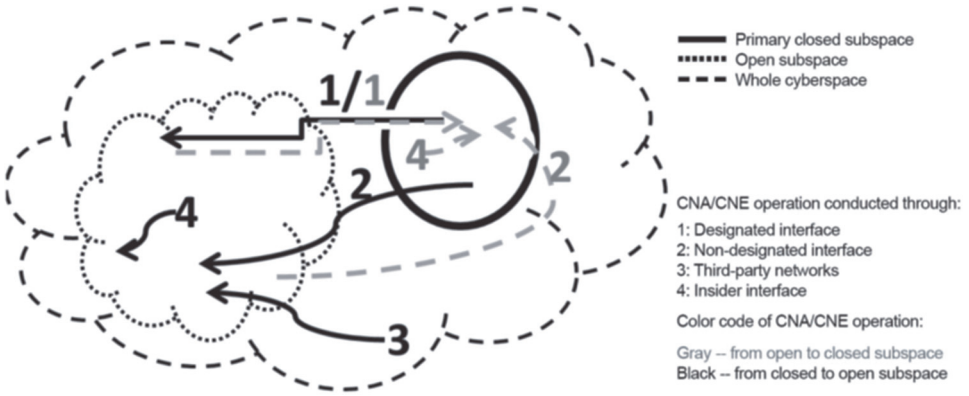
[337] Kukkola, Juha, Ristolainen, Mari & Nikkarila, Juha-Pekka: Confrontation with a closed network nation: Open network society's choices and consequences. *Presented at Military Communications (MILCOM) conference, Baltimore, USA, October 23.-25, 2017*.

[338] Kirjoittajat käyttivät käsitteitä läntiseen sotataidolliseen ajatteluun perustuen, vaikka ne esiintyvät myös suomalaisessa taktisessa ajattelussa (ks. Hollanti, Juha: *Alivoimaisen taktiikka. Suomalaisen taktisen ajattelun tarkastelu*. Akateeminen väitöskirja, Maanpuolustuskorkeakoulu, julkaisusarja 1: tutkimuksia No. 38. Maanpuolustuskorkeakoulu, Helsinki, 2019).

[339] Nikkarila, Juha-Pekka & Ristolainen, Mari: 'RuNet 2020' – Deploying traditional elements of combat power in cyberspace. *Presented in the International Conference on Military Communications and Information Systems (ICMCIS), Oulu, Finland, May 15.-16., 2017*. Konferenssipaperin inspiraationa toimi Ristolainen, Mari: Should 'RuNet 2020' be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West. Teoksessa *Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS) Dublin, Ireland, June 29.-30., 2017. Scanlon, Mark & Le-Khac, Nhien-An (eds.) 2017*, s. 370–379.

(CNA/CNE) hyökkäysvektoreita avoimien ja suljettujen verkkojen välisen asymmetrian tarkasteluun.[340]

Kuva 5 havainnollistaa, miten asymmetria saavutetaan rakentamalla suljettu kansallinen verkko. Kuvan nuolet ovat hyökkäysvektoreita avoimen verkon (pieni pilvi) ja suljetun kansallisen verkon (pallo) välillä kybertilan (iso pilvi) kehyksessä. Kuvaa tarkastellessa on tärkeää ymmärtää, että kansallisen verkon sulkeminen ei välttämättä tarkoita kaiken liikenteen katkaisua vaan liikennettä voidaan rajoittaa asteittain verkkoon, verkosta ja sen sisällä. Sulkemista laajempi käsite sulkemisprosessi viittaa prosessiin, jolla kehitetään ja otetaan käyttöön ne standardit, teknologiat ja hallinnolliset ja tekniset ratkaisut, joilla voidaan kansallisesti kontrolloida datan siirron, säilyttämisen ja muokkaamisen luotettavuutta, eheyttä ja saatavuutta.[341]



Kuva 5: Havainnekuva CNA/CNE operaatioiden toteuttamisesta suljetun kansallisen verkon ja avoimen verkon välillä (Kukkola, Ristolainen & Nikkarila (2017), s. 96)

Verkkonsa avoimena pitäneen ja sulkeneen valtion välisessä konfliktissa CNA/CNE operaatioita voidaan suorittaa suljetusta verkosta avoimeen liikenteelle virallisesti osoitettujen yhteyksien (*designated interface*), epävirallisten yhteyksien (*non-designated interface*), kolmannen tahon verkkojen kautta (*third-party networks*) tai avoimen verkon sisältä (*insider*

[340] Kukkola, Juha, Nikkarila, Juha-Pekka & Ristolainen, Mari: Asymmetric frontlines of cyber battlefields. *Presented at International Command and Control Research and Technology Symposium (ICCRTS), Los Angeles, USA, November 6.-8., 2017*.
[341] Kukkola, Ristolainen & Nikkaril (2017), s. 52.

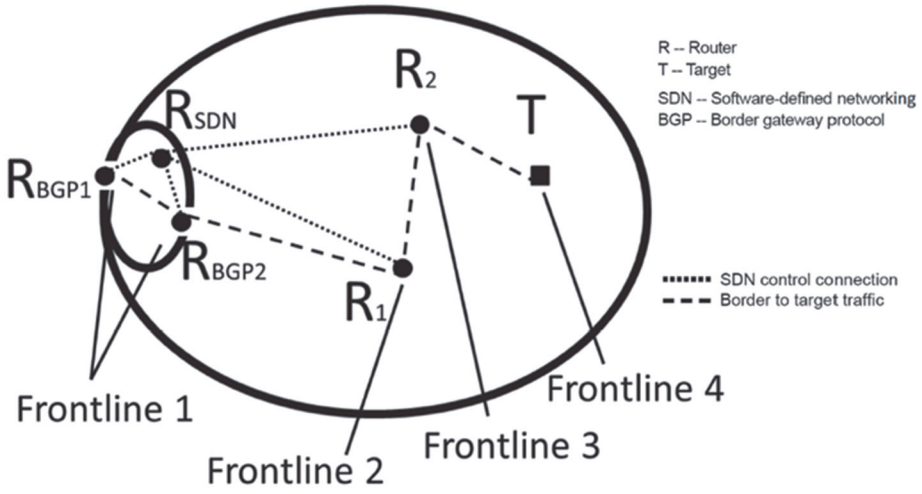
interface). Avoimesta verkosta suljettuun verkkoon operaatiot ovat mahdollisia osoitettujen yhteyksien kautta, epävirallisten yhteyksien kautta, mikä vaatii lisätoimia kyberturvallisuus ja puolustusjärjestelyjen kiertämiseksi, sekä suljetun verkon sisältä. Hyökkäykset kolmannen tahon verkkojen kautta käyttäytyvät kuin epäviralliset yhteydet.

Virallisesti liikenteelle osoitetut yhteydet ovat valvottuja ja säänneltyjä yhteyspisteitä. Ne koostuvat kaupallisiin sopimuksiin perustuvista solmupisteistä (*Internet Exchange Point, IXP*) kansallisten Internet yhteydentarjoajien (ISP) välillä, Border Gatweway protokollan (BGP) reititysalueista (*Autonomous Systems, AS*) ja fyysisistä valokuitu, kupari, mikrolinkki ja satelliittiyhteyksistä. Näiden yhteyspisteiden läpi kulkevaa liikennettä voidaan teoriassa jäljittää, attribuoida vähintään edelliseen liikennepisteeseen, analysoida reaaliajassa ja yhteydet voidaan tarvittaessa katkaista. Epäviralliset yhteydet ovat sääntelemättömiä ja mahdollisesti laittomia rajapintoja, jotka kuitenkin teknisesti sallivat liikenteen kansallisiin verkkoihin. Näitä voivat olla esimerkiksi mobiiliverkot, satelliittiperustaiset internetpalvelut ja sääntelemättömät kaapeliyhteydet. Niihin kuuluvat myös valtion rajojen sisällä olevat yritysverkot, joista pääsy kansallisiin verkkoihin on periaatteessa rajoitettu tai estetty. Lähtökohtaisesti ero virallisiin yhteyksiin on siis lähinnä hallinnollinen. Kolmansien tahojen verkot eivät ole suorassa yhteydessä avoimeen tai suljettuun verkkoon, mutta voivat toimia hyökkäysten lähtö- tai väliasemina. Sisäiset liittymät edellyttävät fyysistä yhteyttä kohdeverkkoon esimerkiksi massamuistisiirtovälinettä käyttäen, sivukanavatekniikalla tai muuten.

Tarkastelemalla CNA/CNE operaatioita eri yhteyksien kautta Kukkola, Ristolainen ja Nikkarila analysoivat avoimen ja suljetun kansallisen verkon suhteellista hyökkäys- ja puolustuskykyä. Analyysi perustui liikkeen vapauden (*freedom of movement*), tilannetietoisuuden (*situation awareness*) ja päätöksenteon (*decision-making*) vertailuun. Liikkeen vapaus viittasi kykyyn suorittaa puolustuksellisia ja hyökkäyksellisiä kyberoperaatioita omissa ja vastustajan verkoissa. Tilannetietoisuus viittasi kykyyn tietää kaikki taistelukentän merkittävät ilmiöt ja muiden toimijoiden aikeet ja kykyyn ennustaa tulevaa. Päätöksenteko viittasi kykyyn tehdä nopeita ja tarkoituksenmukaisia päätöksiä sekä toimeenpanna ne tehokkaasti. Kolmen tekijän kehyksenä toimi kybertaistelukenttä, joka määriteltiin kahden vastakkaisen osapuolen

välisen konfliktin sotilasoperaatioiden digitaalisena ulottuvuutena kybertoimintaympäristössä.[342]

Analyysin tuloksena oli epäsuhtainen ja hyväksikäytettävissä oleva etu verkkonsa sulkeneelle valtiolle. Lisäksi Kukkola et al. väittivät, että suljetun verkon sisällä olevat kerroksiset puolustusjärjestelmät korostivat valtion puolustuksellista etua. Väite perustui Venäjän kansallisen internetsegmentin hankkeesta tehtyihin havaintoihin sekä venäläisten akateemikkojen kirjoituksiin, joiden mukaan maa pyrki luomaan keskitetyn Internetin hallintajärjestelmän. Tämän järjestelmän hypoteettinen kuvaus on esitetty kuvassa 6.



Kuva 6: Yksinkertaistettu havainnekuva suljetun verkon sisäisistä rintamalinjoista (Kukkola, Ristolainen & Nikkarila (2017), s. 102)

Kuvassa reitittimet muodostavat kerroksittaisia rintamalinjoja, joiden läpi liikenteen tulee kulkea ja joissa se autentikoidaan. Liikenne, jolla ei ole lupaa kulkea verkossa, pudotetaan. Periaatteessa tämä järjestely vaikeuttaa myös kansallisen suljetun verkon sisältä tehtyjä hyökkäyksiä. Viimeinen rintamalinja ovat kohdepuolustusjärjestelmät. Kokonaisuutta ohjataan keskitetysti SDN (*software-defined networking*) teknologian avulla. Rintamalinjat ovat asymmetrisiä, koska niitä voi esiintyä vain suljetussa

[342] Kukkola, Nikkarila & Ristolainen (2017).

kansallisessa verkossa. Nikkarila et al. ovat todentaneet tämän asymmetrian matemaattisesti.[343]

Kukkolan et al. pääväite edellä esitettyyn perustuen on, että mikäli jokin valtio tai joukko valtioita päättää rakentaa kansallisen järjestelmän verkkonsa irti kytkemiseksi, eli toteuttaa teoreettisen suljetun kansallisen verkon, ne saavuttavat merkittävän strategisen edun niihin valtioihin nähden, jotka jättävät kansalliset verkkonsa avoimiksi. Varauksena on huomautettava, että Kukkolan et al. malli perustuu operatiivisen ja strategisen tason analyysiin. Se ei ole tekninen malli, eikä ota kantaa toteutuksen teknologiaan tai standardeihin. Olemassa olevat ratkaisut mahdollistavat kansallisen verkon irti kytkemisen, mutta on mahdollista, että tulevaisuuden teknologiat tekevät siitä entistä joustavampaa ja seurannaisvaikutuksiltaan hallitumpaa tai kiistävät irti kytkemisen mahdollisuuden kokonaan.

2.5 Rakenteellisen kyberasymmetrian analyysikäsitteet

Kukkolan, Ristolaisen ja Nikkarilan esittämässä analyyttisessä kehyksessä on puutteensa, joista merkittävin on vaillinainen liikkumisen vapauden, tilannetietoisuuden ja päätöksentekokyvyn käsitteellistäminen ja operationalisointi. Tässä työssä puutteita korjataan. Tilannetietoisuus korvataan yhteisen tilannekuvan käsitteellä ja päätöksenteko korvataan johtamisen käsitteellä. Lisäksi lisätään resilienssin käsite asymmetrian tarkastelemiseksi ja rakenteellisen kyberasymmetrian käsitettä kehitetään edelleen. Kybertilaa tarkastellaan digitaalisena maastona (*digital territory*) ja taistelukenttänä, asymmetrian lähteitä tarkastellaan lähemmin ja asymmetria asetetaan aikaisemmin esitellyn kybervoiman käsitteen kontekstiin. Käsitteen muodostamisen taustaksi on todettava, että kulutussodankäynnin, tuhoamissodankäynnin tai liikesodankäynnin teoriat eivät sellaisenaan toimi kybertoimintaympäristön kehyksessä.[344] Kybersodankäynnin ilmiöiden ymmärtämiseksi tarvitaan täysin uusia

[343] Nikkarila, J-P., Åkesson, B., Kuikka, V., & Hämäläinen, J.: Modelling Closed National Networks: Effects in Cyber Operation Capabilities. *In Proceedings of the 17th European Conference on Cyber Warfare and Security (ECCWS), Oslo, Norway, 2018 June, 28.-29*, s. 323–329.

[344] Näistä käsitteistä ks. Leonhard, Robert R.: *The Art of Maneuver: Maneuver Warfare Theory and Airland Battle*. Ballantine Books, New York, 1991; Hammond, Grant T.: *The Mind of War. John Boyd and American Security*. Smithsonian Books, Washington, D.C., 2001; Liddell Hart (1991).

termejä ja käsitejärjestelmiä. Näiltä osin tässä työssä rakennetaan peruskäsitteistöä kybersodankäynnin ymmärtämiselle strategisella ja operatiivisella tasolla.

Digitaalisen maaston käsite mahdollistaa kybertilan kartoittamisen, sen elementtien tarkastelun asymmetrian löytämiseksi ja kontrolloivan ja muokkaavan kybervoiman kohteen määrittelyn. Se mahdollistaa laitteiden, ohjelmistojen, infrastruktuurin, yhteyksien, informaation, inhimillisten resurssien, protokollien, palvelujen, käyttöpolitiikkojen, standardien ja normien havainnollistamisen. Käsite perustuu kriittisen geopolitiikan teoriaan. Lähtökohtana on, että pelkät tekniset verkonkuvat eivät paljasta, kuinka verkkoja hallitaan ja kontrolloidaan tai mikä on niiden sotilasstrateginen funktio.[345] Yksinkertaisimmillaan digitaalinen maasto viittaa ihmisen rakentamaan ja hallitsemaan informaatioinfrastruktuuriin. Monimutkaisimmillaan se viittaa niihin sosiaalisiin ja ei-sosiaalisiin rakenteisiin, jotka tekevät informaatioinfrastruktuurin merkitykselliseksi. Konkreettisimmillaan digitaalisen maaston objektit koostuvat fyysisistä laitteista, ohjelmista ja prosesseista, sekä tallennetusta tai liikkeessä olevasta informaatiosta. Abstrakteimmillaan digitaalisen maaston käsite mahdollistaa valtioiden rajojen piirtämisen kybertilaan rajaamalla (*delineation*), suojaamalla (*protection*) ja kontrolloimalla (*control*) rajoja objektien ja yhteyksien välillä.[346] Digitaalisen maaston käsite on teknologian, ihmistieteiden ja sotatieteiden leikkauspisteessä ja mahdollistaa kansallisten verkkojen tarkastelun eri tavoin koostuvina järjestelminä tai järjestelmien järjestelminä.

Pelkästään teknologian kautta ymmärretty digitaalisen maaston käsite on teknologinen konsepti, eikä selitä sitä, miksi verkot ja järjestelmät ovat muotoutuneet sellaisiksi kuin ovat. Käytännön esimerkkinä tällaisesta rajallisesta, joskin kattavasta näkemyksestä voidaan mainita ENISA:n Internet Infrastructure Model.[347] Tässä työssä digitaalinen maasto ymmärretään laajemmin kuin fyysisenä tai loogisena verkkokuvana. Digitaalisen maaston kartta sisältää teknisiä, funktionaalisia, normatiivisia,

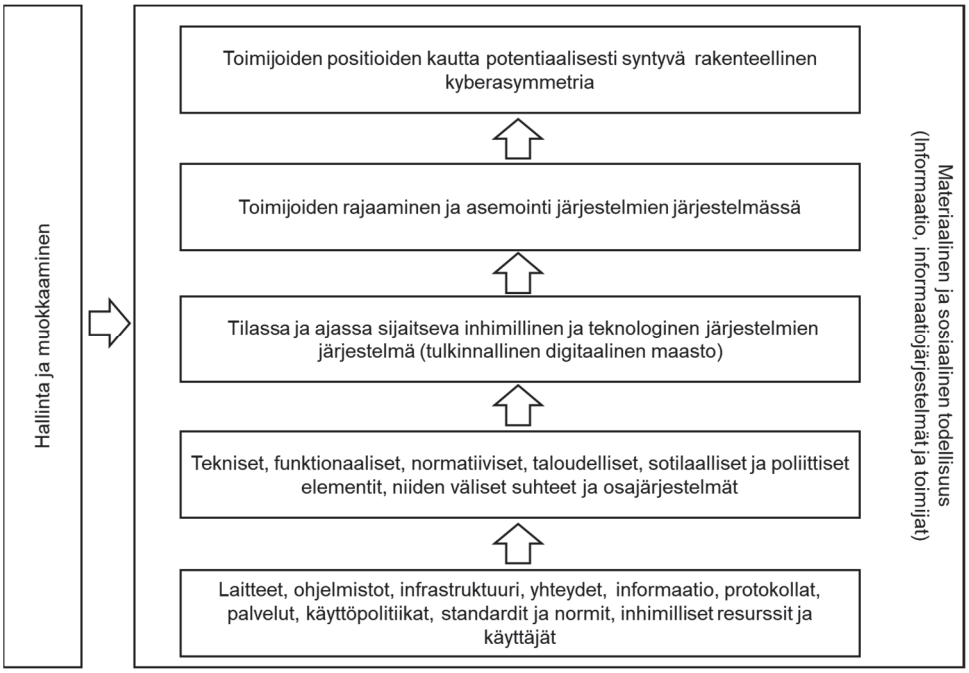
---

[345] Kriittisestä geopolitiikasta ks. Ó Tuathail, Gearoid & Dalby, Simon (eds.): *Rethinking Geopolitics*. Routledge, London, 1998.

[346] Tämä jaottelu on esitetty alunperin Kukkola, Juha & Ristolainen, Mari: Projected Territoriality: A Case Study of the Infrastructure of Russian 'Digital Borders'. *Journal of Information Warfare*, Vol. 17, No. 2 (2018), s. 83–100.

[347] ENISA: *Threat Landscape and Good Practice. Guide for Internet Infrastructure, January 2015.* [https://www.enisa.europa.eu/publications/iitl/at_download/fullReport], luettu 7.5.2020.

taloudellisia, sotilaallisia ja poliittisia elementtejä. Niissä informaation teknisesti vapaa kulku kohtaa inhimillisen hallinnan. Ei ole olemassa mitään yhtä ainutta tapaa kartoittaa digitaalista maastoa, vaan se on tehtävä tapauskohtaisesti. Tässä työssä digitaalisen maaston elementtejä käsitellään informaatioturvallisuuden ja -puolustuksen järjestelmänä alasysteemeinä (ks. Luku 3.1). Kuva 7 havainnollistaa digitaalisen maaston yhtäältä tulkinnallista ja toisaalta hallintaa liittyvää luonnetta ja sen suhdetta rakenteelliseen kyberasymmetriaan.

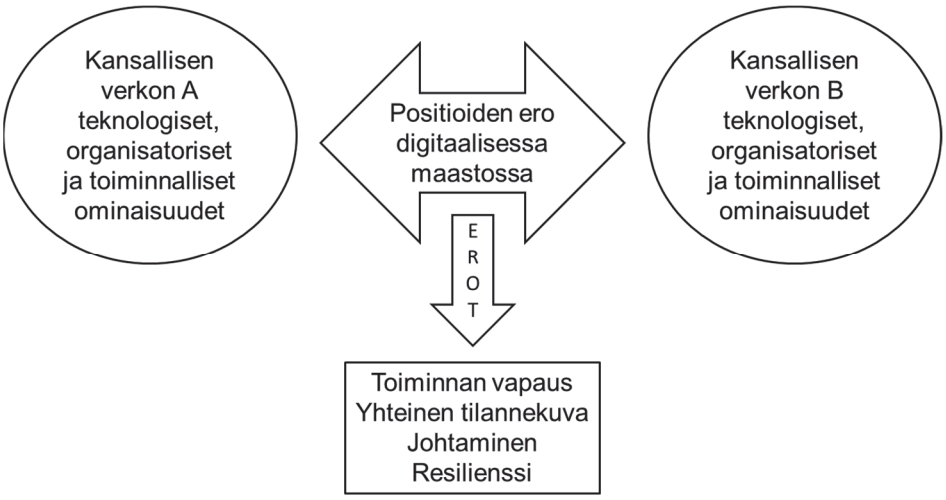


Kuva 7: Digitaalinen maasto ja rakenteellinen kyberasymmetria

Edellä todettiin, että rakenteellinen kyberasymmetria on kybertilan ominaisuus, joka on mahdollista luoda ja käyttää hyväksi. Vaikka asymmetria liittyy toimijan (valtion) resursseihin, se ei ole niiden käytön suora seuraus vaan kybertilan ominaisuus, joka syntyy digitaalisen maaston muutoksesta ja toimijoiden asemasta (positiosta) toistensa suhteen. Asymmetria on siis luovan voimankäytön seurannaistulos ja näin ollen ideoiden ohjaaman tavoitteellisen toiminnan seuraus. Rakenteellista kyberasymmetriaa ei voi luoda suoraan vaan se tapahtuu vaikuttamalla digitaaliseen maastoon teknologialla, hallinnolla (*governance*), normeilla ja politiikalla. Nämä ovat kyberstrategian menetelmiä, joita toimijat, tämän työn kehyksessä valtiot, käyttävät strategian ohjaamina käytössä olevien resurssien ehdoilla. Täten tarkastelemalla valtioiden kyberstrategioita ja

niiden tuloksia voidaan analysoida rakenteellisen kyberasymmetria tarkoituksellista tai tahatonta kehittämistä.

Rakenteellinen kyberasymmetria ei ole itsessään hyökkäyksellinen tai puolustuksellinen ominaisuus, se voi olla molempia. Kybertilan ominaisuuksien tulee kuitenkin tarjota hyväksikäytettävissä olevaa suhteetonta etua yhdelle toimijalle toiseen nähden. Tämän edun tarkastelemiseksi tässä työssä käytetään toiminnan vapauden, yhteisen tilannekuvan, johtamisen ja resilienssin käsitteitä. Ne määritellään seuraavissa alaluvuissa tämän työn kontekstissa. Käsitteiden avulla voidaan potentiaalisen rakenteellisen asymmetrian vaikutuksia tarkastella ja laadullisessa mielessä todentaa. Yksinkertaistaen ne ovat riippuvia muuttujia, jotka kertovat asymmetrian olemassaolosta tai olemattomuudesta. Tämä asetelmä on kuvattu kuvassa 8.



Kuva 8: Rakenteellisen kyberasymmetrian ilmeneminen

Vertaamalla toiminnan vapautta, yhteistä tilannekuvaa, johtamista ja kansallisten verkkojen resilienssiä osapuolten välillä on mahdollisuus tehdä havaintoja suhteettomista ja hyväksikäytettävistä eduista. Yksinkertaisuuden vuoksi toiminnan vapaus, yhteinen tilannekuva, johtaminen ja resilienssi viittaavat tässä työssä suljettujen kansallisten ja avoimien verkkojen teknologisiin, organisatoriisiin ja toiminnallisiin ominaisuuksiin, jotka voivat vaikuttaa niin hyökkäykseen kuin puolustukseen. Tarkastelun ulkopuolelle jäävät siis varsinaiset ”kyberjoukkojen” suorituskyvyt. Käsitteiden muodostuksen on tarkoitus tukea strategisen tason tarkastelun toteuttamista. Valittujen käsitteiden

käyttöä tukee se, että ne resonoivat niin läntisen kuin venäläisen sotilastieteellisen teoriapohjan kanssa.[348] Ne kattavat myös suomalaisen sotataidollisen suorituskyvyn kyvykkyysnäkökulman eri tekijät.[349]

2.5.1 Toiminnan vapaus

Historiallisesti liikehtimiskykyä on pidetty yhtenä sodankäynnin keskeisimpänä käsitteenä niin läntisessä kuin neuvostoliittolaisessa ja venäläisessä sodankäynnin teoriassa.[350] Liike taistelun elementtinä on sidottu ympäristöön.[351] Se saavuttaa täydellisen potentiaalinsa liikkeen vapaudessa (*freedom of movement*), mikä yksinkertaisimmillaan viittaa kykyyn tavoitteellisesti liikuttaa joukkoja ilman, että vastustaja pystyy tätä

---

[348] U.S. DoD JP 3-0 (2018), s. *II-7*; Wardak, Ghulam Dastagir, Turbiville, Graham Hall Jr. & Garthoff, Raymond L.: *The Voroshilov Lectures. Materials from the Soviet General Staff Academy. Volume I: Issues of Soviet Military Strategy*. National Defense University Press, Washington, DC, 1989; Central Intelligence Agency: *General Staff Academy Lectures: Principles of the Automation and Mechanization of Troop Control*. Document VII-211. Prepared 6 September 1968, published October 1969. CIA/DO Intelligence Information Special Report, 11 November 1976 [https://www.cia.gov/library/readingroom/docs/1976-11-11.pdf], luettu 6.7.2020; Lalu (2014); Kukkola (2020a).

[349] Pääkyvykkyysalueita ovat valmistautuminen, projisointi, vaikuttaminen, taistelukyvyn ylläpito, suoja, tilannetietoisuus, johtaminen (Pääesikunta.: *Sotilaallisen suorituskyvyn käsitemalli*. Asiakirja HO46, 31.5.2018).

[350] Liddell Hart (1991), s. 323–328; Fuller (1993); Svechin (1992), s. 276–278; Isserson, G. S.: G. S. *Isserson and the War of the Future: Key Writings of a Soviet Military Theorist*. Richard W. Harrison (trans., ed.). McFarland & Company, Jefferson, NC, 2016, s. 61–65, s. 288; Glantz, David M.: *The Soviet Conduct of Tactical Maneuver*. Frank Cass, New York, 1991, s. 229–230; Lalu (2014), s. 166–170; Main, Steven J.: 'You Cannot Generate Ideas by Orders': The Continuing Importance of Studying Soviet Military History—G. S. Isserson and Russia's Current Geo-Political Stance. *The Journal of Slavic Military Studies*, Vol. 29, No.1 (2016), s. 48–72; Kagan, Frederick W.: The Rise and Fall of Soviet Operational Art, 1917-1941. Teoksessa *The Military History of the Soviet Union*. Higham, Robin & Kagan, Frederick W. (eds) Palgrave, New York, 2002, s. 79–92; *Военный энциклопедический словарь (ВЭС)*: Манёвр. [http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=7483@morfDictionary], luettu 11.1.2021; Рогозин, Дмитрий (под общ.ред.): *Война и мир в терминах и определениях*: Оперативный маневр. Вече, Москва, 2011; The United States Department of Defense (U.S. DoD), Chairman of the Joint Chiefs of Staff: *Joint Vision 2010, 1996.* [http://drseres.com/tavoktatas/irodalom/stb/jv2010.pdf], luettu 8.5.2020; U.S. DoD JP 3-0 (2018), A-1 – A-3

[351] Kantola, Harry, Huttunen, Mika & Kiviharju, Mikko: Taistelun elementit kybertoimintaympäristössä. Teoksessa *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, s.142–152, s. 143.

syystä tai toisesta estämään. Laajemmin ymmärrettynä liikkeen vapaus voi olla kyky ja mahdollisuus vapaasti liikuttaa joukkoja tai ulottaa tilan läpi voimaa vastustajan toimintoihin tai objekteihin vaikuttamiseksi päämääränä häiritseminen, lamauttaminen tai tuhoaminen, ja samalla omien joukkojen ja järjestelmien suojelemiseksi vastustajan vaikutukselta.[352] Tällainen liike liittyy taisteluliikkeen tai manööverin käsitteeseen.[353] Robert Leonhardt määrittelee taisteluliikkeen operatiivisen tai strategisen tason liikkeeksi kohti tavoitetta vihollisen joukkojen lyömiseksi ennaltaehkäisemällä, syrjäyttämällä ratkaisukohdasta tai sekasortoon saattamalla. Tällöin toiminta kohdistetaan yleensä vastustajan voimanlähteeseen (*center of gravity*) vastustajan neutraloimiseksi.[354] Svetšinille operaation perusedellytys oli saattaa omat joukot asemaan, jossa niiden yhteydet (*soobštšnie*) ovat suotuisimmat suhteessa vastustajaan ja jossa saavutetaan paras taktinen asema.[355] Taisteluliike siis antaa liikkeelle operaatiotaidolliset puitteet. Se on tarkoituksellista liikettä suhteessa tavoitteeseen ja/tai vastustajaan.[356] Liike liittyy oleellisesti liikesodankäynnin teoriaan, joka korostaa vastustajan horjuttamista ja hämmentämistä päätaisteluvoiman kuluttamisen tai tuhoamisen sijaan.[357]

Toiminnan vapaus (*freedom of action*) on liikkeen vapautta yleisempi käsite ja tarkoittaa yksinkertaisesti vapautta toimia määrätyssä toimintaympäristössä samalla, kun vihollisen vapaus toimia kiistetään. Tavoiteltua lopputilaa voidaan kutsua toimintaympäristön herruudeksi, kuten ilma- tai meriherruudeksi. Toiminnan vapauden käsite auttaa irrottamaan kybersodankäyntiin liittyvän toiminnan *fyysiseen maantieteeseen* tiiviisti liittyvien tulen, liikkeen ja suojan *taktisista* käsitteistä.[358] Tämä on oleellista, koska kybertilassa liike on sidottu oikeuksiin ja yhteyksiin eikä ole samalla tavalla jatkuvaa kuin fyysisissä

---

[352] U.S. DoD JP 3-0 (2018), *II-7*; *ВЭС (2007),* Манёвр [http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=7483@morfDictionary]; Рогозин, Дмитрий (под общ.ред.): *Война и мир в терминах и определениях*: Оперативный маневр. Вече, Москва, 2011.

[353] Käsitteestä ks. Huttunen (2010).

[354] Leonhard (1991). Huolimatta doktriineissa esitellyistä määritelmistä voimanlähteen käsitteen määriteltämästä ei ole saavutettu yksimielisyyttä läntisissä sotatieteissä (Angström & Widen (2015), s. 61–63).

[355] Svechin (1992), s. 262, s. 280. (alkup. Свечин, А.: *Стратегия*. Военный вестник, Москва, 1927, s. 195 & 211).

[356] Kantola, Huttunen & Kiviharju (2018), s. 143.

[357] Lind, William S.: *Maneuver Warfare Handbook*. Westview Press, Boulder, Colorado, 1985, s. 6–7.

[358] Näiden käsitteiden soveltamisesta ks. Kantola, Huttunen & Kiviharju (2018).

ulottuvuuksissa.[359] Liike on epäjatkuvaa, koska voimalla ei ole pysyvyyttä ja toiminta voi siirtyä kybertilan eri tasojen välillä.[360] Kybertoimintaympäristössä konfliktin osapuolet voivat olla läsnä ja toimia samassa tilassa. Niiden joukot eivät varsinaisesti kohtaa. Ei ole siis kahta toistensa suhteen jatkuvasti liikehtivää ja vaikuttavaa voimaa. Maasto on muuttuvaa ja ”sisä- ja ulkolinjoilla” ei varsinaisesti ole merkitystä.[361] Perinteiset materiaaliset voimasuhdelaskelmat määrätyssä tilassa ja ajassa ovat merkityksettömiä, koska ei ole tilaa tai aikaa mihin ryhmittää joukkoja vastakkain.[362] Toiminnan vapauden käsite myös irrottaa operatiivisella ja strategisella tasolla voiman kohdistamisen ja liikuttamisen ”tulesta” tai aselavetista ja ammuksesta, joka viittaa fyysiseen tuhoamiseen, lamauttamiseen tai kuluttamiseen. Tämä on tärkeää, koska energian säilymislaki puuttuu tai toimii toisin kybertilassa kuin fyysisessä tilassa.[363] Toiminnan vapaus mahdollistaa vaikuttamisen eri ulottuvuuksissa eri keinoin – ja näiden vaikutusten yhdistämisen ajassa ja tilassa ilman vaadetta energian muutoksille. Fyysinen kohteen tuhoaminen korvautuu siis kohdejärjestelmään vaikuttamisella muutoksia synnyttävien vaikutusten kautta, mikä heijastelee vaikutuskeskeisen sodankäynnin teoriaa.[364]

Kybertilassa hyökkääjän kyky saavuttaa tavoitteensa perustuu vähintään yhteen haavoittuvuuteen, jota puolustaja ei tunne omissa järjestelmissään.[365] Kybertilassa hyökkääjän toiminnan vapaus ja siten vaikuttaminen ovat riippuvaisia hyökkäyspinta-alasta, puolustuksen

---

[359] Kiviharju, Mikko & Huttunen, Mika: Kybertaktiikkaa – Yleisten periaatteiden soveltuvuudesta kybertoimintaympäristössä. Teoksessa *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, s.161–180, s. 167.

[360] Kiviharju & Huttunen (2018), s. 170–171.

[361] Sisä- ja ulkolinjoista Svetšin (1992), s. 296–297.

[362] Kallberg, Jan & Cook, Thomas S.: The Unfitness of Traditional Military Thinking in Cyber. Four Cyber Tenets That Undermine Conventional Strategies. *IEEE Access*, Vol. 5, 2017, s. 8126–8130.

[363] Huttunen et al. esittävät kybertulenkäytön käsitteen taktisen tason välittömänä vaikuttamisena kohteeseen, jolla pyritään estämään, muuttamaan, häiritsemään ja tuhoamaan. Tässä tutkielmassa tarkastelutaso on ylempänä, joten vaikuttaminen on valittu toiminnan vapauden osaelementiksi. Kantola, Huttunen & Kiviharju (2018), s. 145–146.

[364] Mälkki, Juha: Vaikutusperusteisen operatiivisen ajattelun (EBAO) sotataidolliset lähtökohdat. *Tiede ja Ase*, Vol 69 (2010), s. 7–31.

[365] Libicki (2009), s. xiv; Libicki (2016), s. 51–52.

syvyydestä ja puolustajan passiivisista ja aktiivisista vastatoimista.[366] S. Taillat on myös esittänyt, että hyökkääjän pyrkiessä vaikuttamaan tarkasti määriteltyyn kohteeseen, lyhyessä ajassa ja aikaisemmin käytetyillä keinoilla sen toiminnan vapaus kapenee.[367] Puolustajan toiminnan vapaus on lähtökohtatilanteessa periaatteessa täydellinen, koska tämä hallitsee puolustettavan tilan toimintaehtoja ja rakennetta.[368] Kuitenkin käytännössä kansallisen verkon tasolla puolustajan toiminnan vapaus on aina rajattu johtuen mm. lainsäädännöstä, toimivaltuuksista ja teknisistä ratkaisuista. Puolustaja ei voi myöskään vaikuttaa hyökkäykseen sen käynnistyttyä, mikäli ei havaitse hyökkäyksen valmistelua. Näin ollen se on lähtökohtaisesti reagoiva osapuoli. Lisäksi hyökkääjä voi kyetä sulkemaan puolustajan ulos omista järjestelmistään tai puolustaja voi muuttaa omia järjestelmiään tai sulkea ne kiistäen paikallisesti ja ajallisesti toiminnan vapauden molemmilta. Täten taistelun kolmas elementti eli suoja, yhdistyy osaksi toiminnan vapautta ja siitä kamppailua kybertaistelutilan operatiivisella ja strategisella tasolla.

Toiminnan vapaus kybertilassa eroaa muista toimintaympäristöistä myös siinä, että se voidaan ymmärtää toimintojen ”ketjuina” tai toimintojen jatkumoina ja vastatoimina. Ketjuja ovat esimerkiksi niin kutsuttu *cyber kill-chain*[369] ja sen eri versiot sekä erilaiset kyberturvallisuusprosessit. Kyse on siis pikemmin prosessista kuin liikkeestä. Kybertaistelutoiminnassa prosessi asettuu prosessia vastaan. Hyökkääjä tiedustelee kohteensa, luo haittaohjelman tai muun keinon päästä kohteeseen, tunkeutuu kohteeseen ja hankkii toimintaoikeudet kohteessa, ylläpitää läsnäolonsa ja suorittaa tehtävänsä.[370] Puolustus pyrkii

---

[366] Kärkkäinen, Anssi: Kyberpuolustuksen taistelukenttä nyt ja tulevaisuudessa. Teoksessa *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, s.72–83, 81.
[367] Taillat (2019), s. 372–373.
[368] Kiviharju & Huttunen (2018), s. 170–171.
[369] Ks. Kim, Hyeob, Kwon, HyukJun & Kim, Kyung Kyu: Modified Cyber Kill Chain Model for Multimedia Service Environments. *Multimedia Tools and Applications*, Vol. 78 (2019), s. 3153–3170.
[370] Hutchins, Eric M., Cloppert, Michael J. & Amin, Rohan M.: *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* [https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf], luettu 29.6.2020; Mandiant: *APT1 Exposing One of China's Cyber Espionage Units.* [https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf], luettu 29.6.2020; Kim, Kwon & Kim (2019); MITRE: *ATT&CK Matrix for Enterprise.* [https://attack.mitre.org/matrices/enterprise/], luettu 29.6.2020; Laari 2019.

poistamaan haavoittuvuuksia, salaamaan järjestelmänsä, harhauttamaan hyökkääjiä, havaitsemaan ja torjumaan hyökkäykset, poistamaan hyökkääjät järjestelmistä ja palauttamaan toiminnot.[371] Vaikutus tuotetaan kohteeseen olemassa olevaa yhteyttä pitkin. Oleellista on myös se, että toiminnan vapaus kumuloituu ja voi johtaa vastustajan kyvyttömyyteen reagoida uusiin tapahtumiin. Tämä kyvyttömyys on kuitenkin ajallisesti ja paikallisesti rajoittunutta ja tilapäistä, sillä energia on näennäisesti rajatonta ja palvelut voidaan palauttaa normaalitilaan vaikutuksen päätyttyä.[372] Kybertilassa toiminnan vapaus siis lisää mahdollisuuksia vaikuttaa ja vaikutusten merkittävyyttä, muttei ole pysyvä ominaisuus tai kyky.

Kybertoimintaympäristössä hyökkääjän ja puolustajan suhde ei ole ajassa tai paikassa vakioitu, muuttumaton tai suljettu. Tila, jossa toimitaan, on luonteeltaan järjestelmä, ei alusta, pinta tai erillisten objektien kokoelma. Näin ollen toiminnan vapaus sekä hyökkääjän että puolustajan osalta on kybertilan reunaehtojen ja kunkin toimijan toimivaltuuksien (suorituskykyjen) summa. Voimasuhteita eivät määrittele massa tai energia vaan prosesseihin tai ”ketjuihin” liittyvät tekijät. *Näin ollen toiminnan vapaus kybertoiminta- tai taistelutilassa määritellään kyvyksi toteuttaa hyökkäyksellisiä ja puolustuksellisia kyberoperaatioita omissa ja vastustajan verkoissa ja kiistää vastustajalta samainen kyky*. Toiminnan vapaus liittyy vastustuksen puutteeseen ja kykyyn käyttää hyväksi tätä puutetta. Toiminnan vapauden analyysin kohteena on digitaalisen maaston tai tarkemmin suljettujen ja avoimien kansallisten verkkojen rajojen ja sisäisen rakenteen vaikutus toimijoiden kykyyn vaikuttaa kohteisiin tai kiistää tuo vaikutus sekä toimijoiden kyky toimia verkoissa. Tässä työssä käsitellään käytössä olevan tilan johdosta vain verkkojen rakenteen vaikutusta eli pääsyä kansallisiin verkkoihin ja mahdollisuutta operoida niissä.

---

[371] National Institute of Standards and Technology (NIST): *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, February 12, 2014.* [https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf], luettu 29.6.2020; Valtiovarainministeriö: *Tietoturvapoikkeamatilanteiden hallinta. Valtiovarainministeriön julkaisuja 8/2017.* [https://www.suomidigi.fi/sites/default/files/2020-06/VM_8_2017.pdf], luettu 29.6.2020; New York State Department Of Financial Services: *Cybersecurity Requirements For Financial Services Companies, 23 NYCRR 500.* [https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf], luettu 29.6.2020; Andress & Winterfeld (2014).

[372] Kiviharju & Huttunen (2018), s. 168–169.

2.5.2 Yhteinen tilannekuva

Tilannekuva, tilannetietoisuus ja -ymmärrys ovat suomen kielessä melko jäsentymättömiä ja suhteellisen epätarkasti käytettyjä käsitteitä.[373] Tuija ja Rauno Kuusisto ovat omissa tutkimuksissaan pyrkineet selventämään käsitteiden suomen kielistä käyttöä.[374] Kuusistojen mukaan tilannetietoisuus ja -ymmärrys liittyvät yksilöiden ja ryhmien kognitiiviseen maailmaan. Tilannetietoisuus on tilanteen tulkinta itsen kautta ja tilannetietoinen tietää, miten ”nyt” pitää toimia. Tilannetietoisuus on eräänlainen esiaste, jonka jälkeen saavutetaan tilanneymmärrys. Se viittaa kokonaisvaltaiseen tulkintaan ympäristöstä systeeminä. Tilanneymmärrys sisältää tiedon itsestä, muista toimijoista, maailmasta ja näiden suhteesta sekä siitä, miten tilanne voi kehittyä pidemmällä aikavälillä. Huolimatta Kuusistojen jaottelusta suomen kieleen näyttää vakiintuneen käytäntö, jossa tilannetietoisuuden käsite sisältää sekä tietoisuuden että ymmärryksen.[375]

Kuusistojen mukaan tilannekuvalla tarkoitetaan analysoitua ja jäsennettyä sekä jatkuvasti päivittyvää koostettua tietoa jonkin toimialueen tilanteesta. Tilannekuva on siis ajallisesti ja paikallisesti rajattua ajankohtaista tietoa, kokoelma menneisyyttä ja nykyisyyttä koskevaa tilannetietoa, jota kerätään johonkin tietojärjestelmään ja esitetään päätöksenteon tueksi. Tilannekuva voi sisältää myös tulevaisuuden arviointiin liittyvän komponentin.[376] *Yhteinen tilannekuva taas on yhden tai useamman käyttäjän yhteisesti käytössä oleva tieto. Se on yhteisesti ymmärrettävä malli ja kuvaus tilanteen tulkintaan vaikuttavista tiedoista*.[377] Yhteinen tilannekuva edellyttää rakenteiden (organisaation), toiminnan (prosessit - palveluarkkitehtuuri) ja tiedon (tietosisällöt ja tietomallit) yhteensovittamista toimivien tietovirtojen tuottamiseksi.[378] Hyvän

---

[373] Kuusisto, Rauno: *Tilannekuvasta täsmäjohtamiseen. Johtamisen tietovirrat kriisin hallinnan verkostossa*. Liikenne- ja viestintäministeriön julkaisuja 81/2005, Helsinki, 2005; Rantanen, Hannu: *Tilannekuvan tuottaminen, hyödyntäminen ja jakaminen - Kriittinen nykytilan tarkastelu*. Aluehallintovirastojen julkaisuja 42/2018, Vaasa, 2018; Hölttä, Niko: *Yhtymän esikunnan tilanneymmärryksen kehittäminen operaatioiden johtamisessa*. Yleisesikuntaupseerikurssi 54:n opinnäytetyö, Maanpuolustuskorkeakoulu 2009.

[374] Kuusisto, Rauno & Kuusisto, Tuija (toim.): *Yhteinen tilanneymmärrys - Strategis-operatiivisten päätösten tukipalvelujen perusteet*. Edita Prima Oy, Helsinki, 2005.

[375] Kuusisto & Kuusisto (2005); Kuusisto (2005), s. 7–9.

[376] Kuusisto (2005), s. 7–9.

[377] Kuusisto (2005), s. 10.

[378] Kuusisto (2005), s. 12–14.

tilannekuvajärjestelmän tuloksena saavutetaan tarkempaa informaatiota ja tietoa, parempi tiedonhallinnan prosessi, laajempi ja hienojakoisempi aika-tilan kokonaisuuden hallita ja kyetään tekemään nopeampia ja varmempia päätöksiä.[379]

Englannin kielessä ja sotilaallisessa ympäristössä *Situation awareness* (SA) terminä viittaa usein miten Mica Endsleyn esittämään dynaamisen päätöksenteon malliin.[380] Eräissä lähteissä termi on muuttunut muotoon *Situational awareness*, mutta Endsleyn mukaan *situational* viittaa vain tilanteeseen liittyvään tietoon.[381] Endsleyn mallissa yksilö käsittelee tilannetietoa kolmessa havaitsemisen (*perception*), ymmärtämisen (*comprehension*) ja ennustamisen (*projection*) vaiheessa, mikä synnyttää henkilökohtaisen ja ainutkertaisen näkemyksen tilanteesta, joka on sidottu tavoitteelliseen toimintaan.[382] Koska Endsleyn määrittelee SA:n ”ympäristön elementtien havaitsemiseksi määrätyssä ajassa ja tilassa, niiden ymmärtämiseksi ja niiden tilan ennustamiseksi lähitulevaisuudessa”[383] se voidaan yhdistää suomen kielen tilannetietoisuuden käsitteeseen. Tilannetietoisuus on myöhemmissä tutkimuksissa jaettu tila-, järjestelmä- ja prosessinäkymiin sen mukaan, mihin kiinnostus on kohdistunut: tietämisen tilaan, SA malleihin vai SA:n ylläpitämiseen (*Situation assessment*).[384]

---

[379] Kuusisto, Rauno: *Aspects on availability: a teleological adventure of information in the lifeworld*. Doctoral Dissertation, Series / National Defence College, Department of Tactics and Operations Art. 1, Julkaisusarja / Maanpuolustuskorkeakoulu, taktiikan laitos. 1, Taktiikan tutkimuksia, 2004.

[380] Endsley, M. R.: Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, Vol. 37, No. 1 (1995), s. 32–64; Endsley, Mica: Theoretical Underpinnings of Situation Awareness: A Critical Review. Teoksessa *Situation Awareness Analysis and Measurement*. Endsley, M. R. and Garland, D. J. (Eds.). Lawrence Erlbaum Associates, Mahwah, NJ, 2000, s. 3–32; Endsley, Mica: Situation Awareness: Operationally Necessary and Scientifically Grounded. *Cognition, Technology & Work*, Vol. 17, No. 2 (May 2015), s. 163–167.

[381] *Situational* termi liittyy mm. verkostokeskeisen sodankäynnin diskurssiin ks. Garstka, John: *Network Centric Operations Conceptual Framework Version 1.0*. Evidence Based Research, Inc, Vienna, VA, 2003; Endsley (1995); Endsley (2000); Endsley (2015).

[382] Endsley, Mica R.: Situation Awareness Misconceptions and Misunderstandings. *Journal of Cognitive Engineering and Decision Making*, Vol. 9, No. 1, (March) 2015, s. 4–32.

[383] Endsley (2000).

[384] Lundberg, Jonas: Situation Awareness Systems, States and Processes: A Holistic Framework. *Theoretical Issues in Ergonomics Science*, Vol. 16, No. 5 (2015), s. 447–473; Pirolli, Peter & Russell, Daniel M.: Introduction to this Special Issue on Sensemaking. *Human–Computer Interaction*, Vol. 26, No. 1-2 (2011), s. 1–8.

Tilannetietoisuuden käsitettä ovat kyber- ja informaatiosodankäynnin kehyksessä käyttäneet ennen kaikkea verkostokeskeisen sodankäynnin teoreetikot.[385] Martin Libicki on määritellyt tilannetietoisuuden (*situational awareness*) vihollisen joukkojen ryhmityksen, sijainnin ja suuntautumisen tietämiseksi, mikä mahdollistaa tehokkaamman suunnittelun, estää yllätetyksi tulemisen ja mahdollistaa vastustajan yllättämisen.[386] Täydellinen tilannetietoisuus sisältää siis tiedon kaikesta oleellisesta taistelukentällä mukaan lukien muiden toimijoiden aikomukset.[387] NCW ajattelun mukaan eräs vastustajaa parempien ja nopeampien päätösten tekemisen ja toimeenpanon tekijöistä, ja täten informaatioylivoiman perusta, on tilannekuvan tarkkuus ja tilanteenmukaisuus. Teoreettisesti tämän ylivoiman, jonka merkityksen niin yhdysvaltalaiset, venäläiset kuin kiinalaiset teoreetikot tunnistavat, tulisi johtaa voittoon modernilla taistelukentällä. Teoriassa se muuttaa informaation vaikuttavaksi voimaksi ja moninkertaistaa materiaalisen voiman vaikutuksen.[388] Lännessä tämä näkemys henkilöityy John Boydin OODA -loop malliin (*Observe, Orient, Decide, Act*).[389]

---

[385] Alberts, David S. & Papp, Daniel S. (eds.): *The Information Age Anthology – Volume I: An Anthology on Its Impact and Consequences – Volume I*. CCRP Publication Series, 1997; Alberts, David S. & Papp, Daniel S. (eds.): *The Information Age Anthology – Volume II: National Security Implications of the Information Age – Volume II*. CCRP Publication Series, 2000; Alberts, David S. & Papp, Daniel S. (eds.): *Information Age Anthology – Volume III: The Information Age Military – Volume III*. CCRP Publication Series, 2001.

[386] Libicki, Martin C.: *What Is Information Warfare?* National Defense University, Institute for National Strategic Studies, Washington, D.C., 1995, s. 5.

[387] Alberts, David: The Future of Command and Control with DBK. Teoksessa *Dominant Battlespace knowledge*. Libicki, Martin & Johnson, Stuart E. (eds.) NDU Press Book, Washington, D.C., 1995, s. 29.

[388] Cebrowski & Garstka (1998); Alberts & Papp (2001); Hayes, Richard E. & Alberts, David S.: *Power to the Edge. Command… Control… in the Information Age*. CCRP, 2005, s. 172–173; Engström (2018); Wortzel, Larry M.: *The Chinese People's Liberation Army And Information Warfare*. Strategic Studies Institute and U.S. Army War College Press, Carlisle Barracks, PA, 2014; Kukkola (2020a).

[389] Hammond (2001); Hasík, James: Beyond the Briefing: Theoretical and Practical Problems in the Works and Legacy of John Boyd. *Contemporary Security Policy*, Vol. 34, No. 3 (2013), s. 583–599; Olsen, John A.: Boyd Revisited: A Great Mind with a Touch of Madness. *Air Power History*, Vol. 64, No. 4 (2012), s. 7–16; Bryant, David J.: Rethinking OODA: Toward a Modern Cognitive Framework of Command Decision Making. *Military Psychology*, Vol. 18, No. 3 (2006), s.183–206, s. 185–187; Osinga, Frans: 'Getting' A Discourse on Winning and Losing: A Primer on Boyd's 'Theory of Intellectual Evolution'. *Contemporary Security Policy*, Vol. 34, No. 3 (2013), s. 603–624.

Kyberturvallisuuden tilannekuvalla tarkoitetaan koottua kuvausta ”tietojärjestelmien tietyllä hetkellä vallitsevasta käytettävyys- ja turvallisuustilanteesta sekä kybertoimintaympäristön vallitsevasta tilasta.”[390] Kybertilassa tilannekuvan muodostamista rajoittavat toimintaympäristön kompleksisuus, muuttuva topologia, hyökkäyksien hukkuminen muuhun dataan, anonymiteetti, konenopeus, hyökkäysten ja seurausten mahdollisesti pitkä aikaero sekä datan käsittelyyn ja jakamiseen liittyvät tekniset haasteet.[391] Näin ollen tilannekuvan ja -tietoisuuden muodostamiseksi tarvitaan kybertilan luonteesta johtuen useita tietolähteitä, pitkälle automatisoitua ja nopeaa tiedon keräämistä, säilöntää, käsittelyä ja analysointia, tiedon jakamista ja integrointia järjestelmien ja organisaatioiden välillä, tiedon suodattamista ja esittämistä tekniseltä tasolta ylemmille päätöksenteon tasoille sopivaksi ja tiedon sekä järjestelmien turvaamista manipuloinnilta ja häiriöiltä.[392] Kybertilannekuvalla on siis oma luonteensa ja vaatimuksensa.

Tilannekuva on kybersodankäynnin merkittävä osa. Se mahdollistaa poikkeamien havaitsemisen järjestelmissä ja toisaalta mahdollistaa operoinnin kohdeverkoissa.[393] Ilman kohdejärjestelmän tuntemusta kyberhyökkäyksen toteuttaminen on käytännössä mahdotonta.[394] Esimerkiksi hyökkäykset kriittistä informaatioinfrastruktuuria vastaan edellyttävät syvää kohdetuntemusta ja huolellista valmistelua.[395] Hyökkäyksen käynnistyttyä tilannetiedolla ei ole yhtä kriittistä merkitystä etenkin käytettäessä autonomisia, muokkautuvia ja itsestään leviäviä haittaohjelmia. Puolustajakin on riippuvainen tilannekuvasta. Jos hän ei tiedä hyökkäyksestä, hän ei voi puolustautua sitä vastaan – ainoastaan ennalta ehkäistä tunnettuja hyökkäyksiä. Johtamisprosessissa tarvitaan tarkkaa ja oikein aikautettua informaatiota, jotta keskitetty johtaminen ja

---

[390] Sanastokeskus TSK (2018), 22.
[391] Kott, Alexander, Wang, Cliff, Erbacher, Robert F. (Eds.): *Cyber Defense and Situational Awareness*. Springer International Publishing, London, 2014.
[392] Kuusisto (2014); Matthews, Earl D., Arata, Harold J. III & Hale, Brian L.: Cyber Situational Awareness. *The Cyber Defense Review*, Vol. 1, No. 1 (Spring 2016), s. 35–46, s. 40; Multinational Experiment 7: *Outcome 3 – Cyber Domain Objective 3.4 Cyber Situational Awareness Standard Operating Procedure. Version 1.0, 1 December 2012.* [https://www.hsdl.org/?view&did=760553], luettu 6.7.2020; NATO: *Military Strategic Level Decision Making within a (Future) Framework of Cyber Resilience*. STO-TR-SAS-116, 24.8.2020. NATO Unclassified Rel To PFP. DOI: 10.14339/STO-TR-SAS-116.
[393] Kärkkäinen (2018).
[394] Brantly (2016).
[395] Ibid., s. 117.

hajautettu toiminta kybertaistelutilassa on mahdollista.[396] Tarkasteltaessa kansallisia verkkoja kybertaistelutilana hyökkääjän ja puolustajan tarvitsema tieto koskee toimijoiden inhimillisiä, materiaalisia ja teknologisia suorituskykyjä, näiden suorituskykyjen keskinäistä suhdetta ja suhdetta kybertoimintaympäristön fyysiseen, loogiseen (semanttinen ja syntaktinen) ja sosiaaliseen tasoon sekä vallitsevia uhkakuvia ja tunnettuja uhkia ja haavoittuvuuksia.[397]

Tilannetietoisuuden analysointi kansallisten verkkojen ja valtioiden kyberoperaatioiden kontekstissa on lähtökohtaisesti haastavaa, koska se muodostuu kognitiivisessa ulottuvuudessa eli päätöksentekijän mielessä.[398] Operatiivisella ja strategisella tasolla tulisi edelleen tarkastella ryhmän jaettua tilanneymmärrystä.[399] Yhtenäisen tilannekuvan edellyttämiä rakenteita, prosesseja ja tietosisältöjä ja -malleja sekä tietovirtoja voidaan sen sijaan tarkastella ulkopäin.[400] Edellä mainittu huomioiden yhteisen tilannekuvan analyysin kohteeksi määrittyvät siis tilannetietojen keräämiseen, tilannekuvan muodostamiseen, analysointiin, jakamiseen ja seurantaan liittyvät tekijät. Näitä voivat olla niin prosesseihin, sosiaalisiin suhteisiin kuin teknologiaan liittyvät elementit.[401] Toisin kuin toiminnan vapaus tilannekuva ei ole riippuvainen vastapuolen tilannekuvasta, koska niin hyökkääjällä kuin puolustajallakin voi teoriassa olla täydellinen tilannekuva omaan tehtäväänsä liittyen. Toisaalta yhden tilannekuva voi olla parempi kuin toisen ja tämä voi periaatteessa johtaa nopeampiin ja parempiin päätöksiin ja edelleen voittoon.

---

[396] Lehto & Limnéll (2017), s. 199.
[397] Brantly (2016), s. 112.
[398] Ks. Esim. Kuusisto 2014; Siukonen, Veikko: *APT-Operaation inhimilliset tekijät: Operaation tarkastelu päätöksenteon näkökulmasta*. Jyväskylän yliopisto, Tietojenkäsittelytiede, pro gradu –tutkielma, 2019.
[399] Hölttä (2009), s. 41.
[400] Ks. esim. Timonen, Jussi: *A Common Operating Picture for Dismounted Operations and Situation*
Room Environments. Doctoral Dissertation. National Defence University Series 1: Research Publications No. 19, Helsinki, 2018.
[401] Koskinen-Kannisto, Anne: *Situational Awareness Concept In A Multinational Collaboration Environment Challenges in the Information Sharing Framework*. Doctoral Dissertation. National Defence University Department of Military Technology Series 1, n:o 31, Helsinki, 2013, s. 198–199.

2.5.3 Johtaminen

Yksinkertaistetusti johtaminen liittyy organisaation tavoitteen saavuttamiseen.[402] Puolustusvoimissa johtamisen nähdään koostuvan tilanneymmärryksen muodostamisen, suunnittelun, päätöksenteon, organisoinnin, toimeenpanon ja arvioinnin kyvykkyysalueista.[403] Johtamisjärjestelmä ymmärretään johtamisrakenteen ja verkostorakenteen kokonaisuutena. Edellinen koostuu johtamisen prosesseista, organisaatioista ja henkilöstöstä sekä johtamisessa tarvittavista tiedoista ja jälkimmäinen johdettavan järjestelmän osajärjestelmät liittävästä verkosta ja järjestelmistä.[404]

Yhdysvaltojen asevoimissa käytetään käsitettä *command and control*, jonka määritelmä on ”toimivaltaisen komentajan auktoriteetin ja ohjausvallan käyttö alaisiin ja alistettuihin joukkoihin tehtävän toteuttamiseksi.”[405] *Command and control system* taas määritellään niiksi ”tiloiksi, laitteiksi, viestiyhteyksiksi, menetelmiksi ja henkilöstöksi, jotka ovat komentajalle välttämättömiä tehtävään käskettyjen joukkojen operaatioiden suunnittelemiseksi, ohjaamiseksi ja kontrolloimiseksi.”[406] Yhdysvaltojen maavoimien ohjesääntö liittää *command and control* käsitteeseen prosessin, joka koostuu suunnittelusta, valmistelusta, toimeenpanosta ja kaikkiin vaiheisiin liittyvästä arvioinnista. *Command* sisältää auktoriteetin, vastuun, päätöksenteon ja johtajuuden. Käsite *command* liittyy komentajaan henkilönä ja tarkoittaa Ross Pigeaun ja Carol McCannin mukaan tehtävän täyttämisen vaatimaa luovan ihmistahdon ilmaisua, joka edellyttää toimintakykyä, auktoriteettia ja vastuuta.[407]

---

[402] Hartikainen, Riku: *Johtamista vai ohjausta? Puolustusvoimien moninaiset johtamis- ja ohjausmallit*. Yleisesikuntaupseerikurssi 57:n opinnäytetyö, Maanpuolustuskorkeakoulu 2015, s. 17–18.
[403] PVOHJEK-PE: *Puolustusvoimien toiminta*. HN707/23.11.2017, liite 1.
[404] PVOHJEK-PE: *Puolustusvoimien toiminta*. HN707/23.11.2017, liite 6.
[405] The United States Department of Defense (U.S. DoD): *DOD Dictionary of Military and Associated Terms, December 2020*: Command and control, s.40. [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2020-06-18-073638-727], luettu 11.1.2021.
[406] U.S. DoD (2020), s.41.
[407] Pigeau, Ross, & McCann, Carol: Re-conceptualizing Command and Control. *Canadian Military Journal*, Vol. 3, No 1. (Spring 2002), s. 53–63. Pigeaun ja McCannin muotoilua ovat vakiinnuttaneet yhdysvaltalaiset NCW teoreetikot ks. Hayes & Alberts (2005), s. 18.

Control sisältää ohjauksen, palautteen, informaation ja kommunikaation.[408] Se on *commandin* instrumentti eli koostuu prosesseista sen toteuttamiseksi ja riskien hallitsemiseksi. Se sisältää valvonnan, prosessien toimeenpanon ja niiden säätämisen. *Controllin* rakenteet ja prosessit sisältävät organisaatiot, SOP:it, ROE:t, ohjesäännöt ja määräykset, tietotekniset ja asejärjestelmät ja doktriinit.[409]

Neuvostoliitossa kyberneetikko Norbert Wienerin käyttämä *control* termi käännettiin termiksi *upravlenie*, joka tarkoitti sääntelyä, hallintoa tai manageerointia asetettuun tavoitetilaan pääsemiseksi.[410] Christopher Donnellyn mukaan *upravlenie* pitäisi sotilaskontekstissa kääntää hallinnoksi (*administration* tai *management*), kun taas *upravlenie voiskami* kääntyy termiksi *command and control*, joka kuitenkin sisältää harjoittelun ja valmiuden ylläpidon. Venäjänkielinen termi *kontrol* tarkoittaa valvontaa ja seurantaa. Komentaminen tai käskeminen ilmaistaan termillä *rukovodstvo voiskami*.[411] Johtamiseen sisältyy tiedon kerääminen ja analysointi, päätöksenteko, käskeminen, suunnittelu, yhteistoiminnan ja tukitoiminnan organisointi ja ylläpitäminen, joukkojen taisteluun valmistelun johtaminen, alajohtoportaiden kontrollin ja tuen organisointi, taistelutoimien suora johtaminen sekä joukkojen moraalin ylläpito. Pääperiaatteina ovat mm. johdon jakamattomuus ja keskitetty johtaminen.[412] Neuvostoliittolaisen johtamistavan onkin nähty perustuneen hierarkiaan ja keskittämiseen, mutta Venäjän osalta tulkinnat ovat epävarmempia.[413] Johtamisjärjestelmistä käytetään sotilas- ja

---

[408] The Department of the Army of the United States of America: *ADP 6-0 31 July 2019. Mission Command: Command and Control of Army Forces*. Headquarters Department of the Army, Washington D.C., 2019.
[409] Pigeau & McCann (2002).
[410] Rindzeviciuté, Eglé: *Constructing Soviet Cultural Policy: Cybernetics and Governance in Lithuania after World War II*. Doctoral Dissertation. Linköping University, Linköping, 2008.
[411] Donnelly, Christopher: *Red Banner. The Soviet Military System in Peace and War*. Jane's Information Group, Coulsdon, 1988, s. 136.
[412] *Военный энциклопедический словарь (ВЭС)*: Управление войсками (силами) [http://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=10705@morfDictionary], luettu 3.7.2020.
[413] Glantz, David M.: *The Role of Soviet Intelligence in Soviet Military Strategy in WWII.* Presidio Press, Novato, CA, 1990; Rice, Condoleezza: The Party, the Military, and Decision Authority in the Soviet Union. *World Politics*, Vol. 40, No. 1. (October 1987), s. 55–81; McDermott, Roger N. & Bartles, Charles K.: *The Russian Military Decision-Making Process & Automated Command and Control*. GIDS research 02/2020, 29. October 2020. [https://gids-hamburg.de/wp-

siviilipuolella yläkäsitettä automatisoidut johtamisjärjestelmät – lyhennettynä ASU (*avtomatizirovannaja sistema upravlenija*). Automatisointi tarkoittaa tietokoneiden, matemaattisten mallien ja organisaatiokompleksien käyttämistä kaikissa johtamisen tehtävissä sekä tulevaisuuden ennustamisessa annetun tavoitteen saavuttamiseksi rationaalisesti. Kyberturvallisuuden puolella ASU:lla viitataan kaikkiin vähänkään autonomisiin laitteisiin, ohjelmistoihin ja prosesseihin.[414] Tekoäly on oma käsitteensä, joka viittaa ihmisen kognitiivista toimintaa jäljitteleviin teknologisiin ratkaisuihin.[415]

Päätöksenteko on olennainen osa johtamista. Said Elbannan mukaan päätöksentekotutkimuksessa päätöksenteon tason on katsottu määrittelevän päätöksenteon piirteitä.[416] Päätöksenteon kohde ei varsinaisesti määrittele tasoa vaan kohteen merkitys organisaatiolle ja kontekstille. Esimerkiksi strateginen päätöksenteko liittyy vuorovaikutukseen organisaation ympäristön kanssa, johtaa useisiin alatason päätöksiin, tapahtuu epävarmuuden vallitessa ja ilman rutiineja ja selkeää parasta vaihtoehtoa.[417] Yargerin mukaan strateginen päätöksenteko pyrkii ympäristöä muokkaaviin vaikutuksiin.[418] Sotatieteen ja taidon parissa strateginen päätöksenteko ja johtaminen liitetään sodan päämäärien saavuttamiseen.[419]

Tilanteessa, jossa on käytettävissä aikaa ja resursseja, voidaan strategisessa päätöksenteossa noudattaa Simonin mallia, jossa määritellään ongelma, tunnistetaan vaihtoehdot, kehitetään arviointikriteerit, arvioidaan

---

content/uploads/2020/10/GIDSresearch2020_02_McDermott_Bartles.pdf], luettu 26.12.2020.

[414] Kukkola (2020a), s. 247–249. Myös Суровикин, С.В. & Кулешов, Ю.В.: Особенности организации управления межвидовой группировкой войск (сил) в интересах комплексной борьбы с противником. *Военная мысль*, № 8 (2017), с. 5–8; Рипенко, Ю. Б.: *Управление войсками*. Gorizont, Москва, 2016; Торгованова, Ю. Б. (под общ. ред.): *Управление подразделениями в мирное время*. Сиб. федер. ун-т, Красноярск, 2015.

[415] Указ-490: Указ Президента РФ от 10.10.2019 N 490 "*О развитии искусственного интеллекта в Российской Федерации (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года*". [http://www.consultant.ru/document/cons_doc_LAW_335184/], luettu 11.1.2021.

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

[417] Elbanna (2006); Johnson, G., Scholes, K. & Whittington, R.: *Exploring Corporate Strategy. Text and Cases*. FT Prentice Hall Financial Times, Harlow, 2005.

[418] Yarger (2006), s. 21–23.

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

vaihtoehdot, valitaan vaihtoehto, toimeenpannaan päätös ja analysoidaan tulokset.[420] Tilanteessa, jossa käytettävissä oleva aika ja resurssit ovat rajalliset, on päätöksentekoa mallintamaan käytetty John Boydin OODA kehää.[421] Mallissa yksilö havainnoi jatkuvasti ympäristöään, reagoi tarvittaessa ja asemoi itsensä sisäisten malliensa avulla, tekee päätöksen ja toimii. Boydin malli perustuu sellaisen tempon (aloitteellisuuden, vaihtelevuuden ja pikaisuuden) ylläpitämiselle päätöksenteossa ja toiminnassa, että vastustajan kitka kasvaa omaa korkeammaksi ja vastustaja saatetaan epätasapainoon.[422] Hammondin mukaan tavoitteena on päästä vastustajan johtamisen (*command and control*) kehän sisälle.[423] Nopeus ei ole kaikki kaikessa, sillä nopeudesta saatavaa etua rapauttavat ajan puute, epäsystemaattisesti luotu tilanneymmärrys sekä erilaiset ajattelun vääristymät.[424]

Taktisen ja operatiivisen (operationaalisen) päätöksenteon suhteen siviili- ja sotilaskäsitteistö poikkeaa selvästi. Talous- ja organisaatiotutkimuksen puolella taktinen liittyy strategian toimeenpanon ennakkoehtojen luomiseen ja operatiivinen jatkuvaan, tilanteenmukaiseen johtamiseen.[425] Taktista päätöksentekoa siviilikontekstissa ohjaavat käytössä olevien resurssien allokaatio, priorisointi ja aikatauluttaminen sekä keskipituinen aikajänne ja keskitason riski.[426] Operatiiviset päätökset nähdään rutiininomaisina, säädeltyinä, puhtaammin rationaalisuutta noudattavina ja

---

[420] Simon, H. A.: Theories of Decision-making in Economic and Behavioral Science. *American Economic Review*, Vol. 49 (1959), s. 253–283; Simon, H.: *The New Science of Management Decision*. Prentice Hall, Englewood Cliffs, NJ, 1997; Kuusisto (2004). Ks. myös Ejimabo, O. N.: An Approach to Understanding Leadership Decision Making in Organization. *European Scientific Journal*, Vol. 11, No. 1 (2015), s. 2–24.

[421] Olsen (2012); Bryant (2006), s. 185–187; Osinga (2013); Coram, Robert: *Boyd. The Fighter Pilot Who Changed the Art of War*. Back Bay Books, New York, 2002.

[422] Osinga (2013), s. 618–619.

[423] Hammond (2001), s. 165.

[424] Osinga (2013); Hammond (2001); Dyndal, Gjert Lage: Airborne Intelligence, Surveillance and Reconnaissance. Teoksessa *Routledge Handbook of Air Power*. Olsen, John Andreas (ed.) Routledge, Abingdon, Oxon, 2018, s. 107–117.

[425] Mätäsniemi, Teemu (ed.): *Operational decision making in the process industry Multidisciplinary approach*. VTT Tiedotteita - Research Notes 2442. VTT, Helsinki, 2008.

[426] Magnanti, Thomas L.: Networks as an Aid in Transportation and Contingency Planning. *Proceedings of Workshop Held 28–30 March 1982*. George Horwich (ed.), Pergamon, 1983, s. 703–723; Singh, Madan G.: Tactical Decision Making for the firm in a competitive environment. *Conference Proceedings 1991 IEEE International Conference on Systems, Man, and Cybernetics, University of Virginia*, 13-16 Oct. 1991, 2003-2008.

hyvin lyhyellä aikajänteellä toteutettavina.[427] Sotilaskäsitteistössä operatiivinen viittaa asevoimien suorituskykyjen käyttöön ja suunnitteluun, edellytysten luomiseen, strategian toimeenpanoon ja toisaalta johtamisen tasoon. Taktinen viittaa taisteluiden käymiseen ja edelleen johtamisen tasoon.[428] Operatiivinen päätöksenteko nähdään sotilaspuolella taitona, tieteenä tai jopa taiteena johtuen operatiivisen tason kompleksisuudesta ja laajuudesta.[429] Tässä työssä johtaminen määritellään sotilaskäsitteistön kautta ymmärrettynä.

Vähemmän yllättäen edellä esitetyt päätöksenteon vaiheet ovat löydettävissä läntisten asevoimien suunnitteluohjeista, sillä poikkeuksella että asevoimat lisäävät mukaan suunnitteluvaiheen.[430] Huomattava on, että strategisen päätöksenteon mallit kuvaavat itse asiassa johtamista kokonaisuutena, josta päätös muodostaa vain yhden osan. Lisäksi kaiken tasoisen johtamisena tukena informaatioteknologian on nähty parantavan päätösten ja niiden toimeenpanon laatua ja nopeutta.[431]

Päätöksenteolla ja johtamisella kybertoimintaympäristössä on omat ominaispiirteensä.[432] Anonymiteetti ja läpinäkyvyyden puute, epävarmuus, kompleksisuus, tilanteiden nopeus (koneaika), auktoriteettikysymykset ja yhteistyötekijät, sekä informaation korostunut merkitys vaikuttavat päätöksentekoon ja toimeenpanoon.[433] S.L. Russell ja S.C. Jackson ovat esittäneet, että nimenomaisesti kyberpäätöksentekoon liittyviä periaatteita ovat kokonaisvaltaisuus (*comprehensivity*), mahdollisuuksien

---

[427] Clegg, Stewart R., Hardy, Cynthia & Nord, Walter R. (eds.): *Handbook of Organization Studies*. SAGE, London, 1996, s. 294–295.
[428] Rekkedal, Nils Marius: *Nykyaikainen sotataito. Sotilaallinen voima muutoksessa*. Maanpuolustuskorkeakoulu, Helsinki, 2013.
[429] Operaatiotaidosta ks. esim. Vego (2017).
[430] NATO: *Allied Command Operations Comprehensive Operations Planning Directive COPD Interim V2.0 04 October 2013, NATO Unclassified.* [https://www.cmdrcoe.org/download.cgf.php?id=9], luettu 13.5.2020.
[431] Molloy, Steve & Schwenk, Charles R.: The Effects of Information Technology on Strategic Decision Making. *Journal of Management Studies*, Vol. 32, No. 3 (1995), s. 283–311.
[432] Johtamisen toimintaympäristöistä ks. Rantapelkonen, Jari & Koistinen, Lotta: *Pohdintoja sotatieteellisistä käsitteistä*. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 2: Tutkimusselosteita nro 1, Helsinki, 2016, s. 42–43.
[433] Smeets, Max & Work, J.D.: Operational Decision-Making for Cyber Operations: In Search of a Model. *The Cyber Defense Review*, Vol. 5, No. 1 (2020), s. 95–112; Chen, Jim Q.: A Strategic Decision-Making Framework in Cyberspace. Teoksessa *Developments in information security and cybernetic wars*. Sarfraz, Muhammad (ed.) IGI Global, Hershey, PA, 2019, s. 64–75; NATO (2020b), s. 41; Brantly (2016).

hyväksikäyttö (*opportunity*), täsmällisyys (*rigor*), hyökkäyspinta-alan minimointi (*minimization*), järjestelmien ja verkkojen segmentointi (*compartmentation*), häiriönsieto (*fault tolerance*) ja kustannusten mitoittaminen (*proportionality*).[434] Kriittisesti voisi todeta osan periaatteista olevan enemmän toimintaan kuin päätöksentekoon liittyviä. Tuija Kuusiston mukaan kybertoimintaympäristö edellyttää hyvin organisoitua ja jatkuvaa tiedonhallintaa, jonka tulee mahdollistaa päätöksenteko ja johtaminen kaikilla tasoilla inhimillisen tiedonkäsittelykyvyn reunaehdot huomioiden.[435] Johtaminen kybertilassa on siis riippuvainen järjestelmistä ja verkoista – siellä tapahtuvaa toimintaa ei voi johtaa tilan ulkopuolelta.

Johtaminen kybertoimintaympäristössä perustuu teknisiin järjestelmiin. Päätöksenteon ja johtamisen tukijärjestelmät auttavat epävarmuuden hallinnassa ja tuottavat luotettavia selityksiä, ennusteita ja toimintavaihtoehtoja, karsivat ajatteluvääristymiä, mahdollistavat yhteistyötä ja koordinointia ja tehostavat toistuvien tehtävien hoitamista.[436] Carvalho et al. mukaan kyberjohtaminen edellyttää kestävää ja hajautettua tuki-infrastruktuuria, joka mahdollistaa fyysisten resurssien ja loogisen organisaation erottamisen. Järjestelmän tulee kyetä integroimaan itseensä useita erilaisia sensoreita ja yhdistämään näiden data ihmisen ymmärtämäksi informaatioksi. Järjestelmän tulee olla joustava ja muuntautua hyökkäysten mukana, mikä edellyttää vähintään rajoitettua autonomiaa.[437] Puolustautuminen perustuu entistä enemmän liikkuvan kohteen puolustukseen eli verkkokonfiguraatioiden muutokseen SDN-teknologiaan ja virtualisointiin perustuen.[438] Johtamisjärjestelmien avulla

---

[434] Russell, S.L. & Jackson, S.C.: Operating in the Dark: Cyber Decision-Making from First Principles. *Journal of Information Warfare*, Vol. 17, No. 1 (Winter 2018), s. 1–15. Ks. myös Smeets & Work (2020).

[435] Kuusisto (2014), s. 44.

[436] Mätäsniemi (2008), s. 30–33; Hutchins, Susan G.: *Principles for Intellihent Decision Aiding*. Technical Report 1718. Naval Command, Control and Ocean Surveillance Center, San Diego SA, 1996.

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

[438] Liikkuvan kohteen puolustus (*Moving Target Defence*) perustuu kyberjärjestelmien konfiguraatioiden jatkuvaan muuttamiseen, mikä lisää hyökkääjän vaikeutta tiedustella kohdejärjestelmiä. Puolustaja voi muuttaa tiedustelupinta-alaa, hyökkäyspinta-alaa ja havainnointi sekä estopinta-alaa. (Sengupta, Sailik, Chowdhary, Ankur, Sabur, Abdulhakim, Alshamrani, Adel, Huang, Dijiang & Kambhampati, Subbarao: A Survey of Moving Target Defenses for Network Security. *IEEE Communications Surveys & Tutorials 2020*, [https://arxiv.org/abs/1905.00964v2], luettu 11.1.2021; Piedrahita,

puolustajat voivat monitoroida liikennettä, havaita poikkeamat ja estää ei-toivotun liikenteen.[439] Komentoyhteydet ovat hyökkäysten osalta kriittisiä onnistumiselle. Hyökkääjät tiedostavat puolustajan kyvyn hallita toimintaympäristöä ja pyrkivät hajauttamaan, salaamaan, häivyttämään ja naamioimaan yhteytensä. Kaikki hyökkäykset eivät toki edellytä komentoyhteyksiä.[440]

Johtamisympäristöjen monimutkaistuessa johtamisjärjestelmistä itsessään tulee järjestelmien järjestelmiä. Lin Manin ja Chaowei Wangin mukaan tämä johtaa hallitsemattomiin emergentteihin ilmiöihin, mikäli päätöksentekijöiden vuorovaikutusta, informaatiovaihtoa ja päätöksenteon sääntöjä ei kontrolloida.[441] Kybertoimintaympäristössä tämä johtaa yhtäältä tarpeeseen automatisoida mahdollisimman paljon perustoimintoja, mutta toisaalta tarpeeseen säilyttää kriittisiin toimintoihin liittyvät päätökset ihmisillä, joita koneet tukevat vaihtoehtosuosituksilla.[442] Kaikki automatisoitu on kuitenkin itsessään manipuloinnin ja hyökkäyksen kohde.[443]

Johtamisen toteuttamiseen vaikuttaa toimintaympäristön ja järjestelmien lisäksi sen tapa. Keskitetyssä päätöksenteossa informaatio kootaan yhteen pisteeseen, jossa tehdään päätös ja käskyt välitetään sitten toteuttajille.

Murillo, Andrés F., Gaur, Vikram, Giraldo, Jairo, Cárdenas, Álvaro A. & Rueda, Sandra Julieta: Leveraging Software-Defined Networking for Incident Response in Industrial Control Systems. *IEEE Software*, Vol. 35, No. 1 (January/February 2018), s. 44–50.

439 Gardiner, Joseph, Cova, Marco & Nagaraja, Shishir: *Command & Control. Understanding, Denying and Detecting*. University of Birmingham, February 2014. [https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf], luettu 2.7.2020.

440 Ibid..

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

442 Chen (2019)

443 Hartmann, Kim & Steup, Christoph: Hacking the AI – the Next Generation of Hijacked Systems. Teoksessa *2020 12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade*. Jančárkova, Lindström, L., Signoretti, M., Tolga, I. & Visky, G. (eds.). CCD COE Publications, Tallinn, 2020, s. 327–349; Siukonen (2019); Gutzwiller, Robert S., Ferguson-Walter, Kimberly J. & Fugate, Sunny J.: Are Cyber Attackers Thinking Fast and Slow? Exploratory Analysis Reveals Evidence of Decision-Making Biases in Red Teamers. *Proceedings of the Human Factors and Ergonomics Society 2019 Annual Meeting*, Vol. 63, No. 1 (2019), s. 217–221; Gutzwiller, Robert S., Fugate, Sunny, D. Sawyer Benjamin D. & Hancock, P. A.: The Human Factors of Cyber Network Defense. *Proceedings of the Human Factors and Ergonomics Society 59th Annual Meeting – 2015*, Vol. 59, No. 1, s. 322–326.

Hajautetussa päätöksentekijöitä on useita ja ne jakavat yhteisen päämäärän ja tilannetiedon. Keskitetty johtamisjärjestelmä on haavoittuvainen mutta kustannustehokas, hajautettu taas tukee verkottumisesta saatavia etuja, kuten itsesynkronointia, mutta maantiede ja funktioiden keskinäisriippuvuudet asettavat sille rajoituksia.[444] Keskitetty johtamisjärjestelmä on jäykkä ja hidas reagoimaan taktisella tasolla ja suljettuna järjestelmänä se voi teoreettisesti vajota entropiaan.[445] Hajautettu järjestelmä voi olla joustava, mutta verkottuminen lisää kompleksisuutta ja häiriöiden ja ennustamattomien ilmiöiden mahdollisuutta.[446] Teoriassa hajautettu päätöksenteko, täydellisten viestiyhteyksien ja optimaalisesti toimivien järjestelmien olosuhteissa, perustuu paremmalle tiedolle ja on nopeampaa kuin keskitetty päätöksenteko.[447] Keskitetyn ja hajautetun järjestelmän välissä on siiloutunut järjestelmä, joka on periaatteessa yhteisen päämäärän tavoittamisen kannalta heikoin ratkaisu, koska tiedonvaihto minimoituu, eikä päätöksenteko palvele yhteistä päämäärää. Lisäksi se on organisaatioltaan haavoittuvaisin johtamisen malli.[448]

Johtaminen on sidoksissa organisaatioon, teknologiaan ja järjestelmän päämäärään. Sitä ohjaavat mm. osallistujien vuorovaikutuksen muoto ja informaation vaihdon taso, organisaatio, prosessit ja toimintamallit ja päätöksenteon säännöt.[449] Kuten todettu kybertoimintaympäristössä johtaminen on lähtökohtaisesti riippuvainen johtamisjärjestelmistä ja verkoista ja pelkkä päätöksentekoon keskittyminen ei riitä kansallisten verkkojen järjestelmien järjestelmän tarkasteluun.[450] On myös selvää, että

---

[444] Athans, Michael: Command and Control (C2) Theory: A Challenge to Control Science. *IEEE Transactions On Automatic Control*, Vol. AC-32, No. 4 (April 1987), s. 286–293; Van Bezooijen, B. J. A., Essens, P. J. M. D. & Vogelaar, A. L. W.: Military Self-synchronization: An Exploration of the Concept. *11TH ICCRTS, Coalition Command And Control In The Networked Era 27 September 2006*.

[445] Hammond (2001), s. 164–165.

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

[447] Lee, Tony S., Ghosh, Sumit & Nerode, Anil: Asynchronous, Distributed, Decision-Making Systems with Semi-Autonomous Entities: A Mathematical Framework. *IEEE Transactions On Systems, Man, And Cybernetics—Part B: Cybernetics*, Vol. 30, No. 1, February 2000, s. 206–212.

[448] Hitchins, D. K.: A General Theory of Command and Control. *1989 Third International Conference on Command, Control, Communications and Management Information Systems, Bournemouth, UK, 1989*, s. 111–126.

[449] Ma & Wang (2012)*;* Hayes & Alberts (2005).

[450] Tran, Huy T., Domercxant, Jean Charles & Mavris, Dimitri N.: Evaluating the agility of adaptive command and control networks from a cyber complex adaptive systems

kybertoiminnan johtamisessa on psykologinen, sosiaalinen ja kulttuurinen puolensa, jota tässä työssä ei kyetä tarkastelemaan.[451] Koska tutkimuksen kohteena ovat kansallisten verkkojen eroavaisuudet, huomio kiinnittyy siis laajasti ymmärrettynä informaation hallinnan, päätöksenteon tuen ja toimeenpanon järjestelmiin strategisella, operatiivisella ja taktisella tasolla.[452] Järjestelmät pitää tässä ymmärtää rakenteina eli teknologiana, organisaationa ja toimintatapoina, joista viimeinen pitää sisällään doktriinin, ohjesäännöt ja harjoittelun. Ne ovat avoimen ja suljetun verkon ominaisuuksista kumpuvia tekijöitä ja osa digitaalista maastoa. Kansallisten verkkojen osalta on myös huomioitava yksityisten toimijoiden rooli ja yhteistoiminta julkisen ja yksityisen välillä. Etenkin avoimissa verkoissa tämä yhteistoiminta voi olla haasteellista.[453] Tässä työssä kyberhyökkäyksen tai puolustuksen johtamisen tulosten arviointi ei myöskään ole tarkastelun kohteena. Työssä keskitytään *johtamisen rakenteisiin, eli missä ja mihin liittyen päätökset tehdään, ja prosesseihin, eli miten päätökset tehdään ja välitetään, sekä teknologiaan, joka*

---

perspective. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, Vol. 12, No. 4 (2015) s. 405–422; Wang, G., Yang, Y., Ren, Q. & Ma, R.: Efficiency of Command and Control in Cyberspace: Visit from the Perspective of Complexity Theory. *2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery,* Beijing 10-12 October 2013, s. 398–401; Czerwinski, Thomas J.: Command and Control at the Crossroads. *Parameters*, Autumn 1996, s. 121–132; Davis, Paul K., Kulick, Jonathan & Egner, Michael: *Implications of Modern Decision Science for Military Decision-Support Systems*. RAND, Santa Monica, 2005.

[451] Young, Thomas-Durell: Legacy Concepts: A Sociology of Command in Central and Eastern Europe. *Parameters*, Vol. 47, No. 1 (Spring 2017), s. 31–42.

[452] O'Brien, James A. & Marakas, George, M.: *Management Information Systems* (10th ed.) McGraw-Hill, Irwin, New York, 2011, s. 393–396.

[453] EU:n NIS direktiivi, EU komission yhteinen tiedonanto kyberturvallisuudesta ja Yhdysvaltojen DHS:n kyberstrategia ja Cyberspace Solarium Commission raportti tiivistävät hyvin tämän problematiikan. (European Union: *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 "NIS Directive".* [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN], luettu 7.7.2020; European Union: *Joint Communication to the European Parliament and the Council:*
Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Brussels, 13.9.2017 JOIN(2017) 450 final. [https://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cyber-security_ec.pdf], luettu 7.7.2020; The United States Department of Homeland Security: *Cybersecurity Strategy, 15th May 2018* [https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf], luettu 7.7.2020; The United States of America (2020).

mahdollistaa rakenteet ja prosessit.[454] Rakenteita, prosesseja ja teknologiaa arvioidaan niiden mahdollistaman nopeuden, tarkkuuden ja hallinnan kautta.

2.5.4 Resilienssi

Kybertilassa on lähestulkoon mahdotonta tuhota hyökkääjän hyökkäyksellisiä suorituskykyjä pysyvästi tai pyrkiä täydelliseen puolustukseen. Sen sijaan kyberresilienssi tai kybersietoisuus on saavutettavissa oleva päämäärä. Tässä työssä käytetään käsitettä resilienssi, koska sillä on vahvempi kotimainen ja kansainvälinen käsitesisällöllinen pohja kuin kybersietoisuudella.[455] Sekä hyökkääjä että puolustaja perustavat toimintansa samaan tilaan, jonka jatkuva toiminta tulee taata. Mikä tärkeintä, tämä tila mahdollistaa modernien informaatioyhteiskuntien kriittiset palvelut. Suojeleminen tai turvaaminen, jota tässä käsitellään, poikkeaa aikaisemmin mainitusta taistelun elementistä, joka on osa toiminnan vapautta ja liittyy ”joukkojen” suorituskykyjen turvaamiseen. Kybertilan suojaaminen toimii kuten linnoitus tai ystävällismielinen alue, joka neutraloi uhan, takaa resurssien ja prosessien hallinnan ja tarjoaa mahdollisuuden saavuttaa toiminnan vapaus omassa tilassa. Tämän tutkielman kehyksessä kybertilan suojaamista käsitellään resilienssinä, ja se sisällyttää itseensä passiivisen kyberpuolustuksen eri muodot operatiivisella ja strategisella tasolla.

Resilienssin käsitteellä ei ole kansainvälisesti jaettua merkitystä ja siitä on osaltaan muotoutunut jopa kiistelty käsite (*contested concept*).[456] Resilienssillä on yleensä viitattu paluuseen normaaliin tilaan, mutta tarkasteltaessa kompleksisia adaptiivisia järjestelmiä, kuten kybertilaa tai informaatioturvallisuuden järjestelmien järjestelmää (ks. Luku 3), on normaalia vaikea määritellä. Resilienssi on siis aina sidottu tarkasteltavaan järjestelmään ja siihen uhkaan tai häiriöön, johon se valmistautuu

---

[454] Päätöksenteon laadun tai oikeellisuuden arviointi edellyttäisi dataa aikomuksista ja tuloksista, mitä ei ole tämän tutkimuksen kehyksessä saatavilla. (Howard, Ronald & Abbas, Ali E.: *Foundations of Decision Analysis*. Pearson, London, 2015).

[455] Libicki (2009), s. 59–61; Nye (2016/2017). Ks. esim. Sanastokeskus TSK (2018); Sanastokeskus TSK: *Kokonaisturvallisuuden sanasto TSK 50*. Sanastokeskus TSK, Helsinki, 2017; Lehto (2019).

[456] Fjäder, Christian: The Nation-state, National Security and Resilience in the Age of Globalisation. *Resilience*, Vol.2, No.2 (2014), s. 114–129; Humbert, Clemence & Joseph, Jonathan: Introduction: The Politics of Resilience: Problematising Current Approaches. *Resilience*, Vol. 7, No. 3 (2019), s. 215–223.

vastaamaan. Alexander Kottin mukaan resilienssiä voidaan tarkastella alhaisena sensitiivisyytenä häiriöille, kykynä vähentää häiriöiden vaikutuksia tai ehkäistä niiden leviämistä, kykynä neutraloida vaikutukset tai kykynä sopeutua vaikutuksiin.[457] Resilienssi sijoittuu vakauden ja antifragiliteetin välille, joista edellinen liittyy toimintojen ylläpitoon ja jälkimmäinen korjautumiseen entistä vahvemmaksi. On kuitenkin huomattava, ettei järjestelmän päämäärä tai toimintaperiaatteet saa muuttua merkittävästi sopeutumisen seurauksena tai muuten se menettää tarkoituksensa.

Kyberresilienssistä on tullut tärkeä suurvaltojen ja mahdollisesti pienempienkin valtioiden kyberstrategioiden osa. Yhdysvaltojen Cyberspace Solarium Comission nosti vuonna 2020 resilienssin yhdeksi Yhdysvaltojen kyberdeterrenssin kulmakiveksi.[458] Kyberresilienssin tulisi kiistää vastustajalta tämän hyökkäyksillään tavoittelemat edut vahvistamalla kansallisen kriittisen infrastruktuurin sietokykyä. Nämä näkemykset heijastelevat läntisten kybertutkijoiden viimeaikaisia kirjoituksia. Esimerkiksi Martin Libicki argumentoi sellaisen kyberresilienssin puolesta, joka sisältää redundanssin, priorisoinnin, monimuotoisuuden, nopean vastekyvyn, löyhät sidossuhteet (*loose coupling*), kyberturvalliset asenteet, testaamisen, analysoinnin ja jatkuvan teknisen kehittämisen.[459] Chris Demchak taas esittää, että kyberresilienssi edellyttää organisaatioiden välistä yhteistyötä ja tiedonvaihtoa, jatkuvaa järjestelmien seurantaa ja kerätyn tiedon analyysiä. Näiden prosessien kautta organisaation kyky vasta häiriöihin kehittyy joustavaksi ja ennakoivaksi.[460]

Venäjällä vuonna 2019 säädetty ns. laki suvereenista Internetistä teki resilienssistä (*ustojtšivost*)[461] yhden Venäjän Internetin peruselementeistä

---

[457] Kott, Alexander: Information Warfare and Organizational Decision-Making. Artech House, London, 2007, s. 216.
[458] Cyber Solarium Commission (2020).
[459] Libicki (2016), s. 176.
[460] Demchak, Chris: *Wars of disruption and resilience: cybered conflict, power, and national security*. University of Georgia Press, Athens, 2011.
[461] Venäläiset käyttävät sanaa 'ustojtšivost' kirjoittaessaan resilienssistä länsimaisesti ymmärrettynä. Sitä on kuvattu järjestelmän kyvyksi toimia stressin vaikutuksen alla ja kyky palata normaaliin tilaan häiriön jälkeen. (Махутов, Н.А., Резников, Д.О., Петров, В.П. Особенности обеспечения безопасности критических Инфраструктур. *Безопасность в техносфере*, №1 (январь–февраль 2014), с. 3–14, с. 9). Sotilaallisessa kontekstissa kyberresilienssiä (kiberustojtšivost') on kuvattu informaatiokommunikaatioverkon kyvyksi tukea johtamistoimintaa kyberhyökkäyksen

turvallisuuden ja eheyden rinnalla.[462] Jo tätä ennen vuoden 2016 informaatioturvallisuusdoktriini oli todennut, että informaatioinfrastruktuurin sietokykyisen ja keskeytymättömän toiminnan takaaminen rauhan ja sodan aikana kuului Venäjän kansallisiin intresseihin. Venäjällä resilienssin käsite on siirtynyt kybertilan puolelle kriittisten objektien ja myöhemmin kriittisen infrastruktuurin suojaamisen normistosta ja liittyy voimakkaasti informaatio- ja johtamissodankäynnin käsitteistöön.[463] Resilienssiin liittyvät mm. seuraavat käsitteet: selviytymiskyky eli kyky jatkaa toimintaa vahingoista huolimatta, redundanssi eli vaihtoehtoisten reittien ja resurssien olemassa olo, resurssiturva eli reservi, sekä kyky palautua nopeasti ja kyky sopeutua muuttuvaan ympäristöön.[464] Toinen venäläisten käyttämä termi on *otkazoustojtšivost,* joka viittaa englanninkieliseen termiin *failure-related durability*, ja sisältää myös käsityksen vihamielisen ja vahingosta aiheutuvan häiriön sietämisestä ja siitä selviytymisestä.[465] Kiinan virallisissa julkaisuissa ei käytetä kyberresilienssin käsitettä. Kiina sisällyttää ajatuksen ”vakaasti ja luotettavasti” toimivista järjestelmistä kyberturvallisuuden määritelmään.[466]

---

aikana. Resilienssi koostuu selviytymiskyvystä, luotettavuudesta ja häiriösietoisuudesta. (Коцыняк М.А., Кулешов И.А., Кудрявцев А.М. & Лаута О.С.: Киберустойчивость Информационнотелекоммуникационной Сети. Бостон-спектр, Санкт-Петербург, 2015, с. 7-8).

462 ФЗ-90 (2019).

463 Pynnöniemi, Katri & Busygina, Irina: Critical Infrastructure Protection and Russia's Hybrid Regime. *European Security*, Vol.22, No.4 (2013), s. 559–575; Kukkola (2020a), s. 241.

464 Махутов, Резников, & Петров (2014); ГОСТ: *ГОСТ Р 51897-2011. Менеджмент риска. Термины и определения. Дата введения 2012-12-01.* [http://docs.cntd.ru/document/gost-r-51897-2011], luettu 7.7.2020.

465 Медриш, М.А. (ред.): *Стабильность, безопасность, отказоустойчивость глобальной инфраструктуры Интернета: технические и правовые вопросы*. ПИР-Цеитр, Москва - Лос Анджелес, 2016, s. 17–18; ГОСТ: *ГОСТ Р 56111-2014. Интегрированная логистическая поддержка экспортируемой продукции военного назначения.* [http://cals.ru/sites/default/files/downloads/56111_.pdf], luettu 7.7.2020; ГОСТ: *ГОСТ 28806-90. Качество программных средств. Термины и определения.* [https://meganorm.ru/Data2/1/4294825/4294825913.pdf], luettu 7.7.2020.

466 Cyberspace Administration of China (2016); Christine, D. Irene & Thinyane, M.: Comparative Analysis of Cyber Resilience Strategy in Asia-Pacific Countries. Teoksessa *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress* (DASC/PiCom/CBDCom/CyberSciTech), Calgary, AB, Canada, 2020, s. 71–78.

Tässä työssä käytettävä kyberresilienssin käsite määriteltiin luvussa 2.2. ”*kyvyksi ennakoida, sietää, palautua, ja sopeutua haitallisiin olosuhteisiin, stressiin, hyökkäyksiin tai muutoksiin järjestelmissä, joihin kuuluu kyberresursseja*.” Se siis viittaa kybertilan muodostaviin palveluihin ja järjestelmiin, joissa on verkko- ja informaatioteknologiaan liittyviä komponentteja.[467] Kyberresilienssi poikkeaa puolustuksesta, koska se perustuu riskin minimointiin ja palautumiseen, ei jonkin kohteen aktiiviseen suojeluun lähtökohtaisesti täydellisesti haitalliselta vaikutukselta.[468] Resilienssillä on yhtäläisyyksiä kiistämiseen perustuvaa deterrenssiin, sillä se perustuu vastustajan toiminnan tyhjäksi tekemiseen ja vaikutusten minimointiin.[469] Resilienssi eroaa turvallisuudesta, jonka perustana on uhkien puute, sillä resilienssi hyväksyy uhkien riskin jatkuvan läsnäolon valmistautumisen ja mukautumisen perustana.[470]

Resilienssiä käytetään tässä tutkielmassa rakenteellisen kyberasymmetrian analyysiin, koska se nostaa tarkastelun kohteeksi kybertilan järjestelmät ja infrastruktuurin. Se myös heijastaa kyberstrategian passiivista puolta, eli voiman kasvattamista paikallaan pysymällä, siinä missä muut kolme käsitettä liittyvät aktiivisempaan strategian tekemiseen. Resilienssin analyysi keskittyy siis kriittiseen informaatioinfrastruktuuriin ja sen toiminnan jatkuvuuden edellytyksiin avoimissa ja suljetuissa kansallisissa verkoissa. Edelleen analyysin kohteeksi nousevat ne järjestelmät ja menetelmät, joilla kriittisen informaatioinfrastruktuurin toimivuuden jatkuvuus taataan.[471]

---

[467] Ross, Graubart, Bodeau, & Mcquaid (2018); Vlacheas et al. (2011); European Commission (2018); Björck et al. (2015); Hyvönen, Ari-Elmeri, Juntunen, Tapio, Mikkola, Harri, Käpylä, Juha, Gustafsberg, Harri, Nyman, Markku, Rättilä, Tiina, Virta, Sirpa & Liljeroos, Johanna: *Kokonaisresilienssi ja turvallisuus: tasot, prosessit ja arviointi*. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 17/2019. Valtioneuvoston kanslia, Helsinki, 2019.

[468] Fjäder (2014).

[469] Gartzke & Lindsay (2015).

[470] Joseph, Jonathan: Resilience as embedded neoliberalism: a governmentality approach. *Resilience*, Vol. 1, No. 1 (2013), s. 38–52.

[471] Geers (2009); McCarthy, J. A., Burrow, C., Dion, M. & Pacheco, O.: Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts. Teoksessa *Cyberpower and National Security*. Kramer, F. D., Starr, S. H. and Wentz, L. (eds.). National Defence University Press, Washington D.C., 2009, s. 543–556; Zhang, Nan, Krishna, Kant & Sajal K.: *Handbook on Securing Cyber-Physical Critical Infrastructure*. Elsevier, Amsterdam, 2012; Vankka, Jouko (ed.): *Critical Infrastructure Protection against Cyber Threats*. National Defence University, Report Series 1, No 36. Juvenes Print, Tampere, 2014; Ross, Graubart, Bodeau & Mcquaid (2018).

3 Venäjän kansallinen internetsegmentti

Tässä luvussa vastataan tutkimuskysymykseen, mikä on Venäjän kansallinen internetsegmentti ja sen suhde informaatioturvallisuuden ja -puolustuksen järjestelmän ja suljetun kansallisen verkon käsitteisiin? Luku alkaa yleisen systeemiteorian ja väitöskirjaani pohjautuvan venäläisen strategisen kulttuurin esittelyllä. Esittely antaa perustan kansallisen internetsegmentin tulkinnalle järjestelmien järjestelmänä. Luvun toisessa osassa tarkastellaan Venäjän valtion ominaispiirteitä, jotka vaikuttavat kansallisen internetsegmentin luonteeseen. Luvun kolmannessa osassa tarkastellaan kansallisen segmentin syntyä ja kehitystä niiltä osin, kuin se on tarpeellista neljännessä osassa esiteltävän kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmän ymmärtämiselle. Luvun viidennessä osassa esitetään teoreettisen avoimen kansallisen verkon ominaispiirteet. Järjestelmien järjestelmän kuvaus antaa perustan rakenteellisen kyberasymmetrian analyysille luvussa 4.

3.1 Systeemi analyysikehikkona

Järjestelmäajattelu auttaa kybertoimintaympäristön jäsentämisessä. Järjestelmäajattelu tai -teoria on kattokäsite moninaiselle joukolle tieteellisiä teorioita ja lähestymistapoja mukaan lukien yleinen järjestelmäteoria, kybernetiikka, informaatioteoria, kontrolliteoria, järjestelmäanalyysi ja operaatioanalyysi.[472] Vaikka näillä lähestymistavoilla on omat määritelmänsä järjestelmän käsitteelle, niitä yhdistää holistinen ontologia. Sen mukaan ilmiöitä tulee lähestyä osien suhteiden, järjestymisen periaatteiden ja kokonaisuuden näkökulmasta rakenteiden ja yksittäisten osien sijaan. Peter Checklandin mukaan järjestelmäajattelussa (*systems approach*) maailman nähdään koostuvan rakenteellisista kokonaisuuksista (*structured wholes*), jotka kykenevät säilyttämään identiteettinsä ja eheytensä suhteessa ympäristöönsä. Järjestelmät eivät ole suoraan havaittavissa vaan tutkijan tehtävänä on

[472] Laszlo, Ervin: Systems Philosophy. *Ultimate Reality and Meaning* January, Vol. 1, No. 3 (1978), s. 223–230; Hammond, Debora: *The Science of Synthesis. Exploring the Social Implications of General Systems Theory*. The University Press of Colorado, Boulder, 2003. Kybernetiikasta ks. Esim. Ashby, Ross W.: *An Introduction to Cybernetics*. London, Chapman & Hall, 1956. [http://pespmc1.vub.ac.be/ASHBBOOK.html], luettu 23.9.2019; Kline, Ronald R.: *The Cybernetics Moment, Or Why We Call Our Age the Information Age*. Johns Hopkins University Press, Baltimore, 2015; Aström, Karl J. & Kumar, P.R. Control: A Perspective: A perspective. *Automatica*, Volume 50, Issue 1, (January 2014), s. 3-43.

tarkastella todellisuutta ja määritellä järjestelmät.[473] Russell Ackoffin mukaan järjestelmäajattelussa identifioidaan ensin kokonaisuus (järjestelmä), jonka osa selitettävä asia on. Sitten selitetään kokonaisuuden ominaisuudet tai toiminta eli päämäärä. Lopuksi selitetään itse selitettävä osa kokonaisuuden roolien tai funktioiden ehdoilla huomioiden vuorovaikutus toisten osien kanssa.[474]

Järjestelmäajattelun mukaan järjestelmät voivat olla niin mekaanisia, biologisia kuin sosiaalisia.[475] Edelleen ne voidaan jakaa itsensä uudelleen tuottaviin (autopoeettisiin) ja jotain muuta tuottaviin tai kontrolloiviin (allopoeettisiin).[476] Järjestelmiä on myös jaoteltu suljettuihin ja avoimiin sen mukaan, vaihtavatko ne materiaa, energiaa tai informaatiota ympäristönsä kanssa vai eivät.[477] Kaikista avoimimpia ovat kompleksiset adaptiiviset järjestelmät, jotka kehittyvät ja muuttuvat ympäristönsä mukana.[478] Kybernetiikan piirissä on eroteltu ensimmäisen asteen (tuottavia), toisen asteen (itsensä uusintavia) ja kolmannen asteen

---

[473] Checkland, Peter: *Systems thinking, Systems Practice*. John Wiley & Sons ltd., New York, 1993. Ks. myös Alker, Hayward R.: The Powers and Pathologies of Networks: Insights from the Political Cybernetics of Karl W. Deutsch and Norbert Wiener. *European Journal of International Relations*, Vol.17, No. 2 (2011), s. 351–378; Checkland, Peter: Soft Systems Methodology: A Thirty Year Retrospective. *Systems Research and Behavioral Science Syst. Res*. 17 (2000), s. 11–58; Deutsch, Karl W.: *The Nerves of Government: Models of Political Communication and Control*. Collier-Macmillan, New York & London, 1963; Easton, David: *A Systems Analysis of Political Life*. John Wiley & Sons, New York, 1965; Easton, David: *A Framework for Political Analysis*. University of Chicago Press, Chicago & London, 1979; Son, Kyong-Min: Cybernetic Freedom: David Easton, Systems Thinking, and the Search for Dynamic Stability. *American Political Thought: A Journal of Ideas, Institutions, and Culture*, Vol. 7 (Fall 2018), s. 614–645; Gare, Arran: Aleksandr Bogdanov and Systems Theory. *Democracy & Nature*, Vol. 6, No. 3, 2000, s. 341–359; Parsons, Talcott: *The Social System*. Routledge, London, 1991; Lillianfeld, Robert: *The Rise of Systems Theory: an Ideological Analysis*. John Wiley and Sons, New York, 1978; von Bertalanffy, Ludvig: *General System Theory*. George Braziller, New York, 1968; Principia Cybernetica Project: *Principia Cybernetica We.b* [http://pespmc1.vub.ac.be/DEFAULT.html], luettu 4.10.2019.

[474] Ackoff, Russell L.: *Ackoff's Best. His Classic Writings on Management*. John Wiley & Sons, Inc., New York, 1999, s. 17.

[475] Checkland (2000).

[476] Mancilla, Roberto Gustavo: Introduction to Sociocybernetics (Part 1): Third Order Cybernetics and a Basic Framework for Society. *Journal of Sociocybernetics*, Vol. 36, No. 9 (2011), s. 35–56.

[477] Ks. Heylighen, Francis: *Web Dictionary of Cybernetics and Systems*. [http://pespmc1.vub.ac.be/ASC/INDEXASC.html], luettu 23.9.2019.

[478] Bousquet, Antoine & Curtis, Simon: Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations. *Cambridge Review of International Affairs*, Vol. 24, No. 1 (March 2011), s. 43–62.

(tiedostavia) järjestelmiä.[479] Viimeaikaisen hallinnon (*governance*) teorian näkökulmasta järjestelmillä voidaan viitata hallinnon mekanismeihin, joilla valvotaan ja kontrolloidaan yhteiskunnan tilaa haluttuun suuntaan palautteen perusteella. Tässä lähestymistavassa sosiaalinen järjestelmä jaotellaan funktionaalisiin systeemeihin (politiikka, talous, laki jne.)[480] ja puretaan organisaatioiden ja sääntöjen regiimeiksi. Niiden avulla voidaan paremmin tarkastella, miten hallinta toteutuu ihmisyhteisöissä.[481] Sosiologisen järjestelmäajattelun näkökulmasta järjestelmien ontologinen status on sekundaarinen verrattuna analyyttiseen merkitykseen.[482] Järjestelmäajattelua voidaan siis soveltaa niin materiaalisiin ja teknologisiin järjestelmiin kuin inhimillisen toiminnan muotoihin.

Sosiaalisten järjestelmien funktionaalisuutta painottavan Talcott Parsonsin mukaan järjestelmillä on neljänlaisia toiminnallisuuksia: adaptiivisia, päämäärähakuisia, integroivia ja ylläpitäviä.[483] Toisaalta Niklas Luhmann on väittänyt, että jokainen järjestelmä on syntynyt ainutkertaisen prosessin ympärille.[484] Tässä työssä noudateltavan ”pehmeän” systeemiajattelun

---

[479] Kybernetiikka on tieteenala, joka tutkii säätöä / hallintaa ja kommunikaatiota kompleksisissa järjestelmissä, päämäärähakuisissa koneissa, elävissä organismeissa ja yhteiskunnassa. Mancilla (2011).

[480] Systeemiteoriat kehittyivät sosiologian piirissä strukturalististen ja funktionaalis-strukturalististen teorioiden kautta ks. Parsons (1991); Luhmann, N.: *Essays on self-reference*. Columbia University Press, New York, 1990; Habermas, Jürgen: Talcott Parsons: Problems of Theory Construction. *Social Inq*. Vol 51, No. ¾ (1981), s. 173–196; Luhmann, Niklas: *The Differentation of Society*. Columbia University Press, New York, 1981.

[481] Esmark, Anders: The Functional Differentiation Of Governance: Public Governance Beyond Hierarchy, Market And Networks. *Public Administration*, Vol. 87, No. 2 (2009), s. 351–370; Schneider, Volker & Bauer, Johannes M.: Governance: Prospects of Complexity Theory in Revisiting System Theory. *Conference paper, presented at the annual meeting of the Midwest Political Science Association. Panel 33.26 Political Theory and Theories of Political Science. Chicago, Illinois, 14 April 2007*; Christou, George, Croft, Stuart, Ceccorulli, Michela & Lucarelli, Sonia: European Union Security Governance: Putting the ‘Security’ Back In. *European Security*, Vol. 19, No. 3 (2010), s. 341–359; Grey, Christopher: Security Studies and Organization Studies: Parallels and Possibilities. *Organization*, Vol. 16, No. 2 (2009), s. 303–316.

[482] Elder-Vass, Dave: Luhmann and Emergentism Competing Paradigms for Social Systems Theory? *Philosophy of the Social Sciences*, Vol. 37, No. 4 (December 2007), s. 408–432; Albert, Mathias & Buzan, Barry: Securitization, Sectors and Functional Differentiation. *Security Dialogue*, Vol. 42, No. 4/5, Special issue on The Politics of Securitization (August-October 2011), s. 413–425.

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

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

mukaan sosiaaliset järjestelmät ovat tutkijan löydettävissä ja määriteltävissä, eikä niille aseteta *a priori* funktioita.[485] Näkökulmana ei kuitenkaan ole kriittisen teoria mukainen näkymättömiä rakenteita ja valtaa paljastava vaan pragmaattinen lähestyminen järjestelmiä kohtaan.[486] Tältä perustalta järjestelmä eli vierasperäisesti systeemi ymmärretään *vuorovaikutuksessa olevien objektien kokonaisuutena, jolla on rajat suhteessa toisiin järjestelmiin, sisäiset väliset suhteet ja järjestymisen periaatteet, ja jolla on funktio ja päämäärä*.[487] Määritelmän valinta perustuu siihen, että työn kiinnostuksen kohteena on ihmisen jotain tarkoitusta varten luoma tai ihmisen toiminnan kautta syntynyt organisoitunut järjestelmä, jossa on teknologisia komponentteja.[488] Tutkimuskohteena oleva järjestelmä nähdään tavoitteellisena (*goal-seeking*)[489] eli se saa informaatioon perustuvaa positiivista tai negatiivista palautetta toiminnastaan suhteessa ympäristöönsä ja kykenee näin muokkaamaan omaa toimintaansa tai ympäristöään tai toista systeemiä entistä tehokkaammin päämääräänsä saavuttamiseksi.[490]

Järjestelmiä voidaan käsitellä alajärjestelmistä muodostuvina kokonaisuuksina.[491] Tällainen järjestelmien järjestelmä (*system of systems*)

---

[485] Checkland (2000).

[486] Kriittisestä systeemiteoriasta ks. Fischer-Lescano, Andreas: Critical Systems Theory. *Philosophy and Social Criticism*, Vol. 38, No. 1 (2012), s. 3–23. Pragmatismista ks. Hellmann (2009); Hamati-Ataya, Inanna: Beyond (Post)Positivism: The Missed Promises of Systemic Pragmatism. *International Studies Quarterly*, Vol. 56 (2012), s. 291–305.

[487] Tämä määritelmä noudattelee de Rosnayn muotoilua (de Rosnay, Joël: *The Macroscope A new world scientific system*. Harper & Row, Publishers, New York, 1975. [http://pespmc1.vub.ac.be/macroscope/], luettu 23.9.2019). Muista määrittelyistä ks. Ackoff (1999), s. 48; Hammond (2003), s. 17; Keating, Charles B., Padilla, Jose J. & Adams, Kevin: System of Systems Engineering Requirements: Challenges and Guidelines. *Engineering Management Journal*, Vol. 20, No. 4 (December 2008), s. 24–31.

[488] Järjestelmien tyypittelystä ks. Ackoff (1999), s. 52, s. 59–61; Boulding, Kenneth: General Systems Theory. The Skeleton of Science. *Management Science*, Vol. 3, No. 2 (1956), s. 197–208. [http://pespmc1.vub.ac.be/books/Boulding.pdf], luettu 15.10.2019; Checkland (1993), s. 111.

[489] Järjestelmiä voi olla esimerkiksi tilansa säilyttäviä (*state-maintaining*), tavoitehakuisia (*goal-seeking*), monitavoitehakuisia ja tarkoituksellisia (*multi-goal-seeking*) sekä tarkoitushakuisia (*purposeful*) (Ackoff (1999), s. 52).

[490] Heylighen, Francis, Joslyn Cliff & Turchin Valentin: What are Cybernetics and Systems Science? *Principia Cybernetica Web (Principia Cybernetica, Brussels), 1999.* [http://pespmc1.vub.ac.be/CYBSWHAT.html], luettu 7.7.2020; Checkland (2000).

[491] Meentemeyer, Scott M., Sauser, Brian & Boardman, John: Analysing a System of Systems Characterisation to Define System of Systems Engineering Practices. *International Journal of System of Systems Engineering*, Vol. 1, No. 3, 2009, s. 329–346.

koostuu useasta alajärjestelmästä, joiden yhteistoiminta mahdollistaa sellaista päämäärien tavoittelun, johon yhden alajärjestelmän suorituskyky ei riitä.[492] Mark Maierin mukaan alajärjestelmillä on omat funktionsa, ne kykenevät operoimaan omillaan, niillä on omat hallintamekanisminsa (*management*) ja ne ovat usein erillään mutta yhteydessä toisiinsa esimerkiksi vaihtamalla informaatiota.[493] Järjestelmien järjestelmiä luonnehtivat John Boardmanin ja Brian Sauserin mukaan autonomia, alajärjestelmien itsenäisyys, moninaiset sisäiset yhteydet, sisäinen moninaisuus ja emergenttiys.[494] Näiden ominaisuuksien perusteella järjestelmien järjestelmiä on esitetty olevan neljää tyyppiä: ohjattu (*directed*), kollaboratiivinen (*collaborative*), tunnustettu (*acknowledged*) ja virtuaalinen (*virtual*), joissa erottavana tekijänä ovat päämäärän (emergentti-tunnistettu), hallinnan (yhteisö-keskitetty) ja osien välisten suhteiden (itsenäinen-alistettu) luonne.[495] Mitä kompleksisempia[496] järjestelmät ja järjestelmien järjestelmät ovat ja mitä tiiviimpiä niiden osien väliset suhteet (*coupling*), sitä todennäköisempää on, että järjestelmät toimivat ennustamattomasti tai tuottavat odottamattomia tuloksia.[497] Etenkin nk. tunnustetut järjestelmät, jossa alajärjestelmät säilyttävät itsenäisyytensä ylemmän johdon ohjauksessa, voivat käyttäytyä resurssien

---

[492] Jamshihi, Mo (ed.): *Systems of Systems Engineering: Principles and Applications*. CRC Press, New York, 2008, s. 3-4; Krygiel, Annette J.: *Behind the Wizard's Curtain: An Integration Environment for a System of Systems*. CCRP Publication Series, 1999, s. 33–34; Keating, Padilla & Adams (2008); Dahmann, Judith S., Rebovich, George Jr. & Lane, Jo Ann: Systems Engineering for Capabilities. *CROSSTALK The Journal of Defense Software Engineering*, November 2008, s. 4–9; The United State Department of Defence (U.S. DoD): *Systems Engineering Guide for Systems of Systems, version 1.0, 2008.* [http://acqnotes.com/wp-content/uploads/2014/09/DoD-Systems-Engineering-Guide-for-Systems-of-Systems-Aug-2008.pdf], luettu 17.10.2019.

[493] Maier, Mark W.: Research Challenges for Systems-of-Systems. *IEEE International Conference on Systems, Man and Cybernetics Waikoloa, HI, USA, October 10-12, 2005,* s. 3149–3154.

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

[495] Assaad, Mohamad Ali, Talj, Reine & Charara, Ali: A view on Systems of Systems (SoS). *20th World Congress of the International Federation of Automatic Control (IFAC WC 2017) - special session, Jul 2016, Toulouse, France*.

[496] Kompleksisuudella viitataan tässä järjestelmien järjestelmän monimutkaisuuteen, monimuotoisuuteen, itseorganisoitumiseen, epälineaarisuuteen ja emergentteihin (ei a priori elementeistä pääteltäviin) ominaisuuksiin, jotka eivät välttämättä ole järjestelmän kontrolloijan täydessä tiedossa ja hallinnassa ja voivat näin johtaa ei toivottuihin tuloksiin tai hallitsemattomiin ja ennalta arvaamattomiin virhetiloihin. (Thurner, Stefan, Hanel, Rudolf & Klimek, Peter: *Introduction to the Theory of Complex Systems*. Oxford, Oxford University Press, 2018; Perrow (1999)).

[497] Perrow (1999).

käytön ja päämäärän saavuttamisen kannalta epäoptimaalisesti.[498] Kompleksisuus ei siis välttämättä ole järjestelmien järjestelmän joustavuuden tai sopeutumiskyvyn kannalta edullinen asia.[499] Myöhemmin käsiteltävä Venäjän informaatioturvallisuuden ja -puolustuksen järjestelmä on eittämättä tyypiltään tunnustettu järjestelmien järjestelmä.

Järjestelmäajattelulla on vahvat yhtymäkohdat sotatieteisiin niin Yhdysvalloissa kuin Venäjällä. Järjestelmäajattelu juurtui yhdysvaltalaiseen sotatieteelliseen ajatteluun jo 1950-luvulla ja vahvisti asemaansa 1990-luvulla.[500] Yhdysvaltalaisessa NCW-ajattelussa sensoreiden, johtamisjärjestelmien ja asejärjestelmien järjestelmien järjestelmän uskottiin lisäävän tilannetietoisuutta uuden teknologian avulla.[501] Systeemiajattelu laajeni 2000-luvulla suorituskykyjen kehittämisen ja rakentamisen hallinnollisiin prosesseihin.[502] Järjestelmäajattelun doktriinitason sovellus *Effects-Based Operations* on kohdannut voimakasta kritiikkiä ja osiltaan hylätty Yhdysvaltojen asevoimissa.[503] Järjestelmäajattelu on johtavien sotateoreetikkojenkin mielestä edelleen alikehitetty ja haastava operationalisoitava.[504]

Venäjällä järjestelmäajattelulla on pitkät juuret kybernetiikassa, jolla oli merkittävä rooli neuvostotieteissä kylmän sodan aikana.[505] Tuolloin mm. talous- ja yhteiskunta pyrittiin hahmottamaan kyberneettisenä

---

[498] Dahmann, Rebovich & Lane (2008).
[499] Henson, S. A., Henshaw, M.J.D., Barot, V., Siemieniuch, C.E., Sinclair, M.A., Dogan, H., Lim, S.L., Ncube, C., Jamshidi, M. & DeLaurentis, D.: Towards a Systems of Systems Engineering EU Strategic Research Agenda. *2013 8th International Conference on System of Systems Engineering, Maui, HI, 2013*, s. 99–104.
[500] Hammond (2003); Owens, William A.: The Emerging System of Systems. *Proceedings*, Vol. 121, No. 5 (1995), s. 36–39.
[501] Cebrowski & Garstka (1998).
[502] Warden, John: The Enemy as a System. *Airpower Journal*, Vol. 9, No. 1 (1995), s. 40–55; Deptula, D.*: Effects Based Operations, Change in the Nature of Warfare*. Aerospace Education Foundation, Arlington, VA, 1996; NATO: *AJP-3.3 Allied Joint Doctrine for Air and Space Operations. Edition B Version 1, April 2016*, 1-1. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/624137/doctrine_nato_air_space_ops_ajp_3_3.pdf], luettu 11.1.2021; U.S. DoD (2008).
[503] Anteroinen, Jukka: The Systems Concepts in Military Operations - Discussion of critique. *Systems Conference (SysCon), 2013 IEEE International*, s. 102–108.
[504] Henson et al. (2013).
[505] Susiluoto (2006); Peters (2016); Vasara (2020).

järjestelmänä.[506] Kylmän sodan jälkeen järjestelmäajattelu on vaikuttanut venäläisessä turvallisuus- ja sotatieteellisessä ajattelussa, vaikka kybernetiikka itsessään hylättiin jo 1980-luvulle tultaessa.[507] Ajattelu vahvistui Venäjän asevoimien omaksuessa yhdysvaltalaiset NCW ja RMA-ajatteluun liittyvät teoriat osana asevoimien reformia 2000-luvulla.[508] Kiinassakin systeemiajattelu toimii sotataidon perustana. Ajattelun juuret ovat todennäköisesti kylmän sodan aikaisen Neuvostoliiton tarjoamassa tiede- ja teknologia-avussa sekä yhdysvaltalaisen sotataidon omaksumisessa 2000-luvulla.[509] Niin Venäjällä kuin Kiinassakin systeemiajattelu heijastuu kansainvälisen politiikan hahmottamisena kilpailevien järjestelmien välisenä vastakkainasetteluna, jossa luokkataistelun on nykyisellään korvannut suurvaltaintresseihin sidottu kamppailu maailmanjärjestyksestä.[510]

Kybernetiikka ja valtioiden kamppailu liittyvät olennaisesti väitöskirjassani tutkimiini Venäjän strategiskulttuurisiin ideoihin.[511] Ne ovat kausaalisia tai periaatteellisia uskomuksia voimankäytöstä ja sillä uhkaamisesta poliittisten päämäärien saavuttamiseksi. Ensimmäinen idea on jatkuva valtioiden tai poliittisten yhteisöjen välinen kamppailu tai -vastakamppailu (*protivoborstvo*). Sen mukaan valtioiden välinen kamppailu vallasta ja selviytymisestä on jatkuvaa ainoastaan keinojen

---

[506] Vidmer, Richard F.: Soviet Studies of Organization and Management: A "Jungle" of Competing Views. *Slavic Review*, Vol. 40, No. 3 (Autumn, 1981), s. 404–422, s. 418; Schwartz, Donald V.: Information and Administration in the Soviet Union: Some Theoretical Considerations. *Canadian Journal of Political Science / Revue canadienne de science politique*, Vol. 7, No. 2 (Jun., 1974), s. 228–247, s. 230; Sanjian, Andrea Stevenson: Constraints on Modernization: The Case of Administrative Theory in the U. S. S. R. *Comparative Politics*, Vol. 18, No. 2 (Jan., 1986), s. 193–210; Vidmer, Richard F.: Management Science in the USSR: The Role of "Americanizers". *International Studies Quarterly,* Vol. 24, No. 3 (Sep., 1980), s. 392–414; White, Ralph K.: Social Science Research in the Soviet Bloc. *The Public Opinion Quarterly*, Vol. 28, No. 1 (Spring, 1964), s. 20–26; Ware, Willis, H. & Holland, Wade B.: *Soviet Cybernetics Technology: I. Soviet Cybernetics 1959-1962*. RAND Corporation, Santa Monica, 1963. Myöhempiä tulkintoja Gerovitch (2002); Susiluoto (2006); Peters (2016); Vasara (2020); Kukkola (2020a).

[507] Vasara (2020); Kukkola (2020a).

[508] Kukkola (2020a).

[509] The United States Department of Defense (U.S. DoD): *Military and Security developments involving the People´s Republic of China, Annual report to congress 2020*. The Office of the Secretary of Defence, 2020, s. 6, s. 83–84; Engström (2018).

[510] Kukkola (2020a); Kallio, Jyrki: *Xi Jinping Thought And China's Future Foreign Policy Multipolarity With Chinese Characteristics*. FIIA Briefing Paper 243, August 2018. FIIA, Helsinki, 2018.

[511] Seuraavat tiivistelmät srategiskulttuurisista ideoista perustuvat Kukkola (2020a).

muuttuessa rauhan ja sodan välillä. Idean nykyinen tulkinta korostaa informaation tärkeyttä globaalin kamppailun muotona ja keinona. Informaatiokamppailu (*informatsionnoe protivoborstvo*) mahdollistaa strategisen ylivoiman hankkimisen jo rauhan aikana. Tämä ajatus on osiltaan ohjannut venäläistä sotatiedettä kehittämään värivallankumousten ja ns. hallitun kaaoksen teorioita. Niiden mukaan valtiot pyrkivät heikentämään toisiaan ensisijaisesti epäsuorilla ja ei-sotilaallisilla keinoilla.

Toinen idea on valtiosuvereniteetti ja etenkin sen alamuoto digitaalinen tai informaatiosuvereniteetti (*tsifrovoj / informatsionnoj suverenitet*). Venäläisessä oikeustieteellisessä ajattelussa valtiosuvereniteetti jaotellaan alueittain (poliittinen, talous jne.) ja informaatiosuvereniteetin idea kehittyi 1990-luvulta alkaen osoittamaan valtion auktoriteettia informaatioon, informaatiojärjestelmiin ja sen käyttäjiin alueellaan. Sen rinnakkaiskäsite digitaalinen suvereniteetti kehittyi määrittelemään niitä järjestelmiä, infrastruktuuria, talousjärjestelyjä ja teknologiaa, jotka toimivat informaatiosuvereniteetin perustana. Tässä yhteydessä on käytetty myös käsitettä teknologinen itsenäisyys.

Kolmas idea on strateginen deterrenssi (*strategitšeskoe sderživanie*). Se on venäläinen tulkinta läntisestä deterrenssiajattelusta ja tarjoaa yhdenlaisen vastauksen jatkuvan kamppailun idean esittämään turvallisuusuhkaan. Pyrkimyksenä on taata strateginen tasapaino ja täten idea on sidoksissa sotilaalliset ja ei-sotilaalliset tekijät huomioiviin voimasuhdelaskelmiin. Idean mukaan valtion turvallisuus voidaan taata sotilaallisilla ja ei-sotilaallisilla keinoilla uhkaamalla ja aiheuttamalla kohteelle vahinkoa. Strategista deterrenssiä toteutetaan kaikissa valtiosuhteiden vaiheissa ja se sisältää myös konfliktin aikaisen eskalaation hallinnan. Deterrenssi ei ole vain julistuksellinen politiikka vaan aktiivista toimintaa voiman kasvattamiseksi ja voimatasapainon muuttamiseksi kaikin valtion käytettävissä olevin keinoin.

Neljäs idea on asymmetrinen vaste (*asimmetritšnyi otvet*).[512] Sillä on juuret venäläisessä sotataidollisessa ajattelussa, joka korostaa oveluutta, luovuutta, harhauttamista ja salaamista. Strategisella tasolla asymmetrinen vaste on kustannustehokas keino vastustajan voiman neutraloimiseksi, omien heikkouksien suojaamiseksi ja voimien kasvattamiseksi. Operatiivisella tasolla asymmetria liittyy asymmetrisiin toimiin eli

[512] Venäläisiä tulkintoja asymmetriasta on käsitelty myös luvussa 2.3.

epätavanomaisiin keinoihin, vastustajan voiman kiertämiseen, olosuhteiden hyväksikäyttöön, maskirovkaan, yllätykseen ja keinojen sekä välineiden uudenlaiseen käyttöön. Sitä voisi kuvata voimasuhdelaskelmien epäsuhtaiseksi muuttujaksi, jonka olemassa olo on riippuvainen subjektista eli komentajasta.

Loput ideat liittyvät kiinteämmin informaatiotoimintaympäristöön. Viides idea on informaatiosodankäynti (*informatsionnaja voina/borba*). Sillä on teknologinen ja psykologinen puolensa. Teknologinen puoli nojaa vahvasti läntiseen NCW-ajatteluun. Se korostaa johtamis- ja järjestelmäsodankäynnin ja -teorioiden merkitystä sekä teknologian tuomia mahdollisuuksia kamppailun välineenä sekä etenkin vastakeinojen etsimistä teknologisesti kehittyneempää vastustajaa vastaan. Psykologinen puoli korostaa ihmismieleen vaikuttamista ja liittyy usein miten strategisen tasan kamppailuun.[513] Kuudes idea on informaatioylivoima (*informatsionnoe prevoshodstvo*). Läntisistä näkemyksistä se poikkeaa lähinnä korostaessaan informaation strategisia vaikutuksia sekä jakautuessan selkeästi teknologiseen ja psykologiseen puoleen informaatiosodankäynnin idean ohjaamana. Psykologisen ylivoiman merkitystä vahvistaa tulkintaa siitä, että Länsi tuhosi Neuvostoliiton nimenomaan psykologisen sodankäynnin keinoin. Informaatioylivoima ei siis tarkoita pelkästään informaation käsittelyn nopeutta tai laatua vaan kykyä manipuloida vastustajaa. Ylivoima voi siis tarkoittaa kykyä hallita ihmismieliä määrätyssä ajassa ja paikassa.

Seitsemäs idea ovat automatisoidut johtamisjärjestelmät (*avtomatizirovannaja sistema upravlenija*). Idean juuret ovat neuvostoliitossa ja järjestelmätieteissä. Idea ei määrittele pelkästään tietokoneita tai tietoverkkoja vaan niiden käytön periaatteita. Se kuvaa tavan, jolla monimutkaisia järjestelmiä rakennetaan ja informaatiota hallitaan. Idea korostaa kontrolloivan subjektin suhdetta objektiin ja palautekanavien merkitystä. Idean sisältämä ajatus hierarkiasta, toimintojen erottamisesta ja kontrollin keskittämisestä on vaikuttanut venäläiseen ajatteluun informaatioyhteiskunnasta.

Kahdeksas idea on yhtenäisen informaatiotilan käsite (*edinoe informatsionnoe prostranstvo*). Se koskee kansallista, yhtenäistä informaatiotilaa, jota kontrolloidaan hallinta- ja ohjausjärjestelmien

[513] Informaatiosodankäynnin psykologinen puoli liittyy refleksiivisen kontrollin teoriaan, jota ovat tarkastelleet etenkin Thomas (2019) ja Vasara (2020).

järjestelmällä. Informaatiotila pitää sisällään informaatioteknisen infrastruktuurin, joka läntisessä kielenkäytössä ymmärretään kybertilana. Tila perustuu vertikaaliin hallintaan ja horisontaaliin integraatioon, keskittämiseen, rajojen määrittelyyn kybertilassa ja tieteellisteknologiseen omavaraisuuteen. Tilan rakentamisen systeemiteoreettinen rationaliteetti perustuu informaatioylivoiman hankkimiseen kontrolloimalla informaation kulkua, informaatiota itseään ja informaatiota käsitteleviä järjestelmiä.

Useat venäläiset siviili- ja sotilastutkijat jäsentävät informaatiotilan järjestelmänä, informaatiosodankäynnin järjestelmien välisenä kamppailuna ja tuon kamppailun hallinnan kansallisen johtamis- ja hallintajärjestelmän tehtävänä.[514] Tähän liittyen useat heistä ovat esittäneet ajatuksen valtion informaatioturvallisuusjärjestelmästä, jonka on tarkoitus ehkäistä niin psykologisia kuin teknologisia yhteiskuntaan ja valtioon kohdistuvia uhkia. Tällainen järjestelmä koostuisi useasta alajärjestelmästä ja olisi luonteeltaan poikkihallinnollinnollinen ja keskitetysti johdettu.

Tässä työssä järjestelmien järjestelmän käsitettä sovelletaan Venäjän kansallisen internetsegmentin tarkasteluun, koska se ensinnäkin resonoi edellä esitettyjen venäläisen strategisen kulttuurin ideoiden kanssa ja toiseksi tarjoaa mahdollisuuden jäsentää monimuotoinen sotilaallinen, poliittinen, taloudellinen ja kulttuurinen eri toimintojen kokonaisuus funktionaalisella ja loogisella tavalla. Koska järjestelmäteorialla on vahva vaikutus läntisissäkin sotilastieteissä kansallisen segmentin tarkastelu kyetään sitomaan laajempaan sotatieteelliseen teoreettiseen keskusteluun yhteisen käsite- ja teoriapohjan kautta.[515] ”Holistisista” ja ”systeemisistä”

---

[514] Näitä ovat mm. E. A. Derbin, S. A. Komov, E. G. Šalamberidze, D. Tšereškin, G. Smoljan, V. Tsygitško, A. A. Sidak, Ju. G. Botškareva, V.K. Novikov, S. I. Makarenko, H. I. Saijfetdinov, V. Kruglov, V. V. Tsyganov, S. N. Buharin, A. V. Manoilo, ja I.Panarin. Heidän kirjoituksiaan on analysoitu tarkemmin Kukkola (2020a).

[515] Bousquet, Antoine: Cyberneticizing the American War Machine: Science and Computers in the Cold War. *Cold War History*, Vol. 8, No. 1 (February 2008), s. 77–102; Lawson, Sean: Cold War Military Systems Science and the Emergence of a Nonlinear View of War in the US military. *Cold War History*, Vol. 11, No. 3 (August 2011), s. 421–440; The United States Department of Defense (U.S. DoD), Chairman of the Joint Chiefs of Staff: *Concept for Future Operations. Expanding Joint Vision 2010, 1996.* [http://web.archive.org/web/20040225022332/http://www.dtic.mil/jointvision/history/cfjoprn1.pdf], luettu 8.5.2020; Alberts & Papp (1997); Alberts, David S., Garstka, John J., Hayes, Richard E. & Signori, David A.: *Understanding Information Age Warfare*. CCRP. Washington, DC., 2001; Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering: *Systems Engineering Guide for*

turvallisuusratkaisuista on itse asiassa tullut Lännessä uusi kyberturvallisuuden suuntaus.[516] Näin ollen tässä työssä yhdistetään venäläisten informaatioturvallisuustutkijoiden esittämä ajatus valtion informaatioturvallisuusjärjestelmästä läntisen systeemiajattelun periaatteisiin kansallisen segmentin hahmottamiseksi järjestelmien järjestelmänä.

Kansallisella informaatioturvallisuuden ja -puolustuksen järjestelmällä tarkoitetaan informaatioturvallisuutta tuottavaa järjestelmien järjestelmää. Informaatioturvallisuus ymmärretään tässä yhteydessä venäläisittäin ja valtiokeskeisittäin eli valtion suojaksi ulkoisilta ja sisäisiltä informaatiouhilta, mikä turvaa valtion suvereniteetin, alueellisen eheyden, taloudellisen kehityksen, puolustuksen ja turvallisuuden.[517] Se koostuu funktionaalisista alajärjestelmistä, jotka tuottavat, muokkaavat, ohjaavat ja kontrolloivat informaatiota, eli kontekstin ja merkityksen saanutta dataa, siihen liittyviä rakenteita, prosesseja ja käyttäjiä valtiossa.[518] Informaatioturvallisuuden ja -puolustuksen järjestelmä toimii itsessään kontrollimekanismina tuottaen sisäistä ja ulkoista turvallisuutta. Sisäinen turvallisuus viittaa valtion sisäiseen järjestykseen ja ulkoinen turvallisuus puolustukseen.[519] Järjestelmien järjestelmän sisällä on itsessään kontrollista[520] ja palautteen (*feedback*) yhdistämisestä ja

---

Systems of Systems, Version 1.0. ODUSD(A&T)SSE, Washington, DC, 2008; NATO (2013).

[516] Libicki (2016); Clarke & Knake (2019), s. 83; Lewis (2018); Limnéll, Jarno: *Holistic Approach is Necessary to Solve Security Issues of This Decade*. Cyberwarch Finland, 1/2021, s. 14–15.

[517] Määritelmä perustuu Venäjän federation voimassa olevaan informaatioturvallisuusdoktriiniin. (Указ-646 (2016)). Turvallisuuden käsitteestä yleisesti ks. Smith, Steve: The increasing insecurity of security studies: Conceptualizing security in the last twenty years. *Contemporary Security Policy*, Vol. 20, No. 3 (1999), s. 72–101; Miller (2001); Williams, Paul D. (ed.): *Security Studies: an Introduction*. Routledge, London, 2008; Buzan, Barry: *People, States and Fear. An agenda for international security studies in the post-cold war era*. ECPR Press, Colchester, 2007. Suomalaisesta turvallisuuskäsitteen merkityksestä ks. Sanastokeskus TSK (2017), s. 16; Sanastokeskus TSK (2018).

[518] Informaation määritelmästä ks. Rowley (2007); Chaim (2007).

[519] Sisäisestä ja ulkoisesta turvallisuudesta ks. Eriksson, Johan & Rhinard, Mark: The Internal–External Security Nexus: Notes on an Emerging Research Agenda. *Cooperation and Conflict*, Special Issue On The Internal-External Nexus, Vol. 44, No. 3 (September 2009), s. 243–267.

[520] Kontrollin käsitteestä ks. Åström Karl J. & Kumar, P.R.: Control: A perspective. *Automatica*, Vol. 50 (2014), s. 3–43; Giddens, Anthony: *The Nation State and Violence: Volume Two of A Contemporary Critique of Historical Materialism*. Polity, Cambridge, 1985, s. 11. Ackoff kontrollista ks. Ackoff (1999), s. 61.

käsittelystä vastaava alajärjestelmä (kahdeksas alajärjestelmä ks. Luku 3.4). Järjestelmä toimii ulko- ja turvallisuuspoliittisten päätöksentekijöiden tavoitteiden mukaisesti. Lähtökohtaisesti järjestelmä ymmärretään valtioeliitin vallankäytön välineenä – näin etenkin autoritaaristen valtioiden tapauksessa.[521] Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä on siis kiinnittynyt valtion ja yhteiskunnan sosiaalisiin, poliittisiin ja taloudellisiin ominaispiirteisiin. Näiden muuttuessa järjestelmäkin muuttuu. Tässä työssä kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä saa sisältönsä Venäjän kansallisen internetsegmentin hankkeen tavoitetilasta ja Venäjä valtion ominaispiirteistä. (Luku 3.2 ja 3.3)

Yksikään informaatioturvallisuuden ja -puolustuksen järjestelmän alajärjestelmä ei itsessään ole riittävä tuottamaan valtion informaatioturvallisuutta. Informaatiouhkien luonne ja sisältö ovat jatkuvan poliittisen kamppailun kohteena.[522] Venäläisittäin ne voidaan karkeasti jakaa informaatioteknologisiin ja -psykologisiin.[523] Tässä työssä päähuomio kiinnitetään edellisiin, joihin kuuluvat tietoverkko- ja järjestelmähyökkäykset eli kybersodankäynti ja -operaatiot.[524] Koska informaatiotila, sen elementit, toiminnot, prosessit ja toimijat muuttuvat jatkuvasti teknologisen ja yhteiskunnallisen kehityksen johdosta, täytyy informaatioturvallisuuden järjestelmän olla adaptiivinen ja kompleksinen.[525] Informaatioturvallisuuden ja -puolustuksen järjestelmä on siis rakenteensa johdosta jatkuvasti kehittyvä, monimuotoinen kokonaisuus, joka on vuorovaikutuksessa ympäristönsä kanssa.[526] Vain

---

[521] Eliitti on joukko ihmisiä, jotka tekevät päätöksiä voimankäytöstä ja vastaamisesta havaittuihin uhkiin valtiossa (Kukkola 2020).

[522] Kavanagh, Camino: *The United Nations, Cyberspace and International Peace and Security – Responding to Complexity in the 21st Century. UNIDIR, 2017.* [https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf], luettu 17.10.2019; Tikk & Kerttunen (2018).

[523] Thomas (2005).

[524] Kukkola (2020a).

[525] Ihmisjärjestelmien adaptiivisuudesta ja kompleksisuudesta ks. Waldrop, Mitchell M.: *The Emerging Science at the Edge of Order and Chaos*. Touchstone, New York, 1992, s. 11–12.

[526] Anderson et al. ovat esimerkiksi esittäneet adaptiivisen kompleksisen järjestelmän pääpiirteiksi toimijoita (*agents*), epälineaarisia eri tasojen välisiä keskinäisriippuvuuksia (*interconnections*), itseorganisoitumista (*self-organization*), emergenssiä (*emergence*) ja järjestelmän ja ympäristön yhteisevoluutiota (*coevolution*) (Anderson, Ruth A., Crabtree, Benjamin F., Steele, David J. & McDaniel, Reuben R, Jr.: Case Study Research: The View

äärimmäisessä muodossaan se kattaa yhteiskunnan koko informaatiotilan. Yleensä sen ulkopuolelle jää vapaa tai vähemmän säädelty tila. Järjestelmästä voidaan esittää vain yleisille periaatteille rakennettu tuokiokuva. Se on teoreettinen rakennelma, epätäydellinen malli, kuvaus ja tulkinta ilmiöistä. Nämä ilmiöt ovat ihmisten rakentamia normatiivisia ja teknologisia ainutkertaisia ”mekanismeja” ajassa, eivät ihmisyhteisöjen yleisiä ominaisuuksia.[527]

3.2 Venäjän valtion ominaispiirteet

Tässä työssä käsiteltävä suljettu kansallinen verkko ja sen tosimaailman ilmentymä Venäjän kansallinen internetsegmentti saa muotonsa ja sisältönsä informaatioturvallisuuden ja -puolustuksen järjestelmän mallin ja Venäjä valtion ominaispiirteiden kautta. Alla esitellään aikaisempaan tutkimukseen perustuen Venäjän valtion olennaisimmat ominaispiirteet. Nämä ominaispiirteet vaikuttavat informaatioturvallisuuden ja -puolustuksen järjestelmä alajärjestelmien kuvauksiin ja analyysiin luvussa neljä.

Venäjän ulko- ja turvallisuuspoliittista käytöstä on selitetty kansainvälisen politiikan tutkimuksen realismin teorian edellyttämällä suurvaltakäytöksellä, strategisella kulttuurilla (suurvaltastatuksen kaipuu, geopoliittinen ajattelu, piiritetyn linnakkeen mentaliteetti, imperialismi, messianismi, kärsimysvalmius), eliitin näkemyksillä tai turvallisuusorganisaatioiden intresseillä, sisäisellä poliittisella järjestelmällä (*sistema*)[528], hallitsevilla diskursseilla ja presidentti Vladimir Putinin persoonallisuudella.[529] Ulko- ja turvallisuuspolitiikan taustavaikuttimien osalta vallitsee tutkijoiden piirissä siis erimielisyys.

From Complexity Science. *Qualitative Health Research*, Vol. 15, No. 5 (May 2005), s. 669–685, s. 673).

[527] Mancilla (2011); Forrester, Jay W.: *Industrial Dynamics*. Productivity Press, Cambridge, MA, 1961, s. 49–54.

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

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

Käytöksen osalta ollaan melko yksimielisiä siitä, että Venäjä on viimeistään presidentti Putinin toisesta kaudesta (2004–2008) lähtien pyrkinyt aktiivisesti palauttamaan suurvalta-asemansa, luomaan maantieteelliselle lähialueelleen taloudellisen, poliittisen ja sotilaallisen liittolaisjärjestelmän ja suojellut monimuotoisin keinoin, mukaan lukien voimakeinoin, intressejään lähialueillaan. Vuoden 2013 jälkeen Venäjän ja Lännen suhde heikkeni Ukrainan sodan takia ja Venäjä on kiinnittänyt entistä suurempaa huomiota kansallisen turvallisuutensa takaamiseen. Venäjän aikaisempi pyrkimys luoda Lännelle vastakkaisia tai rinnakkaisia liittokuntia on yhä enemmän keskittynyt strategiseen kumppanuuteen Kiinan kanssa ja hyvien suhteiden vaalimiseen Lähi-idän ja Pohjois-Afrikan valtioihin.[530] Toisaalta Venäjä on pyrkinyt horjuttamaan ja heikentämään vastustajikseen kokemia Yhdysvaltoja, Natoa ja EU:ta mm. kyberavusteisilla informaatio-operaatioilla. Se on kiistänyt omien kybersuorituskykyjensä olemassaolon ja käyttänyt laajaa joukkoa viranomais- ja sijaistoimijoita operaatioiden toimeenpanoon[531]. Kybersuorituskyvyt ovat osa Venäjän strategista deterrenssiä ja konfliktin aikaista eskalaation hallintaa.[532]

Venäjän ulko- ja turvallisuuspoliittinen päätöksenteko on henkilöitynyt presidentti Vladimir Putiniin. Venäjä on autokraattinen presidentinvaltaisesti hallittu maa, jossa on muodollinen parlamentaarinen demokratia.[533] Venäjällä on vahva ”laillisuuden” (*zakonnost’*) periaate, mutta laki on usein miten ollut valtiojohdon vallankäytön väline ja Venäjän

---

[530] Ibid.

[531] Lilly & Cheravitch (2020); Maurer (2018).

[532] Kukkola 2020; Adamsky, Dmitry: Deterrence à la Ruse: Its Uniqueness, Sources and Implications. Teoksessa *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice*. Osinga, Frans & Sweijs, Tim (Eds.) Springer, Berlin, 2020, s. 161–175; Bruusgard, Kristin Ven: *Russian Concept of Deterrence*. Russia Seminar 2021, 26.2.2021, National Defence University, Helsinki [https://www.youtube.com/watch?v=PURKPOeskBk&t=33s], luettu 21.2.2021.

[533] Sakwa, Richard: Dualism at Home and abroad: Russian Foreign Policy Neo-Revisionism and Bicontinentalism. Teoksessa *Russia’s Foreing Policy. Ideas, Domestic Politics and External Relations*. Teoksessa Cadier, David & Light, Margot (Eds.) Palgrave Macmillan, Basingstoke, 2015, s. 65–79; Treisman (2018); Pomerantsev, Peter & Weiss, Michael: *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Institute of Modern Russia, Inc., New York, 2014; Oliker (2017); Tóth, Gábor Attila: Authoritarianism. *Oxford Constitutional Law*, February 2017. [https://oxcon.ouplaw.com/view/10.1093/law-mpeccol/law-mpeccol-e205], luettu 12.1.2021.

oikeuslaitos on poliittisen johdon hallinnassa.[534] Omistusoikeuksien turva rikollisuutta ja valtion mielivaltaa vastaan on heikko.[535] Putinin ympärillä on joukko hänestä riippuvaisia institutionaalisen tai taloudellisen aseman omaavia vaikutusvaltaisia henkilöitä.[536] Presidentinhallinnon ja ministeriöiden valta-asetelmat ovat vaihdelleet ajan kuluessa niitä johtaneiden henkilöiden poliittisista taidoista riippuen.[537] Käytännössä maan kaksikamarisen parlamentin ylä- ja alahuoneet ovat yhden puolueen (Yhtenäinen Venäjä) edustajien tai presidentistä riippuvaisten henkilöiden hallinnassa. Parlamenttivaalit ovat viimeistään vuodesta 2011 lähtien olleet epävapaat.[538] Venäjän poliittinen järjestelmä ei ole kuitenkaan totalitaarinen. Valtionjohto pyrkii ottamaan huomioon kansalaisten tarpeet säilyttääkseen kannatuksensa.[539] Valtion sosiaalimenot ja epäsuorat tulonsiirrot valtioyritysten kautta kansalaisille ovat valtiovaltaa legitimoiva

---

[534] Pomeranz, William E.: *Law and the Russian State: Russia's Legal Evolution from Peter the Great to Vladimir Putin*. Bloomsbury, London & New York, 2019, s. 148–149, s. 164–165.

[535] Sakwa, Richard: *The Putin Paradox*. I. B. Taurus, London, 2020, s. 97–98; Galeotti, Mark: *The Vory: Russia's Super Mafia*. Yale University Press, New Haven and London, 2018, s. 258; Becker, Uwe & Vasileva, Alexandra: Russia's Political Economy Re-conceptualized: A Changing Hybrid of Liberalism, Statism and Patrimonialism. *Journal of Eurasian Studies*, Vol. 8, No. 1 (January 2017), s. 83–96.

[536] Konyshev, Valery & Sergunin, Alexander: Military. Teoksessa *Routledge Handbook of Russian Foreign Policy*. Tsyganov, Andrei P. (ed.) Routledge, London and New York, 2018, s. 168–181; Vendil, Carolina: The Russian Security Council. *European Security*, Vol.10, No.2 (Summer 2001), s. 67–94; Mankoff, Jeffrey: *Russian Foreign Policy: The Return of Great Power Politics* (2nd ed.) Rowman & Littlefield Publishers, Inc., Lanham, 2012, s. 55–56; Gvosdev, Nikolas K. & Marsh, Christopher: *Russian Foreign Policy: Interests, Vectors, and Sectors*. SAGE Publications, Inc., Los Angeles, 2014, s. 35–36; Bacon, Edwin: Security Council and decision-making. Teoksessa *Routledge Handbook of Russian Security*. Kanet, Roger E. (ed.) Routledge, London and New York, 2019, s. 119–130; Herspring, Dale R.: *The Kremlin and the High Command: Presidential Impact on the Russian Military from Gorbachev to Putin*. University Press of Kansas, Lawrence, KS, 2006.

[537] Konyshev, Valery & Sergunin, Alexander: Military. Teoksessa *Routledge Handbook of Russian Foreign Policy*. Tsyganov, Andrei P. (ed.) Routledge, London and New York, 2018, s. 168–181. Ks. myös Herspring (2005); Vendil (2001); Mankoff (2012), s. 55–56; Gvosdev & Marsh (2014), s. 35–36; Bacon (2019).

[538] Vaaleista ks. Noble, Ben & Schulmann, Ekaterina: Not Just a Rubber Stamp. Parliament and Lawmaking. Teoksessa *The New Autocracy: Information, Politics, and Policy in Putin's Russia.* Treisman, Daniel (ed.) Brookings Institution Press, Washington, D.C., 2018, s. 47–78; Sakwa (2020), s. 87–89.

[539] Oliker (2017); Robinson, Neil & Milne, Sarah: Populism and political development in hybrid regimes: Russia and the development of official populism. *International Political Science Review*, Vol. 38, No. 4, s. 412–425.

tekijä.[540] Monien tutkijoiden mukaan hallinnon jatkuvuus ja valtiojohdon kannatuksen säilyttäminen ovat Venäjän johdon primaarinen turvallisuusintressi.[541]

Virallisesti Venäjän valtio perustuu instituutioihin, mutta niiden sisällä ja rinnalla verkostot, henkilökohtaiset suhteet, epävirallinen valta, neuvottelu ja kaupankäynti määrittelevät valta-asetelmat ja resurssien hallinnan. Arkipäiväinen vallankäyttö on usein epävirallista ja tapahtuu virallisten menettelyjen ulkopuolella.[542] Valtion ominaispiirteet ovat muuttuneet ajan kuluessa. Esimerkiksi turvallisuuspalveluiden katsottiin nousseen Venäjän johtoon Putinin ensimmäisellä kahdella kaudella. Sittemmin turvallisuuspalveluiden rooliksi näyttää vakiintuneet valvojan, tiedon hankkijan ja tiedon välittäjän rooli.[543] Toisaalta Venäjän yhteiskunnan militarisoituminen on kiihtynyt vuoden 2014 jälkeen.[544] Valtiojohto on myös voimistanut vuoden 2007 tienoilla aloitettuja pyrkimyksiä vahvistaa kansan yhtenäisyyttä ja suhdetta valtioon patrioottisen kasvatuksen ja historian tulkintojen hallinnan avulla. Hallinnon autoritaarisuuden oikeutus, patriotismi ja militarismi liittyvät yhä voimakkaammin toisiinsa.[545] Kansallisten ja kansainvälisten kansalaisjärjestöjen toimintaa on rajoitettu, ulkomaisten medioiden toimintaa vaikeutettu tai ulkomaisia mediaomistuksia hankaloitettu. Televisiokanavat ovat valtion hallinnassa

---

[540] Solanko, Laura*: From reforms to stagnation – 20 years of economic policies in Putin's Russia*. BOFIT Policy Brief 2020 No. 1. [https://helda.helsinki.fi/bof/bitstream/handle/123456789/16548/bpb0120.pdf?sequence=1&isAllowed=y], luettu 31.1.2021; Sokhey, Sarah Wilson: What Does Putin Promise Russians? Russia's Authoritarian Social Policy. *Orbis*, Vol. 64, No. 3 (2020), s. 390–402.
[541] Person, Robert: Balance of Threat: The Domestic Insecurity of Vladimir Putin. *Journal of Eurasian Studies,* Vol. 8, No. 1 (January 2017), s. 44–59; Lo (2015), s. 37; Cadier & Light (2015), s. 8–9; Treisman (2018); Donaldson & Nadkarni (2019), s. 429; Ministry of Defence: *Russia of Power*. Punamusta, Helsinki, 2019, s. 17.
[542] Ledeneva (2013).
[543] Marten, Kimberly: The 'KGB State' and Russian Political and Foreign Policy Culture. *Journal of Slavic Military Studies*, Vol. 30, No. 2 (2017), s. 131–151; Soldatov, Andrei: From the "New Nobility" to the KGB. *Russian Politics and Law*, Vol. 55, No. 2 (2017), s. 133–146; Soldatov, Andrei & Rochlitz, Michael: The Siloviki in Russian Politics. Teoksessa *The New Autocracy: Information, Politics, and Policy in Putin's Russia*. Treisman, Daniel (ed.) Brookings Institution Press, Washington, D.C., 2018, s. 79–103.
[544] Golts, Aleksandr: *Military Reform and Militarism in Russia*. The Jamestown Foundation, Washington, D.C., 2019.
[545] Pynnöniemi, K. (ed.): *Nexus of Patriotism and Militarism in Russia: A Quest for Internal Cohesion*. Helsinki University Press, Helsinki, 2021.

samoin kuin yhä suuremmassa määrin merkittävimmät uutisia tuottavat mediayhtiöt.[546]

Valtiolla on merkittävä rooli taloudessa energiatulojen jakamisen ja valtion omistamien suuryritysten kautta. Boris Porfiriev ja Greg Simons ovat tiivistäneet Venäjän poliittisen ja taloudellisen järjestelmän ominaispiirteiksi suurvaltakompleksin, disinformaation käytön, salailun ja epäluottamuksen, kokeilullisen ja *ad hoc* suhtautumisen kriiseihin, sekä patron-klientti nomenklatuuran. Jälkimmäinen piirre johtaa hallinnolliseen siiloutumiseen, investointien puutteeseen ja hallinnon suoraan johtamiin strategisiin hankkeisiin, läpinäkymättömyyteen, vastuun puutteeseen, ja taipumukseen "tempauksenomaisiin" kampanjoihin ja projekteihin harkitun kehittämisen sijaan.[547]

Edellä mainituista ominaispiirteistä, laajalle levinneestä harmaasta ja pimeästä taloudesta ja Venäjän valtion aktiivisesta finanssi- ja omistajapolitiikasta johtuen korruptio on Venäjän yhteiskunnan systemaattinen piirre.[548] Korruption vaikutuksia vahvistaa hallinnonalojen kilpailu resursseista ja vallasta. Kyber- ja informaatiotilan osalta erityiseksi ongelmaksi nousee lukuisten erilaisten toimijoiden osallistuminen kansallisen internetsegmentin määrittelyyn ja rakentamiseen. Esimerkiksi Venäjän liittovaltion turvallisuuspalvelu (FSB) ja Digitaalisen talouden ja kehityksen ministeriö ovat kamppailleet kansallisen Internetin hallinnasta.[549] Samaan aikaan yksityiset toimijat pyrkivät hidastamaan tai vesittämään hallinnon toimet, koska kansallisen internetsegmentin rakentaminen nostaa niiden kustannuksia.[550] Yleisesti ottaen yksityiset ja julkiset toimijat kilpailevat käytännössä läpinäkymättömällä tavalla valtion jakamista varoista. Kaikki tämä johtaa välistä vetämiseen tai kuppaamiseen (*rent-seeking*), korruptioon ja tehokkuutta alentavaan instituutioiden väliseen kilpailuun. Venäjä on yksi maailman korruptoituneimmista

---

[546] Freedom House: *Nations in Transit 2020: Russia*. [https://freedomhouse.org/country/russia/freedom-world/2020], luettu 19.2.2021.
[547] Porfiriev, Boris & Simons, Greg (Eds.): *Crisis in Russia: Contemporary Management Policy and Practice From a Historical Perspective. Routledge*, New York, 2016 (org. 2012).
[548] Ministry of Defence (2019), s. 111; Sakwa (2020), s. 46; Luhn, Alec & Harding, Luke: Putin dismisses Panama Papers as an attempt to destabilise Russia. *Guardian*, April 7th, 2016. [https://www.theguardian.com/news/2016/apr/07/putin-dismisses-panama-papers-as-an-attempt-to-destabilise-russia], luettu 1.5.2019.
[549] Kukkola (2020a).
[550] Kukkola (2020a).

valtioista.[551] Julkisen ja yksityisen sektorin kanssakäymistä haittaa lisäksi salaamisen kulttuuri.[552] Tänä päivänä se näkyy alati laajenevan salaiseksi luokiteltavan tiedon määrässä.[553] Edellä esitetty tiivistäen, *yhä kiristyvä autoritaarinen hallintotapa, vallan keskittäminen, valtion vahva asema taloudessa, turvallisuuskoneiston vaikutusvalta, julkishallinnon organisaatioiden keskinäinen kilpailu ja siiloutuminen, epävirallliset verkostot, korruptio ja valtiojohtoinen militarismi ja nationalismi ovat Venäjän valtion ominaispiirteitä*. Näiden vaikutukseen Venäjän kansalliseen internetsegmenttiin palataan luvussa 4.2.

3.3 Kansallisen internetsegmentin käsitteet ja tausta

Venäjän kansallisen segmentin ymmärtämiseksi on ensin määriteltävä siihen liittyvät keskeiset käsitteet.[554] Näitä ovat suljettu kansallinen verkko, venäläinen Internet (RuNet), kansallinen internetsegmentti, yhtenäinen informaatiotila ja informaatioturvallisuuden ja -puolustuksen järjestelmä sekä informaatio-/digitaalinen suvereniteetti. Suljettu kansallinen verkko on teoreettinen käsite, joka kuvaa globaalista Internetistä irrotettua sisäisesti toimivaa tietoverkkoa. Sen vastakohtana on avoin kansallinen verkko, joka ei ole valtion suoraan kontrolloima, eikä sitä voida lähtökohtaisesti kytkeä irti globaalista kybertilasta ilman erityisiä valmisteluja tai yhteiskunnan kriittisen toimintojen ja talouselämän vakavia häiriöitä. Kansallinen internetsegmentti on suljetun kansallisen verkon venäläinen käytännön ilmenemismuoto. Se koostuu valtion alueella sijaitsevasta ja sen suvereenin määräämisvallan alla olevasta Internetin infrastruktuurista ja palveluista sekä muista tietoverkoista- ja järjestelmistä. Se määrittelee valtion rajat kybertilassa. Yhtenäinen informaatiotila on strategiskulttuurinen idea, joka ohjaa kansallisen internetsegmentin toteuttamista Venäjällä. Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä on

---

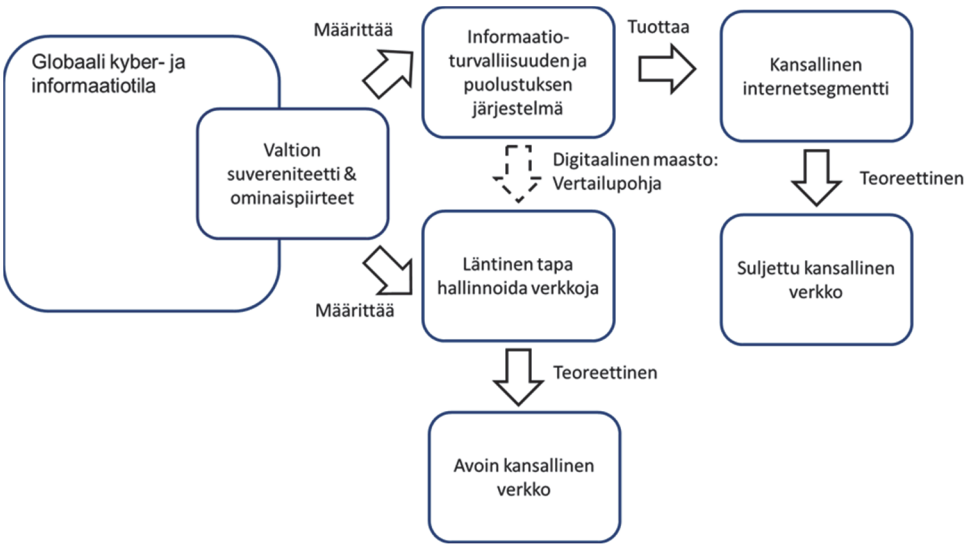
[551] GAN: *Russia Corruption Report*, June 2020. [https://www.ganintegrity.com/portal/country-profiles/russia/], luettu 29.1.2021.

[552] Mikoyan, Sergo A.: Eroding the Soviet "Culture of Secrecy". *Studies in Intelligence*, Vol. 45, No. 5 (2001) [https://www.cia.gov/static/b8834854dbda7fb29d04ee27e368b3e7/Eroding-the-Soviet-Culture.pdf], luettu 29.1.2021.

[553] ФЗ-5485-1: Федеральный закон от 21.07.1993 N 5485-1 "*О государственной тайне*" [http://www.consultant.ru/document/cons_doc_LAW_2481/], luettu 29.1.2021.

[554] Osia luvuista 3.3–3.5 ja 4 on julkaistu aikaisemmin: Kukkola, Juha: The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry. Teoksessa *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Ertan, A., Floyd, K., Pernik, P. & Stevens, T. (Eds.) CCD COE, Tallinn, 2020, s. 9–30.

informaatioturvallisuutta tuottavaa järjestelmien järjestelmä. Se on yhtenäinen kokoelma valtiojohdon välineitä ja keinoja kansallisen internetsegmentin rajaamiseksi, rakentamiseksi ja turvaamiseksi kybertilassa. Se suojelee valtiota ulkoisilta ja sisäisiltä kyber- ja informaatiouhilta, turvaa osaltaan sen suvereniteetin ja toimii sen voimanlähteenä. Informaatioturvallisuuden ja -puolustuksen järjestelmä on tässä työssä sovellettu tapa kuvata tai ”kartoittaa” inhimillisen toiminnan jälki digitaalisessa maastossa. Se on johdettu Venäjän kansallisen internetsegmentin hankkeen tavoitetilasta. Digitaalinen suvereniteetti[555] on valtion maantieteeseen sidotun auktoriteetin ja hallinnan jatkumo kybertilassa. Informaatiosuvereniteetti on laajempi käsite, joka sisältää kybertilan järjestelmissä sijaitsevan tai läpikulkevan informaation ja sen käyttäjien vuorovaikutuksen. Yleisesti käytetty RuNet viittaa sosiaaliseen ja kulttuuriseen online-ympäristöön, joka perustuu venäjänkielelle, palveluille ja sosiaalisille suhteille. Se on syntynyt 1990- ja 2000-luvuilla ilman Venäjän valtion vaikutusta.[556] Käsitteiden suhteet on esitetty kuvassa 9.



Kuva 9: Kansallisen kybertilan ja – toimintaympäristön keskeiset käsitteet

[555] Määritelmä alun perin Kukkola & Ristolainen (2018).

[556] Alkuperäisestä ajatuksesta ks. Ristolainen (2017). RuNetin luonteesta ks. myös Asmolov G. & Kolozaridi P.: Run Runet Runaway: The Transformation of the Russian Internet as a Cultural-Historical Object. Teoksessa *The Palgrave Handbook of Digital Russia Studies*. Gritsenko D., Wijermars M., Kopotev M. (eds.) Palgrave Macmillan, Cham, 2021, s. 227–296.

Tässä työssä ei tilanpuutteen vuoksi tarkastella syvällisesti Venäjän Internetin historiallista kehitystä vaan keskitytään Venäjän Internetin ja laajemman kybertoimintaympäristön nykytilan valottamiseen. Olen kuvannut kansallisen verkon kehitystä seikkaperäisesti väitöskirjassani.[557] Lyhyesti todettakoon, että Venäjän kansallisen tietoverkon ja valtion suhde on kehittynyt viidessä vaiheessa. Ensimmäisessä vaiheessa 1990-luvun alusta alkaen verkko kehittyi pitkälti yksityisyritysten ja tiedeinstituuttien rakentamana. Valtio suhtautui verkon kehittymiseen välinpitämättömästi tai jopa myönteisesti. Toisessa vaiheessa vuosituhannen taitteessa informaatiovallankumous saavutti todenteolla Venäjän ja Internet kehittyi nopeasti. Samalla valtiovalta tuli tietoiseksi informaatiotilan psykologisista ja teknologisista uhista. Venäjällä julkaistiin mm. vuonna 2000 ensimmäinen informaatioturvallisuusdoktriini ja suvereniteetin ajatus alkoi määritellä Venäjän suhtautumista globaaliin kybertoimintaympäristöön. Neuvostoaikaiset tiedustelujärjestelmät ulotettiin verkkoliikenteen puolelle, mutta sääntely säilyi minimaalisena. Kolmannessa vaiheessa, 2000-luvun ensimmäisellä vuosikymmenellä, valtiovalta pyrki valtiontalouden vahvistamiseksi tukemaan informaatioyhteiskunnan kehitystä. Sääntely koski lähinnä tekijänoikeuksiin liittyvän verkkorikollisuuden rajoittamista. Samaan aikaan ymmärrys kriittisen informaatioinfrastruktuurin merkityksestä alkoi kasvaa ja ajatus informaatiosuvereniteetista vahvistui. Neljännessä vaiheessa, vuosina 2011–2013, Venäjän poliittinen johto tuli Arabikevään ja Venäjän omien mielenosoitusten johdosta akuutin tietoiseksi Internetin kasvaneesta merkityksestä kansalliselle vakaudelle. Valtio alkoi aktiivisesti säännellä Internetin käyttöä ja sisältöä ja yksityisiä yrityksiä alettiin painostaa yhteistyöhön valtiovallan ja turvallisuuspalveluiden kanssa. Huomattakoon, että turvallisuuspalvelut olivat olleet erittäin tietoisia Internetin uhkatekijöistä jo 1990-luvun loppupuoliskolta asti. Kriittisestä informaatioinfrastruktuurista tuli keskeinen valtioturvallisuuden käsite. Viidennessä vaiheessa, joka on seurannut Krimin valtausta ja sotaa Itä-Ukrainassa, kansallisesta verkosta on tullut kansallisen turvallisuuden objekti. Venäjän valtio pyrkii hankkimaan kansallisen Internetsegmentin keskitettyyn hallintaansa ja turvaamaan sen toimivuuden ulkoisilta ja sisäisiltä uhilta – ennen kaikkea varmistamaan ettei segmentti muodostu uhan lähteeksi. Doktriineilla, strategioilla, kansallisilla ohjelmilla ja lukuisilla laeilla alhaalta ylös kehittynyt kansallinen verkko pyritään satamaan vertikaaliin hallintaan. Tavoitteena on yhtenäinen,

[557] Kukkola (2020a), s. 376–378. Lukuun on lisätty joitain lähteitä väitöskirjan julkaisun jälkeisten tapahtumien päivittämiseksi.

valtakunnallinen, keskitetysti kontrolloitu informaatiotila, jonka tavoitetila muistuttaa neuvostoliittolaisia suunnitelmia valtakunnallisesta, kyberneettisestä informaatio- ja hallintaverkosta.

Nykyisellään Venäjän kansallinen internetsegmentti perustuu erittäin häiriösietoiselle tietoverkolle, jolla on hyvät sisäiset ja ulkoiset yhteydet. Internetissä olevan informaation sisältöä rajoitetaan ääriajattelun kitkemisen ja lastensuojelun varjolla. Informaation levittäjiä säännellään rekistereillä ja vastuuttamalla nämä palveluiden ja sivustojen sisällöstä. Anonymiteettiä ja VPN:n käyttöä on rajoitettu laeilla. Internetpalveluntarjoajat on velvoitettu tallentamaan kaikki dataliikenne kuudeksi kuukaudeksi ja venäläisten käyttäjien tiedot Venäjällä sijaitseville palvelimille. Turvallisuusviranomaisten käytössä jo Neuvostoliiton aikana ollut SORM-järjestelmä (*Sistema Operativno-Rozysknyh Meroprijati*) päivitettiin vuonna 2015 Internet- ja mobiililiikenteen valvontaan kykeneväksi.[558]

Vuodesta 2015 alkaen Venäjän valtio on pyrkinyt lisäämään vaikutusvaltaansa Internetin infrastruktuuriin liittyvissä asioissa. Vuonna 2017 säädettiin laki kriittisestä informaatioinfrastruktuurista, joka on käytännössä asettanut tietoliikenneinfrastruktuurin valtiovallan sääntelyn alaiseksi. Pääosa Internetin toiminnan kannalta kriittisistä palveluista on siirretty valtion instituutioiden tai korporaatioiden hallintaan vuoteen 2021 mennessä ja yksityistoimijat on käsketty rangaistuksen uhalla luokittelemaan ja suojelemaan niiden haltuun jääneet järjestelmät. Vuoden 2017 laki myös viimeisteli GOSSOPKA-järjestelmän eli valtakunnallisen tietoverkkohyökkäysten monitorointi- ja torjuntajärjestelmän konseptin. Se on kansallinen SIEM-järjestelmä (*Security information and event management*), jota hallinnoivat turvallisuuspalvelut. Järjestelmään liitetään ainakin valtionhallinto sekä strategisiksi katsotut yritykset.[559] Kriittinen informaatioinfrastruktuuri tarjoaa luonnollisen kiintopisteen kansallisista hallintajärjestelmistä haaveileville teoreetikoille.[560] Toisaalta pyrkimys saattaa määrätyt verkkosisällöt ja palvelut kriittiseen informaatioinfrastruktuuriin ja strategisiin resursseihin verrattaviksi kohteiksi lainsäädännön avulla, ja täten rajoittaa niiden ulkomaisia

[558] Kukkola (2020a).
[559] Ibid.
[560] Viimeisimpänä Махутов, Н. А., Балановский, В.Л. & Подъяконов, В.М.: Обеспечение безопасности высокорисковых критически и стратегически важных объектов городской инфраструктуры в условиях появления новых видов угроз. *Вестник Академии Военных Наук*, № 1 (70) 2020, с. 31–36.

omistussuhteita, ei ole vuoteen 2020 mennessä onnistunut. Vuoden 2021 heinäkuussa hyväksytty laki tosin mahdollistaa ulkomaalaisten toiminnan rajoittamisen ”Venäjän alueella sijaitsevassa Internetissä.”[561] Lain on tarkoitus saattaa ylikansalliset yritykset Venäjän lainsäädännön piiriin.

Vuonna 2019 säädettiin laki kansallisen segmentin irrottamiseksi Internetistä ja aloitettiin kansalliset harjoitukset kyberuhkiin vastaamiseksi. Hallituksen määräyksellä aloitettiin myös ”kyberharjoitusalueiden” kehittäminen.[562] Samana vuonna jatkettiin Venäjän vuonna 1998 käynnistynyttä normihanketta Internetin hallinnon saattamiseksi valtioiden valvontaan ja ”informaatioaseiden” kieltämiseksi.[563] Vuoden 2020 alkuun mennessä Venäjän kansallisen kyberturvallisuuden perustaksi on muotoutunut Venäjän alueella toimivan Internetin ja yleisten viestiverkkojen resilienssi, turvallisuus ja eheys. Näitä turvataan keskitetyllä valvonta- ja hallintajärjestelmällä (TsMUSSOP – *Tsentr monitoringa i upravlenija setju svjazi obštšego polzovanija*). Siihen liittyvillä operaattoreiden verkkoihin asennettavilla laitteilla (TSPU – *tehnitšeskoe sredsto protivodejstvija ugrozam*) voidana valikoivasti rajoittaa liikennettä ja tarvittaessa eristää Venäjän tietoliikenneverkot globaalista Internetistä.[564]

Vuonna 2017 hyväksyttiin digitaalisen talouden ohjelma, joka muutettiin vuonna 2019 kansalliseksi ohjelmaksi. Sen tavoitteena on toteuttaa Venäjän talouden ja hallinnon digitalisaatio ja samalla saattaa maa Internet palveluiltaan ja sisällöltään valtiovallan kontrolliin vuoteen 2024 mennessä. Päämääränä on ”teknologinen suvereniteetti” eli laaja-alainen

---

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

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

[563] Черненко, Елена: «Без договоренностей глобального характера эту проблему не решить» Глава нового департамента МИД РФ Андрей Крутских о конфронтации в интернете. *Коммерсантъ*, №33 от 25.02.2020. [https://www.kommersant.ru/doc/4267456], luettu 8.7.2020.

[564] Kukkola (2020a); ПП-127b: Постановление Правительства РФ от 12 февраля 2020 г. N 127 ”*Об утверждении Правил централизованного управления сетью связи общего пользования*”. [http://www.consultant.ru/document/cons_doc_LAW_345574/], luettu 14.5.2020;

kotimainen ohjelmisto- ja laitekehitys sekä -tuotanto.[565] Hanketta on tuettu määräämällä julkishallinnon toimijat hankkimaan venäläisvalmisteista laitteistoja ja ohjelmistoja. Kehitys- ja rahoitusvaikeuksista johtuen käskettyjä määräaikoja on muutettu kerta toisensa jälkeen ja tällä hetkellä tavoitellaan siirtymistä kotimaiseen teknologiaan vuosina 2023–2024.[566] Digitaalisen talouden ohjelman ohessa kehitetään myös ns. kansan Internettiä (*dostupnyi internet*). Alun perin se tarkoitti ilmaista pääsyä julkishallinnon palveluihin tai ns. sosiaalisesti merkittäville sivustoille. Parissa vuodessa hanke on kasvanut ja eräät ovat jopa esittäneet jonkinlaisen vaihtoehto-Internetin rakentamista.[567]

Edelleen vuonna 2017 Venäjän hallitus hyväksyi informaatioyhteiskunnan kehittämisohjelman, joka virallisti kansallisen internetsegmentin käsitteen liittäen sen samalla valtiosuvereniteettiin ja sotilaallisiin uhkiin. Digitaalisen talouden ohjelman ja strategian mukaisesti presidentinhallinnolle, liittovaltion hallinnolle ja paikallishallinnolle luodaan omia tietoverkkoja- ja järjestelmiä sekä datakeskuksia. Vastaavia järjestelmiä on rakennettu puolustus- ja energiateollisuudelle. Valtiohallinto rakentaa näiden pohjalle kansallista informaation keräys- ja analyysijärjestelmää, jolla on selvät yhteydet neuvostoaikaiseen OGAS(U)-järjestelmään.[568] Ajatus hallinnon ja talouden automaatiosta, tehostamisesta ja nopeuttamisesta on läsnä myös venäläisessä tekoälyyn liittyvässä ajattelussa ja strategiassa.[569]

Kehittämisohjelmien vaatiman kotimaisen teknologian ja tuotannon kehittämiseksi Venäjän valtio on tukeutunut tiedeinstituutteihin ja

---

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

[566] Ks. esim. Воейков, Денис: МВД потратит 270 миллионов на серверы с «Эльбрусами» «не хуже» Intel и AMD. *CNEWS*, 7.7.2020. [https://www.cnews.ru/news/top/2020-07-07_mvd_potratit_270_millionov], luettu 8.7.2020; Чернышова, Евгения & Балашова, Анна: Банки договорились с властями о постепенном переходе на российский софт Требование об импортозамещении должно вступить в силу с начала 2023 года. *РБК*, 16.7.2021. [https://www.rbc.ru/finances/16/07/2021/60f14f009a794702b097f76a?from=from_main_9], luettu 28.7.2021.

[567] Гаврилюк, Анастасия & Шестоперов, Дмитрий: Отступный интернет Законопроект о бесплатном доступе к значимым сайтам предложено доработать. *Коммерсантъ* №38 от 05.03.2021. [https://www.kommersant.ru/doc/4713549], luettu 28.7.2021.

[568] Kukkola (2020a). OGAS(U) osalta ks. Peters (2016).

[569] Указ-490 (2019).

innovaatiopuistokonsepteihin. Näiden menestyksestä ei kuitenkaan ole selkeää näyttöä.[570] Lisäksi vuodesta 2019 Venäjä on tiivistänyt teknologiayhteistyötä Kiinan kanssa ja kiinalaiset yritykset ovat sopineet yhteistyöhankkeista venäläisten ICT-alan yritysten kanssa.[571] Kiinan kanssa tehtävä yhteistyö ei kuitenkaan pitkällä tähtäimellä palvele digitaalisen suvereniteetin tai omavaraisuuden päämäärää.

Kansallisen internetsegmentin hallintaa toimeenpanevat useat julkishallinnon toimijat. Pääroolissa ovat Digitaalisen kehityksen, tietoliikenneyhteyksien ja joukkotiedotuksen ministeriö, sen alainen valvontaviranomainen Roskomnadzor, Liittovaltion teknologia ja vientiviranomainen (FSTEK) sekä turvallisuuspalvelut. Sääntely kohdistuu pääosiltaan yksityisyrityksiin, joiden hallussa on pääosa verkkoinfrastruktuurista ja venäjänkielisestä palvelutuotannosta ja sosiaalisesta mediasta.[572] Valtion hallintapyrkimykset eivät kuitenkaan rajoitu yksityisyritysten sääntelyyn. Yritysten itsenäisyys suhteessa Kremliin on vuosi vuodelta kaventunut ja monien yritysten taustalta löytyy valtiosidonnaisia omistajia tai sijoittajia kuten Sberpank pankki.[573] Valtion omistussuhteen vahvistuminen ei välttämättä tavoittele kansallistamista, mutta mahdollistaa tiukemman kontrollin. Lisäksi Venäjän suurin teleoperaattori ja internetpalveluntarjoaja Rostelekom on valtionyhtiö. Sen hallussa on merkittäviä osia kriittisestä informaatioinfrastruktuurista ja sen

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

[571] 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.

[572] Kukkola (2020a), s. 272–273.

[573] Vendil Pallin, Carolina: Internet control through ownership: the case of Russia. *Post-Soviet Affairs*, Vol. 33 No. 1, (2017), s. 16-33, s. 22; Inozemtsev, Vladislav: The Yandex Affair: Insider Trading and Institutionalized State Control. *Eurasia Daily Monitor* Volume: 16 Issue: 174 [https://jamestown.org/program/the-yandex-affair-insider-trading-and-institutionalized-state-control/], luettu 28.7.2021; Хабибрахимов, Альберт: «Сбербанк» стал совладельцем Mail.ru Group и Rambler Group, Андрей Андреев продал Badoo: заметные сделки 2019 года. *VC.ru*, 2.1.2020 [https://bit.ly/377BTby], luettu 28.7.2021.

palveluista.[574] Myös johtavat tietoturvayhtiöt tekevät kiinteää yhteistyötä valtionhallinnon kanssa.[575]

Lakitekstien vaatimukset ja hankesuunnitelmien tavoitteet eivät täysin huomioi byrokratian, markkinatalouden ja yhteiskunnan todellisuutta. Lakien toteuttamiseen tarvittava ohjeistus on myöhästynyt useita kertoja.[576] Osa yrityskenttää vastustaa suvereneenin Internetin ja siihen liittyvien palvelujen rakentamista.[577] Merkittävä kiistanaihe ovat verkkoliikennettä valvovien laitteiden vaikutus palvelun laatuun ja vaatimus siitä, että operaattorit maksavat itse valvontalaitteista koituvat kustannukset.[578] Digitaalisen talouden kilpailutukset eivät myöskään ole läpinäkyviä ja korruptio on ongelma.[579] Kansalaisyhteiskunnan (h)aktivistit haastavat valtion teknologiset kontrollipyrkimykset.[580] Lisäksi COVID-19 pandemia ja öljyn maailmanmarkkinahinnan romahtaminen

[574] Kukkola (2020a), s. 269, 273 & 350.

[575] O'Neill, Patrick Howell: The $1 billion Russian cyber company that the US says hacks for Moscow. *MIT Review*, April 15, 2021 [https://www.technologyreview.com/2021/04/15/1022895/us-sanctions-russia-positive-hacking/], luettu 28.7.2021.

[576] Tietoturva-asiantuntija Aleksei Lukatskin blogi vuosilta 2007–2021 tarjoaa hyvän ikkunan ohjeiden puutteesta syntyneisiin ongelmiin Venäjän IT-alalla [Лукацкий, Алексей: *Бизнес без опасности*. Blogi. [https://lukatsky.blogspot.com/], luettu 28.7.2021.

[577] Корченкова, Наталья & Тишина, Юлия: Суверенный рунет вышел на связь С критикой законопроекта выступила РСПП. *Коммерсантъ* №23 от 08.02.2019. [https://www.kommersant.ru/doc/3875941?from=main_4], luettu 28.7.2021; Криворучко, Владимир: Вооружение в лабиринтах программ. *Военно-промышленный курьер*, 18.06.2020. [https://vpk.name/news/411648_vooruzhenie_v_labirintah_programm.html], luettu 8.7.2020.

[578] Гаврилюк, Анастасия: «Суверенный рунет» сочли угрозой стабильности. Операторы критикуют новые требования Роскомнадзора. *Коммерсантъ* №132, 29.07.2021. [https://www.kommersant.ru/doc/4919761?from=main_9], luettu 29.7.2021.

[579] Воейков, Денис: Власти хотят признавать «железо» российским за деньги. В этой идее нашлись «коррупциогенные факторы». *CNEWS*, 16.7.2021. [https://cnews.ru/link/n532505], luettu 28.7.2021; Welt, Cory & Nelson, Rebecca M.: *Russia: Domestic Politics and Economy*, September 9, 2020. Congressional Research Service, R46518 – Version 4. [https://fas.org/sgp/crs/row/R46518.pdf], luettu 28.7.2021.

[580] Daucé, Françoise & Musiani, Francesca (eds.): Infrastructure-Embedded Control, Circumvention and Sovereignty in the Russian Internet. *First Monday*, 26(5), special issue, 3 May 2021 [https://firstmonday.org/ojs/index.php/fm/issue/view/693], luettu 28.7.2021.

ovat vaikuttaneet hidastavasti kaikkiin Venäjän kansallisiin hankkeisiin, myös kansallisen internetsegmentin rakentamiseen.[581]

Kansallisen internetsegmentin rakentaminen siis edistyy, muttei siinä aikataulussa, tehokkuudella ja venäläiseen osaamisen perustuen kuin tahtotila olisi.[582] Kansallinen internetsegmentti, ja digitaalinen suvereniteetti ja itsenäisyys perustuvat suurilta osin yksityiselle omaisuudelle. Valtiovallan on siirrettävä tai alistettava hallintaansa tämä omaisuus, jotta kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä voidaan täysimääräisesti toteuttaa. Tavoitteen toteutumisen aikataulu ja sen lopullinen muoto ovat vielä auki. Poliittinen tahto on kuitenkin olemassa. Keväällä 2021 useat poliitikot vaativat presidentti Putinin johdolla Internetin hallinnan edelleen tiukentamista.[583]

Asevoimien tietoverkkoja- ja järjestelmiä ei voida ohittaa tarkasteltaessa kansallisen internetsegmentin tuottamaa mahdollista asymmetriaa ja strategisia vaikutuksia. Vaikka verkkoja operoivat Venäjän asevoimat ja vaikka ne ovatkin osiltaan erotettuja muista tietoverkoista, ei kansallisen internetsegmentin rakentaminen voi olla vaikuttamatta niihin. Esimerkiksi sotilasteollisen kompleksin yhteydet, turvallisuusviranomaisten yhteistyö ja kansainvälinen sotilastoiminta muodostavat keskinäisriippuvaisten toimijoiden rajapinnan. Lisäksi siviili- ja sotilasresurssien yhteiskäyttö, kriittisen informaatioinfrastruktuurin kehittyminen sodankäynnin kohteeksi ja kyberoperaatioiden logiikka hämärtävät eroja verkkojen välillä. Asevoimien järjestelmät ovat osa kybertilaa ja valtion väkivallan monopolia ja näin ollen osa kybertilasta rajattavaa kansallista internetsegmenttiä. Läntinen kansainvälisen lain tulkinta on tässä Venäjän ja Kiinan ajaman politiikan tukena.[584] Huomattava toki on, että asevoimien verkot kuuluvat Venäjän lainsäädännössä ”erikoisverkkojen” kategoriaan,

---

[581] Президент России: Указ о национальных целях развития России до 2030 года. *Kremlin.ru* 21.7.2020. [http://kremlin.ru/events/president/news/63728], luettu 31.7.2020.
[582] Kukkola (2020a). Esimerkiksi Keith Dear on varsin vakuuttavasti argumentoinut, että venäläisen AI teknologian kohtalona on korruptio, mutta muualta hankitun AI teknologian soveltaminen voi onnistua (Dear (2019).
[583] Тадтаев, Георгий: Путин заявил об угрозе разрушения общества из-за интернета. *РБК*, 4.3.2021. [https://www.rbc.ru/politics/04/03/2021/6040c97c9a7947263f812b1c?from=from_main_6], luettu 28.7.2021.
[584] Schmitt, Michael N. (ed.): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, Cambridge, U.K., 2013; Schmitt (2017).

josta käsketään erikseen, ja joka on erillinen yleisestä televerkosta, johon Internet kuuluu.[585]

Venäjän asevoimat ovat pyrkineet kehittämään omaa yhtenäistä informaatioverkkoaan eli integroitua automatisoitua digitaalista kommunikaatiojärjestelmää (OATsSS) ainakin vuodesta 2008. Se on asevoimien visionäärien kirjoituksissa asevoimat ja muut valtion turvallisuustoimijat yhdistävä tietoverkko- ja järjestelmä palvelinkeskuksineen ja palveluineen. OATsSS:n tarkoituksena on muodostaa valtakunnan laajuinen, ja tarvittaessa rajat ylittävä, perusta asevoimien johtamisjärjestelmille ja -yhteyksille. Periaatteessa sen tulisi mahdollistaa yksittäisten aselavettien johtaminen Kansallisen puolustuksen johtokeskuksesta tai strategisten yhteisjohtoportaiden komentopaikoilta.[586] Todennäköisesti OATsSS:n piti alun perin perustua siviiliteleliikenneverkkoihin, mutta vuonna 2019 asevoimat ilmoitti kehittävänsä täysin erillistä *Multiservice Transport Networkia* (MTSS) omiin tarpeisiinsa. Lisäksi se on aloittanut katastrofin kestävien palvelinkeskusten rakentamisen sotilaspiireihin. Asevoimat operoi omaa ”sotilasinternetiään”, joka perustuu venäläisiin ohjelmistopalveluihin ja tarjoaa salatut palvelut ja yhteydet asevoimien tarpeisiin. Näiden kiinteiden palveluiden ja verkkojen lisäksi asevoimilla on lukuisia kenttäviestijärjestelmiä strategisoperatiiviselta (sotilaspiirit) tasolta aina taktiselle (pataljoonien taisteluosastot) tasolle.[587] Viestijärjestelmien yhteydet perustuvat kaapeli, radio, radiolinkki ja satelliittiyhteyksiin. Puolustushaaroilla ja aselajeilla on myös omat tietoverkkonsa ja -järjestelmänsä, jotka eivät välttämättä ole keskenään yhteensopivia.

---

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

[586] Venäjän asevoimien organisaatiosta ja komentoportaiden roolista ks. Whisler, Greg: Strategic Command and Control in the Russian Armed Forces: Untangling the General Staff, Military Districts, and Service Main Commands (Part One). *The Journal of Slavic Military Studies*, Vol. 32, No. 4 (2019), s. 463–484; Whisler, Greg: Strategic Command and Control in the Russian Armed Forces: Untangling the General Staff, Military Districts, and Service Main Commands (Part Two). *The Journal of Slavic Military Studies*, Vol. 33, No. 1 (2020), s. 89–112; Whisler, Greg: Strategic Command and Control in the Russian Armed Forces: Untangling the General Staff, Military Districts, and Service Main Commands (Part Three). *The Journal of Slavic Military Studies*, Vol. 33, No. 2 (2020), s. 237–258.

[587] Venäjän asevoimat harjoittelevat radioverkkojen käyttöä säännöllisesti (Myers, Nicholas J.: Radio Exercises and Trends in Russian C2 Capabilities. *Eurasia Daily Monitor*, Vol. 17, No. 65. [https://jamestown.org/program/radio-exercises-and-trends-in-russian-c2-capabilities/], luettu 14.5.2020)

Sotilasteollisella kompleksilla (OPK) on oma tietoliikenneverkkonsa samoin kuin asevoimien mobilisaatiojärjestelmällä. Asevoimien ja sen liitännäisten verkot ovat visioista huolimatta varsin todennäköisesti sirpaloituneita ja tietoa niiden välillä vaihdetaan erilaisin tilapäismenettelyin.[588] Lisäksi asevoimien viestijärjestelmä tuskin tulee toimeen ilman siviiliverkkojen tuottamaa sähköä tai kaksoiskäyttöistä infrastruktuuria. Muussa tapauksessa asevoimat olisi käynnistänyt sähköverkon ja Internetin täydelliseen kahdentamiseen tähtäävän hankkeen, joka olisi triljoonia ruplia maksava projekti. Näin ollen MTSS:kin tulee käyttämään vähintään samoja viestiasemia ja kaapelikuiluja kuin siviililiikennekin. Pelkästään Venäjän maantiede sanelee tämän.

Asevoimien tietoverkoista strategisen deterrenssin ydinasekomponenttiin liittyvä ydinaseiskun ennakkovaroitusjärjestelmä ja itse strategisten ydinaseiden johtamisjärjestelmä muodostavat erikoistapauksen. Johtamisjärjestelmä Signal perustuu monimuotoiseen joukkoon analogisia ja digitaalisia tietoverkkoja ja -järjestelmiä mukaan lukien useita radioverkkoja, komento-ohjuksia, lentokoneita ja satelliitteja, joita on vuosien varrella modernisoitu useaan kertaan.[589] Ennakkovaroitusjärjestelmä koostuu hieman alle kahdestakymmenestä OTH -tutkasta (*Over-the-Horizon*), optisista sensoreista ja 3–4 satelliitista (nk. *edinaja kosmitsheskaja sistema*, EKS).[590] Johtamisjärjestelmän päätarkoitus on riittävän ennakkovaroituksen antaminen satelliitti- ja sensoritietoihin perustuen ja strategisten ydinaseiden positiivisen ja negatiivisen kontrollin mahdollistaminen.[591] Järjestelmän automatisoinnin aste on ollut spekulaation aiheena 1990-luvun alusta alkaen. Syynä on Neuvostoliiton ja Venäjän ydinasedoktriini, jonka uskotaan perustuneen ja perustuvan aseiden laukaisuun varoitukseen perustuen (vrt. laukaisu iskun alla tai iskun jälkeen). Doktriini edellyttää erittäin nopeaa päätöksentekoa ja käskyjen tehokasta välittämistä, mikä nostaa teknisestä viasta ja

---

[588] Kukkola (2020a).
[589] Blair, Bruce, G.: *The Logic of Accidental Nuclear War*. The Brookings Institution, Washington, D.C., 1993; Подвиг, П. Л.: *Стратегическое ядерное вооружение Россиии*. ИздАТ, Москва, 1998; Blair, Bruce G.: *Strategic Command and Control: Redefining the Nuclear Threat*. The Brookings Institution, Washington, D.C., 1985; Yarynich, Valeri E.: *C3: Nuclear Command, Control, Cooperation*. Center for Defence Information, Washington, D.C., 2003.
[590] Honkova, Jana: *The Russian Federation's Approach to Military Space and Its Military Space Capabilities*. George Marshall Institute, Arlington, VA, 2013.
[591] Blair (1985); Blair (1993).

väärinymmärryksestä seuraavan laukaisun riskiä. Niin Yhdysvalloilla kuin Venäjälläkin on käytössään järjestelmiä, joiden tarkoitus on mahdollistaa ydinasevastaiskun toteuttaminen, vaikka ennakkovaroituksessa epäonnistuttaisiin.[592]

Ydinasedeterrenssiin liittyvät myös ilma- ja avaruusjoukkojen johtamisjärjestelmät, joiden tehtävänä on mm. mahdollistaa tavanomaisen täsmäasein tehtävän yllätyshyökkäyksen torjunta. Tällaisen hyökkäyksen tavoitteena voisi olla Venäjän strategisen ydinasevastaiskukyvyn lamauttaminen.[593] Lisäksi Venäjällä on alati kehittyvä lyhyen ja keskipitkän kantaman ballististen ohjusten torjuntakyky ja rajoitettu kyky torjua strategisia ballistisia ohjuksia. Torjuntajärjestelmät on pyritty verkottamaan sensoreihin ja eri tason komentopaikkoihin.[594] Venäjän asevoimat operoi myös merkittävää satelliittilaivastoa, joka tarjoaa paikannus- ja viestipalveluja asevoimille niin Venäjällä kuin maailmanlaajuisesti.[595] Avaruussuorituskykyjen merkitys nykyaikaiselle sodankäynnille ymmärretään hyvin ja Venäjä on pyrkinyt kehittämään elektroniseen sodankäyntiin ja antisatelliittiaseisiin perustuvaa kykyä vaikuttaa potentiaalisten vastustajan suorituskykyihin.[596]

---

[592] Hoffman, David E.: *The Dead Hand. The Untold Story of the Cold War Arms Race and Its Dangerous Legacy*. Anchor Books, New York, 2009; Trevithick, Joseph: No, The United States Doesn't Have An Automatic "Dead Hand" Trigger For Its ICBMs. *The Drive: The Warzone*, February 7, 2020. [https://www.thedrive.com/the-war-zone/32114/no-the-united-states-doesnt-have-an-automatic-dead-hand-trigger-for-its-icbms], luettu 8.7.2020.

[593] Arbatov, Alexei & Dvorkin, Vladimir (Eds.): *Missile Defense: Confrontation and Cooperation*. Carnegie Moscow Center, Moscow, 2013; Thomas (2015), s. 174–175; Андреев, В.: 5 Этапов развития АСУ. *Воздушно-космическая оборона*, №2, 2011 г; Persson, Gudrun (ed.): *Russian Military Capability in a Ten-Year Perspective – 2016*. FOI, Stockholm, 2016.

[594] Plopsky, G.: Russia's Big Plans for Air Defense in Eurasia: Big plans, indeed, but will they materialize? *The Diplomat* (2017, Apr, 7). [https://thediplomat.com/2017/04/russias-big-plans-for-air-defensein-eurasia/], luettu 8.7.2020; Шувертков, Валерий: Систему ПВО ОДКБ еще предстоит создавать. *Воздушно-космическая сфера*, 2015, No. 3, с. 46–49; Суровикин, С.В.: Формы применения и организация управления межвидовой группировкой войск (сил) на театре военных действий. *Вестник Академии военных наук*, №. 1 (46) 2014, с. 40–43; Defence Intelligence Agency: *Russia Military Power: Building a Military to Support Great Power Ambitions*, 2017 , s. 33. [http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf], luettu 8.7.2020.

[595] Honkova (2013).

[596] Harrison et al. (2020).

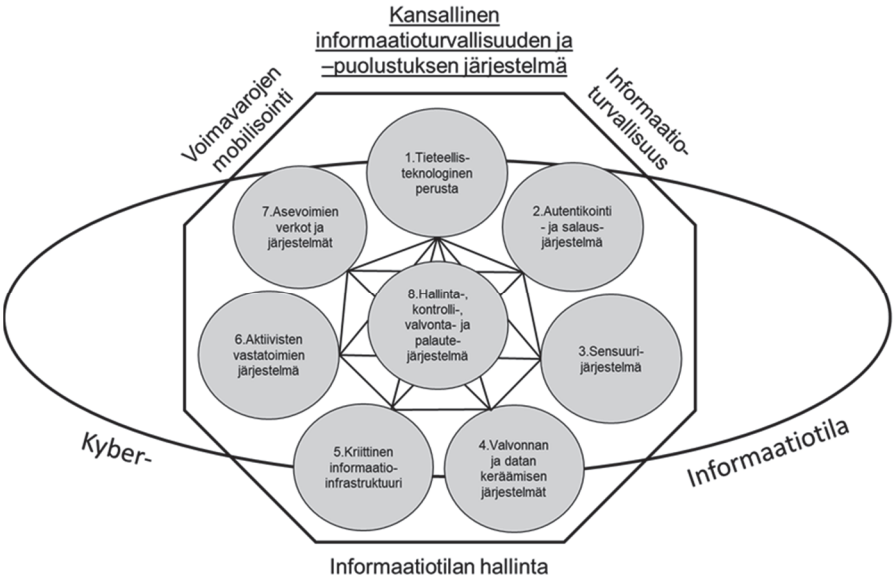
3.4 Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä

Seuraavaksi esitellään väitöskirjassani esittämän informaatioturvallisuuden ja -puolustuksen järjestelmän päivitetty versio.[597] Kuten aiemmin on todettu, malli perustuu Venäjän kansallisen internetsegmentin hankkeen tavoitetilaan ja Venäjä valtion ominaispiirteisiin. Malli on ideaalitapaus, jollaisena Venäjän valtion kansallisen internetsegmentin hanke tulee tuskin täysin toteutumaan. Malli on yleinen suljetun kansallisen verkon malli, jonka pohjalta voidaan vertailla suljettuja ja avoimia kansallisia verkkoja. Mallin rakentamiseen käytetyt lähteet on esitelty väitöskirjassani ja tämän työn luvussa 3.3. Toteutukseen liittyviä heikkouksia ja yksityiskohtia tarkastellaan asymmetrian analyysiluvuissa. Järjestelmien järjestelmä koostuu kahdeksasta alajärjestelmästä, jotka on eroteltu perustuen niiden tarkoitukseen, osiin, funktioihin, toimintaperiaatteisiin ja päämäärään. Järjestelmillä on keskinäiset suhteensa, mutta niiden toimintaa ja koko järjestelmän toimintaa ohjaa kahdeksas, monitoroiva ja kontrolloiva alajärjestelmä. Mallin osajärjestelmät ovat periaatteessa sovellettavissa muihin vastaaviin valtiollisiin informaatiotilan kontrollijärjestelmiin.[598]

Alkuperäisellä mallilla on rajoitteensa. Se ei huomioinut siviili- ja sotilasverkkojen ja -järjestelmien suhdetta ja keskinäisriippuvuuksia. Malli jätti myös kyberdiplomatiaa lukuun ottamatta huomiotta ympäristön aktiivisen muokkaamisen informaatioturvallisuuden saavuttamiseksi. Malli keskittyi sotilasstrategisiin elementteihin ja jätti huomiotta kybertoimintaympäristön muut piirteet. Malli on lähtökohtaisesti sidoksissa venäläiseen strategiseen ajatteluun, politiikkaan ja maan informaatioyhteiskunnan luonteeseen ja kansallisen informaatioinfrastruktuurin rakenteeseen. Rajoitteita korjataan tässä työssä huomioimalla asevoimien verkot ja järjestelmät, laajentamalla kyberdiplomatian järjestelmä aktiivisten vastatoimenpiteiden alajärjestelmäksi ja tarkastelemalla järjestelmän suhdetta kybertoimintaympäristöön laajemmasta näkökulmasta. On kuitenkin

[597] Kukkola (2020a), s. 361.
[598] Vastaavanlaista järjestelmää rakennetaan parhaillaan Kiinassa (Chandel, Sonali, Jingji, Zang, Yunnan, Yu, Jingyao, Sun & Zhipeng, Zhang: The Golden Shield Project of China: A Decade Later An in-depth study of the Great Firewall. *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 17-19 October, Guilin, China*).

huomioitava, että tarvitaan lisää vertailevaa tutkimusta Venäjän informaatioturvallisuuden ja -puolustuksen järjestelmän käyttämiseksi rakenteellisen kyberasymmetrian yleiseen ja yleistävään tarkasteluun. Alajärjestelmät on esitetty yksinkertaistetusti kuvassa 10.



Kuva 10: Kansallisen informaatioturvallisuuden ja puolustuksen järjestelmä

Informaatioturvallisuuden ja -puolustuksen järjestelmien järjestelmän ensimmäinen alajärjestelmä on taloudellinen ja tieteellinen järjestelmä eli valtion tieteellisteknologinen perusta. Se perustuu autarkiseen talouspolitiikkaan ml. vienninkorvausohjemaan, ja valtion investoinneille koulutukseen ja tieteeseen. Alajärjestelmän pääfunktiona on edistää talouden digitalisaatiota, lisätä Venäjä taloudellista voimaa ja edistää yhteiskunnan tasapainoa luomalla hyvinvointia. Lisäksi se epäsuorasti muokkaa kybertilaa valtiojohdolle suotuisaan suuntaan tuottamalla valtaan sidoksissa olevia palveluja ja järjestelmiä. Se tuottaa myös kansallista turvallisuutta kotimaisen laite- ja ohjelmistotuotannon kautta ehkäisemällä tuotantoketjuihin kohdistuvia haavoittuvuuksia ja takaamalla kriittisen informaatioinfrastruktuurin ja tietoturvajärjestelmien riippumattomuuden ulkomaisista toimittajista. Periaatteessa omaperäiset venäläiset ratkaisut tarjoavat myös välillistä suojaa (*security through obscurity*). Kotimaiset valmistajat on velvoitettu rakentamaan pääsy turvallisuuspalveluille niiden

palveluihin ja tuotteisiin. Turvallisuuspalveluilla (ja asevoimilla) on näin ollen pääsy myös ulkomailla käytettäviin venäläisiin järjestelmiin.[599]

Toinen alajärjestelmä koostuu valtion salaus- ja autentikointipalveluista. Se perustuu digitaalisen talouden ohjelmassa toteutettavaan valtiohallinnon salaus- ja autentikointijärjestelmään, jonka on tarkoitus korvata ulkomaiset järjestelmät. Aluksi järjestelmä ulotetaan pakollisena vain julkishallintoon, mutta tuodaan vähitellen vapaaehtoisuuden ja ”valinnanvapauden” kautta myös yritysten ja yksityishenkilöiden käyttöön. Tavoitteena on tehdä kaikki kansallisen internetsegmentin liikenne läpinäkyväksi turvallisuuspalveluille. Järjestelmään voi kuulua kvanttisalauksella toteutettava runkoverkko. Venäjän internetsegmentin läpi kulkevaan salattuun tietoliikenteeseen alajärjestelmä ei vaikuta, mutta ulkomaisetkin toimijat voidaan velvoittaa käyttämään valtiollista salausta tai sen hyväksymiä järjestelmiä tai ohjaamaan liikenteensä valtiollisten välityspalvelimien kautta.[600]

Kolmas alajärjestelmä koostuu hallinnollisista ja teknisistä toimenpiteistä, joilla poistetaan ja rajoitetaan pääsy valtion turvallisuuden kannalta epätoivottuun internetsisältöön. Se toimii valtiollisen sensuurijärjestelmän osana. Siihen kuuluu materiaalin poistaminen, pääsyn esto ja palveluiden sekä käyttäjätilien sulkeminen. Vapaan ilmaisun rajoittaminen ja poliittisten mielipiteiden ilmaisun saattaminen rikosoikeuden piiriin perustellaan kansallisilla moraali- ja arvotekijöillä esimerkiksi alaikäisten suojelemisella. Järjestelmä mahdollistaa ulkomaisten yritysten toiminnan rajoittamisen ja kieltämisen. Järjestelmään kuuluvat myös käyttäjien ja palveluntarjoajien itsesensuuri ja kansalaisten vapaaehtoiset aktivistiryhmät, jotka etsivät verkosta ”laitonta” sisältöä. Alajärjestelmä on pääsääntöisesti tarkoitettu poliittisen kontrollin välineeksi, vaikka se on virallisesti lainvalvonnan väline.[601]

Neljäs alajärjestelmä koostuu kohdennetuista tiedustelujärjestelmistä kuten SORM sekä massiivisesta internetdata keräämisestä ja lokalisaatiosta. Edellisestä vastaavat turvallisuuspalvelut ja jälkimmäisestä internetpalveluntarjoajat, joiden on annettava turvallisuuspalveluille pääsy datavarantoihinsa. Järjestelmä perustuu hajautetuista datakeskuksista ja verkotetuista valvonta- ja analyysijärjestelmistä. Se tuottaa laaja-alaista

[599] Kukkola (2020a), s. 361–362.
[600] Ibid.
[601] Kukkola (2020a), s. 363.

tiedustelutietoa ja varoituksen informaatiouhista ja käynnissä olevista hyökkäyksistä. Järjestelmän tuottamaa tietoa voidaan käyttää niin teknisessä kuin poliittisessa attribuutioinnissa kuin omissa vaikutusoperaatioissa kybertoimintaympäristössä ja sen ulkopuolella. Alajärjestelmä lisää kansallisen internetsegmentin läpinäkyvyyttä turvallisuustoimijoiden suuntaan (ei siis muiden toimijoiden suuntaan) edellä mainitun valtiollisen salauksen ohella.[602]

Viides alajärjestelmä koostuu kriittisestä informaatioinfrastruktuurista ja sen säätelystä. Se määrittelee kriittisen infrastruktuurin ja sen suojelusta vastuussa olevat tahot. Nämä tahot ovat pääsääntöisesti yksityistoimijoita, joiden velvollisuus perustuu lakiin ja rangaistukseen. Niitä valvovat turvallisuuspalvelut. Järjestelmä sisältää myös kahdennetut kriittiset internetpalvelut kuten nimipalvelimet, reititystaulukot ja liikenteen solmupisteet. Sen pohjalle on rakennettu kyky kierrättää maan sisäinen verkkoliikenne sen rajojen sisällä. Täten alajärjestelmä mahdollistaa internetsegmentin irrottamisen globaalista Internetistä niin, että kriittiset palvelut jatkavat toimintaansa. Lisäksi alajärjestelmä vahvistaa tietoverkkojen resilienssiä kyberhyökkäyksiä vastaan.[603]

Kuudes alajärjestelmä koostuu aktiivisista informaatioteknologisista ja informaatiopsykologisista vastatoimista. Yhtäältä alajärjestelmä koostuu valtion omistamista tai sen kontrolloimista uutispalveluista sekä kasvatuksellisista, patrioottisista ja uskonnollisista instituutioista. Toisaalta siihen kuuluvat varta vasten luodut kyberdiplomatiaa harjoittavat organisaatiot sekä turvallisuuspalveluiden ja asevoimien kybervakoilu sekä informaatiosodankäyntiyksiköt. Alajärjestelmä hallitsee kotimaista informaatiotilaa tuottamalla ja muokkaamalla informaatiota. Lisäksi se suorittaa vakoilu-, vaikuttamis- ja kyberoperaatioita uhkien syntymisen ennalta ehkäisemiseksi. Alajärjestelmä lisää informaatioturvallisuutta heikentämällä potentiaalisia vastustajia ja sitouttamalla niitä normeihin ja rajoittamalla kehittyneiden vastustajien toimintakykyä luomalla suorituskykyjen käyttöön liittyviä tabuja.[604]

Seitsemäs alajärjestelmä koostuu asevoimien verkoista ja -järjestelmistä. Alajärjestelmä on pitkälti erillinen muista seitsemästä järjestelmästä, mutta on riippuvainen muun muassa kriittisestä informaatioinfrastruktuurista

---

[602] Ibid.
[603] Ibid.
[604] Kukkola (2020b), s. 18.

suorituskykyjensä osalta. Se sisältää ylijohdon, puolustushaarojen, aselajien, laitosten, alueellisten johtoportaiden ja instituuttien sekä laitosten järjestelmät. Asevoimat valvoo ja ylläpitää itse omat järjestelmänsä, mutta tukeutuu osiltaan siviilipalveluntuottajiin ja verkko-operaattoreihin. Alajärjestelmä takaa asevoimien johtamiskyvyn sekä yhteydet muuhun valtionhallintoon rauhan ja sodan aikana. Se mahdollistaa valtion sotilaallisen puolustamisen ja kansallisen turvallisuuden ylläpitämisen.[605]

Kahdeksas alajärjestelmä koostuu hallinta-, kontrolli-, valvonta- ja palautejärjestelmistä. Se sisältää mm. GosSOPKA:n, TsMUSSOP:in, valtion informaatiohallintajärjestelmän (*Upravlenie*), julkisissa ja yksityisissä verkoissa toimivien CERTien verkoston ja siviili- ja asevoimien tilannekeskusten verkoston. Alajärjestelmä takaa kansallisen internetsegmentin vertikaalin hallinnan ja horisontaalin integraation. Se kerää valtiovallan käyttöön informaatiota kansallisesta segmentistä ja koko yhteiskunnasta ja tuottaa uhka-analyysiä niin teknologisista kuin informaatiouhista ja mahdollistaa informaatiovirtojen kontrollin. Alajärjestelmä vastaa kaikkien muiden alajärjestelmien kontrollista ja kansallisen internetsegmentin aktiivisesta puolustamisesta valtiotason kyberhyökkäyksiä vastaan.[606]

Järjestelmän alajärjestelmät ovat tiiviissä vuorovaikutuksessa kansallisen informaatioturvallisuuden tuottamiseksi. Tieteellisteknologinen perusta tuottaa suorituskyvyt kaikille muille järjestelmille. Alajärjestelmän teknologiset heikkoudet tai jälkeenjääneisyys ja haavoittuvuudet muodostavat riskin muille alajärjestelmille. Autentikointi- ja salausjärjestelmä turvaa muiden yhteydet ja informaation ja luo perustan järjestelmien palveluiden luotettavuudelle. Sen haavoittuvuudet muodostavat kuitenkin riskin kaikille muille alajärjestelmille. Sensuurijärjestelmä edesauttaa talouden, informaatioinfrastruktuurin ja kontrollin toteuttamista heikentämällä yhteiskunnallista vastarintaa ja vahvistaa kriittisten resurssien kansallista hallintaa. Se poistaa tai rajoittaa informaatiota. Alajärjestelmän käyttö voi kuitenkin synnyttää vastareaktion, joka lisää sisäisiä uhkia ja heikentää tieteellisteknologisen perustan innovaatiopotentiaalia.[607] Massiivinen datan keruu ja valvonta tuottaa data- ja informaatiovarantoa kansallisiin projekteihin ja

[605] Ks. Luku 3.3.
[606] Kukkola (2020a), s. 364.
[607] Lassila, Jussi: Aivovuoto Venäjältä: Kremlin kaksiteräinen miekka. *FIIA Comment 6*, Toukokuu 2019. [https://www.fiia.fi/wp-content/uploads/2019/05/comment6_emigration_from_russia_fi.pdf], luettu 29.7.2021.

kontrollijärjestelmälle. Se kuitenkin muodostaa tietovuotouhan kautta riskin kaikille muille järjestelmille ja koko järjestelmän päämäärälle. Räätälöidyt tiedustelujärjestelmät mahdollistavat muihin järjestelmiin kohdistuvien informaatiouhkien torjunnan paljastamalla hankkeita, mutta niiden sijoittaminen informaatioinfrastruktuuriin tuottaa haavoittuvuuksia samaiseen infrastruktuuriin. Kriittisen infrastruktuurin toimivuus ja resilienssi on perusta koko järjestelmälle ja kansalliselle segmentille. Toisaalta infrastruktuurin hallinnoinnin tavat voivat muodostaa riskin niin taloudelle kuin kansalliselle turvallisuudelle.[608] Aktiiviset vastatoimet legitimoivat järjestelmien järjestelmän ja vähentävät sen muihin osiin kohdistuvia uhkia. Toisaalta ne voivat aiheuttaa niin sisäisiä kuin ulkoisia vastareaktioita, jotka voivat johtaa uusien uhkien materialisoitumiseen.[609] Asevoimien verkot ja -järjestelmät luovat kysyntää siviilimaailman tuottamalle teknologialle ja osaamiselle, mutta ovat samalla haavoittuvaisia kriittisen infrastruktuurin häiriöille. Kontrollijärjestelmä turvaa toimiessaan talouden ja infrastruktuurin. Se muodostaa kuitenkin itsessään tietoturvauhan, jonka äärimmäisenä riskinä on kansallisen internetsegmentin lamautuminen.[610]

Informaatioturvallisuuden ja -puolustuksen järjestelmä tuottaa siis turvallisuutta takaamalla kansallisen internetsegmentin informaatiopsykologisen ja -teknologisen eheyden, resilienssin ja turvallisuuden samalla, kun se luo perustan Venäjän digitaaliselle suvereniteetille pystyttämällä rajat Venäjän kybertilaan ja valvomalla niitä. Järjestelmä on periaatteessa suhteellisen joustava ja mahdollistaa koko kansakunnan tieteellisteknologisten voimavarojen mobilisoinnin Venäjän

---

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

[609] Yhdysvallat asetti keväällä 2021 sanktioita venäläiselle Positive Technologies yritykselle, joka tarjoaa tietoturvapalveluja kriittiselle informaatioinfrastruktuurille, kyberhyökkäysten johdosta (Степанова, Юлия, Занина, Анна & Гаврилюк, Анастасия: Техноложная тревога. Чем займутся российские IT-компании под санкциями США. *Коммерсантъ* №67, 16.04.2021. [https://www.kommersant.ru/doc/4773434?from=main_5], luettu 29.7.2021.)

[610] Tästä hyvänä esimerkkinä SolarWinds hyökkäys joulukuussa 2020 (Gatlan, Sergiu: SolarWinds Victims Revealed after Cracking the Sunburst Malware DGA. *Bleeping Computer*, December 22, 2020. [https://www.bleepingcomputer.com/news/security/solarwinds-victims-revealed-after-cracking-the-sunburst-malware-dga/], luettu 28.12.2020).

intressien turvaamiseksi kybertoimintaympäristössä. Joustavuudestaan huolimatta järjestelmä on eittämättä myös erittäin kompleksinen. Ei vähintään siksi, että eri alajärjestelmillä on omat organisatoriset käyttäjänsä. Järjestelmä on tarkoitettu yhtenäisen kansallisen informaatiotilan luomiseksi ja rajoittamiseksi valtiollista territoriaalista suvereniteettia noudatellen ja näin kehityksen äärimmäinen tulos on järjestelmän ja kansallisen segmentin sulautuminen – ja ”vapaan” tilan katoaminen. Järjestelmä ei kuitenkaan nykyisellään tavoita koko kybertoimintaympäristöä ja osa siitä jää todennäköisesti aina valtiovallan ulottumattomiin ja täten potentiaalisten uhkien lähteeksi.

3.5 Teoreettisen avoimen kansallisen verkon rakenne ja ominaispiirteet

Teoreettinen avoin kansallinen verkko perustuu tapaan, jolla Internettiä hallinnoitiin teknologisesti kehittyneissä länsimaissa 2010-luvun puolivälissä.[611] Verkon kuvaus perustuu aikalaislähteisiin, joista on päätelty ilmaistujen vahvuuksien ja heikkouksien kautta avoimen verkon ominaisuudet.[612] Lähteitä on täydennetty tekijän omilla

---

[611] Näitä ovat Saksa, Iso-Britannia, Ranska, Italia ja Espanja BKT:n perusteella (World Bank: *World Bank Open Data.* [https://data.worldbank.org], luettu 14.7.2020). *The Digital Economy and Society Indexin* perusteella eurooppalaista keskiarvoa tai hieman parempaa edustavat edellä mainituista Saksa, Iso-Britannia ja Ranska. Hajonta EU-maiden sisällä on suurta Itä- ja Keski-Euroopan maiden ollessa vähiten kehittyneitä. (European Commission: *Digital Economy and Society Index (DESI) 2020).* [https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi], luettu 14.7.2020).

[612] Työssä käytetyn kyberkirjallisuuden lisäksi muita avoimen kansallisen verkon määrittelyssä käytettyjä lähteitä ovat: International Telecommunication Union (ITU): *Global Cybersecurity Index & Cyberwellness Profiles*, April 2015. [https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf], luettu 15.9.2020; ENISA: *Critical Information Infrastructures Protection approaches in EU*, July 2015. [https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf], luettu 15.9.2020; Hitchens, Theresa & Goren, Nilsu: *International Cybersecurity Information Sharing Agreements*. University of Maryland Center for International & Security Studies, Maryland, 2017; European Commission: *Reports and Studies about Digital Economy and Society Index*, 2020. [https://ec.europa.eu/digital-single-market/en/reports-and-studies/76018/3650], luettu 14.7.2020; NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE): *Strategy and Governance* (verkkosivu). [https://ccdcoe.org/library/strategy-and-governance/], luettu 14.7.2020; Tikk, Eneken & Kerttunen, Mika (Eds.): *Routledge Handbook of International Cybersecurity*. Routledge, London and New York, 2020; Tikk-Ringas, Eneken (ed.): *Evolution of the Cyber Domain. The Implications for National and*

aikalaishavainnoilla. Aika- ja aluerajaus perustuu siihen, että Venäjä muodosti kansallisen internetsegmenttinsä rakennusohjelman perusperiaatteet suhteessa siihen, miten Internettiä hallinnoitiin Lännessä. Venäjän hanke on vastaus noissa hallintamuodoissa havaittuihin vahvuuksiin ja heikkouksiin informaatioturvallisuusdoktriinin ja Digitaalisen talouden ohjelman laadintatyön alkaessa vuoden 2015 tienoilla. Vaikka Yhdysvallat ovat Venäjän pääsuurvaltakilpailija, malli ei perustu suoraan Yhdysvaltoihin johtuen tämän erityisestä suhteesta Internetin kehitykseen ja taloudellisesta sekä tieteellisteknologisesta voimasta. Yhdysvaltojen käyttö mallin pohjana häivyttäisi näkyvistä sen tosiseikan, että muu maailma on hyvin riippuvainen sen yritysten tarjoamista informaatioteknologian tuotteista ja palveluista. Yhdysvaltojen käyttö johtaisi myös avoimen kansallisen verkon tiedustelu-, valvonta- ja informaatio-operaatiosuorituskykyjen yliarviointiin. Tästä syystä teoreettinen avoin verkko perustuu eurooppalaisiin valtioihin. Toki esimerkiksi Yhdysvaltojen liittolaisten kyky tukeutua sen suorituskykyihin on huomioitu avoimen verkon kuvauksessa kansainvälisen yhteistyön kautta. Lisäksi alla suoritettava suljettujen ja avoimien kansallisten verkkojen vertailu on tarkoitettu korostamaan Venäjän projektin asymmetrisia vaikutuksia. Se on tarkoituksellisesti kärjistävä ilmiön erityispiirteiden esiin tuomiseksi. Läntinen kyberturvallisuuspolitiikka on muuttunut 2010-luvun puolivälistä lähtien. Muutos huomioidaan alaluvun lopussa ja luvussa 5 tarkasteltaessa rakenteellisen kyberasymmetrian strategisia vaikutuksia sekä luvun 6 pohdinnoissa.

Vaikkakaan avoin kansallinen verkko ei ole samassa mielessä järjestelmien järjestelmä kuin kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä, sitä lähestytään alla Venäjän järjestelmän alajärjestelmien kautta. Nämä alajärjestelmät kattavat lähes kaikki maantieteellisesti rajatun kybertilan teknologiset, hallinnolliset, taloudelliset, normatiiviset, poliittiset ja turvallisuusaspektit. Lähestymistapa auttaa käsitteellistämään

---

Global Security. IISS, London, 2015; Centre for International Governance Innovation & IPSOS: *2014 CIGI-Ipsos Global Survey on Internet Security and Trust*. [https://www.cigionline.org/sites/default/files/documents/internet-survey-2014-factum.pdf], luettu 12.1.2021; OECD: *Digital Security Risk Management for Economic and Social Prosperity*. OECD Recommendation and Companion Document, 2015. [https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf], luettu 12.1.2021; ENISA: *Supply Chain Integrity. An overview of the ICT supply chain risks and challenges, and vision for the way forward*, Version 1.1, August 2015 [https://www.enisa.europa.eu/publications/sci-2015/at_download/fullReport], luettu 12.1.2021.

kansalliset verkot teknologisia ilmiöitä laajempina kokonaisuuksina ja helpottaa niiden vertailua, vaikka ne eroaisivat toisistaan voimakkaasti. Avoimen kansallisen verkon malli on siis yksinkertaistus, mutta sen funktio onkin korostaa kahden erilaisen verkon erilaisuutta ja samankaltaisuuksia.

Avoimen kansallisen verkon tieteellisteknologinen perusta perustuu pääosin kansallisten ja kansainvälisten yksityisyritysten tuotekehittelylle ja tuotannolle. Valtiolla on rooli tieteellisessä kehitystyössä innovaatiotukien ja yliopistojen sekä tiedeinstituuttien rahoituksen kautta, mutta näidenkin osalta yksityisiltä sijoittajilta ja tukijoilta kerättävän rahoituksen osuus on merkittävä. ICT-markkinat ovat avoimet. Vain valtionhallinnossa ja asevoimissa on rajoituksia ulkomaisten ohjelmistojen tai laitteiden käytön osalta. Rajoitukset koskevat harvoin kaikkia ulkomaisia tuotteita. Avoin lähdekoodi nähdään pääsääntöisesti positiivisena asiana, mutta yritykset käyttävät pääsääntöisesti kansainvälisten yritysten tuottamia ohjelmistoja hallinnolliseen johtamiseensa. Yksityisten kansalaisten osalta käytetty ohjelmistokirjo on laajempi. Haavoittuvuuksia pyritään ehkäisemään ja tuotantoketjuja suojelemaan sopimusten, tiedonvaihdon ja luotettujen kumppanien avulla. ICT-talouden keskinäisriippuvuudet hyväksytään ja kansainvälinen yhteistyö nähdään positiivisena asiana. Haasteena on julkisen ja yksityisen puolen toimittaja- ja palveluntarjoajaverkoston pirstaloituminen. Komponenttituotannon osalta valtiolla ei ole resursseja tai halua pyrkiä kotimaisuuteen kuin joillain erittäin kapeilla sektoreilla. Turvallisuuspalvelujen kyky laaja-alaisesti tunkeutua käytettyihin ohjelmistoihin tai laitteistoihin tuotantoketjujen kautta ilman kansainvälistä julkisen ja yksityisen sektorin yhteistyötä on rajoittunut.

Avoimessa kansallisessa verkossa ei käytetä laajamittaisesti kansallisia salaus- tai autentikointipalveluita. Niiden merkitys valtion turvallisuudelle on kuitenkin tiedostettu ja kriittisillä turvallisuusaloilla on käytössä kansallisia tai liittolaisten kanssa yhdessä tuotettuja järjestelmiä. ISP:t suojaavat oman liikenteensä ja järjestelmänsä kansainvälisten yritysten ratkaisuilla. Talous- ja finanssialalla käytetään laajasti kaupallisia, pääsääntöisesti kansainvälisiä, ratkaisuja. Kansalaisyhteiskunta käyttää aktiivisesti kansainvälisten yritysten tarjoamia salauspalveluja, joista ainakin osa perustuu avoimeen lähdekoodiin. Turvallisuuspalveluilla on lainsäädännön mukaan lupa seurata ja purkaa salattua liikennettä sekä hankkia tietoja valtion kansalaisista. Niiden suorituskyvyt ovat kuitenkin rajoittuneet. Yrityksillä on velvollisuus luovuttaa käyttäjien tietoja turvallisuuspalveluille, mutta salatun tiedon avaaminen vaatii läpinäkyvän oikeusprosessin tai on teknisesti mahdotonta yritykselle itselleenkin. Avoin kansallinen verkko ei ole läpinäkyvä turvallisuuspalveluille.

Avoimessa kansallisessa verkossa ei ole keskitettyä sensuurijärjestelmää. Materiaalin poistamiselle, suodattamiselle tai pääsyn estämiselle ei ole luotu valtiojohtoista järjestelmää, johon palvelun- tai sisällöntarjoajat (vast.) olisi velvoitettu osallistumaan. Lainsäädäntö voi kieltää määrätyn hyvin rajoitetun sisällön levittämisen tai tietoliikenteen rikolliset käyttötarkoitukset. Materiaalin poistaminen kansallisista palveluista on mahdollista toteuttaa oikeusprosessin kautta, kansainvälisten palveluiden osalta materiaalin poistaminen on vaikeaa ja hidasta. Kansalaisten vapaaehtoisella toiminnalla ei ole suurta roolia. Poliittinen itsesensuuri on vähäistä.

Avoimessa kansallisessa verkossa tiedustelupalveluilla on käytössään kohdennettuja tiedonkeruujärjestelmiä tarkasti rajattuja kansalliseen turvallisuuteen tai rikostutkintaa liittyviä tehtäviä varten. Niiden käyttö vaatii tapauskohtaisen oikeuden tai hallinnollisen päätöksen ja turvallisuuspalvelujen toimintaa valvotaan parlamentaarisesti. Avoimissa verkoissa ei kerätä ja säilytetä massamaisesti dataa valtion omista kansalaisista valtion turvallisuuden takaamiseksi, kaupallisista syistä kylläkin. Kansalaisia koskevia tietoja ei ole velvollisuutta säilyttää näiden kotimaassa, mutta henkilötietojen ja henkilöön liittyvän datan käyttöä säädellään enenevässä määrin sopimusteitse. Suuri osa talous- ja finanssialalle sekä yhteiskunnan elintärkeille toiminnoille välttämättömästä datasta sijaitsee valtion rajojen ulkopuolella. Turvallisuuspalveluiden kyky valvoa kansallista verkkoa omilla järjestelmillään on rajoittunut. Ulkomaantiedustelupalveluilla on kyky kohdennettuun ulkomaan tietoverkko- ja -järjestelmätiedusteluun ja ne vaihtavat tietoja liittolaisvaltioiden organisaatioiden kanssa.

Avoimen kansallisen verkon kriittinen informaatioinfrastruktuuri on yksityissektorin hallussa. Valtionhallinnon kriittiset informaatiopalvelut on isolta osin ulkoistettu. Kriittistä informaatioinfrastruktuuria on kartoitettu, mutta sen turvaamista säädellään lähinnä palvelusopimusten ehdoilla. Valtio voi tukea kriittisen informaatioinfrastruktuurin kehityshankkeita, mutta järjestelmien kahdentaminen perustuu liiketaloudellisiin tekijöihin. Järjestely voi johtaa merkittäviin riskeihin yksittäisten kriittisten yhdyspisteiden tai järjestelmien osalta. Avoimeen kansalliseen verkkoon voi kuulua valtionhallinnolle omistettuja datakeskuksia, joiden kapasiteetti on kuitenkin rajallinen ja rajoitettu hallinnon turvaluokitellun datan säilyttämiseen. Pääosa kapasiteetista vuokrataan yksityisiltä toimijoilta. Avoin kansallinen verkko on toimivuudeltaan hyvin riippuvainen valtion rajojen ulkopuolella sijaitsevista palveluista, eikä verkkoa voida irrottaa globaalista Internetistä ilman merkittäviä ja pitkäkestoisia yhteyskatkoksia, toimintahäiriöitä ja palvelualenemia.

Valtiot, joiden kansallinen verkko on avoin, mediatila on vapaa ja poliittinen järjestelmä demokraattinen. Uutispalvelut ovat yksityisessä omistuksessa, eikä ulkomaisten uutispalveluiden toimintaa ole merkittävästi rajoitettu. Valtiot tukevat lähtökohtaisesti Yhdysvaltojen ja ”saman mielisten” kyberdiplomatiaa. Vastapuolena on Venäjän ja Kiinan ajama malli.[613] Valtioilla ei ole vahvaa omaa agendaa, vaan diplomatiaa toimeenpannaan liittoumien tai liittokuntien kautta (EU/Nato). Liittoumat eivät ole aina yhtenäisiä kannoissaan. Avoimien kansallisten verkkojen valtioiden ”vastatoimet” perustuvat pehmeään voimaan, strategiseen kommunikaatioon ja räätälöityihin informaatio-operaatioihin, joita ulkomaan tiedustelupalvelut tukevat. Nämä operaatiot ja niiden yhteydet regiiminvaihto-operaatioihin koetaan kielteisiksi, eikä niistä yleensä kerrota julkisuuteen.[614] Kyber- ja informaatiosuorituskyvyt on sotataidollisesti sidottu osaksi sotilasoperaatioita ja niiden strateginen käyttö koetaan alikehittyneeksi tai kilpailijoista jälkeen jääneeksi.[615] Toisaalta tiedusteluyhteistyö Naton, EU:n ja bilateriaalisten kumppanuuksien (etenkin Yhdysvaltojen kanssa) kehyksessä mahdollistaa laajamittaisen ulkomaan verkkotiedustelun.[616] Resurssit ovat tosin rajalliset, samoin tavoitteet. Tiedustelupalveluiden operaatiot perustuvat lakiin ja niiden toimintaa rajoittaa tiukka hallinnollinen ja kansalaisyhteiskunnan valvonta. Kyberpuolustus nähdään puolustuksellisena ja hyökkäysoperaatioiden toteuttaminen on poliittisesti hankalaa. Tästä huolimatta asevoimien kybersuorituskyvyt nähdään enenevässä määrin osana normaalia sodankuvaa.[617]

---

[613] Broeders, Dennis & van den Berg, Bibi (eds.): *Governing Cyberspace. Behavior, Power, and Diplomacy*. Rowman & Littlefield, Lanham, Maryland, 2020.
[614] Rid (2020); O’Rourke (2018).
[615] Inglis, John C., Lumpkin, Michael D., Waltzman, Rand & Watts, Clint: *Cyber-enabled Information Operations*. Subcommittee on Cybersecurity, Committee on Armed Services, United States Senate, One Hundred Fifteenth Congress, First Session, April 27, 2017. [https://www.hsdl.org/?view&did=802817], luettu 21.2.2021; European Parliament: *Cyber defence in the EU Preparing for cyber warfare?* Briefing, October 2014. [https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf], luettu 21.2.2021; Paul, Christopher, Clarke, Colin P., Schwille, Michael, Hlavka, Jakub P., Brown, Michael A., Davenport, Steven, Porche, Isaac R. III & Harding, Joel: *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment*. RAND, Santa Monica, 2018. [https://www.rand.org/pubs/research_reports/RR1925z1.html], luettu 21.2.2021.
[616] Kilcullen (2020), s. 76–77.
[617] NATO: *Wales Summit Declaration*. Press Release (2014) 120, Issued on 05 Sep. 2014. [https://www.nato.int/cps/en/natohq/official_texts_112964.htm], luettu 19.2.2021.

Tietoliikennetiedustelutietojen jakaminen ns. Five-Eyes-maiden välillä on normaalia ja Nato-jäsenmaiden piirissä vähintään tavoitetila.[618]

Avoimissa verkoissa ei ole keskitettyä hallinta-, kontrolli-, valvonta- ja palautejärjestelmää. Niissä voi olla kansallinen tietoturvauhkien monitorointijärjestelmä (Einstein, Havaro), jonka käyttöönotto on kuitenkin yksityissektorilla vapaaehtoista, eikä se parhaassakaan tapauksessa kata kaikkia kriittisiä aloja. Pääasiassa kansallisen tason tietoturvapoikkeamien valvonta- ja reagointijärjestelmä perustuu kansallisen CSIRT/CERT ja yksityistoimijoiden yhteistyöhön ja tiedonjakoon.[619] Vastuu- ja toimivaltuuskysymykset ovat osittain määrittelemättömät ja julkisen vallan kyky puuttua yksityistoimijoiden toimintaan on erittäin rajoittunut. Kyberturvallisuuden osalta puuttuu yksi kansallinen toimija, joka vastaisi julkishallinnon ja valtionyritysten verkkojen tietoturvasta ja valtiolle kriittisten yksityisten toimijoiden tietoturvan valvonnasta. Lisäksi julkinen sektori on järjestelmiltään ja tietoturvaratkaisuiltaan siiloutunut. Viranomaiset harjoittelevat yhteistoimintaa jonkin verran kansallisella tasolla. Yksityiset tahot ovat rajoitetusti mukana mm. liikesalaisuus- ja kilpailusyistä. Kansalliset tietoturvaviranomaiset ovat verkottuneet mm. EU:n kehyksessä ja vaihtavat tietoa keskenään.[620] Kyberrikosten torjunnan osalta viranomaisten ja yksityisten toimijoiden yhteistyö on toimivaa, mutta edelleen kehitysasteella.[621]

Asevoimien verkot ja järjestelmät ovat kiinteä osa avoimia kansallisia verkkoja. Asevoimilla ei ole resursseja erottaa kaikkia kiinteitä tietoverkkojaan ja -järjestelmiään yksityisten palveluntarjoajien verkoista. Erottaminen perustuukin pääosin palvelusopimuksiin ja loogisen tason toimintoihin. Monet asevoimien hallinnollisista yhteyksistä on ulkoistettu

---

[618] Ibid.; Gold, Josh: *The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'*. NATO CCD COE, Tallinn, 2020. [https://ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf], luettu 19.2.2021.

[619] ENISA: *CSIRTs by Country - Interactive Map.* [https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map], luettu 10.7.2020.

[620] ENISA: *EU Member States incident response development status report*, November 27, 2019 [https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report], luettu 10.7.2020.

[621] ENISA: *An overview on enhancing technical cooperation between CSIRTs and LE*, May 07, 2020. [https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-tools-for-enhancing-cooperation-between-csirts-and-le], luettu 10.7.2020.

ja yhteiskäytössä muiden viranomaisten kanssa. Asevoimat operoi itse kriittisimpiä yhteyksiä ja järjestelmiä (ml. ydinaseet) ja ne pyrkivät kahdentamaan tärkeimmät järjestelmänsä ja yhteytensä. Kenttäviestijärjestelmät ovat pääosin asevoimien hallussa ja erillisiä julkisista televerkoista. Asevoimilla on rajoittunut kyky hyökkäyksellisiin ja puolustuksellisiin kyberoperaatioihin. Avoimien verkkojen valtioiden asevoimien toimintalogiikka ei siis varsinaisesti eroa Venäjän asevoimien tahtotilasta, mutta resurssit ja toimivaltuudet ovat selkeästi rajatummat.

Läntisten valtioiden suhde Internettiin ja kybertilaan laajemmin on alkanut muuttua merkittävästi 2010-luvun puolivälistä alkaen. Muutos johtuu useasta tekijästä. Yhdysvallat perusti asevoimien kyberjoukot vuonna 2009, kansainvälisen terrorismin vastainen taistelu siirtyi osiltaan kybertoimintaympäristöön, Edward Snowden paljasti NSA kybervakoiluohjelman 2013, Kiinan teollisuusvakoilu ylitti Yhdysvaltojen kipukynnyksen samalla, kun suurvaltojen voimatasapaino alkoi kääntyä ja Ukrainan sodan seuraukset tehostivat Venäjän vaikutusoperaatioita Länttä kohtaan.[622] Esimerkiksi IoT (*Internet of Things*) ja 5G -teknologiaan ja tuotantoketjuihin liittyvät uhat ovat kiristäneet markkinoiden säätelyä.[623] Useat valtiot pyrkivät vähintään rajattuun omavaraisuuteen kryptografian, laitteistojen ja ohjelmistojen osalta.[624] Kansalliseen kyberturvallisuuteen kuuluu lisääntyvässä määrin haitallisten tai vaarallisten sivustojen ja palveluiden blokkaaminen sekä vaatimukset ylikansallisille yrityksille määrätyn materiaalin poistamisesta.[625] Valtioittain tai alueittain laaditaan tietosuojalainsäädäntöä, joka pyrkii lokalisoimaan käyttäjien ja yritysten datan. Kriittisen datan päätymistä rajojen ulkopuolelle pyritään ehkäisemään rakentamalla kansallisia palvelinkeskuksia.[626] Kansallisia

---

[622] Viime vuosien tapahtumista ks. Kaplan (2016); Rid (2017); Sanger (2019); Greenberg, Andy: *Sandworm. A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday, New York, 2019.

[623] NIS Cooperation Group: *EU coordinated risk assessment of the cybersecurity of 5G networks*, 9 October 2019 [https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132], luettu 12.1.2021.

[624] Ks. EU-maiden kyberstrategiat osoitteesta: ENISA: *National Cyber Security Strategies - Interactive Map* [https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map], luettu 12.1.2021.

[625] Scott, Mark: Welcome to New Era of Global Digital Censorship. It's Dangerous to Ask Tech Companies to Decide What's Legitimate Free Speech. *Politico*, January 14, 2018. [https://www.politico.eu/article/google-facebook-twitter-censorship-europe-commission-hate-speech-propaganda-terrorist/], luettu 12.1.2021.

[626] Knight, Ben: German Data Storage Laws 'threaten free trade'. *DW*, 12.1.2017. [https://www.dw.com/en/german-data-storage-laws-threaten-free-trade/a-37110699],

yksityisiä ja julkisia CERT/CSIRT:eja ohjataan yhteistyöhön ja monet maat rakentavat kansallista kyberturvallisuuden johtamisjärjestelmää.[627] Asevoimien ja tiedustelupalveluiden kybersuorituskykyjä halutaan enenevissä määrin käyttää ”aktiiviseen deterrenssiin” puolustustehtävien sijaan ja tiedustelupalveluille kehitetään parempaa ja kattavampaa kykyä ulkomaan tietoverkko- ja järjestelmätiedusteluun.[628] Kybersodankäynnin sijaan puhutaan yhä enemmän tarpeesta kehittää kyberavusteisia informaatio-operaatioita (*cyber-enabled information operations*).[629]

Monet edellä mainituista hankkeista ovat vapaaehtoisia ja perustuvat yksityissektorin ja julkishallinnon yhteistyöhön. Niiden juuret ovat kuitenkin selkeästi kansallisissa turvallisuusintresseissä. Intressien suojelu vaikuttaisi myös ajavan läntisiä maita omaksumaan jonkinlaisen version kybersuvereniteetista. Valtiosuvereniteetti on kiinnittymässä informaatioinfrastruktuuriin, jonka katsotaan olevan valtion toiminnanvapauden ja itsenäisyyden lähde.[630] Samaan aikaan kyberuhat ja

---

luettu 12.1.2021; European Commission: *A European strategy for data*. COM(2020) 66 final, 19.2.2020. [https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066], luettu 12.1.2021.

627 ENISA: *Study on CSIRT landscape and IR capabilities in Europe 2025*, February 2019 [https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025/at_download/fullReport], luettu 12.1.2021.

628 Davis, Susan: NATO in The Cyber Age: Strengthening Security & Defence, Stabilising Deterrence. NATO Parliamentary Assembly, Science And Technology Committee (STC) 13 August 2019. [https://www.nato-pa.int/download-file?filename=sites/default/files/2019-09/148%20STC%20Davis%20-%20NATO%20IN%20THE%20CYBER%20AGE%20-%20fall%20revision%20-%20clean%2011.9.19.pdf], luettu 12.1.2021; Pernik, Piret: National Cyber Commands. Teoksessa *Routledge Handbook of International Cybersecurity*. Tikk, Eneken & Kerttunen, Mika (eds.) Routledge, London, 2020; Lubin, Asaf: A New Era of Mass Surveillance is Emerging Across Europe. *Just Security*, January 9, 2017 [https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe/], luettu 12.1.2021.

629 Congressional Research Service: *Defense Primer: Information Operations, Updated December 15, 2020*. [https://fas.org/sgp/crs/natsec/IF10771.pdf], luettu 21.2.2021.

630 Eneken & Kerttunen (2020); Madiega, Tambiama: *Digital sovereignty for Europe*. European Parliament, July 2020. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf], luettu 17.10.2020; Hobbs, Carla (ed.): *Europe's Digital Sovereignty: From Rulemaker To Superpower In The Age Of Us-China Rivalry*. European Council on Foreign Relations, July 2020. [https://www.ecfr.eu/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf], luettu 17.10.2020; European Commission (2020).

laajemmin informaatiouhat nähdään enenevässä määrin "kansallisina hätätiloina", joiden selvittäminen edellyttää poikkihallinnollista ja koko yhteiskunnan varat mobilisoivaa resilienssiä tai jopa "siviilipuolustusta."[631] Näin ollen avoimien kansallisten verkkojen luonne on muuttumassa ja on hyvin mahdollista, että seuraavassa luvussa esitettävä rakenteellisen kyberasymmetrian analyysi ei enää 2030-luvulla ole sellaisenaan paikkaansa pitävä.

[631] Austin, Greg & Sharma, Munish: From Cyber Resilience to Civil Defence. Teoksessa *National Cyber Emergencies*. Austin, Greg (ed.) Routledge, London & Newy York, 2020, s. 10–30, s. 26–27.

4 Asymmetrian analyysi

Tässä luvussa analysoidaan Venäjän kansallisen internetsegmentin tapauksesta johdetun suljetun kansallisen verkon ja teoreettisen avoimen kansallisen verkon välisestä suhteesta muodostuvaa rakenteellista kyberasymmetriaa. Analyysi on muodoltaan laadullinen ja perustuu abduktiiviseen päättelyyn kansallisten verkkojen kuvausten ja kyberasymmetriaan liittyvän teorian rajapinnassa. Luvun päälähteinä ovat aikaisempien lukujen esittelemät havainnot, käsitteet ja teoriat. Analyysin pääkäsitteitä ovat aikaisemmin muodostetut toiminnan vapauden, yhteisen tilannekuvan, johtamisen ja resilienssin käsitteet. Analyysissä käytetyt hyökkääjän ja puolustajan käsitteet liittyvät valtiotoimijoihin tai niiden sijaistoimijoihin. Tarkastelu keskittyy siis valtioihin.

Luvun ensimmäisessä osassa täydennetään Kukkolan, Ristolaisen ja Nikkarilan aikaisempaa hyökkäysvektoreihin perustuvaa tarkastelua uusien ja edelleen kehitettyjen käsitteiden avulla.[632] Toisessa osassa tarkastellaan suljettua ja avointa kansallista verkkoa luvussa kolme esitellyn kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmän alajärjestelmien kautta käyttäen toiminnan vapauden, yhteisen tilannekuvan, johtamisen ja resilienssin käsitteitä verkkojen vertailuun. Tavoitteena on saada verkkojen väliset sisäiset rakenteelliset erot paremmin esille. Kolmannessa osassa suljettua ja avointa kansallista verkkoa verrataan valtiosuhteiden kehityksen eri vaiheissa. Tavoitteen on tuoda esiin verkkojen muutoksen vaikutukset niiden väliseen suhteeseen. Neljännessä osassa suoritetaan yhteenveto ja pohditaan rakenteellisesta kyberasymmetriasta nousseita havaintoja, joita käytetään luvussa viisi asymmetrian strategisten vaikutusten arviointiin. Tässä luvussa esitetty rakenteellisen kyberasymmetrian analyysi perustuu yhdestä tapaustutkimuksesta yleistettyyn malliin eli Venäjän valtioon ja sen kansallisen internetsegmentin hankkeeseen. Malli on siis induktiivinen, kompleksinen, inhimillinen, teknologinen ja poliittinen.[633] Edelleen on huomattava, että teoreettista avointa verkkoa ei sellaisenaan ole olemassa vaan se on yleistys määrätystä ajan hetkestä. Avoimien verkkojen muutokseen palataan luvussa 6.

---

[632] Kukkola, Ristolainen & Nikkarila (2017).

[633] Jervis, Robert: Complexity and the Analysis of Political and Social Life. *Political Science Quarterly*, Vol. 112, No. 4 (Winter, 1997-1998), s. 569–593, s. 578.

4.1 Suljetun ja avoimen kansallisen verkon väliset hyökkäysvektorit

Luvussa kaksi on esitetty aikaisemmassa tutkimuksessa suoritettu hyökkäysvektorianalyysi. Kukkola, Ristolainen ja Nikkarila tiivistävät sen tulokset seuraavasti: ”Olemme analyysissämme osoittaneet, että suljetun verkon sisäiset rintamalinjat, mahdollisuus kokonaan irti kytkeä suljettu verkko muista verkoista sekä suhteellinen toiminnanvapaus avoimien verkkojen yhteiskunnissa luovat kyberasymmetriaa, mikä suosii valtiota, joka sulkee verkkonsa. Sillä on suurempi tilannetietoisuus, nopeampi päätöksentekosykli ja enemmän liikkeen vapautta kuin avoimen verkon yhteiskunnalla. Se voi hyökätä missä ja milloin haluaa.”[634] Tässä luvussa aikaisempaa analyysiä täydennetään lisäämällä tarkasteluun resilienssin käsite ja jatkokehittämällä analyysiä luvussa 2.5 tarkennettujen toiminnan vapauden, yhteisen tilannekuvan ja johtamisen käsitteiden kautta. Hyökkäysvektoreina toimivat aikaisemman analyysin tunnistamat liikenteelle virallisesti osoitetut yhteydet, epäviralliset yhteydet, kolmannen tahon verkot tai sisäiset ns. sisäpiirihyökkäykset. Aikaisempaa analyysiä ei tässä toisteta, vaan alla on esitetty pelkästään uudet havainnot.[635]

Alkuperäinen hyökkäysvektorianalyysi tarkasteli toiminnan vapautta kansallisten verkkojen liityntöjen ja sisäisten rajapintojen läpäisynä. Aikaisemmin esitetty täydennetty toiminnan vapauden määritelmä laajentaa analyysia tilan muokkaamisen ja hallinnan tarkasteluun. Suljetun kansallisen verkon puolustaja pystyy kansallisella tasolla verkkoa muokkaamalla joustavasti ja vastustajan toimintaan sopeutuen kiistämään hyökkääjän toiminnan vapauden. Osia kansallisesta verkosta voidaan sulkea, yhteyksiä voidaan muuttaa ja liikenteeseen puuttua helpommin kuin avoimissa verkoissa. Hyökkääjän toiminnan vapaus voidaan myös kiistää korjaamalla haavoittuvuuksia keskitetysti ja suhteellisen nopeasti. Edellä mainittuja ominaisuuksia esiintyy avoimissa kansallisissa verkoissa vain toisistaan erillisissä ja eri tahojen hallinnoimissa sisäverkoissa. Suljetussa kansallisessa verkossa on myös avoimia verkkoja merkittävästi vähemmän sisäisiä hallinnollisia tai liiketaloudellisia rajapintoja, joihin kansallisen verkon turvallisuudesta vastaavilla ei olisi pääsyä. Avoimen verkon puolustajalla ei siis ole toiminnan vapautta, koska sillä on pääsy

[634] Kukkola, Ristolainen & Nikkarila (2017), s. 103.
[635] Aikaisemman analyysin tuloksista ks. luvut 2.4 ja 2.5.

vain murto-osaan tärkeistä avoimen verkon osaverkoista ja yhteyksistä. Suljetun verkon puolustaja kykenee liikkumaan omassa verkossaan melko vapaasti ja se voi olla ennalta ehkäisevästi läsnä mahdollisissa kohdejärjestelmissä sen sijaan, että puolustustoimet aloitettaisiin reagoimalla vihollisen vaikutukseen päässeeseen hyökkäykseen. Lisäksi suljetun kansallisen verkon ohjelmistot ja laitteistot todennäköisesti poikkeavat hyökkääjän vastaavista. Hyökkääjä joutuu toimimaan poikkeavassa ympäristössä ja käyttämään merkittävästi aikaa ja resursseja takaisinmallinnukseen. Lisäksi suljetussa verkossa turvallisuusjärjestelmiä on useassa tasossa, eikä jonkin ulkoyhteyden menestyksekäs käyttö vielä takaa pääsyä kohteelle. Hyökkääjien on myös pyrittävä yhä nopeampaan vaikutukseen, koska suljetuissa verkoissa piileskely muuttuu vaikeammaksi ja tiedustelutoiminta voi helpommin paljastaa operaation.

Suljettu verkko ei ole kuitenkaan aukoton. Suljettuun verkkoon hyökkäävän näkökulmasta mahdollisuus vaikuttaa kohteeseen korostuu liikkeen vapautta enemmän. Kohdejärjestelmiin voidaan vaikuttaa useilla eri tavoilla, eikä siihen välttämättä tarvita suoraa, jatkuvasti ylläpidettävää pääsyä kohteelle ja sen manipulointia. Tunnistettujen hyökkäysvektoreiden sulkeminen ei poista kaikkia mahdollisia vektoreita. Osa suljetun verkon puolustusjärjestelmistä voidaan kiertää tai ohittaa. Avoimen hyökkääjän kyky käyttäjien manipulointiin ja sisäpiirihyökkäysten käyttöön korostuu entisestään. Hyökkääjä voi lisäksi muokata kybertilaa tai saada puolustaja muokkaamaan sitä haluamallaan tavalla. Tämä on oleellinen heikkous suljetuissa kansallisissa verkoissa. Niiden hallintajärjestelmät, suljetut ekosysteemit ja verkkojen keskinäisriippuvuudet voivat synnyttää hyökkääjälle hyödyllisiä heijaste- ja kerrannaisvaikutuksia ja näin avata uusia hyökkäysvektoreita. Toinen heikkous liittyy suljetun kansallisen verkon ulkoyhteyksien toteutukseen. Jos se perustuu vain muutamaan virallisesti osoitettuun yhteyteen, niistä muodostuu kriittinen haavoittuvuus, mikäli valtion pääsy globaaliin Internetiin halutaan estää ulkopuolelta. Jos taas yhteyksiä on useita, niiden valvonta keskitetysti ilman yksityissektorin osallistamista on haastavaa. Yksityissektorin osallistuminen taas lisää järjestelmän toimivuuden epävarmuutta etenkin kriisitilanteessa. Edellä todetut heikkoudet eivät varsinaisesti vaikuta aikaisemman analyysin tuloksiin. Ne kuitenkin painottavat tilan sisäisen hallinnan tärkeyttä rajojen hallinnan rinnalla ja korostavat suljetun verkon onnistuneen ulkoyhteyksien hallinnan vaatimuksia.

Yhteisen tilannekuvan käyttö hyökkäysvektorianalyysin välineenä tilannetietoisuuden sijaan ei merkittävästi vaikuta aikaisempiin tutkimustuloksiin, sillä alkuperäinen analyysi itse asiassa tarkasteli tilannekuvaa, ei tietoisuutta. Uuden käsitteen soveltaminen mahdollistaa

kuitenkin tarkemman käsityksen saamisen suljetun ja avoimen verkon suhteesta. Suljetun verkon puolustajan yhteinen tilannekuva on kiistämättä parempi kuin avoimen verkon puolustajan. Edellisellä on käytössään organisaatio, prosessit, tietomallit ja tietovirrat kansallisen kybertilannekuvan[636] luomiseksi. Avoimessa kansallisessa verkossa puolustajalla ei ole mahdollisuutta samanlaiseen tietofuusioon. Lisäksi suljetun verkon puolustaja kykenee keräämään tietoa koko verkon syvyydeltä usealta tasolta. Sillä on kansallisen verkon kaikissa osissa sensoreita, joiden tuottama data kyetään analysoimaan automatisoiduilla järjestelmillä. Avoimen verkon puolustajalla voi olla samanlaisia järjestelmiä, mutta ne eivät vaihda tai vaihtavat vain rajoitetusti tietoa keskenään, eikä yhteistä tilannekuvaa synny. Suljetun verkon yhteydet ja liitynnät ovat yhteisen tilannekuvan takia huomattavasti paremmin valvotut kuin avoimen.

Periaatteessa suljettuun verkkoon hyökkäävän täytyy kiinnittää erityistä huomiota jälkiensä peittämiseen, taktiikoiden muunteluun ja ainutkertaisten haavoittuvuuksien tai täysin uusien hyökkäystapojen käyttämiseen. Näin siksi, että suljetun verkon puolustaja kerää ja analysoi keskitetysti tilannekuvaa koko järjestelmästä. Lisäksi suljettuun verkkoon hyökkäävän yhteistä tilannekuvaa rajoittavat tilan muuttuva luonne, kansalliset laitteisto- ja ohjelmistoratkaisut ja puolustajan aktiivinen harhauttaminen ja vastaoperaatiot. Avoimessa verkossa nämä samat ominaisuudet esiintyvät sirpaloituneina, toisistaan riippumattomina ja yksityisten intressien ohjaamina. Suljetun verkon puolustajalla on siis täydellisempi ja ajankohtaisempi tilannekuva omasta ja vastustajan toiminnasta kuin avoimen verkon puolustajalla.

Vaikka tilannekuvan jakaminen suljetussa kansallisessa verkossa on yksi järjestelmän tarjoamista päähyödyistä, ei jakamisen toteutuminen ole täysin varmaa. Hallinnon siiloutuminen voi heikentää teknisten ratkaisujen toimivuutta. Tekniset järjestelmät eivät myöskään täysin varmista sitä, että

---

[636] Kybertilannekuva sisältää teknisen järjestelmä- ja verkonkuvan, potentiaaliset uhat, tunnistetut hyökkäykset sekä käynnistetyt vastatoimet sekä organisaation kybertoimintaympäristöön vaikuttavan nykyisen ja tulevan toiminnan (Pahi, T., Leitner, M & Skopik, F.: Preparation, Modelling, and Visualisation of Cyber Common Operating Pictures for National Cyber Security Centres. *Journal of Information Warfare*, Vol. 16, No. 4 (Fall 2017), s, 26-4; Conti, Gregory, Nelson, John & Raymond, David: Towards a Cyber Common Operating Picture. Teoksessa *2013 5th International Conference on Cyber Conflict*. Podins, K., Stinissen, J. & Maybaum, M. (Eds.) NATO CCD COE Publications, Tallinn, 2013, s. 179–295.

päätöksentekijöille muodostuu oikea tilanneymmärrys. Automatisoituja ja tekoälyyn perustuvia järjestelmiä voidaan harhauttaa. Avoimet verkot eivät myöskään ole täysin vailla hyödyllisiä piirteitä. Avoimeen verkkoon kohdistuvaa tiedustelua vaikeuttaa esimerkiksi osa- ja aliverkkojen järjestelmien tietosuojakäytäntöjen moninaisuus. Rajoituksista huolimatta avoimeen kansalliseen verkkoon hyökkäävän tilannekuva on suhteellisesti parempi kuin suljettuun verkkoon hyökkäävän.

Hyökkäysvektorianalyysissä päätöksenteon korvaaminen johtamisen käsitteellä syventää analyysiä, muttei muuta aikaisemman tutkimuksen tuloksia. Näin siksi, että aikaisempi analyysi keskittyi tarkastelemaan päätöksentekoon käytössä olevan tiedon saatavuutta ja toimeenpanon nopeutta sekä tehokkuutta. Ne ovat itse asiassa ovat johtamisjärjestelmän, eivät päätöksenteon, ominaisuuksia. Johtamisen käsite kuitenkin ohjaa huomion teknologiaan, organisaatioon ja toimintatapoihin. Suljetun verkon puolustus perustuu keskitettyyn johtamisjärjestelmään, jonka mahdollistaa korkeatasoinen yhteinen tilannekuva sekä alempiin tasoihin rakennetut johtamisyhteydet. Järjestelmällä on hierarkkinen rakenne, jossa eri järjestelmien johtamistasot kohtaavat samoissa pisteissä - käytännössä turvallisuusviranomaisten verkonvalvontakeskuksissa. Keskitettyyn johtamisjärjestelmään liittyy olennaisesti organisoitu koneoppimiseen perustuva tiedonhallinta, jonka ehkäisee informaation liiallisen määrän aiheuttamia haasteita. Järjestelmän onkin oltava pitkälle automatisoitu. Johtamisjärjestelmä mahdollistaa suljetun kansallisen verkon ulkoisten ja sisäisten liittymien tehokkaan ja nopean hallinnan. Näin ollen suljettuun verkkoon hyökkääjän haasteeksi muodostuu se, että hyökkääjän on vaikeampia käyttää hyväkseen teknologisia ja organisatorisia rajapintoja. Puolustajia on nimittäin käytännössä yksi. Lisäksi puolustaja kykenee reagoimaan eri vektoreista tuleviin hyökkäyksiin varsin nopeasti. Hyökkääjän on myös jatkuvasti suojeltava omia johtamisyhteyksiään, mikä edellyttää monimutkaisempaa operaatiota suljetun verkon yhteyksien ollessa valvottuja.

Käytännössä suljetun verkon johtamisessa voi esiintyä kriittisiä haavoittuvuuksia. Johtamisjärjestelmä voi sirpaloitua byrokraattisista tai teknologisista syistä. Suljetun kansallisen verkon johtamisjärjestelmä voi täten käytännössä siiloutua ja yhdistyä vasta hierarkian huipulla. Tällöin suuri osa suljetun verkon johtamisen tarjoamista eduista menetetään. Lisäksi hyökkääjä voi päästä käsiksi suljetun verkon johtamisjärjestelmään, mikä mahdollistaa koko suljetun verkon sabotoinnin tai hyökkääjän toiminnan salaamisen.

Avoimen kansallisen verkon puolustajalta puuttuu kansallinen johtamisjärjestelmä. Sen johtaminen perustuu erillisiin järjestelmiin, jotka vaihtavat tietoa rajallisesti keskenään. Reagointi hyökkäyksiin tapahtuu siiloissa ja merkittävällä viiveellä etenkin silloin, kun hyökkäykset ylittävät johtamisjärjestelmien rajat. Uhkatietoa voidaan pantata viranomaisilta tai kumppaneilta taloudellisista tai poliittisista syistä. Avoimen verkon järjestelmä ei myöskään kykene kokonaisuutena muuntautumaan hyökkäysten mukana. Toisaalta sen johtamisjärjestelmä ei ole yhtä haavoittuvainen siihen itseensä kohdistuville hyökkäyksille kuin suljetun verkon järjestelmä johtuen toisistaan poikkeavista moninaisista teknologisista ratkaisuista ja verkkojen segmentoinnista. Yhtä kaikki suljetun verkon johtamisjärjestelmä mahdollistaa yhteyksien ja liityntöjen sulkemisen tavalla, johon avoimen verkon puolustajalla ei ole mahdollisuutta.

Resilienssin lisääminen hyökkäysvektoreiden analyysiin vahvistaa väitettä rakenteellisen kyberasymmetrian olemassaolosta. Riippumatta hyökkäysvektorista suljetun verkon puolustajalla on selvä etu johtuen tavasta, jolla kansallisen verkon resilienssi on toteutettu. Kahdennetut ja valvotut liitynnät ja kriittiset palvelut kestävät hyökkäyksiä ja mahdollistavat niiden vaikutusten lieventämisen. Hyökkäykset verkon sisältä (*insider*) ovat toki edelleen vaarallisia, mutta niidenkin vaikutukset kyetään rajoittamaan. Kriittinen infrastruktuuri on tiedossa, suojattu, osittain kahdennettu ja jatkuvasti valvonnassa. Edelleen suljettu verkko voidaan jakaa osiin hyökkäyksen väistämiseksi ja palautumista on kansallisella tasolla harjoiteltu. Hyökkääjän mahdollisuus saada aikaan merkittävää, pitkäaikaista vaikutusta on täten rajoittunut. Toiminnan vapautta tarkasteltaessa mainitulla ulkoyhteyksien määrän säätelyllä ja hallinnalla on merkittävä vaikutus suljetun verkon resilienssiin.

Avoimien verkkojen resilienssi riippuu siitä verkon osasta ja järjestelmästä, joka on hyökkäyksen kohteena. Verkon resilienssi on fragmentoitunut ja on laadultaan vaihteleva, koska avoimen verkon osaverkkoja hallinnoivat toisistaan riippumattomat yksityiset ja julkiset tahot. Hyökkääjä voi käyttää eri yhteyksiä iskeäkseen saman aikaisesti kohteeseen usealta eri suunnalta tai useisiin kohteisiin eri yhteyksien kautta. Tämä mahdollistaa avoimeen kansalliseen verkkoon tukeutuvien palveluiden saattamisen laajaan häiriötilaan keskinäisriippuvuuksista johtuen. Koska yhteistoimintaa ja palautumista ei ole harjoiteltu kansallisella tasolla, heijastevaikutusten hallinta on vaikeaa. Toisaalta pelkkä sattumanvarainen hyökkääminen avointa kansallista verkkoa kohtaan ei todennäköisesti tuota kriittistä vahinkoa, sillä verkon heterogeenisyys toimii myös resilienssin lähteenä. Niin suljetulla kuin avoimella verkolla on resilienssin suhteen vahvuutensa.

Näin ollen suljetun ja avoimen kansallisen verkon resilienssiä hyökkäysvektoreiden kautta tarkasteltaessa merkittäväksi tekijäksi nousee yhtäältä liityntöjen hallinta ja toisaalta niiden keskinäisriippuvuuksien tunnistaminen.

4.2 Suljetun ja avoimen kansallisen verkon sisäiset rakenteelliset erot

Vertailemalla osajärjestelmien alle koottuja suljetun ja avoimen kansallisen verkon ominaisuuksia toiminnan vapauden, yhteisen tilannekuva, johtamisen ja resilienssin kautta voidaan täydentää edellisen luvun hyökkäysvektorianalyysiä. Taulukossa 1 on esitetty rinnakkain suljetun avoimen kansallisen verkon ominaisuudet kansallisen informaatiopuolustuksen ja turvallisuuden järjestelmän osajärjestelmien kautta tarkasteltuna. Taulukkoon listatut ominaisuudet perustuvat luvuissa 3.2–3.5 esiteltyihin Venäjän valtion ominaispiirteiden, kansallisen internetsegmentin tavoitetilan sekä teoreettisen avoimen verkon kuvauksiin. Osajärjestelmiä käytetään tarkastelun perustana, koska niiden avulla kyetään hahmottamaan alueellisesti rajatun kybertilan teknologiset, hallinnolliset, taloudelliset, normatiiviset, poliittiset ja turvallisuustekijät - eli ”piirtämään” digitaalisen maasto kartta (ks. Luku 2.5). Avoin kansallinen verkko määrittyy tässä lähestymistavassa suljetun verkon eli informaatioturvallisuuden ja -puolustuksen järjestelmän kautta. Tämä on tarkoituksen mukainen lähestymistapa, koska työssä tutkitaan venäläisen kansallisen internetsegmentin erityispiirteitä ja sen suhdetta rakenteelliseen kyberasymmetriaan.

Tauluko 1: Suljetun ja avoimen kansallisen verkon vertailu osa-järjestelmien kautta.[637]

Verkkotyyppi: Suljettu verkko	**Verkkotyyppi: Avoin kansallinen verkko**
Osajärjestelmät: 1.Tieteellis-teknologinen perusta	
- Valtiojohtoinen - Pyrkimys laaja-alaiseen omavaraisuuteen ja kansainvälisten keskinäisriippuvuuksien välttämiseen - Ulkomaisten tuotteiden käytön voimakas sääntely - Strategiset yritykset valtion omistuksessa - ulkomainen omistus hyvin kontrolloitu	- Valtion osallistuminen vaihtelee - Omavaraisuutta ei tavoitella kuin erittäin kapeilla aloilla - Tiedettä ja teknologiaa kehitetään markkinaperustaisesti - Merkittäviä kansainvälisiä keskinäisriippuvuuksia (etenkin tuotantoketjut)

[637] Taulukko ja seuraava analyysi on julkaistu aikaisemmin Kukkola (2020b).

- Kansallinen ohjelmisto- ja laitteistoekosysteemi - Lähtökohtaisesti vain omisteista lähdekoodia - Kansainvälinen kyberturvallisuusyhteistyö rajoitettua	- Strategisten yritysten privatisointi - ulkomainen omistus säädeltyä - Vähän kansallisesti tuotettuja ohjelmistoja tai laitteistoja - Pirstaloitunut toimittajakenttä
Osajärjestelmät: 2.Autentikointi- ja salausjärjestelmä	
- Kotimaisia ratkaisuja - Kryptografiatuotteet vaativat valtion sertifikaatin - Turvallisuustoimijat kykenevät avaamaan salauksen ilman oikeudellista tai hallinnollista prosessia	- Rajoitetusti kotimaisia ratkaisuja - Valtio tarjoaa sertifiointeja hallinnolle ja suosittelee hyviä käytänteitä - Salauksen avaaminen hidasta poliittisista ja oikeudellisista syistä johtuen
Osajärjestelmät: 3.Sensuurijärjestelmä	
- Valtiojohtoinen keskitetty järjestelmä - Laaja poliittinen sensuuri sekä median itsesensuuri - Poliittisesti ei-toivotun materiaalin poistaminen informaatiotilasta tai pääsyn estäminen - Ulkomaisten toimijoiden sulkeminen pois informaatiotilasta - Käyttäjien anonymiteetin poistaminen - Merkittävästi vapaaehtoistoimintaa	- Ei keskitettyä järjestelmää - Ei poliittista sensuuria - Vapaa media, joka voi harjoittaa itsesensuuria rajatuissa kansallisissa kysymyksissä - Materiaalin poistamisella tai pääsyn rajoittaminen muut kuin poliittiset perusteet - Identiteetin suoja ja viestintäsalaisuus viestinnän periaatteina - Vähän vapaaehtoistoimintaa
Osajärjestelmät: 4.Räätälöidyt valvonnan ja massamaiset datan keräämisen järjestelmät	
- Turvallisuuspalvelut valvovat keskitetysti ja ilman parlamentaarista valvontaa kansallista dataliikennettä - Massiivinen datan kerääminen kansallisen verkon tietoliikenteestä - Kansalaisten ja yritysten kriittisen datan lokalisaatio kansallisen turvallisuuden nojalla	- Rajoitettua ja parlamentaarisesti valvottua - Ei valtion massamaista datan keräämistä turvallisuustarkoituksiin omista kansalaisista - Tietosuoja ja datan lokalisaatio perustuvat henkilösuojaan - Yritysten ja valtion kriittistä dataa ulkomailla
Osajärjestelmät: 5.Kriittinen informaatio-infrastruktuuri	
- Valtion ja yksityissektorin hallussa - Lailla velvoitettu kartoittaminen, ylläpito ja turvaaminen - Kriittiset palvelut valtion hallussa ja kahdennettu - Kyky irrota hallitusti globaalista Internetistä	- Yksityissektorin hallussa - Liiketaloudelliset tekijät määräävät turvaamista - Jonkin verran valtiosääntelyä ja sertifiointia - Valtio ei kahdenna kriittisiä palveluja - Ei kykyä irrota hallitusti globaalista Internetistä
Osajärjestelmät: 6.Aktiiviset vastatoimet	
- Valtion kontrolloima media - Ulkomaisten medioiden toiminta ja ulkomaiset omistukset rajoitettu - Valtion johtoa tukevia ja sen johtamia patrioottisia ja uskonnollisia instituutioita ja historian tulkintojen ohjaamista - Kyberdiplomatia-organisaatio, jolla selkeät kansalliset tavoitteet - Aktiivinen propaganda, salatut ja horjuttavat informaatio-operaatiot - Kybersodankäynnin suorituskykyjä peitellään, toimijoita on useita, sijaistoimijoiden käyttö on laajaa	- Valtion omistama ja kaupallinen media - Vähän rajoituksia ulkomaisen median toiminnalle - Kansalaiskasvatus poliittisesti sitoutumattoman varhaiskasvatus- ja koululaitoksen toimesta - Kyberdiplomatialla ei erityistä roolia osana ulkopolitiikkaa, eikä yhtenäistä linjaa liittolaisten kanssa - Pehmeä voima, strateginen kommunikaatio ja kohdennetut kyber- ja informaatio-operaatiot - Kybersodankäynnin joukot perustettu avoimesti, toiminta valvottua ja puolustuksellista

- Kyber- ja informaatiosodankäynnin kyvyt osa deterrenssiä ja sodanaikaista eskalaation hallintaa - Kansainvälinen yhteistyö rajoittunutta	- Aktiivinen kansainvälinen yhteistyö ulkomaan tietoliikenne tiedustelun osalta
Osajärjestelmät: 7.Asevoimien verkot ja järjestelmät	
- Asevoimat puolustavat omia verkkojaan normaalioloissa ja poikkeusoloissa kriittistä infrastruktuuria - Erilliset ja omat operatiiviset verkot, järjestelmät ja tietoturvaratkaisut - Rajalliset rajapinnat muihin turvallisuustoimijoihin - Kahdennettu ja maantieteellisesti hajautettu infrastruktuuri	- Asevoimat puolustaa enintään omia verkkojaan - Asevoimien verkot rinnakkaiset ja päällekkäiset siviili- ja muiden turvallisuustoimijoiden verkkojen kanssa - Yhteistyö yksityisten teleoperaattoreiden ja kyberturvayritysten kanssa - Erilliset kenttäviesti- ja kriittisimmät järjestelmät
Osajärjestelmät: 8.Hallinta-, kontrolli-, valvonta- ja palautejärjestelmä	
- Turvallisuuspalvelut johtavat - Useita keskitettyjä informaation hallinta- ja turvallisuusjärjestelmiä - Kansallisesti hallittu teknologisten ja psykologisten turvallisuusuhkien torjunta - Rajoittunut kansainvälinen yhteistyö ja tiedonvaihto	- Ei kansallista johtoa - Rajoittunut ja kapea-alainen kansallinen kyberturvallisuusjärjestelmä - Keskittyy rikostorjuntaan - Kansallinen nCSIRT koordinoi ja kokoelma sektorikohtaisia CSIRT toteuttaa kyberturvaa - Kehittyvä kansainvälinen yhteistyö ja tiedonvaihto

Taulukko 1 mahdollistaa suljetun ja avoimen kansallisen verkon ominaisuuksien tarkastelun puolustajan näkökulmasta. Koska suljettu tai avoin kansallinen verkko itsessään ei varsinaisessa merkityksessä ”hyökkää”, verkkojen hyökkäysominaisuuksia olisi epätarkoituksenmukaista verrata. Hyökkääjää analyysissä edustaa siis geneerinen toimija. Poikkeuksen muodostaa aktiivisten vastatoimien järjestelmä, mihin palataan alempana. Alla esitettyjä tuloksia seuraa kriittinen tarkastelu, jossa tuodaan esiin etenkin suljetun kansallisen verkon käytännön toteuttamisesta syntyviä puolustuksellisia heikkouksia.

Suljetun verkon tieteellisteknologinen perusta tarjoaa selvän puolustuksellisen edun, sillä hyökkääjän täytyy takaisin mallintaa (*reverse-engineer*) kansalliset laitteisto- ja ohjelmistoratkaisut. Tämä hidastaa hyökkääjää ja rajoittaa sen toiminnan vapautta. Puolustaja taas tuntee ne järjestelmät, joita se puolustaa ja kykenee muokkaamaan niitä ja liikkumaan niissä vapaasti. Kotimaisesti tuotettu teknologia ja integroidut järjestelmät hyödyttävät suljetun verkon puolustajan yhtenäistä tilannekuvaa ja johtamista. Lisäksi resilienssiä edistää kotimainen ja valtion kontrolloima kyberekosysteemi, jossa havaitut haavoittuvuudet voidaan paikata nopeasti jopa pakkokeinoin. Avoimien verkkojen sirpaloitunut luonne haittaa niiden puolustajan toiminnan vapautta. Yhteinen tilannekuva on rajoittunut johtuen hallinnollisista ja laillisista toimivaltuuskysymyksistä sekä epäyhteensopivista järjestelmistä. Johtamiselta puuttuvat integroidut johtamisen tukijärjestelmät. Avoimien

kansallisten verkkojen resilienssi on erittäin riippuvainen yksityisten palveluntarjoajien riskilaskelmista, mutta kansainvälinen yhteistyö voi tarjota välineitä resilienssin kehittämiseksi.

Suljetun verkon kansallinen autentikointi- ja salausjärjestelmä takaa puolustajalle selkeän edun toiminnan vapaudessa ja yhteisessä tilannekuvassa. Kaikki liikenne on periaatteessa läpinäkyvää, eikä verkossa on puolustajalle suljettuja yhteyksiä, tiloja tai informaatiota. Avoimen verkon puolustajan kyky purkaa liikenteen salaus on vastavuoroisesti rajoittunut. Yksityissektorin ja kansalaisten käyttämät salausratkaisut ovat lähtökohtaisesti suljettuja puolustajalle. Niiden purkaminen vaatii aikaa ja usein miten hallinnollisen päätöksen. Lisäksi kotimaisia sertifioituja salausjärjestelmiä käytetään vain joissain järjestelmissä ja niiden laatu on vaihtelevaa. Usean salaus- ja autentikointiratkaisun käyttö voi kuitenkin tuottaa avoimissa verkoissa resilienssiä redundanssin kautta. Yhden ratkaisun haavoittuvuus ei uhkaa koko verkkoa.

Suljetun verkon sensuurijärjestelmä takaa puolustajalle selkeän edun toiminnan vapaudessa. Informaatiopsykologisten ja -teknologisten hyökkäysten toiminnan vapaus voidaan kiistää poistamalla tarvittavat resurssit ja alustat kansallisesta kybertoimintaympäristöstä. Puolustajan tilannekuvaa vahvistaa anonymiteetin poistaminen, joka mahdollistaa kybertoimintaympäristön laitteiden ja toimijoiden yksilöinnin. Lisäksi aktivistiryhmät voivat tukea yhteisen tilannekuvan muodostumista raportoimalla havaintojaan viranomaisille. Keskitetty sensuurijärjestelmä edistää puolustustoimenpiteiden johtamisen nopeutta ja tehokkuutta. Sensuurijärjestelmän eri osien testaaminen jatkuvasti jo normaaliolojen aikana vahvistaa suljetun verkon resilienssiä. Avoimien verkkojen puolustajat ovat epäedullisessa asemassa kaikkien tekijöiden suhteen. He eivät ole täysin voimattomia, mutta sensuurijärjestelmän, sikäli kuin järjestelmää varsinaisesti edes on, käyttö on hidasta ja siihen kohdistuu laillisia, poliittisia ja taloudellisia rajoituksia.

Suljetun verkon valvonnan ja datan keräämisen järjestelmät takaavat puolustajalle merkittävän edun yhteisessä tilannekuvassa. Lisäksi nämä järjestelmät takaavat puolustajalle suoran pääsyn julkisiin ja avoimiin verkkoihin ja niiden sisältöön, mikä edelleen parantaa yhteistä tilannekuvaa ja toiminnan vapautta. Sisällönvalvontajärjestelmien ollessa yhteydessä keskitetyn valvonnan ja hallinnan järjestelmiin ne tukevat myös johtamista tarjoamalla oikea-aikaista ja tarkkaa tietoa kyber- ja informaatiouhkista. Suurista datavarastoista voidaan etsiä viitteitä uhkista mm. datalouhinnan keinoin jatkuvasti ilman erillistä hallinnon päätöstä. Lisäksi datan lokalisaatio kansallisiin palvelinkeskuksiin lisää verkon

resilienssiä. Avoimelta verkolta puuttuvat periaatteessa verkon sisällön valvonnan ja datan keräämisen järjestelmät. Sellaisten käyttöarvo olisi rajoitettu niiden olemassaolon paljastumisesta koituvien poliittisten seurannaisvaikutusten takia. Resilienssiä heikentää kriittisen datan sijainti ulkomailla tai ulkomaisten palveluntarjoajien datakeskuksissa. Avoimen verkon puolustajilla on kuitenkin kyky ja mandaatti toimeenpanna valvonta, kunhan vihamielisestä toiminnasta on riittävästi todisteita.

Suljetun verkon kriittinen informaatioinfrastruktuuri takaa puolustajalle edun kaikkien analyysikäsitteiden suhteen. Toiminnan vapauden takaa se, että kriittiset järjestelmät ovat valtion omistamia tai kontrolloimia ja pääsyn yksityisiin järjestelmiin takaa laki. Kriittinen informaatioinfrastruktuuri on yhteydessä keskitetyn valvonnan ja hallinnan järjestelmiin, mikä tuottaa edun yhteisessä tilannekuvassa ja johtamisessa. Infrastruktuurin valvonnan, kahdennuksen ja turvaamisen takia koko verkon resilienssi on korkea. Kansallinen verkko tai sen osia voidaan irrottaa globaalista tietoverkosta uhkien hallitsemiseksi ja järjestelmien palauttamiseksi. Resilienssin vahvuus on kuitenkin käytännössä riippuvainen tavasta, jolla ulkoyhteyksiä hallitaan ja rajoitetaan. Vaikka avoimen verkon puolustajat ovat huonommassa asemassa, paljon riippuu niiden, yleensä yksityisten, tahojen toimista, jotka ovat vastuussa infrastruktuurista. Resilienssi voi olla varsin hyväkin johtuen yksityisten palveluntarjoajien kahdennetuista ja rinnakkaisista järjestelmistä. Sen sijaan toiminnan vapautta rajoittavat samaisten palveluntarjoajien verkkojen rajat. Kansallisia järjestelmiä, jotka tukisivat tilannekuvaa tai johtamista, on avoimissa verkoissa enintään rajoitetuilla sektoreilla. Monet olemassa olevista järjestelmistä ovat hallinnollisesti siiloutuneita tai tarkoitettu yksityisten yritysten tietoturvan ylläpitoon.

Suljetun verkon aktiivinen informaatioteknologinen ja -psykologinen vastatoimijärjestelmä tarjoaa puolustajalle selkeän edun toiminnan vapaudessa. Tämä perustuu informaation manipulointiin, vastustajien horjuttamiseen ja niiden yhtenäisyyden rapauttamiseen jatkuvasti ja kaikissa oloissa. Kun toiminta suuntautuu kansallisen verkon ulkopuolelle, tätä voidaan pitää myös hyökkäyksellisenä etuna. Jatkuva agressiivinen, kotimainen monitorointi ja tiedustelu(vakoilu)operaatiot takaavat edun yhteisessä tilannekuvassa. Samainen tiedonkeruu voidaan helposti ulottaa ulkomaisiin verkkoihin ja toimii näin hyökkäyksellisenä etuna. Viranomaisten yhteensovitettu toiminta ja johtamisjärjestelmät takaavat edun vastatoimien johtamisessa. Vastatoimijärjestelmän johtaminen mahdollistaa ulkoisiin verkkoihin suunnattaessa monivektorisen, -alaisen ja -suorituskykyisen hyökkäyksen ja tarjoaa näin selvän edun. Mediatilan hallinta ja patrioottinen kasvatus tuottavat edun informaatiopsykologisessa

resilienssissä. Ne yhtäältä torjuvat ulkoista informaatiovaikuttamista ja toisaalta yhdistävät kansaa. Koska on hyvin epätodennäköistä, että informaatioturvallisuuden ja -puolustuksen järjestelmä kykenee kattamaan koko kansallisen informaatiotilan, psykologinen resilienssi jää aina haavoittuvaiseksi etenkin, jos valtion legitimiteetti on heikko. Avoimen verkon informaatiopsykologista resilienssiä vahvistavatkin demokratia ja läpinäkyvyys. Muiden tekijöiden osalta avoimen verkon puolustaja on heikommassa asemassa johtuen johtamisen hajaantumisesta eri hallinnonaloille, liittolaissuhteiden vaatimasta koordinoinnista, kotimaisesta lainsäädännöstä ja kansainvälisen lainsäädännön ja sopimusten rajoituksista sekä julkisten ja yksityisten toimijoiden epäselvästä vastuujaosta. Tämä ei kuitenkaan tarkoita, ettei sillä tarvittaessa olisi riittäviä vastatoiminnan suorituskykyjä suhteellisen nopeasti käytettävissään, mukana lukien hyökkäyksellisiä.

Asevoimien verkkojen ja järjestelmien osalta avoimien ja suljettujen kansallisten verkkojen välille ei muodostu selkeitä etu- tai haittasuhteita. Tämä johtuu siitä, että molemmissa verkkotyypeissä asevoimat pyrkivät erottamaan yhteytensä ja palvelunsa julkisista verkoista, tilannekuva pyritään lähtökohtaisesti jakamaan vain tarvitsijoille, johtaminen toteuttamaan hierarkkisten, alueellisesti jakautuneiden johtoportaiden kautta tavoitteen ollessa mahdollisimman korkea resilienssi. Erot syntyvät lähinnä teknologisista ratkaisuista, eivät periaatteellisista rakenteellisista eroavaisuuksista. Avoimen verkon valtioiden asevoimat ovat tukeutuneet yhteistyöhön siviilioperaattoreiden kanssa, kun taas suljetun verkon valtioiden asevoimat ovat pyrkineet säilyttämään johtamisjärjestelmäinfrastruktuurin omassa hallussaan. Ensimmäinen malli rajoittaa puolustajan toiminnan vapautta, mutta on lisännyt resilienssiä. Jälkimmäinen malli periaatteessa takaa puolustajan toiminnan vapauden ja edistää yhteistä tilannekuvaa ja johtamista, mutta voi käytännössä johtaa aselajien ja puolustushaarojen siiloutumiseen ja pahimmillaan teknologiseen jälkeenjääneisyyteen. Kehitys kybertoimintaympäristön osalta on molempien verkkojen osalta johtamassa asevoimien yhä laajempaan mandaattiin operoida puolustuksellisesti omien verkkojensa ulkopuolella. Sotilas- ja siviiliverkkojen ja järjestelmien rajat ovat ainakin madaltumassa, elleivät katoamassa.

Suljetun kansallisen verkon hallinta-, kontrolli-, valvonta- ja palautejärjestelmät takaavat puolustajalle edun kaikkien analysoitavien tekijöiden suhteen. Yhteen liitetyt valtion hallinnoimat järjestelmät mahdollistavat toiminnanvapauden ja tuottavat kansallisen tason yhteisen tilannekuvan. Hallinta- ja tukijärjestelmät sekä keskitetyt ja hierarkkiset

johtamisjärjestelmät takaavat ylivoimaisen johtamiskyvyn. Kriittisen informaatioinfrastruktuurin jatkuva monitorointi, uhkien torjunta ja sitä operoivan henkilökunnan koulutus sekä kansalliset harjoitukset lisäävät resilienssiä. Toisaalta, kuten aikaisemmin on todettu, keskitetyt järjestelmät ovat myös riskitekijä resilienssin osalta. Avoimen verkon puolustaja on alakynnessä johtuen hallinnollisesta siiloutumisesta. Se voisi saavuttaa edun yhteisessä tilannekuvassa kansainvälisen yhteistyön ja vapaaehtoisen sekä velvoittavan yksityisen sektorin osallistumisen avulla. Tällöin informaatio pitää kuitenkin kyetä keräämään, analysoimaan ja jakamaan kaikille osallistujille sopivalla tavalla, mikä on haasteellista.

Vaikka edellä esitetty ominaisuuksien vertailu näyttäisi suosivan suljettuja kansallisia verkkoja tämä ei välttämättä käytännössä pidä kaikilta osin paikkaansa. Suljetut verkot ovat erittäin riippuvaisia valtion osallistumisesta eli valtion resursseista, tuloista ja tehokkaasta hallinnosta. Epäreilut kilpailuasetelmat kotimaan markkinoilla voivat tukahduttaa innovaatioita samoin kuin tiedeinstituuttien tiivis suhde valtiovaltaan. Byrokratia ja korruptio heikentävät hankkeiden ja organisaatioiden toiminnan (johtamisen) tuloksellisuutta. Kotimaiset salausratkaisut tai omisteiset (*proprietary*) ohjelmistot tai laitteistot eivät automaattisesti takaa parempaa tietoturvaa kuin esimerkiksi avoin, jatkuvasti testattava lähdekoodi. Poliittisesti motivoitunut sensuuri ruokkii poliittista apatiaa ja vastarintaa, mikä voi pahimmillaan lisätä sisäpiirihyökkäysten riskiä. Keskittäminen voi lisätä riskejä. Datan massamainen kerääminen luo datavarantoja, jotka tarjoavat houkuttelevan kohteen niin rikollisille kuin valtiollisille toimijoille. Potentiaalisiksi kohteiksi muodostuvat myös kriittisen informaatioinfrastruktuurin kartoituksen perusteella syntyneet tietokannat. Lisäksi kansallisten verkkojen valvonta- ja hallintajärjestelmien häirinnän avulla voidaan lamauttaa merkittäviä osia suljetusta kansallisesta verkosta.

Kyberdiplomatian keinoin on vaikea peittää suljettujen verkkojen taustalla vaikuttavaa autoritaarista ja suurvaltakeskeistä politiikkaa, mikä heikentää mallin kansainvälistä vetovoimaa. Aktiiviset vastatoimet eivät aina ole niin ”holistisia” tai keskitetysti johdettuja kuin päällepäin voisi vaikuttaa. Ainakin Venäjän tapauksessa informaatioturvallisuuden ja -puolustuksen järjestelmää operoi laaja joukko kansallisia toimijoita, joilla voi olla ristiriitaisia intressejä.[638] Tämä voi haitata suljetun verkon kehitystä ja

[638] Radin, Andrew, Demus, Alyssa & Marcinek, Krystyna: *Understanding Russian Subversion Patterns, Threats, and Responses*. RAND, Santa Monica CA, 2020, s. 16.

toimintaa. Hallinnollinen tai teknologinen siiloutuminen voi olla paljon merkittävämpää kuin julkiset tiedot antavat ymmärtää, mikä herättää täysin legitiimin kysymyksen siitä, onko järjestelmien järjestelmää suljetun verkon ytimessä todella olemassa. Esimerkiksi kriittisen informaatioinfrastruktuurin resilienssi voi jäädä näennäiseksi, jos ohjeita ei noudateta ja valvonta on heikkoa tai poliittisesta tai taloudellisesti motivoitunutta. Suljettu verkko on varsin kompleksinen kokonaisuus, jossa kybertilan pakottaminen määrättyihin rakenteisiin ja prosesseihin voi johtaa ennalta arvaamattomiin ilmiöihin ja virhetiloihin täysin ilman ulkopuolistakin vaikutusta. Lisäksi informaatiotilaa on mahdoton sulkea täydellisesti, joten suljetun verkon tai informaatioturvallisuuden ja -puolustuksen järjestelmän ulkopuolelle jää aina jokin pala valvomatonta tilaa. Tämä tila toimii potentiaalisena hyökkäysalustana.

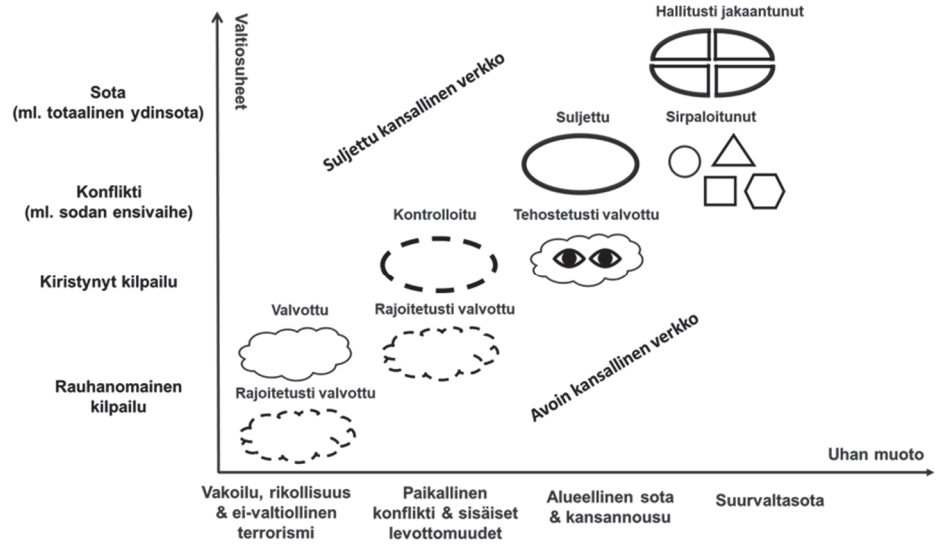
Huolimatta yllä esitetyistä kriittisistä varauksista on selvää, että rakenteellinen kyberasymmetria on läsnä myös verkkojen sisäisten ominaisuuksien tasolla. Tehdyt havainnot vahvistavat hyökkäysvektorianalyysiä samoin resilienssin lisääminen analyysin kohteeksi. Resilienssin osalta on huomioitava, että avoimien verkkojen monimuotoisuus voi lisätä resilienssiä, mutta vain jos yksityiset toimijat noudattavat parhaita mahdollisia käytänteitä ja kilpailu ei johda palveluiden keskittämiseen samoihin fyysisiin ja loogisiin järjestelmiin. Esitetyt varaukset tulee kuitenkin ottaa huomioon pohdittaessa rakenteellisen kyberasymmetrian strategisia vaikutuksia luvussa 5. Ne muodostava reunaehtoja valtioiden päätöksille käyttää voimaa kybertoimintaympäristössä ja vaikuttavat voimankäytön vaikutuksiin.

4.3 Suljetun ja avoimen kansallisen verkon erot valtiosuhteiden jatkumolla

Olen väitöskirjassani kuvannut, kuinka Venäjän kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä voisi toimia valtioiden välisten suhteiden muuttuessa sekä erilaisiin uhkakuviin liittyen.[639] Tuon kuvauksen rinnalle lisätään tässä työssä teoreettinen avoin kansallinen verkko rakenteellisen kyberasymmetrian tarkastelemiseksi ajassa. Tarkoituksena ei ole toistaa aikaisemman tutkimuksen havaintoja vaan keskittyä kahden erilaisen verkon suhteeseen. Yleisesti voidaan todeta, että suljetun kansallisen verkon toimintalogiikka perustuu

[639] Kukkola (2020), s. 366–367.

informaatioturvallisuuden ja -puolustuksen järjestelmän osajärjestelmien avulla toteutettavaan joustavaan sääntelyyn. Avoin kansallinen verkko taas toimii huomattavasti hajautetummin usein konsultointiin perustuen ja sopimuspohjaisesti. Alla esitetyn analyysin tulokset on esitetty tiivistetysti kuvassa 11.



Kuva 11: Suljetun ja avoimen kansallisen verkon suhde valtiosuhteiden ja uhkien jatkumossa

Kuvassa 11 pystyakselille sijoittuvat valtioiden välisten suhteiden vaiheet ja vaaka-akselille mahdollisten uhkien muodot. Kuvan akselit eivät edusta toisistaan riippumattomia muuttujia vaan kuvaavat kansallisten verkkojen strategista ympäristöä eri näkökulmista. Valtioiden välisiä suhteita ovat luvussa 2.2 kuvatulla tavalla rauhanomainen kilpailu, kiristynyt kilpailu, konflikti mukaan lukien sodan alkuvaihe ja sota. Vaaka-akselille sijoittuvat uhat perustuvat valtion turvallisuutta koskeviin epäsuorien ja suorien sotilaallisten uhkien ilmenemismuotoihin, toimijoiden tyyppiin ja toimien intensiteettiin.[640] Vakoilu, rikollisuus ja ei-valtiollinen terrorismi ovat

[640] Jaottelun taustalla ovat Venäjän sotilasdoktriinin (Указ-2976 (2014)) esittämät uhkakuvat ja E.G. Šalamberidze esittämä jaottelu valtioiden välisen kamppailun keinoista (Шаламберидзе Е.Г.: Теоретические вопросы развития политики национальной обороны России в условиях мирного времени с использованием системы мер невоенного и военного характера. *Вестник Академии военных наук*, № 4 (37) 2011, с. 35–43; Шаламберидзе Е.Г.: Национальная оборона Российской Федерации:

valtioihin kohdistuvia arkipäiväisiä uhkia, joilla voi kuitenkin olla merkitystä kansallisen turvallisuuden kannalta. Niiden lähteinä voivat olla valtiolliset ja ei-valtiolliset toimijat. Paikalliset konfliktit ovat tavanomaisin asevoimin toteutettuja rajoitettuja strategisoperatiivisen tai alemman tason lyhyt kestoisia sotatoimia toista valtiota kohtaan rajoitetuin tavoittein. Taistelut ovat maantieteellisesti ja toimintaympäristöllisesti rajattuja. Sisäiset levottomuudet sisältävät järjestäytynyttä kansalaistottelemattomuutta, rajoitetusti väkivaltaa ja saavat mahdollisesti tukea ulkopuolelta. Levottomuudet ovat spontaaneja, eivätkä lähtökohtaisesti pyri poliittisen vallan kaappaamiseen. Alueelliseen sotaan osallistuu useita valtioita tai liittokuntia ja ne ratkotaan tavanomaisin asevoimin strategisissa operaatioissa yhdellä maantieteellisellä suunnalla. Alueellisen sodan kesto vaihtelee ja voi edellyttää yhteiskunnan saattamista täydelliseen sotatilaan. Operaatioita toteutetaan osallistujien koko syvyydessä ja kaikissa toimintaympäristöissä. Kansannousu tarkoittaa väkivaltaista, aseellista vallankumousta, joka pyrkii kaappaamaan poliittisen vallan. Se saa todennäköisesti tukea valtion rajojen ulkopuolelta ja voi johtaa ulkopuolelta suoritettuun sotilaalliseen interventioon. Suursotaan osallistuu useita valtioita tai liittokuntia. Se käydään kaikin käytettävissä olevin keinoin, mukaan lukien ydinaseet. Osallistujien päämääränä on selviytyminen. Suursota voi kestää pitkään, tosin ydinaseiden käyttö tekee vihollisuuksien jatkamisesta vaikeaa ja todennäköisesti epätarkoituksenmukaista.

Suljetun kansallisen verkon (kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmän) kaikki alajärjestelmät ovat toiminnassa kaikissa valtiosuhteiden vaiheissa ja eri uhkia kohdattaessa, mutta niiden toiminnan laatu ja aktiivisuustaso vaihtelevat. Myös teoreettisen avoimen kansallisen verkon alajärjestelmät ovat toiminnassa, mutta niiden toiminnassa tapahtuu vähemmän muutoksia valtiosuhteiden tai uhkien muuttuessa. Rauhanomaisen kilpailun aikana valtiot käyvät kamppailua yleisesti hyväksytyillä ei-väkivaltaisilla ja ei-sotilaallisilla keinoilla. Uhat perustuvat lähtökohtaisesti vakoiluun tai ei-valtiollisten toimijoiden toteuttamaan terrorismiin. Suljetun kansallisen verkon etuna on avoimia verkkoja tehokkaampi kybertoimintaympäristön valvonta ja kyky vastata yksittäisiin kyberoperaatioihin keskitetysti kansallisella tasolla. Lisäksi aktiiviset vastatoimet ylläpitävät psykologista resilienssiä ja haastavat ja horjuttavat jatkuvasti potentiaalisia vihollisia. Avoimissa kansallisissa

---

стратегические задачи и возможные перспективы. *Вестник Академии военных наук*, № 4 (41) 2012, с. 30–37).

verkoissa kyetään valvomaan vain osa verkoista ja järjestelmistä. Avoin kansallinen verkko hyötyy kyber- ja informaatiotoimintaympäristön avoimuudesta vastatoimissaan, mahdollisuudesta jakaa kyberuhkiin liittyvää tietoa kansainvälisesti ja toimitusketjujen sekä markkinoiden kansainvälisyydestä. Suljettuja kansallisia verkkoja voidaan tässä valtiosuhteiden vaiheessa kutsua ”valvotuiksi”, kun taas avoimet ovat enintään ”rajoitetusti valvottuja.” Merkittävin ero on siinä, että suljetun kansallisen verkon valtio voi viestiä kykenevänsä kiristämään verkon hallintaa nopeastikin, siinä missä avoimen verkon valtion toiminnan vapaus on rajallisempi, koska se ei tosiasiallisesti hallitse omaa kansallista kybertoimintaympäristöään.

Kiristyneen kilpailun aikana vähintään toinen osapuolista tunnistaa jonkin tasoisen kansallisen kriisin olemassaolon. Valtioiden keinot ovat ei-sotilaallisia, salassa pidettäviä ja epäsuoria sekä päämäärät rajoitettuja. Uhkakuvina esiintyvät paikalliset konfliktit ja sisäiset, rajoitetut levottomuudet ja terrorismi. Niihin voi todellisuudessa tai väitetysti liittyä tai olla liittymättä vieraan valtion tuki. Suljetun verkon tapauksessa kansallinen salausjärjestelmä, sensuurijärjestelmä ja räätälöidyt valvonnan järjestelmät sekä massiivinen datan kerääminen tekevät kansallisesta kybertoimintaympäristöstä läpinäkyvän kyber- ja informaatiopuolustuksesta vastaaville tahoille. Kriittistä informaatioinfrastruktuuria kyetään suojelemaan tehostetusti ja kansallisia kyberturvallisuustoimia johtamaan keskitetysti. Hyvän tilannekuvan avulla voidaan attribuoida hyökkääjiä nopeasti ja käyttää attribuutiotietoa poliittisten päämäärien tavoittelun tukemiseksi. Vähintäänkin voidaan kaventaa epäillyn hyökkääjän toiminnan vapautta. Aktiiviset vastatoimet mahdollistavat oman informaatiotilan hallinnan ja puolustamisen. Vastustajien haastaminen muuttuu vaikeammaksi näiden kohotettua valmiutta, mutta suljettujen verkkojen valtioilla on silti etulyöntiasema. Sekä suljetun että avoimen kansallisen verkon valtiot kykenevät aktivoimaan erilaisia liittokuntia, mutta avoimien verkkojen valtioiden liittokunnat voivat olla tehokkaampia yhteisen tilannekuvan luomisessa ja mahdollisesti uhkien torjunnassa. Avoimien verkkojen valtioiden haaste on kansallisen kriisin tunnistaminen. Resilienssin kasvattamisen tai aktiiviset vastatoimet edellyttävät poliittista päätöstä demokraattisissa valtioissa ja liittokuntien sisällä. Avoimien kansallisten verkkojen valtioiden yksityiset yritykset ja valtion virastot ja hallinnonalat joutuvat torjumaan uhkia omilla, eriytetyillä voimavaroillaan. Avoimien verkkojen valtioilla ei ole käytössään vastaavaa kansallista tilannekuvaa kuin suljettujen verkkojen operoijilla. Tässä valtiosuhteiden vaiheessa suljettuja verkkoja voidaan kutsua ”kontrolloiduksi” ja avoimia edelleen ”rajoitetusti valvotuiksi.”

Konfliktin aikana valtioiden kamppailu ei vielä ylitä avoimen, julistetun sodan kynnystä. Valtioiden keinot ovat edelleen rajoitettuja. Tilanne voi kuitenkin hyvin nopeasti kehittyä sodan alkuvaiheeseen, johon liittyy avoin, suora sotilaallisen voiman käyttö. Molemmissa tapauksissa valtio katsoo olemassaolonsa olevan uhattuna joko valtiollisten tai ei-valtiollisten tahojen toimesta. Uhkakuvina korostuvat kansannousut tai joutuminen alueelliseen sotaan. Suljettu kansallinen verkko toimii tässä vaiheessa täydellä suorituskyvyllään. Kansallinen kybertoimintaympäristö ja sen myötä informaatiotila kyetään sulkemaan globaalista kyber- ja informaatioympäristöstä ja hallinnoimaan sisäisesti. Yhteiskuntaa kyetään hallitsemaan ja sisäiset kumoukselliset toimijat kyetään eristämään ulkoisista tukijoista. Koska sulkeminen on ennalta suunniteltua, valtion puolustuksen ja välttämättömien toimintojen (mm. vesihuolto, sähkö, ruokahuolto) kannalta kriittiset toiminnot kyetään turvaamaan. Johtaminen on keskitettyä ja niin teknologinen kuin psykologinen resilienssi on maksimoitu. Aktiiviset vastatoimet voidaan kohdistaa konfliktin vastapuoleen liittolaisten tai muiden verkkojen kautta. Kaikki edellä mainitut toimet voidaan toteuttaa joustavasti ja suljettu kansallinen verkko voidaan palauttaa normaalitilaan poliittisen tilanteen salliessa.

Avoimien verkkojen valtioilla ei ole konfliktin aikana mahdollisuutta vastaavaan toimintatapaan kuin suljetun verkon valtioilla. Turvallisuustoimijoiden toimivaltaa ja kansallisen verkon valvontaa voidaan lisätä, mutta lainsäädännöllisistä ja liiketaloudellisista syistä suorituskykyjen vahvistuminen tapahtuu hitaasti. Kyberturvallisuustoimijoiden saattaminen yhteistyöhön edellyttää sektorirajojen ylittämistä, koordinointia ja neuvotteluja. Yhteiskunnalliset, liiketaloudelliset ja normatiiviset tekijät voivat vaikuttaa negatiivisesti avoimien verkkojen valtioiden asevoimien tai turvallisuustoimijoiden toiminnanvapauteen niiden puolustaessa kansallisia verkkoja. Konflikti ja sodan alku voivat häiritä tieteellisteknologista perustaa tavalla, joka heikentää avoimien kansallisten verkkojen resilienssiä. Kansainväliset keskinäisriippuvuudet voivat joutua tarkoituksella tai tahattomasti negatiivisten vaikutusten kohteeksi. Suljettujen ja avoimien verkkojen voimasuhteeseen vaikuttaa ennen kaikkea toimenpiteiden nopeus ja ajoitus sekä tilannetiedon jakaminen ja täten tilanneymmärryksen muodostuminen sodan alkuvaiheessa. Tässä valtiosuhteiden vaiheessa suljettuja verkkoja voidaan kutsua ”suljetuksi” ja avoimia verkkoja ”tehostetusti valvotuksi.”

Sota on valtioiden välinen tila, jossa poliittisten päämäärien tavoittelemiseksi käytetään avointa sotilaallista voimaa. Hallitseva uhkakuva suurvaltojen tapauksessa on suurvaltojen välinen sota, joka voi eskaloitua totaaliseksi ydinsodaksi. Pienempien valtioiden tapauksessa

uhkakuvana on laajamittainen konventionaalinen sota. Osa suljetun ja avoimen kansallisen verkon alajärjestelmistä menettänee toimintakykynsä. Suljetun verkon etuna on kyky fragmentoitua hallitulla tavalla sisäisesti maantieteellisiin osiin. Tämä on mahdollista sen valtiojohtoisesti rakennetun ja kontrolloidun kriittisen infrastruktuurin takia. Keskitetyn johdon tuhouduttua tai lamauduttua alueelliset siviili- ja sotilasjohtoportaat kykenevät jatkamaan toimintaansa. Suljetun verkon asevoimat kykenevät jatkamaan operointiaan, vaikka ylin johto olisi eristetty joukoista tai tuhottu. Siihen asti, kunnes verkko alkaa hajota osiin, suljetun verkon järjestelmiin on helpompi tuottaa korjaavia päivityksiä kotimaisen tuotannon pohjalta. Aktiivisten sotatoimien aikana suljettujen verkkojen kansalliset ohjelmisto- ja laitejärjestelmät voivat taata aikavoiton hyökkääjän joutuessa takaisinmallintamaan niitä ja etsimään niistä heikkouksia. Toisaalta suljetun verkon keskitetyt järjestelmät voivat osoittautua avoimessa sodassa myös kriittisiksi heikkouksiksi.

Sodan aikana avoimia kansallisia verkkoja ei kyetä eristämään globaalista kybertilasta. Niiden puolustajilla ei ole kykyä hallita verkkojen hajoamista osiin. Toiminnan vapaus menetetään ja yhteinen tilannekuva sirpaloituu. Siviilihallinnon johtaminen halvaantuu. Avoimen verkon valtion asevoimilla voi olla kyky jatkaa toimintaa saarekkeisesti, mutta niiden aikaisempi tiivis yhteistyö siviilioperaattoreiden kanssa suorituskykyjen rakentamiseksi on voinut tuottaa kriittisiä keskinäisriippuvuuksia ja johtaa lamauttaviin heijastevaikutuksiin. Liiketaloudellisiin sopimuksiin perustuvat kahdennetut yhteydet voivat osoittautua epätarkoituksenmukaisesti tai olemattomasti toteutetuksi.[641] Tässä valtiosuhteiden vaiheessa suljettuja verkkoja voidaan ääritapauksessa kutsua ”hallitusti jakautuneeksi” ja avoimia verkkoja ”sirpaloituneeksi”.

Suljetut ja avoimet verkot eroavat toisistaan valtiosuhteiden jatkumolla myös sen suhteen, mikä taho vastaa niiden toiminnasta ja turvallisuudesta ja millä periaatteella verkkoja hallinnoidaan. Rauhanomaisen kilpailun aikana suljetun verkon turvallisuudesta vastaavat turvallisuuspalvelut tai muut nimetyt viranomaiset. Yksityiset toimijat on velvoitettu lailla suojelemaan niiden hallussa olevaa kriittistä informaatioinfrastruktuuria. Ne vastaavat velvoitteiden kustannuksista. Avoimen kansallisen verkon turvallisuudesta vastaa teoriassa kansallinen nCERT/CSIRT. Tosiasiassa

[641] Esim. ks. Korhonen, Suvi: Valtorin pelko osui oikeaan: katkenneet ”kahdennetut” kaapelit samassa kourussa – TietoEvryltä saatetaan vaatia korvauksia. *Tivi*, 22.7.2021 [https://bit.ly/3C7Hxce], luettu 30.7.2021.

palveluntarjoajien ja operaattoreiden tietoverkko- ja tietoturvavalvomot (NOC/SOC) vastaavat turvallisuudesta. Yksityisyritykset tarjoavat tietoturvapalveluja asiakkailleen. Yhteistyö julkisen ja yksityisen sektorin välillä on vapaaehtoista ja perustuu vain löyhästi lakiin tai suosituksiin. Vaikka kansainvälinen yhteistyö ja sopimukset tuovat avoimissa verkoissa kybertilan hallintaan lisää välineitä, avoimissa verkoissa markkinat ja riskit määrittelevät kyberturvallisuuden tason.

Kiristyneen kilpailun aikana suljetun kansallisen verkon turvallisuus siirtyy yksinomaan valtiolle. Turvallisuustoimintaa johdetaan keskitetysti valtionhallinnon poikkihallinnollisten toimielinten kuten turvallisuusneuvoston johdolla. Toimeenpanoa johtavat turvallisuuspalvelut ja kansallinen verkonhallintaviranomainen. Yksityisestä sektorista tulee toimeenpanon väline. Laki toimii tässä vaiheessa lähinnä autoritaaristen toimenpiteiden verhona. Avoimissa verkoissa ei turvallisuuden organisatorisen johtamisen ja verkkojen hallinnan periaatteiden kannalta tapahdu juurikaan muutoksia. Sen sijaan erilaiset sopimusmenettelyt voivat tulla voimaan, jolloin julkisen ja yksityisen sektorin yhteistyö voi tiivistyä ja kansalliset ja kansainväliset yhteistyömekanismit aktivoitua.

Konfliktissa ja sodan alkuvaiheessa suljetun verkon hallinta ja turvallisuus ovat valtiojohdon käsissä ja sen toimeenpanevat turvallisuuspalvelut, verkonhallintaviranomaiset ja rajatusti asevoimat. Sodan alkuvaiheeseen ja kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmän täyteen aktivointiin liittyen voi esiintyä kitkaa eri toimijoiden välillä kybertilan hallinnan siirtyessä yhä suuremmassa määrin asevoimille. Avoimen verkon osalta kansallinen lainsäädäntö tai sen puute, olemassa olevat järjestelmät ja aikaisempi harjoittelu määrittelevät pitkälti johtamisen vastuut ja toimeenpanon onnistumisen. Toimijakenttä voi hajaantua voimakkaasti hallinnonaloittain ja alueellisten sekä paikallisten toimijoiden vastuualueiksi. Yksityissektori vastaa omista verkoistaan valtionhallinnon tarjotessa lähinnä konsultaatio-, synkronointi-, integrointi- ja tiedonvälityspalveluita. Pyrkimys kokonaisvaltaisuuteen on olemassa, mutta sitä ei ole helppo saavuttaa aikakriittisessä tilanteessa.

Sodassa suljetusta kansallisesta verkosta vastaavat asevoimat yhteistyössä aluehallinnon kanssa. Valtiojohto on siirtynyt sodan ajan kokoonpanoon. Tarvittaessa verkon hallinta ja turvallisuus voidaan johtaa strategisoperatiivisten yhtymien ja alue- sekä paikallishallinnon toimenpitein hajautetusti. Avoin kansallinen verkko voi pirstaloituessaan joutua tilanteeseen, jossa hallintaa ja turvallisuutta ei kyetä valtakunnallisella tasolla koordinoimaan. Alueellisten toimijoiden

yhteistyö on *ad hoc* -perustaista. Yhteydenpito sekä tiedonvaihto pirstaloituneen verkon osien välillä on vaikeaa. Valtion keskushallinnon lamauduttua avoimella verkolla ei ole kykyä siirtyä saarekkeisesti johdettuun toimintaan.

Valtiosuhteiden jatkumon kautta tehty tarkastelu syventää suljetun ja avoimen kansallisen verkon välisen rakenteellisen kyberasymmetrian analyysiä. Suljetun kansallisen verkon etu toiminnan vapauden suhteen osoittautuu entistä suuremmaksi. Sillä on hallussaan aloite ja se voi muokata omaa taistelutilaansa kriisin edetessä. Se on nopeampi ja ketterämpi. Sen sijaan yhteisen tilannekuvan osalta kansainvälinen yhteistyö ja avoin tieteellisteollinen perusta antavat rauhanomaisen ja kiristyneen kilpailun aikana edun avoimelle kansalliselle verkolle. Konfliktissa ja sodassa yhteistyömekanismien merkitys heikkenee, muttei katoa. Johtaminen on suljetun kansallisen verkon vahvuus kaikissa suhteiden vaiheessa. Keskitetystä johtamisesta ja etenkin sitä tukevista järjestelmistä voi kuitenkin muodostua myös haavoittuvuus. Resilienssi kääntyy valtiosuhteiden kiristyessä lähtökohtaisesti suljetun kansallisen verkon eduksi. Alkuvaiheessa avoin verkko hyötyy globaaleista tuotantoketjuista ja palveluista, mutta konfliktissa ja sodassa näistä muodostuu riski. Paljon riippuu siitä, missä määrin yksityiset palveluntarjoajat ovat suojanneet järjestelmänsä ja kansallisessa verkossa on terveen kilpailun tuottamaan redundassia. Suljettu verkko sen sijaan alkaa nauttia kansallisen tieteellisteknologisen perustan ja kriittisen informaatioinfrastruktuurin suojaamisen eteen tehdyistä investoinneista konfliktivaiheesta alkaen. Nämä investoinnit eivät kuitenkaan takaa täydellistä suojaa.

4.4 Analyysin yhteenveto

Tässä luvussa Venäjän kansallinen internetsegmentti tulkittiin kansallisen informaatiopuolustuksen ja -turvallisuuden järjestelmän alajärjestelmien kautta suljetun kansallisen verkon malliksi. Suljetun verkon malleja voi olla muitakin. Avoin kansallinen verkko puolestaan johdettiin läntisestä 2010-luvun tavasta hallinnoida kansallista kybertilaa ja käsitteellistettiin samojen alajärjestelmien kautta kuin suljettu verkko. Avoimen kansallisen verkon malleja voi niitäkin olla muita. Analyysin perusteella voidaan väittää, että hyökkäysvektoreiden, kansallisten verkkojen rakenteiden ja valtiosuhteiden jatkumon kautta tarkasteltuna suljetun ja avoimen kansallisen verkon suhteesta muodostuu toiminnan vapauden, yhteisen tilannekuva, johtamisen ja resilienssin erojen kautta rakenteellista kyberasymmetriaa. Asymmetrialla on kuitenkin merkittäviä reunaehtoja, jotka liittyvät varsinkin verkkojen käytännön toteutukseen ja toimivuuteen.

Täydennetyn hyökkäysvektorianalyysin oleellinen lisä aikaisempaan tutkimukseen on sen toteaminen, että suljetun kansallisen verkon puolustaja kykenee muokkaamaan omaa verkkoaan ja korjaamaan sen haavoittuvuuksia huomattavasti tehokkaammin kuin avoimen verkon puolustaja ja täten kiistämään hyökkääjän toiminnan vapauden kybertaistelutilassa. Toisaalta on todettava, että tämä suljetun verkon puolustajan kyky voi osoittautua myös haavoittuvuudeksi, mikäli hyökkääjä kykenee manipuloimaan sitä. Suljetun verkon puolustajan yhteinen tilannekuva on tietojärjestelmien, verkottumisen, automatisoinnin ja organisaation johdosta huomattavasti parempi kuin avoimen verkon puolustajalla. Suljettuun verkkoon hyökkääjän tilannekuvaa rajoittavat verkon muuttuva luonne, kansalliset ratkaisut, aktiivinen harhauttaminen ja vastaoperaatiot. Suljetun verkon keskitetty johtamis- ja toimeenpanojärjestelmä takaa puolustajalle nopean ja joustavan päätöksenteon, tehokkaan toimeenpanon ja mahdollisuuden tulosten arviointiin lähes reaaliajassa. Avoimen verkon puolustajalta puuttuu vastaava järjestelmä. Suljettuun verkkoon hyökkääjä voi kuitenkin kohdistaa hyökkäyksensä suljetun verkon johtamisjärjestelmään, mikä on oleellinen haavoittuvuus. Suljetun verkon puolustajalla on etu resilienssissä. Liitynnät on kahdennettu ja valvottu, kriittiset palvelut kestävät hyökkäyksiä ja kriittinen informaatioinfrastruktuuri on suojattu. Avoimen verkon resilienssi on fragmentoitunut osaverkkojen hallinnoitsijoiden riskiarvioiden vaihtelun takia. Toisaalta avoimen kansallisen verkon heterogeenisyys voi toimia myös resilienssin lähteenä.

Suljetun ja avoimen kansallisen verkon sisäisten rakenteiden tarkastelu vahvistaa havaintoa rakenteellisen kyberasymmetria olemassaolosta. Analyysi tosin nostaa esiin huomionarvoisia seikkoja avoimen verkon ominaisuuksissa. Kansainvälinen yhteistyö ja globaalit toimitusketjut voivat edistää yhteistä tilannekuvaa ja resilienssiä. Verkkojen segmentointi ja teknologisten ratkaisujen heterogeenisyys voivat kääntyä avoimen verkon näkökulmasta vahvuudeksi. Avoimen kansallisen verkon puolustajan kyky rajoittaa hyökkääjän toiminnan vapautta ei ole olematon ja se kykenee vastatoimiin. Resiliensiäkään ei pitäisi nähdä täysin informaatiotilan hallinnasta johtuvana vaan se on teknologisten ja psykologisten tekijöiden summa, jota ei voi täysin irrottaa kulttuurisista, sosiaalisista, taloudellisista ja poliittisista tekijöistä. Avoimen verkon toiminnan vapauden, yhteisen tilannekuvan, johtamisen ja resilienssin ominaispiirteet kytkeytyvät vahvasti valtionhallinnon ja yksityisen sektorin yhteistyön järjestelyihin ja onnistuneeseen toimeenpanoon. Huomion arvoista on myös se, että vaikka verkkojen vertailu näyttäisi suosivan suljettuja kansallisia verkkoja, tämä ei välttämättä käytännössä aina pidä

paikkaansa. Monet suljetun verkon vahvuuksista voivat sisältää ristiriitaisia elementtejä ja muuttua heikkouksiksi määrätyissä tilanteissa.

Valtiosuhteiden jatkumon kautta suoritettu analyysi tarjoaa sekin monivivahteisemman kuvan kuin alkuasetelmasta olisi voinut päätellä. Ensiksikin on todettava, että suljettu kansallinen verkko ei ole yhtä kuin niin kutsutut *Internet shutdown* -prosessit, jossa kansalliset yhteydet globaaliin Internetiin yksinkertaisesti kytketään irti palveluntarjoajien toimesta valtiovallan käskiessä. Irti kytkeminen on äärimmäinen suljetun kansallisen verkon hallinnan muoto. Suljetun kansallisen verkon etu on ennen kaikkea kyvyssä muokata taistelutilaa kriisin kehittyessä ja kyvyssä ylläpitää teknologisen omavaraisuuden avulla järjestelmien toimintaa kansainvälisten toimitusketjujen katketessa. Mitä pidemmälle valtiosuhteiden kriisi etenee sitä suuremmaksi suljetun verkon etu hyökkäyksellisessä ja puolustuksellisessa toiminnan vapaudessa kasvaa, puolustuksellinen johtaminen tehostuu ja resilienssi paranee suhteellisesti verrattuna avoimiin verkkoihin. Yhteisen tilannekuvan osalta tilanne ei ole yhtä selkeä, sillä avoimien verkkojen kansainvälinen yhteistyö mahdollistaa tiedon vaihtamisen kumppaneiden ja liittolaisten kanssa. Mikäli avoimen kansallisen verkon yhteydet ulkomaailmaan kyetään katkaisemaan, se menettää kaikki mahdolliset edut ja kärsii kaikki mahdolliset haitat. Suljettu kansallinen verkko on lähtökohtaisesti rakennettu juuri tällaista tapahtumaa silmällä pitäen.

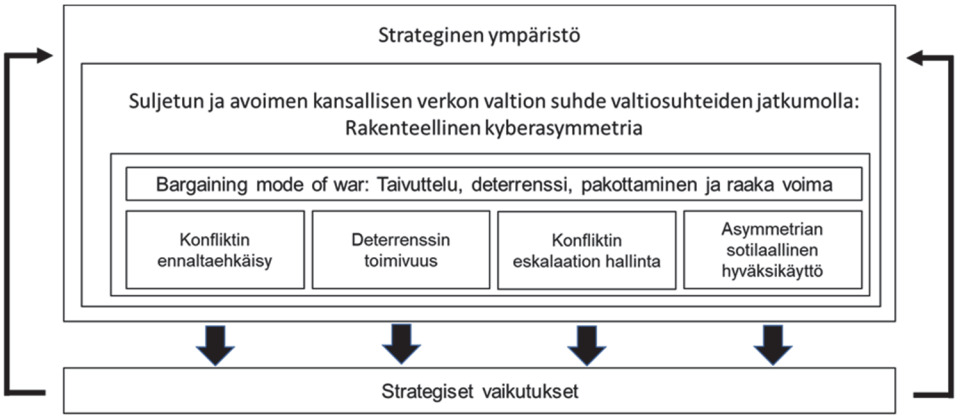
Suljetun ja avoimen kansallisen verkon tarkastelu hyökkäysvektoreiden, kansallisten verkkojen rakenteiden ja valtiosuhteiden jatkumon kautta osoittaa rakenteellisen kyberasymmetrian olemassaolon lisäksi asymmetrian monimutkaisen luonteen. Ensiksikin on ymmärrettävä, että rakenteellinen kyberasymmetria on strategisen tason ilmiö. Edellä esitetty analyysi ei kiistä sitä, etteikö yksittäisillä kyberhaavoittuvuuksilla voisi olla merkittävä vaikutus suljettujen verkkojen toimivuuteen. Kokonaisuutena ja pitkällä aikavälillä informaatioturvallisuuden ja -puolustuksen järjestelmä on kuitenkin kykenevämpi puolustamaan itseään, palautumaan ja tukemaan hyökkäystä kuin avoin kansallinen verkko. Toiseksi on todettava, että suljetun kansallisen verkon sisällä on merkittäviä keskinäisriippuvuuksia, kuten jo luvussa 3.4 tuotiin esiin. Koska suljettu verkko on avointa tiiviimpi, on haitallisten seurauksien leviäminen siinä todennäköisempää ja potentiaalisesti tuhoisampaa. Samalla on kuitenkin huomioitava, että informaatioturvallisuuden ja puolustuksen järjestelmän alajärjestelmät tukevat toisiaan. Suljetussa verkossa on siis sisäsyntyisiä toisiaan kompensoivia vahvuuksia ja heikkouksia. Kolmanneksi on todettava, että suljetun kansallisen verkon vahvuudet perustuvat pitkälti autoritaariseen poliittiseen järjestelmään ja

valtiojohtoiseen talouteen. Suljetun verkon toteuttaminen toisenlaiseen järjestelmään perustuen kohtaisi todennäköisesti lähes ylitsepääsemätöntä vastarintaa talouselämän ja kansalaisyhteiskunnan taholta. Itse asiassa kansallisen internetsegmentin rakentaminen voisi muuttaa pysyvästi valtion luonnetta autoritaariseen suuntaan. Voidaankin pohtia, onko rakenteellisen kyberasymmetrian perimmäinen luonne sittenkin teknologian sijaan poliittinen.

5 Strategiset vaikutukset

Tässä luvussa vastataan kysymykseen, miten rakenteellinen kyberasymmetria vaikuttaa voimankäyttöön tai sillä uhkaamiseen poliittisten tavoitteiden saavuttamiseksi valtioiden välisten suhteiden eri vaiheissa. Näkökulma on luvussa 2 kuvattujen strategisten vaikutusten tarkastelussa. Näitä ovat yhtäältä sellaiset rakenteellisen kyberasymmetrian vaikutukset valtioiden toimintaympäristöön, jotka muuttavat valtioiden voimasuhdetta. Toisaalta tarkastellaan valtioiden välisen kilpailun ja konfliktin voimankäytön ja päämäärän tavoittamisen reunaehtojen muutosta strategisella tasolla. Luvussa esitettävä analyysi on abduktiivinen, historiallinen ja pohdiskeleva.

Luku rakentuu neljästä alaluvusta, joissa strategisia vaikutuksia analysoidaan asettamalla luvussa 4 tehdyt havainnot suljetun ja avoimen kansallisen verkon suhteesta voimankäytön muotojen eli taivuttelun, deterrenssin, pakottamisen ja raa'an voiman kehykseen. Voimankäytön eri muodot sidotaan valtioiden välisen konfliktin eri vaiheisiin tarkastelemalla uhkien ennaltaehkäisyä, deterrenssin toimivuutta, eskaloituvan konfliktin hallintaa ja rakenteellisen kyberasymmetrian sotilaallista hyväksikäyttöä. Luvussa tarkastellaan siis kyberstrategian tekemistä, eli suunnittelua ja toimeenpanoa, muuttuvassa ja muita toimijoita sisältävässä ympäristössä. Luvussa ei ole erillistä yhteenvetoa vaan se esitetään luvussa 6. Analyysin käsitekehys on esitetty kuvassa 12.



Kuva 12: Rakenteellisen kyberasymmetrian strategisten vaikutusten analyysin käsitekehys

Käytetty voimankäytön jaottelu perustuu osiltaan luvussa 2.2 esiteltyyn länsimaiseen *bargaining model of war* -malliin. Tätä rationalistista ja mekanistista näkökulmaa täydennetään analyysissä sosiaalisilla ja kulttuurisilla tekijöillä. Analyysi sidotaan teoreettisen suljetun verkon historialliseen ilmentymään eli Venäjän informaatioturvallisuuden ja -puolustuksen järjestelmään ja sen suhteeseen teoreettiseen avoimeen kansalliseen verkkoon. Venäjän järjestelmää tarkastellaan sen omassa strategisessa ympäristössä. Ympäristön tekijöistä tärkeimmäksi nostetaan voimajakaumaan perustuva rakenne eli toiset suurvallat, maantiede eli kybertoimintaympäristön rakenne sekä hyökkäys-puolustustasapaino, joka tulkitaan suljettujen ja avoimien verkkojen suhteen muutoksen seuraukseksi. Samalla analyysi sidotaan tiiviimmin työn tutkimusongelmaan eli nimenomaisesti Venäjän kansallisen internetsegmentin tuottaman rakenteellisen kyberasymmetrian strategisten vaikutusten tarkasteluun.

5.1 Konfliktin ennaltaehkäisy

Konfliktin ennaltaehkäisy on potentiaalisen uhan neutralointia kaikilla käytettävissä olevilla toimilla niin, että suoraa aseellisen voiman käyttöä tai sillä uhkaamista ei tarvita. Se liittyy valtiosuhteiden rauhanomaisen kilpailun ja kiristyneen kilpailun vaiheisiin, jolloin uhkakuvina korostuvat vakoilu, terrorismi, paikalliset konfliktit ja sisäiset levottomuudet. Kybertoiminnan osalta konfliktien ennaltaehkäisy liittyy tiedusteluun, ennakkovaroituksen hankkimiseen, taivutteluun informaatiovaikuttamista tukemalla, kansainvälisten normien ja liittokuntien rakentamiseen sekä toimintaympäristön muokkaamiseen potentiaalisten uhkien ehkäisemiseksi. Uhkien ennaltaehkäisyllä pyritään kansallisten intressien turvaamiseen estämällä toimintaympäristön potentiaalisista haasteista kehittyvien akuuttien ja todellisten uhkien syntyminen. Ennaltaehkäisyyn pyritään, koska se on kustannustehokkaampaa kuin uhkien torjuminen ja samalla säilytetään valtion kansainvälispoliittinen toiminnanvapaus omien intressien ajamiseksi.

Rakenteellinen kyberasymmetria ei ole vahvimmillaan tilanteessa, jossa konflikteja voidaan vielä ennaltaehkäistä. Suljettujen ja avoimien kansallisten verkkojen erot ovat pienimmillään. Toisaalta suljetun kansallisen verkon informaatioturvallisuuden ja -puolustuksen järjestelmän alajärjestelmät ovat toiminnassa ja tarjoavat keinoja uhkien hallitsemiseksi ja toimintaympäristön muokkaamiseksi. Järjestelmä toimii ulkoisen ja sisäisen viestinnän välineenä, edes auttaa normien, sääntöjen ja suvereenien rajojen rakentamista kybertilaan, tuottaa teknologista itsenäisyyttä ja omavaraisuutta, rakentaa kansallisesti yhtenäisen

mediaympäristön, kerää kansallista kyber- ja informaatiotilannekuvaa ja toimeenpanee valtiojohtoisen, keskitetyn kokonaisinformaatioturvallisuuden mallin. Vastavuoroisesti avoimet kansalliset verkot ovat määritelmän omaisesti avoimia vaikuttamiselle. Niillä on suljettuja verkkoja vähemmän mahdollisuuksia torjua ei-sotilaallisen ja rajoitetun voimankäytön keinoja. Niiden tehokas toiminta on sidoksissa kansainvälisen järjestyksen tasapainoon, toimitusketjuihin ja moninaisiin yhteistyön mekanismeihin.

Tiedustelu taloudellisen, poliittisen ja sotilaallisen edun ja ennakkovaroituksen hankkimiseksi on oleellinen osa informaatioturvallisuuden ja -puolustuksen järjestelmän toimintaa. Tiedustelu muodostaa merkittävän osan rauhanomaisen ja kiristyneen kilpailun jatkuvasta matalan intensiteetin ”kyberkonfliktista.”[642] Venäjän tapauksessa suurvaltojen välisen vastakamppailun strategiskulttuurinen idea edellyttää tiedonhankintaa. Muulla tavoin toimiminen johtaisi yllätetyksi tulemiseen. Tiedonhankinta koskee otaksuttujen uhkakuvien valossa niin ulkomaisia kuin kotimaisia toimijoita. Samaan aikaan pyritään vastapuolen tiedonhankinta estämään tai syöttämään vastapuolelle haluttua tietoa.[643] Avoimia kansallisia verkkoja on lähtökohtaisesti helpompi tiedustella kuin suljettuja. Suljettu informaatioturvallisuuden ja -puolustuksen järjestelmä edesauttaa salaamista, mutta synnyttää myös ongelmia. Salaaminen aikaansaa epäluuloa ja epävarmuutta potentiaalisissa vastustajissa ja lisää niiden tiedustelupyrkimyksiä. Tiedustelun intensiteetin kasvu voidaan tulkita provokatiiviseksi. Oman informaatioympäristön voimakas valvonta ja hallinta voi johtaa siitä tehtyjen havaintojen ja tulkintojen vääristymiseen. Autoritaarisen valtiojohdon pelot ja peilikuva-ajattelu voivat johtaa virhearviointeihin.[644] Täten suljetun kansallisen verkon valvonnan ja kontrollin vääristämä kotimainen informaatiotila voi tuottaa niin puutteellisia havaintoja kuin virheellisiä tulkintoja. Lopputuloksena ennakkovaroitus voi epäonnistua joko olemalla ennen aikainen tai myöhästymällä. Tuloksena voi myös olla kyberasevarustelukierre.

---

[642] Rid (2017); Valeriano & Maness (2015).
[643] Johnson, Loch K.: *Handbook of Intelligence Studies*. Routledge, London & New York, 2007.
[644] Bar-Joseph, Uri & Levy, Jack S.: Conscious Action and Intelligence Failure. *Political Science Quarterly*, Vol. 124, No. 3 (Fall 2009), s. 461–488.

Monimuotoinen informaatiovaikuttaminen[645] on osa konfliktin ennalta ehkäisyä. Kybertoimintaympäristö toimii sen välineenä ja alustana. Suljettujen kansallisten verkkojen informaatioturvallisuuden ja -puolustuksen järjestelmä ennaltaehkäisee uhkia valvomalla omaa tilaansa, puuttumalla sen vapaaseen käyttöön ja tukemalla vastavaikuttamista. Kun informaatiotila on kansallisessa hallinnassa, kyetään paremmin ehkäisemään ”informaatioaseen” käyttäminen ulkopuolelta. Sisäisiä levottomuuksia ei syty, kun kansalaisyhteiskunnasta nousevat ryhmät ja/tai niiden ulkopuoliset tukijat eivät voi vapaasti viestiä, verkostoitua ja mobilisoitua. Ulkopuolelle ei välity tietoa, joka oikeuttaisi ulkopuolisten toimenpitein toteutetun kansalaisten ihmisoikeuksien puolustamisen alistavaa valtiovaltaa vastaan. Terroristinen propaganda ja värväystoiminta kiistetään. Oman kansakunnan eheyttä ja resilienssiä vahvistetaan markkinoimalla patriotismia, nationalismia ja perinteisiä, omaperäisiä arvoja sekä kiistämällä vaihtoehtoiset arvojärjestelmät. Poikkeavat mielipiteet ajetaan marginaaliin ja ääritilanteessa tukahdutetaan väkivalloin. Potentiaalisilta uhilta ikään kuin kiistetään ”happi” eli informaatiotila, jossa ne voisivat versoa. Kansallista internetsegmenttiä ei kuitenkaan täysin suljeta tai edes pyritä tekemään täysin ”tiiviiksi” ilmaisun vapauden osalta. Järjestelmässä on oltava ”paineventtiili”[646], jotta toisinajattelu ei johtaisi vallankumoukseen. Tiedustelun kannalta tilassa on oltava jonkin verran vapautta, jotta oppositiota, terroristeja, ulkomaisia toimijoita ja vallankumouksellisia voidaan seurata.

Niin suljetun kuin avoimen kansallisen verkon valtion ulkopuolelle suuntautuvat aktiiviset toimenpiteet pyrkivät muokkaamaan globaalin kyber- ja informaatiotilan vihamielisestä jopa suotuisaksi. Itsestään selvimmät menetelmät perustuvat vakoiluun, manipulaatioon, väärän tiedon levittämiseen ja harhauttamiseen.[647] Keinot eivät voi kuitenkaan olla pelkästään vihamielisiä tai salattuja. Toimenpiteillä on useita eri suuntia, yleisöjä ja linjoja.[648] Venäjän tapauksessa taivuttelun kohteina ovat Lännen lisäksi pseudokommunistinen Kiina, entiset Neuvostoliiton maat autokratioista demokratioihin, Lähi-idän muslimi- ja arabimaat, Afrikan ja

---

[645] Ks. käsitteestä: Sanastokeskus TSK (2018), s.29.
[646] Paineventtiilin idea on lainattu: Whyte & Mazanec (2019), s. 178–179.
[647] Näistä ks. Ajir, Media & Vailliant, Bethany: Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*, Vol. 12, No. 3 (Fall 2018), s. 70–89; Kelly, Alan & Christopher, Paul: *Decoding Crimea. Pinpointing The Influence Strategies Of Modern Information Warfare*. NATO Strategic Communications Centre of Excellence, Riga, 2020; Rid (2020).
[648] Gioe et al. (2020).

Latinalaisen-Amerikan monimuotoiset valtiot. Näissä maissa positiivisen Venäjä-kuvan luominen on hyödyllisempää kuin vihamielinen propaganda ja kohdemaan horjuttaminen. Venäjän kansallinen internetsegmentti voi tarjota positiivisen kehitysvaihtoehdon mallin, markkinoita ja kilpailukykyisiä tuotteita. Informaatioturvallisuuden ja -puolustuksen järjestelmästä tulee suurvallan statuksen symboli ja se voi vetää puoleensa ihmisryhmiä ja valtioita.

Kansallinen internetsegmentti ei ole siis pelkästään eristäytymisen väline. Se voi toimia vahvistaa valtion vaikutusvaltaa ja täten ennaltaehkäistä uhkia ja konflikteja vetovoiman kautta. Potentiaalinen ”kybersaarto” eli ulkopuolelta suoritettu internetyhteyksien katkaiseminen on vaikea toteuttaa tai sen vaikutus vähenee, mikäli suurvalta kykenee luomaan oman kyberetupiirin tai edes luotettujen liittolaisten verkoston. Kääntöpuolena vetovoiman luomisessa on se, että keskinäisriippuvuuksien takia suljetun verkon turvallisuuslogiikka alkaa rapautua. Esimerkiksi Venäjän ja Kiinan lisääntyvä yhteistyö 5G ja tekoälyteknologian saralla voi synnyttää keskinäisriippuvuuksia, haavoittuvuuksia ja siteitä, joita Venäjän on vaikea halutessaan katkoa. Kiinan tulokulma kybertoimintaympäristön hallintaan on eri kuin Venäjällä. Se on vientiriippuvainen maa, jolle sulkeutuminen tarkoittaisi talouden romahtamista. Kiinan intresseissä on uusi, globaali, kiinalaisille standardeille perustuva Internet, joka on verkottunut Kiinaan digitaalisen silkkitien kautta.[649]

Huolimatta keskinäisistä eroista Venäjän ja Kiinan nykyinen yhteistyö rapauttaa avoimien kansallisten verkkojen perustaa. Ne haastavat läntisille arvoille ja taloudellisille eduille perustuvan avoimen globaalin kyber- ja informaatiotilan hallinnan. Teknologian ihmisoikeuksia kunnioittava käyttö alistetaan valtiojohdon turvallisuusintresseille.[650] Vaihtoehtoiset standardit ja teknologiat voivat muuttaa globaalin informaatiotilan

---

[649] Bendett, Samuel & Kania, Elsa B.: *A new Sino-Russia high-tech partnership. Authoritarian innovation in an era of great-power rivalry*. ASPI Policy brief Report No. 22/2019. [https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership], luettu 7.5.2021; Chuanying, Lu: Forging Stability in Cyberspace. *Survival*, Vol. 62, No. 2 (2020), s. 125–136; Hoffmann, Stacie, Lazanski, Dominique & Taylor, Emily: Standardising the Splinternet: How China’s Technical Standards Could Fragment the Internet. *Journal of Cyber Policy*, Vol. 5, No. 2 (2020), s. 239–264.

[650] Shahbaz, Adrian: *Freedom on the Net 2018. The Rise of Digital Authoritarianism*. Freedom House, 2019. [https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism], luettu 29.12.2020.

hallinnan voimasuhteita. Syntyy kysyntää ja painetta neuvotella uudelleen kyber- ja informaatiotilan säännöt.

Kyberdiplomatialla on vähintään yhtä merkittävä rooli kuin salaisella ja epäsuoralla informaatiovaikuttamisella. Sen avulla voidaan kansainvälisten ja alueellisten instituutioiden ja kahden- sekä monenkeskisten suhteiden kautta muokata toisten valtioiden toimintaa, intressejä ja arvoja itselle sopivampaan suuntaan. Suljettujen kansallisten verkkojen toteuttamista tukee informaatio- ja kybersuvereenisuuden sekä informaatio- ja kyberaseiden kiellon normien rakentaminen. Venäjä, Kiinan ohella, ajaa voimakkaasti kumpaakin.[651] Normeilla on ennaltaehkäisevä vaikutus. Jos maailma hyväksyy kybersuvereniteetin normin Venäjän ja Kiinan ajamassa muodossa ja kansalliset internetsegmentit suvereenina tilana, teknologisesti heikommat valtiot saavat lisäsuojaa informaatiovaikutuksilta ja globaaleilta markkinavoimilta, autoritaariset valtiot luvan polkea ihmisoikeuksia ja liberaalidemokraattiseen universaaliin arvopohjaan perustuvat liittokunnat joutuvat uudelleen määrittelemään arvonsa ja intressinsä. Informaatiotilan, -talouden ja -yhteiskunnan valvonta normalisoituu ja valtion väkivallan monopoli laajenee. Levittäessään kybersuvereenisuuden sanomaa Venäjä kykenee esiintymään valikoidulle yleisöille heikompien esitaistelijana ja vahvojen entisenä uhrina, joka maksaa takaisin kokemansa kohtelun. Toisaalta vähemmän autoritaarinen kybersuvereniteetin määrittely saattaa parantaa pienten valtioiden asemaa suhteessa suurvaltoihin ja monikansallisiin teknologia- ja internetyrityksiin.

Kyberdiplomatia ei perustu pelkästään voimankäyttöä hillitsevien jaettujen arvojen ja intressien tai riippuvuuksien luomiseen.[652] Diplomatian retoriikka voidaan yhdistää muihin vaikuttamisen muotoihin kohteiden manipuloimiseksi toistuvalla, vähittäin kumuloituvalla toiminnalla.[653] Diplomatian ja hyökkäyksellisten, aseellisen toiminnan kynnyksen alle jäävien kyber- ja informaatio-operaatioiden avulla voidaan muuttaa

---

[651] Boeders, Dennis & van den Berg, Bibi: *Governing Cyberspace: Behavior, Power, and Diplomacy*. Rowman & Littlefield, New York & London, 2020; Flonk, Daniëlle, Jachtenfuchs, Markus & Obendiek, Anke S.: Authority Conflicts in Internet Governance: Liberals vs. Sovereigntists? *Global Constitutionalism*, Vol. 9, No. 2 (2020), s. 364–386.
[652] Nye (2016/2017), s. 58–62; Brantly, Aaron F.: Entanglement in Cyberspace: Minding the Deterrence Gap. *Democracy and Security*, Vol. 16, No. 3 (2020), s. 210–233.
[653] Whyte, Christopher: Beyond Tit-for-tat in Cyberspace: Political Warfare and Lateral Sources of Escalation Online. *European Journal of International Security*, Vol. 5, No. 2 (2020), s. 195–214.

potentiaalisten vastustajien suhdetta kyber- ja informaatiotilaan. Venäjä näyttää osittain onnistuneen tässä. Viimeisen parin vuoden aikana eräät läntiset akateemikot, poliitikot ja instituutiot ovat alkaneet julkisesti pohtia valtioiden digitaalisen suvereniteetin määrittelyn välttämättömyyttä.[654] Lisäksi Venäjän, ja muidenkin, kyberhyökkäyksiin on päätetty vastata kehittämällä erityistä kyberdeterrenssin politiikkaa. Vihamielisiin kyberhyökkäyksiin pyritään vastaamaan välittömästi ja suhteellisesti sekä attribuoimaan syylliset jopa yksittäisen henkilön tarkkuudella.[655] Toimien ja vastatoimien logiikka voi kärjistäen johtaa neljään lopputulemaan: Lännen vastustajat jatkavat avoimien verkkojen heikkouksien hyväksikäyttöä loputtomiin potentiaalisia vastustajia horjuttaakseen, deterrenssiviestintä ja / tai yksityissektorin aloitteet toimivat ja suurvallat pääsevät sopuu pienimmän mahdollisen nimittäjän normeista, latentti globaali kyberkonflikti eskaloituu niin, että kansainvälinen suvereenisuuteen perustuva normisto koetaan lopulta välttämättömäksi tai kyberkonflikti ylittää hallitsemattomasti aseellisen voimankäytön rajan ja sitä seuranneen sodan jälkiseurauksena sovitaan globaalisti kybervoimankäytön ja -vakoilun säännöistä.

Konfliktien ennaltaehkäisy perustuu informaatioturvallisuuden ja -puolustuksen järjestelmän näkökulmasta pitkälti globaalin kybertoimintaympäristön eli valtion strategisen ympäristön muokkaamiseen. Strategisiin vaikutuksiin päästään kontrolloimalla omaa informaatiotilaa, rakentamalla potentiaalista kybervoimaa tasapainon säilyttämiseksi ja muokkaamalla globaalia kybertilaa ja sen toimijoiden intressejä teknologisilla, taloudellisilla ja normatiivisilla keinoilla. Tätä strategiaa edes auttaa se, että avoimien verkkojen kansakunnat ovat manipuloitavissa ja globaali kybertila muokattavissa diplomatian keinoin.

---

[654] Mazarr, Michael J.: Virtual Territorial Integrity: The Next International Norm. *Survival*, Vol. 62, No. 4 (2020), s. 101–118; Ulkoministeriö: *Kansainvälinen oikeus kyberympäristössä - Suomen kansallisia kantoja*. Ulkoministeriö, 15.10.2020. [https://um.fi/documents/35732/0/Suomennos+Kansainv%C3%A4linen+oikeus+kyberymp%C3%A4rist%C3%B6ss%C3%A4.pdf/26706a43-4d7e-07da-8c4f-7c53b6ca51ab?t=1602581216672], luettu 16.10.2020; Ministère des Armées: *Droit International Appliqué Aux Opérations Dans Le Cyberespace*, 2019. [https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf], luettu 8.10.2020.

[655] Braw & Brown (2020).

Konfliktien ennaltaehkäisyn mahdollistavien tiedustelun, vastavaikuttamisen, diplomatian ja toimintaympäristön muokkaamisen taustalla on kansallisen internetsegmentin kybervoimaa tuottava luonne. Se tukee kotimaista osaamista, tuotantoa ja infrastruktuurin vahvistumista. Tätä kautta suljettu kansallinen verkko voi vaikuttaa strategiseen tasapainoon, suurvaltojen suhteisiin ja pienempien valtioiden liittoutumisratkaisuihin. Suurvaltojen voimatasapaino on periaatteessa vakauden tae.[656] Internetsegmentti voi siis ennalta ehkäistä uhkia omavaraisen ja itsenäisen teknologisen kehityksen kautta ja luoda varmuutta sekä poistaa pelkoja. Toisaalta niin Yhdysvaltojen, Kiinan kuin Venäjän johto on viimeaikaisissa lausunnoissaan ja strategia-asiakirjoissaan asettanut informaatioteknologisen suorituskyvyn valtion voimanlähteeksi. Tämä suorituskyky ei voi olla kilpailijoita heikompi. Tästä seuraa, että oma jälkeenjääneisyys tai kilpailevan suurvallan etumatka nähdään rauhaa ja valtion olemassaoloa uhkaavana tekijänä.[657] Informaatioturvallisuuden ja -puolustuksen järjestelmän toimiessa liian hyvin se voidaan kokea suurvaltatasapainoa uhkaavaksi tekijäksi. Avoimien verkkojen valtiot voivat tuntea itsensä haavoittuvaisiksi potentiaalisen rakenteellisen kyberasymmetrian uhatessa. Tällöin pyrkimys konfliktin ennaltaehkäisemiseen muuttuukin tahattoman eskalaatio lähteeksi.

On täysin perusteltua kysyä, onko informaatioturvallisuuden ja -puolustuksen järjestelmä, suljettu kansallinen verkko, suhteeton ratkaisu informaatiotilasta kumpuavaan turvallisuusuhkaa? Eikö kiinalainen malli, joka keskittyy hajautettuun sensuuriin, olisi kustannustehokkaampi vaihtoehto autoritaarisille valtioille?[658] Suljetun verkon ennaltaehkäisyn malli voi synnyttää vastarintaa ja aiheuttaa pelkoa potentiaalisissa vastustajissa synnyttäen uusia uhkia.[659] Toisaalta kansallinen

---

[656] Schörnig, Niklas: Neorealism. Teoksessa *Theories of International Relations*. Schieder, Siegfried & Spindler, Manuela (ed.) Routledge, New York, 2015, s. 37–55.
[657] Chekov, Alexander D., Makarycheva, Anna V., Solomentseva, Anastasia M., Suchkov, Maxim A. & Sushentsov, Andrey A.: War of the Future: A View from Russia. *Survival*, Vol. 61, No. 6 (2019), s. 25–48; Kania, Elsa B & Costello, John: Seizing the Commanding Heights: The PLA Strategic Support Force in Chinese Military Power. *Journal of Strategic Studies*, 2020, DOI: 10.1080/01402390.2020.1747444; Raska, Michael: The sixth RMA wave: Disruption in Military Affairs? *Journal of Strategic Studies*, 2020, DOI: 10.1080/01402390.2020.1848818.
[658] Ramesh, Reethika et al.: Decentralized Control: A Case Study of Russia. *Network and Distributed Systems Security (NDSS) Symposium 2020 23-26 February 2020, San Diego, CA, USA*.
[659] Olettaen, että turvallisuusdilemmateoria pitää paikkansa (Glaser (1997)).

internetsegmentti sitoo yhteen valtion turvallisuustoimijoita ja tarjoaa näin paremman tilannekuvan ja -ymmärryksen potentiaalisista uhista, joihin voidaan siten yrittää ennakolta vaikuttaa. Niin tai näin kansallinen kyberturvallisuuden ja -puolustuksen järjestelmä ei ole täydellinen kyberstrategian väline uhkien ennaltaehkäisemiseksi. Sen luonne edellyttää rakentajaltaan suurvallan resursseja ja määrättyä poliittista järjestelmää tuottaakseen tarjolla olevat edut.

5.2 Deterrenssin toimivuus

Deterrenssi on toiminnassa samaan aikaan kuin konfliktien ennaltaehkäiseminen, mutta perustuu taivuttelun sijaan lupaukseen kivusta. Kyberdeterrenssi on potentiaalisen vastustajan taivuttelua pidättäytymään voimankäytöstä kybertilassa, kybertilasta tai muussa tilassa uhkaamalla sitä sietämättömällä rangaistuksella, kiistämällä potentiaaliset hyödyt tai muutoin vaikuttamalla vastustajan hyötykustannuslaskelmiin kybertilaan liittyvillä suorituskyvyillä. Kohteen päätettyä käyttää avoimesti aseellista voimaa tavoitteidensa saavuttamiseksi deterrenssi on pettänyt. Kyberdeterrenssi liittyy valtiosuhteiden rauhanomaisen kilpailun, kiristyneen kilpailun ja konfliktin vaiheisiin, jolloin uhkakuvina korostuvat vakoilu, terrorismi, paikalliset konfliktit, sisäiset levottomuudet, alueellinen sota ja kansannousu. Kyberdeterrenssin keinot vaihtelevat ei-sotilaallisista sotilaallisiin, mutta jäävät avoimen sotilaallisen aseellisen voimankäytön rajan alle.

Rakenteellisella kyberasymmetrialla on merkittävä vaikutus deterrenssiin, mutta sen vahvuus vaihtelee suljetun ja avoimen kansallisen verkon tilojen mukaan. Rauhanomaisen kilpailun, kiristyneen kilpailun ja konfliktin aikana kansallisen internetsegmentin tilaa kyetään valvomaan ja muuttamaan sekä uhkiin vastaamaan keskitetysti ja nopeasti. Informaatioturvallisuuden ja -puolustuksen järjestelmä tuottaa kansallista kyber- ja informaatiotilannekuvaa, tukee keskitetyn kokonaisinformaatioturvallisuuden mallin toimeenpanoa, edistää kyberresilienssiä ja vahvaa henkistä kriisinkestävyyttä sekä maanpuolustustahtoa ja turvaa kansallisen informaatiotilan ja sen rajojen hallinnan. Nämä tekijät vahvistavat kiistämisdeterrenssiä. Toisaalta kansallinen internetsegmentti turvaa ydinasein, tavanomaisia asein ja muin keinoin (ml. kyber) suoritettavan ensi- ja vastaiskukyvyn. Suljetun kansallisen verkon valtio kykenee siirtymään kyber- ja informaatiouhkien torjuntaan minimaalisilla lisäkustannuksilla – toisin kuin avoin kansallinen verkko. Avoin kansallinen verkko ei itsessään toimi deterrenssin välineenä

tai tue sen toteuttamista. Tämän ovat viime aikoina huomanneet niin Yhdysvallat kuin Euroopan Unionin jäsenmaatkin.[660]

Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä hyödyttää ennen kaikkea kiistämiseen perustuvaa deterrenssiä. Järjestelmä sitoo siviili- ja sotilastoimijat poikkihallinnolliseen yhteistyömalliin, jonka tehtävä on turvata valtio muun muassa kyber- ja informaatiouhilta. Tämä malli kehittää suorituskykyjä ja antaa viestin koko kansakunnan sitoutumisesta uhkien torjuntaan tarvittaessa. Toisaalta korkeatasoinen ja ajanmukainen kyber- ja informaatiotilannekuva mahdollistaa sotatoimia alempien hyökkäysten attribuution ja kasvattaa hyökkääjien kustannuksia ja tavoitteiden saavuttamisen epävarmuutta.

Toimiakseen täydellisesti kiistämiseen perustuvan deterrenssin osana kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmän tulee ulottua Internetin lisäksi avaruuteen ja koko vapaan tilan sähkömagneettiseen spektriin. Datan kulku tulee kyetä valvomaan ja estämään kaikissa tiloissa. Täydellinen eristäminen ei kuitenkaan ole deterrenssin edellytys. Riittää, että hyökkäämisestä tulee liian kallista ja epävarmaa tavoitteisiin nähden. Sitä paitsi järjestelmän ulkopuolelle jää aina jokin tila, josta vallanpitäjiä voidaan uhata.Voi kuitenkin olla, että täydelliseen eristämiseen pyritään päätöksentekijöiden epävarmuuden ja pelkojen takia. Kun informaatiotilaa ja sen rajoja aletaan hallita, syntyy helposti täydellisyyteen pyrkivä kierre.

Informaatiotilan hallinnan rinnalla ajatus Yhdysvaltojen teknologisen ylivoiman kiistämisestä on Venäjän kansallisen internetsegmentin rakentamisen perusargumentti. Internetsegmentin tulee estää valtion kytkeminen irti Internetistä ulkopuolelta tai vähintään lievittää irti kytkemisen haitallisia vaikutuksia. Sen tulee estää vihamielinen informaatiovaikuttaminen ja iskut kriittiseen informaatioinfrastruktuuriin. Sen tulee suojella valtiota painostukselta, kiristykseltä ja johdon lamauttamiselta. Haasteena on, että informaatioturvallisuuden ja -puolustuksen järjestelmällä on deterrenssiarvoa vain, mikäli potentiaaliset hyökkääjät näin kokevat.[661] Valtion kansalliseen internetsegmenttiin uhraamien varojen pitäisi periaatteessa kasvattaa sen kiistämiseen perustuvan deterrenssin uskottavuutta ja kompensoida niitä potentiaalisia

[660] Cyberspace Solarium Commission (2020); European Commission (2020).
[661] Morgan, Patrick M. (Ed.): *Deterrence Now*. Cambridge University Press, Cambridge, UK, 2003; Mazarr, Michael J.: *Understanding Deterrence*. RAND, Santa Monica, 2018.

etuja, jotka se menettää jättämällä osallistumatta kansainväliseen yhteistyöhön. Taloudelliset uhraukset osoittavat sitoutumista. Venäjän kansallisen digitaalisen talouden ohjelman budjetti ja ”suvereenin Internetin” rakentamiseen liittyvät kustannukset ovat osa sitoumuksen viestimistä.[662]

Informaatioturvallisuuden ja -puolustuksen järjestelmä vahvistaa merkittävästi suljetun kansallisen verkon resilienssiä. Tämä vaikuttaa potentiaalisen hyökkääjän laskelmiin pienentämällä todennäköisyyttä tuottaa kyberhyökkäyksellä pysyvää vahinkoa. Järjestelmä tekee hyökkäysten valmistelusta vaikeampaa, mikä nostaa hyökkääjän kustannuksia ja lisää onnistumisen epävarmuutta. Resilienssin johdosta kohteen pakottaminen muodostuu liian kalliiksi ja tulos epävarmaksi. Resilienssistä johtuva konfliktin pitkittyminen voi merkitä hyökkääjälle kansainvälispoliittisen aseman vaikeutumista. Hyökkääjän on arvioitava oma kykynsä ja halunsa eskaloida konfliktia, mikäli kohdevaltio ei taivu hyökkäyksen edessä. Jos suljetun kansallisen verkon valtioon hyökkääjä käyttää pelkkiä informaatio- ja kyberkeinoja, sen pitää olla valmis sietämään pitkittynyttä konfliktia. Tavoitteiden saavuttamisen nopeuttaminen voi edellyttää voimankäytön laajentamista muihin toimintaympäristöihin. Tähän hyökkääjällä ei välttämättä ole tahtoa tai resursseja ja se voisi johtaa kansainvälisen yhteisön kielteiseen reaktioon.

Kansallinen informaatiopuolustuksen ja -turvallisuuden järjestelmä ei ole aukoton. Luvussa 4 todettiin, että järjestelmän hallinta-alajärjestelmä on luonteensa vuoksi haavoittuvainen hyökkäyksille. Määrätietoinen hyökkääjä voi kohdistaa hyökkäyksensä hallintajärjestelmään, johon päästyään sen jatkotoiminnan kulut ja informaatioturvallisuuden ja -puolustuksen uskottavuus romahtavat.[663] Sama pätee rajatusti muihinkin alajärjestelmiin. Esimerkiksi kotimaiset ohjelmisto- ja laiteratkaisut voivat muuttua kriittisiksi haavoittuvuuksiksi, jos (kun) niistä löytyy 0-päivä

---

[662] Digitaalisen talouden ohjelman budjetti vuosille 2018–2024 oli vuonna 2018 21,1 $ miljardia. Vuosina 2019–2020 summa on jonkin verran laskenut. ”Jarovaja-lain” ja ”suvereenin Internetin” lain seurauksena Internet- ja mobiililiittymien on arvioitu kallistuvan 10–15 % (Полякова, Виктория: СМИ узнали о возможном росте цен на домашний интернет и ТВ на 15–20 %. *РБК* 26 июл 2020. [https://www.rbc.ru/technology_and_media/26/07/2020/5f1cd34d9a79471490c2fa3e], luettu 5.1.2021; Воейков, Денис: «Цифровая экономика» исполнила бюджет хуже всех нацпроектов. *CNews.ru*, 13.1.2020. [https://www.cnews.ru/news/top/2020-01-13_tsifrovaya_ekonomika_provalila], luettu 5.1.2020.

[663] Ajatus hyökkäjän kulujen romahtamisesta on Aaron Brantlyltä (Brantly (2020)).

haavoittuvuuksia tai omille turvallisuusviranomaisille jätettyjä takaovia. Hyökkääjä voi olla valmis käyttämään merkittäviä resursseja saadakseen salatun pääsyn järjestelmään myöhempää hyväksikäyttöä silmällä pitäen. Suljetun vekon valvontaa varten kerätty massiivinen datavaranto voidaan varastaa ja hyödyntää myöhemmin.

Kiistämiseen perustuvan deterrenssin toteuttaminen informaatioturvallisuuden ja -puolustuksen järjestelmän tarjoamien keinojen avulla edellyttää jatkuvaa ylläpitoa, kehittämistä ja resursseja. Kansallisen segmentin tietoturvaratkaisujen tulee perustua uusimpaan teknologiaan. Tekoäly- ja kvanttiteknologian kehittäminen ja käyttöön saaminen ovat kriittisiä tekijöitä. Toisaalta niin tekoäly kuin kvanttiteknologia synnyttävä uusia haavoittuvuuksia ja riskejä.[664] Ne korostavat kybertoimintaympäristön riippuvuutta nopeasti kehittyvästä ja vanhenevasta teknologiasta. Verrokkina todettakoon, että Yhdysvaltojen mannertenvälinen Minuteman III ohjus otettiin käyttöön 1970-luvulla.[665] Nykyaikaisen käyttöjärjestelmän keski-ikä merkittävien päivitysten osalta on joitain vuosia.[666]

Kansallisten internetsegmenttien riippuvuus teknologiasta lisää oleellisesti kyberasevarustelukierteen riskejä. Varustelukierre korostaa sitä seikkaa, että kun järjestelmä on kerran luotu, siitä on vaikea luopua avaamatta merkittäviä haavoittuvuuksia siirtymäkauden aikana.[667] Yksikään suurvalta ei ole ollut vielä valmis vapaaehtoisesti ja yksipuolisesti luopumaan strategista etua tuottavasta asejärjestelmästä.

---

[664] Crane, Keith W., Joneckis, Lance G., Acheson-Field, Hannah, Boyd, Iain D., Corbin, Benjamin A., Han, Xueying & Rozansky, Robert N.: *Assessment of the Future Economic Impact of Quantum Information Science*.
Institute for Defense Analyses, 2017; ID Quantique: *Understanding Quantum Cryptography*, White paper, May 2020. [https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf], luettu 24.11.2020.

[665] Kristensen, Hans M. & Korda, Matt: United States Nuclear Forces, 2020. *Bulletin of the Atomic Scientists*, Vol. 76, No. 1 (2020), s. 46–60.

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

[667] Esimerkiksi Microsoftilla on ollut merkittäviä haasteita saada käyttäjät luopumaan Windows XP ja 7 käyttöjärjestelmistä, vaikka niiden tuki on lakkautettu (Warren, Tom: Microsoft Bids Farewell to Windows 7 and the Millions Of PCs That Still Run It: An End of the Traditional Windows Era. *The Verge*, 14.1.2020. [https://www.theverge.com/2020/1/14/21065122/microsoft-windows-7-end-of-support-lifecycle-millions-pcs], luettu 5.1.2021).

Kansallisen internetsegmentin idea resonoi niin venäläisessä, kiinalaisessa kuin amerikkalaisessa ajattelussa informaatioylivoiman saavuttamiseen liittyvän vastustajan toiminnan vapauden kiistämisen kanssa.[668] Tästä näkökulmasta kiistämiseen perustuvan deterrenssin funktio on vaikeuttaa hyökkääjän pyrkimystä hankkia informaatioylivoima. Mikäli informaatioylivoimaa ei kyetä hankkimaan, on hyökkääjän mahdollisuus saavuttaa menestystä modernilla taistelukentällä kyseenalainen, eikä se siis välttämättä päätä hyökätä. Kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmä on siis toimintaympäristöjen rajat ylittävän deterrenssin väline. Kyber- ja informaatioympäristön käytön kiistämisellä on vaikutusta muidenkin toimintaympäristöjen voimankäytön edellytyksiin.

Suljetun kansallisen verkon rakentaminen vaikuttaa myös rankaisuun perustuvaan kyberdeterrenssiin. Vaikutukset eivät ole välttämättä strategista tasapainoa ylläpitäviä. Suljettu kansallinen verkko vain pahentaa luvussa 2.2 esitettyjä rankaisudeterrenssin ongelmia. Merkittävin muutos on salailun lisääntyminen. Tiedon puute kansallisen internetsegmentin ominaisuuksista vähentää suljetun verkon valtioon kohdistettavan rankaisudeterrenssin uskottavuutta ja ennustettavuutta. Tämä johtaa yhä suuremmalla todennäköisyydellä turvallisuusdilemmaan ja kyberasevarustelukierteeseen. Lisäksi kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä voidaan tulkita suhteettomana panostuksena siviilipuolustukseen. Kylmän sodan aikaisen logiikan mukaan siviilipuolustus alentaa kynnystä ensi-iskuun oman väestön ollessa suhteellisessa suojassa kostoiskulta.[669] Deterrenssitasapainoa on vaikea saavuttaa, mikäli osapuolet pyrkivät samanaikaisesti suojaamaan itsensä täydellisesti ja kehittämään keinoja toisen suojauksen läpäisemiseksi.

Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä ei pelkästään hankaloita rankaisun uskottavuutta tai toteuttamista. Se voi tarjota suojan, ohjuspuolustuksen tapaan, jonka takaa kyetään suorittamaan

---

[668] Kukkola (2020a); McReynolds, Joe: China's Military Strategy for Network Warfare. Teoksessa *China's Evolving Military Strategy*. McReynolds, Joe (ed.) Jamestown Foundation, Washington DC, 2016, s.195–240; The United States Department of Defense (U.S. DoD): *Summary of the 2018 National Defense Strategy: Sharpening the American Military's Competitive Edge.* [https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf], luettu 5.1.2021.

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

ensi-isku tai kostoisku. Järjestelmä mahdollistaa vastatoimien alajärjestelmän avulla avoimien kansallisten verkkojen aggressiivisen tiedustelun ennakkovaroituksen hankkimiseksi samalla, kun avoimien verkkojen valtion on vaikeampi saada vastaavaa tietoa suljetuista verkoista. Avoin kansallinen verkko ei kykene suojaamaan kriittistä infrastruktuuriaan samalla tavalla kuin suljettu. Koska kybertoimintaympäristössä on käytännössä mahdotonta tuhota ensi-iskulla kohteen vastaiskukykyä (*counterforce*), avoin verkko jää haavoittuvaiseksi kostoiskulle. Sen sijaan suljetun verkon tarjoama suoja yhdistettynä kyberaseiden soveltuvuuteen ensi-iskuun laskee suljetun verkon valtion kynnystä hyödyntää yllätystä.

Yllätyshyökkäyksen houkuttelevuuden kasvattamisen lisäksi suljettu kansallinen verkko voi laskea kynnystä käyttää kyberaseita muiden sotilaallisten suorituskykyjen rinnalla osana rankaisupelotetta. Aseiden käytöllä voidaan kompensoida heikkouksia muissa toimintaympäristöissä, kun omat merkittävät kohteet oletetaan suojatuksi vastaavilta vaikutuksilta. Tätä ajattelua voi vahvistaa informaatioylivoiman korostunut merkitys nykyaikaisessa sodankäynnissä. Esimerkiksi kyber-, elektronisen ja avaruussodankäynnin kyvyt nähdään pakollisena osana uskottavaa rankaisudeterrenssiä. Kansallisen verkon sulkeminen voi suojata omien asevoimien verkkoja ja johtamisjärjestelmiä, jolloin muut rankaisudeterrenssin muodot ovat suojatumpia ja näin kyvykkyydeltään uskottavampia.

Ensi-iskun, yllätyksen ja horisontaalin eskalaatioriskin vähentämiseksi rankaisupelotteeseen voidaan liittää viesti, joka määrittää iskut kriittistä infrastruktuuria, mukaan lukien informaatioturvallisuuden ja -puolustuksen järjestelmän, vastaan kynnykseksi, jonka ylittämiseen voidaan vastata tavanomaisilla ja ydinaseilla. Yhdysvallat ja Venäjä ovat jo ilmoittaneet ydinasejohtamisjärjestelmien kuuluvan tällaisten maalien joukkoon.[670] On kuitenkin erittäin kyseenalaista jättäisivätkö suurvallat keskinäisessä konfliktissa, joka uhkaa laajeta sodaksi, käyttämättä mahdollisuutta lamauttaa vastustajan johtamisjärjestelmät. Attribuutio-ongelmien takia tällaisen iskun todistaminen jonkin määrätyn tahon tekemäksi on myös hidasta ja nykyteknologialle epävarmaa.

---

[670] Указ-355: Указ Президента РФ от 2.6.2019 N 355 “Об основах государственной политика Российской Федерации в области ядерного сдерживания”. [http://www.kremlin.ru/acts/bank/45562], luettu 30.12.2020; U.S. DoD (2018a).

Rankaisudeterrenssin osana voidaan pitää myös kykyä uhata kansainvälistä dataliikennettä ja kansainvälistä yritystoimintaa sekä logistiikkavirtoja joko katkaisemalla globaalin Internetin yhteydet määrätyllä alueella, ohjaamalla ne ”mustaan aukkoon” tai uhkaamalla valjastaa maan IoT-laitteet osaksi massiivista palvelunestohyökkäystä. Deterrenssilaskelmiin vaikuttanee se, että nämä hyökkäykset ovat vaikutuksiltaan lyhytaikaisia ja voivat aiheuttaa vahinkoa myös käyttäjälleen. Edelleen kansallisen segmenttinsä sulkeva valtio voi valmistaa haittaohjelmia, joilta sen omat järjestelmät ovat suojassa. Se voi uhata kilpailijoidensa yhteyksiä luomalla kyvyn katkoa niitä merenpohjassa, avaruudessa ja vapaassa tilassa. Se voi tehdä tiettäväksi, että se on ryhmittänyt pysyvästi hyökkäyksellisiä kyberjoukkoja rajojensa ulkopuolelle. Rakenteellinen kyberasymmetria lisääkin rankaisudeterrenssin uskottavuutta, koska verkkonsa sulkevalla valtiolla on kiistaton kyky iskeä takaisin samaan aikaan, kun sen omat arvokkaat kohteet ovat suhteellisesti paremmassa suojassa kuin avoimien verkkojen valtioiden.

Kansallisen internetsegmentin varsinainen irrottaminen globaalista Internetistä voi siis vahvistaa rankaisudeterrenssin viestinnän uskottavuutta. Toisaalta se voi myös toimia väärin tulkittuna signaalina ensi-iskuun valmistautumisesta. Omien tärkeiden kohteiden tai vastaiskukyvyn suojaaminen voidaan tulkita yllätysiskun valmisteluksi. Uhkatasapainon pohjana pitäisi teoriassa toimia molemmin puolinen haavoittuvuus kostoiskulle eli niin kutsuttu *Mutually Assured Destruction* (MAD). Käytännössä osapuolet eivät uskoneet tähän asetelmaan edes kylmän sodan aikana.[671] Kybertoimintaympäristöön päivitetty *Mutually Assured Disruption*[672] ei siis välttämättä toimi. Se edellyttäisi, että kaikki valtiot pitävät verkkonsa suhteellisen avoimina ja haavoittuvina. Toteutuessaan Venäjän kansallinen internetsegmentti rikkoisi tämän logiikan. Yhden osapuolen pystyessä rajoittamaan tai estämään normaalinkin eli hyväksyttävän kybervakoilun ja operaatioiden valmistelun toisten osapuolien olisi laajennettava operaatioitaan muihin toimintaympäristöihin. Tapahtuisi siis horisontaalia eskalaatiota. Tämän lisäksi muissa toimintaympäristöissä tapahtuva ei-sotilaallinen toiminta voi olla kybertoimintaa eskalaatioherkempää, mikä voi johtaa tahattomaan

[671] Green, Brendan R. & Long, Austin: The MAD Who Wasn't There: Soviet Reactions to the Late Cold War Nuclear Balance. *Security Studies*, Vol. 26, No. 4 (2017), s. 606–641.
[672] Maker, Simran R.: Mutually Assured Disruption: *Framing Cybersecurity In Nuclear Terms A National Committee on American Foreign Policy Report*, January 2018. [https://www.ncafp.org/2016/wp-content/uploads/2018/01/Mutually-Assured-Disruption-S.-Maker.pdf], luettu 5.1.2021.

vertikaaliin eskalaatioon. Rankaisudeterrenssin tasapaino olisi saavutettavissa vain, jos kaikki valtiot rakentaisivat kansallisen internetsegmentin. MAD-logiikka on tosin venäläisten mielestä jo valmiiksi rikki Yhdysvaltojen ylivoimaisten sotilaallisten kybersuorituskykyjen ja väitetyn Internetin hallinnan johdosta.[673] Venäjällä kyberaseita on usein verrattu strategisiin ydinaseisiin ja kyberdiplomatian argumenteissa on vastaavuuksia ydinaseriisuntaneuvottelujen argumentteihin.[674] Venäjän kyberdiplomatian tavoiteena oleva kyberhyökkäyskykyjen rajoittaminen onkin pyrkimys korjata strategista tasapainoa Venäjän hyväksi ja lisätä deterrenssin uskottavuutta.

Rankaisudeterrenssin katsotaan vaativan kestävää attribuutiota.[675] Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä voi edesauttaa attribuutiota määrättyyn pisteeseen asti. Se on tiedustelujärjestelmä, joka kykenee tuottamaan hyvän tilannekuvan toimista, toimijoista, kohteista ja motiiveista kansallisen internetsegmentin sisällä. Se ei kuitenkaan helpota attribuutiota kansallisen internetsegmentin ulkoa tulleiden hyökkäysten osalta. Järjestelmä itse asiassa haittaa kansainvälistä tiedon hankkimista ja jakamista, eikä itsessään ehkäise teknisten jälkien peittelymenetelmien käyttöä.[676]

On myös huomattava, että teknologinen kyky attribuutioon ei yksinään riitä deterrenssin toimeenpanoon. Useat kybertoimintaympäristön toimet jäävät ns. harmaalle vyöhykkeelle. Tällöin poliittisesta päätöksenteosta ja tahdosta tulee teknologisia suorituskykyjä tärkeämpi tekijä.[677] Rankaisudeterrenssin toimeenpanoa helpottaakin parlamentaarisen tai laillisuusvalvonnan puuttuminen, mikä nopeuttaa poliittisen tason attribuutioprosessia. Prosessin nopeus ei tietenkään takaa sen

---

[673] Крутских, А.В. (Под общ. ред.): *Международная информационная безопасность: Теория и практика: В трех томах. Том 1: Учебник для вузов*. Издательство «Аспект Пресс», Москва, 2019, s. 151–152, s. 204, s. 216–271.

[674] Vertaa esimerkiksi Arbato & Dvorkin (2013); Дылевский И. Н., Запивахин, В. О., Комов С. А., Петрунин, А. В. & Эльяс, В. П.: Военно-политические аспекты государственной политики Российской Федерации в области международной информационной безопасности. *Военная мысль* № 1/2015, с. 11–17; Комов, С.А. (под общ. редакцией). *Международная информационная безопасность: дипломатия мира*. Сборник статей. Военинформ, Москва, 2009.

[675] Brantly (2020).

[676] Goel, Sanjay: How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race. *Connections*, Vol. 19, No. 1 (Winter 2020), s. 87–95.

[677] Kilcullen (2020), s.152–153.

virheettömyyttä ja oikeellisuutta, päinvastoin. Autoritaariset hallinnot ovat vähintään yhtä taipuvaisia tiedustelupalveluiden ja päätöksentekijöiden ajatusvääristymiin kuin demokraattiset hallinnot.[678]

Attribuutiota helpottaisi, jos koko Internet muuttuisi tukemaan Kiinan ajamia protokollastandardeja, joilla pakettiliikenteestä voitaisiin tehdä jäljitettävää ja anonymiteetti Internet-liikenteessä hävitettäisiin.[679] Tämän ratkaisun sisältämät poliittiset ja ihmisoikeudelliset seuraukset eivät tällä hetkellä ole hyväksyttäviä Lännelle. Toisaalta attribuutio deterrenssin viestinnän välineenä ei välttämättä ole autoritaariselle harmaalla alueella operoivalle toimijalle yhtä tärkeä asia kuin se on ollut Lännelle. Venäjä ja Kiina ovat jatkaneet kyberhyökkäyksiään ja teollisuusvakoiluaan Yhdysvaltojen julkaisemista todisteista ja nostamista syytteistä huolimatta.[680] Tämä on synnyttänyt turhautumista läntisissä akateemikoissa ja päätöksentekijöissä. Esimerkiksi David Blagden on esittänyt, ettei teknisen attribuution puute ole välttämättä ongelma rankaisudeterrenssin toimeenpanolle. Hyökkääjien toimista voitaisiin johtaa intressit ja siten uhata kostoiskulla näitä intressejä.[681]

Läntisestä näkökulmasta kyberdeterrenssin toimimattomuuden katsotaan perustuvan pitkälti edellä käsiteltyyn attribuutio-ongelmaan: Koska kiinni jäämisen riski on pieni, houkutus käyttää suorituskykyjä on liian suuri. Mahdollisuuteen vaikuttaa hyökkääjän hyötylaskelmiin suhtaudutaan skeptisesti. Näin ollen deterrenssi kybertilassa ei voi perustua pelkästään aseiden käytön uhkaan vaan edellyttää aktiivista puolustautumista.[682] USA ja Iso-Britannia ovat viime vuosina rakentaneet kyberdeterrenssinsä etupainotteisen puolustuksen (*defence forward*), toimintaympäristöjen

---

[678] McVicar, Michael: Decisions in Crisis—An Examination. *Comparative Strategy*, Vol. 34, No. 1 (2015), s. 14–43; Honig, Or Arthur & Zimskind, Sarah: Not Completely Blind: What Dictators Do to Improve Their Reading of the World. *Comparative Strategy*, Vol. 36, No. 3 (2017), s. 241–256.

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

[680] The United States Department of Justice: *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, May 19, 2014. [https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor], luettu 30.12.2020.

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

[682] Ks. Brantly (2020).

rajat ylittävän deterrenssin ja jatkuvan vastavuoroisuuden perustalle (*persistent engagement*).[683] Ajatuksena on, että aktiivinen vastatoiminta viestii tahtoa ja kykyä puuttua negatiiviseen käytökseen, muokkaa kohteen käytöstä ja muodostaa ajan kuluessa kynnykset, jotka ylittävä toiminta oikeuttaa aseelliseen voimankäyttöön verrattavan kostoiskun. Kyberdeterrenssi kehittyy siis molemmin puolin ymmärrettäväksi toiminnan kautta.[684] Mallista voidaan käyttää myös nimitystä aktiivinen tai kumulatiivinen deterrenssi.[685] Se on uusi kybervoimankäytön vektori, joka hämärtää taivuttelun, pakottamisen ja deterrenssin rajat. Sen vaikutukset tähän mennessä, kuten Valeriano, Jensen ja Maness ovat todenneet, ovat tuottaneet vain rajoitettua vaikutusta.[686] Lisäksi ”aktiivinen deterrenssi” näyttäytyy kohteilleen eli Venäjälle, Kiinalle, Pohjois-Korealle ja Iranille valtiosuvereniteetin loukkauksena.[687]

Informaatioturvallisuuden ja -puolustuksen järjestelmä ehkäisee ”aktiivisen deterrenssin” vaikutuksia. Se pyrkii vähentämään sellaisten merkityksellisten kohteiden määrää, johon matalan intensiteetin vastahyökkäykset voivat vaikuttaa, ja lisää jäljelle jäävien kohteiden resilienssiä. Järjestelmä estää ”aktiivista deterrenssiä” vaikuttamasta kansalaismielipiteeseen ja vahvistaa näin kansakunnan psykologista resilienssiä. Järjestelmä myös kerää tietoa hyökkäyksistä vastustajan suorituskykyjen arvioimiseksi ja tuottaa uusia vastakeinoja jatkuvan oppimisen ja kehittämisen kautta. Tehokkaimmillaan järjestelmä kykenee omilla vastatoimillaan ohjaamaan hyökkääjien ”aktiivista deterrenssiä” haluamaansa suuntaan. Lisäksi ”aktiivinen deterrenssi” tulee legitimoineeksi suljetun kansallisen verkon mallin. Kansallinen internetsegmentti nostaa valtion kipukynnystä ja tarjoaa laajemmat vastatoimikyvyt ja valtuudet kuin, mitä avoimen verkon valtiolla on käytössään.

Martin Libicki on väittänyt, että signaloimalla kybersuorituskykyjensä ylivoimaa rauhan aikana, Yhdysvallat voi pakottaa vastustansa koventamaan kansalliset verkkonsa siihen pisteeseen asti, että vastustaja menettää verkostoitumisen tuomat edut.[688] Venäjän kansallisen

[683] Blagden (2020).
[684] Fischerkell, Michael P. & Harknett, Richard J.: Deterrence Is Not a Credible Strategy for Cyberspace (and What Is). *Orbis,* Vol. 61, No. 3 (2017), s. 381–393.
[685] Wilner (2020).
[686] Valeriano, Jensen & Maness (2018), s. 203.
[687] Chuanying (2020).
[688] Libicki (2016), s. 169–170.

internetsegmentin tapaus vaikuttaisi osittain tukevan Libickin väitettä. Toisaalta, jos ”aktiivinen deterrenssi” edesauttaa globaalin Internetin fragmentoitumista, johtaa kyberasevarustelukierteeseen ja ylläpitää latenttia kyberkonfliktia ja pelon ilmapiiriä, voidaan kysyä, onko hyöty sen seurannaisvaikutusten arvoista. Ydinasedeterrenssi ei edes 1970-luvun liennytyksen kaudella lopettanut suurvaltakilpailua, proxy-sotia ja ns. aktiivisia toimia.[689] On mahdollista, että ”aktiivinen deterrenssi” johtaa rajoitettujen kyberoperaatioiden hyväksymiseen osaksi suurvaltapolitiikkaa, jossa deterrenssin käsitteen alle piilotetaan muita voimankäytön muotoja.[690]

Kyberdeterrenssiajattelun taustalla voi vaikuttaa ääneen lausumaton toive uudesta halvasta rankaisudeterrenssin välineestä. Esimerkiksi ydinasedeterrenssi nähtiin Yhdysvalloissa ja Iso-Britanniassa 1950-luvulla halvempana ja sisäpoliittisesti helpompana vaihtoehtona kuin tavanomaisten joukkojen rakentaminen Neuvostoliiton uhkaa vastaan.[691] Tämä näkemys on osoittautunut historian valossa vähintään kyseenalaiseksi.[692] Kyberaseet voisivat täyttää Herman Kahnin deterrenssille asettamat vaatimukset, joita ovat pelottavuus, vääjäämättömyys, suostuttelevuus, kontrolloitavuus, ei-vahinkoalttius ja tietenkin halpuus.[693] Tämä ajatus ei kuitenkaan pidä paikkaansa (ks. Luku 2).

Puutteistaan huolimatta kyberaseet voivat näyttäytyä sellaisena teknologisena lupauksena – ja heikomman osapuolen näkökulmasta uhkana – että kansallisen internetsegmentin rakentamisessa on järkeä vastapuolen voimankäytön kiistämiseksi. Koska kybertila on avoin hyökkäyksille, ei ole hallittavissa täydellisesti, eikä rankaisudeterrenssiä

---

[689] Black, Jeremy: *The Cold War. A Military History*. Bloomsbury, London, 2015, s. 156–160.

[690] Tällaisesta lähestymistavasta ks. Goldman, Emily O.: From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy. *Texas National Security Review*, Vol. 3, No. 4 (Fall 2020), s. 84–101.

[691] Wheeler, N. J.: British Nuclear Weapons and Anglo-American Relations 1945-54. *International Affairs*, Vol. 62, No. 1 (Winter, 1985-1986), s. 71–86; House, Jonathan M.: *A Military History of the Cold War 1944-1962*. University of Oklahoma Press, Norman, 2012, s. 128, s. 224.

[692] Schwartz, Stephen I.: *The Costs of U.S. Nuclear Weapons*. Nuclear Threat Initiative, October 1, 2008. [https://www.nti.org/analysis/articles/costs-us-nuclear-weapons/], luettu 22.2.2021.

[693] Listaus on Herman Khanilta (Kahn, Herman: *On Thermonuclear War*. Princeton University Press, Princeton, 1960).

ole mahdollista rakentaa puhtaasti tuhoavan, uskottavan, toistettavissa olevan ja pysyvää vauriota tuottavan koston varaan, kansallinen internetsegmentti voi hyvin olla venäläisen kiistämiseen perustuva deterrenssikäsityksen ilmentymä.

Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä ehkäisee myös sitouttamiseen perustuvan deterrenssin vaikutusta. Venäjän tapauksessa sitouttaminen toimii jo lähtökohtaisesti huonosti, koska sen ulkopolitiikka nojaa ajatukseen voimaepätasapainosta, nollasummapelistä ja suurvaltojen vastakkaisista intresseistä.[694] Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä tarjoaa periaatteessa uskottavan arvo- ja talouspohjaisen vaihtoehdon universaaleille arvoille ja keskinäisriippuvuudelle. Sen olemassaolon tarkoitus on lähtökohtaisesti katkaista riippuvuudet, joita suurvallan statuksen omaavalla valtiolla ei voi olla. Tästä syystä henkilöihin kohdistettava deterrenssi (eli rankaisu) toimii heikosti. Kansallisen internetsegmentin päämääränä on luoda rinnakkainen tila ja todellisuus, jossa asuviin ulkopuolisilla sanktioilla ei ole vaikutusta. Venäjä ja Kiina voivat rekrytoida kybersotureita patriotismilla, statuksella suljetussa yhteisössä ja taloudellisilla eduilla. Yksilöön kohdistuva deterrenssi heijasteleekin voimakkaasti läntistä arvomaailmaa.[695] Informaatioturvallisuuden ja -puolustuksen järjestelmä on itse asiassa eräissä tapauksissa tehokkaampi sisäinen deterrentti yksilöitä vastaan kuin henkilökohtaisten sanktioiden ja häpäisemisen tekniikat. Sopivasti valittujen esimerkkien avulla toisinajattelijat, vallankumoukselliset ja terroristit saadaan puntaroimaan toiminnan riskejä uudelleen.

Kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmä muokkaa kybertilaa ja -toimintaympäristöä ja vaikuttaa kiistämiseen sekä rankaisuun perustuvaan deterrenssiin. Tästä syystä olisi läntisessä sotataidollisessa ajattelussa syytä pohtia taistelutilan muokkaamisen (*shaping*) käsitteen irrottamista pelkästään operatiivisen tason tarkastelusta.[696] Kybervoiman käyttö muokkaa strategisen tason voimankäytön edellytyksiä. Deterrenssiteorian hintakustannus- sekä todennäköisyyslaskelmiin ilmestyy uusia muuttujia suljettujen ja avoimien kansallisten verkkojen suhdetta tarkasteltaessa. Tämä suhde ei ole vakaa vaan muuttuu jatkuvasti. ”Aktiivinen deterrenssi” on yksi esimerkki

[694] Brantly (2020), s.228–229.
[695] Ks. esim. Braw & Brown (2020).
[696] U.S. DoD JP 3-0 (2018), s. II-7.

muutoksesta, toinen on resilienssin kehittyminen osaksi kiistämiseen perustuvaa deterrenssiä. Kolmas esimerkki on digitaalinen suvereniteetti. Yhdysvalloissa ja Euroopassakin on alettua hyväksyä ajatus kybertilan rajoista.[697] Ajan kuluessa tältä pohjalta voidaan johtaa kynnyksiä, joiden ylittäminen muodostaa oikeutuksen rankaisudeterrenssin käytölle.

Voidaankin väittää, että kansallisen internetsegmentin sulkeminen on osa kyberstrategiaa, jossa rankaisu, kiistäminen ja puolustautuminen integroituvat. Kuten edellä on osoitettu, jokaisella niistä keinoista voidaan osoittaa olevan yksittäiset heikkoutensa, mutta yhdessä ne tukevat toisiaan. Kansallinen internetsegmentti on pelkällä olemassaolollaan deterrenssin väline. Se mahdollistaa kansakunnan osan selviytymisen totaalisesta sodasta avoimen verkon valtion informaatioyhteiskunnan tuhoutuessa. Läntinen deterrenssiteoria ei kuitenkaan täydellisesti selitä kansallisen segmentin luonnetta tai venäläistä ajattelua.

Joss Meakinsin mukaan venäläiset suhtautuvat kriittisesti rangaistukseen perustuvan kyberdeterrenssin toimivuuteen. Venäläiset näkevät kyberaseet offensiivisina ensi-iskuaseina ja pelkäävät niiden kehittymisen horjuttavan ydinasestabiliteettia, joka on heidän suurvaltastatuksensa perusta. Meakins väittää, että Venäjän epävirallinen kyberdeterrenssipolitiikka perustuu vastaiskulla uhkaamiseen Venäjän valitsemassa toimintaympäristössä. Lisäksi Meakins väittää, että Venäjän julkilausumien epämääräisyys kyberdeterrenssin käsitteen ja kynnysten suhteen tarjoaa turvallisuuspalveluille toiminnanvapauden kybertoimintaympäristössä.[698] Meakinsin väitteeseen on helppo yhtyä. Kansallinen internetsegmentti on tarkoitettu ennaltaehkäisyn ja deterrenssin lisäksi myös informaatiotilan hallintaan ja konfliktin voittamiseen. Sillä on aktiivinen ja koko valtion hallinnon ja turvallisuuskoneiston sitouttava luonne. Itse asiassa näkökulmaeroista huolimatta venäläinen ja läntinen kyberturvallisuusajattelu lähestyvät toisiaan siinä, että kyberdeterrenssi nähdään koko valtionhallinnon ja kansakunnan asiaksi.[699] Erityinen venäläinen deterrenssin elementti on siinä, että kyberkeinot nähdään osana laajempaa strategista deterrenssiä. Se on rauhan ajasta sotaan ulottuva politiikan jatkumo, joka koostuu puolustuksellisen voiman rakentamisen,

[697] Burwell & Propp (2020).
[698] Meakins (2018)
[699] Kukkola (2020a); Wilner (2020).

uhkien materialisoitumisen estämisestä ja kiistämisestä ja rankaisusta perustuvasta deterrenssistä sekä konfliktin hallinnasta.[700]

Avoimella kansallisella verkolla on omista ominaispiirteistään johtuvat vaikutukset suljetun ja avoimen kansallisen verkon valtioiden väliseen deterrenssisuhteeseen. Avoimen kansallisen verkon puolustajan näkökulmasta kriisin kiristyminen vaikeuttaa entisestään kyberdeterrenssin onnistumista, koska avoimen verkon suojaamisen ja suljettuun verkkoon hyökkäämisen kustannukset ja onnistumisen todennäköisyys pienenevät konfliktin edetessä. Avoimen verkon valtion on siten vaikea säilyttää uskottava deterrenssi suhteessa suljetun verkon valtioon. Rakenteellisen kybersymmetrian kasvaessa suljetun verkon sulkeutuessa ennaltaehkäisevän tai ensi-iskun toteuttaminen näyttäytyy avoimen verkon valtiolle kustannusten ja todennäköisyyden näkökulmasta rationaalisemmalta ratkaisulta kuin odottaminen. Avoimen verkon valtion suljettuja huonompi tilannekuva kärjistää tilannetta. Ensi-iskun järkevyys riippuu siitä, uskooko avoimen verkon valtio olevansa uhattuna ja miten se arvottaa omat tavoitteensa.

Valtioiden välisissä suhteissa kyberensi-iskun logiikkaa on sidoksissa muihin toimintaympäristöihin ja voimankäytön muotoihin. Johtuen kyberhyökkäyksen vaikutusten väliaikaisuudesta ja epävarmuudesta tulee ensi-isku yhdistää muihin pakottamisen muotoihin, mikäli epäillään, että kybervoimankäyttö ei saa aikaan haluttua vaikutusta. Kansallisella informaatioturvallisuuden ja -puolustuksen järjestelmän tarjoamalla deterrenssillä voi siis olla tahaton vertikaalinen ja horisontaalinen eskaloiva vaikutus. Avoimen verkon valtio voi kokea välttämättömäksi suorittaa ensi-iskun useissa toimintaympäristöissä pelkästään perustuen havaintoon kansallisen internetsegmentin sulkeutumisesta.

Avoimen kansallisen verkon valtion pelko ei ole ainut tahattoman eskalaation lähde. Sen sijaan, että potentiaalinen hyökkääjä uskoisi liikaa informaatioturvallisuuden ja -puolustuksen järjestelmän suorituskykyyn, puolustaja itse voi uskoa siihen liikaa. Tällöin puolustaja voi päätyä ottamaan liian suuria riskejä muissa toimintaympäristöissä luottaessaan kansallisen internetsegmentin deterrenssivaikutukseen. Haasteeksi päätöksentekijöille muodostuu tässä tilanteessa sen ymmärtäminen, milloin deterrenssi yhdessä toimintaympäristössä joko mahdollistaa tai kiistää voimankäytön toisissa toimintaympäristöissä. Tilanne monimutkaistuu

[700] Forsström (2019); Kukkola (2020); Bruusgard (2021).

entisestään, jos kumpikaan osapuoli ei usko kansallisen internetsegmentin kyvykkyyksiin, mutta epäuskoon yhdistyy epävarmuus. Pahimmassa tapauksessa vastustajan kyvykkyyksiä, joihin ei uskota, käytetään kotimaisen politiikan välineenä esimerkiksi tuen mobilisoimiseksi aggressiiviselle ulkopolitiikalle tai asevarustelumenojen kasvattamista varten.

Edellä esitetystä voidaan päätellä, että mikäli Venäjän kansallisesta internetsegmentistä ei kyetä rakentamaan potentiaalisen vastustajan silmissä uskottavaa kiistävän deterrenssin välinettä, se on hyödytön ja mahdollisesti haitallinenkin projekti. Ensinnäkin kansallinen suljettu verkko viestii varsin huonosti, kuka määrätty potentiaalinen vastustaja on. Toiseksi se voi lisätä vastapuolen pelkoja tuottamatta todellista suojaa. Kolmanneksi vahvaksi koettu puolustus voi johtaa väärään turvallisuuden tunteeseen, haluun tai ”pakkoon” käyttää sotilaallista voimaa ennen potentiaalista vastustajaa. Luetellut tekijät lisäävät globaalin kybertoimintaympäristön epävakautta. Kansallinen internetsegmentti voi olla eskaloiva ja haitallinen projekti.

Lopuksi on deterrenssin toimivuuden osalta huomioitava deterrenssin uhkaaman vahingon tulkinnan subjektiivisuus. Suljetun kansallisen verkon rakentaja ei pysty päättämään sitä, mitä potentiaalinen hyökkääjä pitää arvokkaana ja miten se arvottaa hankalasta ja kalliista hyökkäyksestä koituvat hyödyt. Resilienssi ei estä hyökkäystä, jos hyökkääjä on valmis maksamaan kiistodeterrenssin hinnan ja ottamaan riskin epäonnistumisesta. Toisaalta hyökkääjä ei välttämättä osaa arvioida, minkälainen vahinko esimerkiksi kriittisiä informaatiojärjestelmiä kohtaan tai minkälainen psykologisen vaikuttamisen muoto ylittää kynnyksen, jonka kohdemaan johto katsoo viestivän suljetun verkon muodostaman deterrenssin pettämisestä. Seurauksena voi olla rankaisuiskun toimeenpano sellaisella tavalla ja sellaisessa toimintaympäristössä, jota hyökkääjä ei ole osannut aavistaa.

5.3 Konfliktin eskalaation hallinta

Konfliktin eskalaation hallinta kybertoimintaympäristössä tarkoittaa käynnistyneen konfliktin intensiteetin säätelyä käyttämällä voimaa tai sillä uhkaamalla kybertilassa tai sen kautta. Tavoitteena on saada vastustaja lopettamaan voimankäyttö itselle hyödyllisellä ja poliittisten päämäärien tavoittelua palvelevalla tavalla sekä samalla estää tahaton ja vahingossa tapahtuva eskalaatio. Konfliktin eskalaation hallinnassa voimankäyttö perustuu neuvotteluun pakottamisen kautta. Eskalaation hallinta liittyy valtiosuhteiden konfliktin ja sodan alkuvaiheen sekä sodan vaiheisiin,

jolloin uhkakuvina korostuvat alueellinen sota, kansannousu ja suurvaltasota. Sodan alkuvaiheen aikana vastapuolet taistelevat rauhanaikana perustetuilla ja ryhmitetyillä joukoilla ennen lisävoimien perustamista ja ryhmittämistä. Sen päähaaste on, miten muodostaa uskottava deterrenssi, sen pettäessä välttää yllätetyksi tuleminen ja miten mobilisoida lisävoima vastahyökkäystä ja vastustajan lyömistä varten.

Sodan aikana rakenteellinen kyberasymmetria saavuttaa täyden muotonsa kansallisen internetsegmentin sulkeutuessa ja äärimmäisessä tapauksessa jakaantuessa hallitusti, kun taas avoin kansallinen verkko muuttuu valvotusta sirpaloituneeksi. Avoin verkko voi menettää suurelta osin toimintakykynsä ja ulkoiset yhteytensä, kun taas suljettu verkko kykenee tarjoamaan kriittiset palvelut ainakin alueellisesti. Käytännössä ne suljetun verkon ominaisuudet, joita käytettiin deterrenssin osana, otetaan nyt varsinaisesti käyttöön. Resilienssi ja puolustusjärjestelmät torjuvat hyökkäyksiä ja lieventävät niiden seurauksia ja vastatoimet rankaisevat kohdetta suljetun verkon ulkopuolelta toteutettavilla hyökkäyksillä. Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä turvaa konfliktin ja sodan aikana kansallisen kyber- ja informaatiotilan ja sen rajojen joustavan säätelyn, sisäisten informaatiouhkien neutraloinnin, ulkoisten informaatiouhkien rajoittamisen, teknologisen ja henkisen resilienssin, strategisten suorituskykyjen suojaamisen sekä vaikuttamisen vastustajan informaatioympäristöön ensi- ja vastaiskukyvyillä. Konfliktissa ja sodassa käytössä oleva keinovalikoima kattaa kaikki ei-sotilaalliset ja sotilaalliset avoimet ja salatut keinot ja menetelmät. Eskalaation hallintaa toteutetaan siis suljetun verkon valtion näkökulmasta tilanteessa, jossa kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä tarjoaa suurimman mahdollisen toiminnan vapauden ja laajimmat toimintavaihtoehdot.

Sodan alkuvaihe ja varsinainen sota voivat muuttaa voimakkaasti valtion strategisen toimintaympäristön kaikkia ulottuvuuksia. Suljettujen ja avoimien kansallisten verkkojen osalta on huomioitava, että eri toimintaympäristöt kietoutuvat yhteen tavoilla, jotka voivat aiheuttaa ennustamattomia seurannais- ja heijastevaikutuksia. Kybertoimintaympäristön eskalaation hallinta ei siis liity pelkästään pakottamiseen vaan myös tahattoman ja vahingossa tapahtuvan eskalaation hallintaan riskejä ja seurauksia pienentämällä.

Eskalaationhallinnan on katsottu olevan vaikeaa kybertoimintaympäristössä johtuen sen ominaispiirteistä. Erityisesti huomiota on kohdistettu strategisten ennakkovaroitusjärjestelmien sekä

strategisten ydinaseiden johtamisjärjestelmien kyberhaavoittuvuuksiin.[701] Eskalaatioriskiä kasvattavat voimatasapainon erot toimintaympäristöihin välillä, päätöksentekijöiden huono tilannekuva ja -ymmärrys sekä erot osapuolten preferensseissä, eskalaatioportaiden järjestykseen vaikuttavat uudet teknologiat sekä aggressiivisiksi tulkitut strategiat ja jäykät toimintatavat.[702] Ben Buchananin mukaan valtioiden on turvallisuusdilemma johdosta tunkeuduttava toistensa verkkoihin varmistaakseen oman puolustuksensa. Koska tiedustelua ja vastahyökkäyksen valmistelua on vaikea erottaa toisistaan, syntyy paine vastatoimiin.[703] Toisaalta Fischerkeller ja Harknett ovat väittäneet, että kybertoimintaympäristön luonteesta johtuen kyberoperaatioita hyödyntävä kilpailu, jossa säännöt ovat osapuolten tiedossa, kykenee välttämään eskalaatiota.[704] Tätä väitettä tukee Benjamin Jensenin ja Brandon Valerianon tutkimus, jossa he osoittavat kyberhyökkäyksien harvoin eskaloituvan.[705] Ratkaisevana tekijänä eskalaatiossa kybertoimintaympäristössä, niin kuin muissakin ympäristöissä, ovat lopulta päätöksentekijöiden tulkinnat vastustajan aikeista.

Tarkasteltaessa informaatioturvallisuuden ja -puolustuksen järjestelmän ja rakenteellisen kyberasymmetrian vaikutusta eskalaation hallintaan tulee ensinnäkin erottaa toisistaan pitkän ja lyhyen aikajänteen vaikutukset. Lisäksi tulee erottaa toisistaan pyrkimys eskalaatioherruuteen (*escalation dominance*) ja tahattomien seurausten hallinta (*escalation control*). Pitkällä aikajänteellä tarkoitetaan useita vuosia, joiden aikana potentiaaliset konfliktin osapuolet pyrkivät ylläpitämään strategista tasapainoa tai hankkimaan etulyöntiaseman kehittämällä uusia hyökkäyksellisiä ja puolustuksellisia välineitä ja menetelmiä. Tästä näkökulmasta tarkasteltuna

---

[701] Cimbala (2017); Acton (2018).
[702] Fitzsimmons, Michael: The False Allure Of Escalation Dominance. *War on the Rocks*, November 16, 2017 [https://warontherocks.com/2017/11/false-allure-escalation-dominance/], luettu 27.11.2020; Healey, Jason & Jervis, Robert: The Escalation Inversion and Other Oddities of Situational Cyber Stability. *Texas National Security Review*, Vol. 3, No. 4 (Fall 2020), s. 30–53.
[703] Nye, Joseph S. Jr.: *ISSF Roundtable 10-6 on The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Discussion published by George Fujii on Friday, January 19, 2018. [https://networks.h-net.org/node/1252924/pdf], luettu 23.11.2020.
[704] Fischerkeller & Harknett (2019); Fischerkell & Harknett (2017).
[705] Valeriano, Jensen & Maness (2018); Jensen, Benjamin & Valeriano, Brandon: *What Do We Know about Cyber Escalation? Observations from Simulations and Surveys*. Atlantic Council, 2019. [https://www.atlanticcouncil.org/wp-content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf], luettu 12.1.2021.

Venäjän kansallinen internetsegmentti voidaan nähdä vastauksena Yhdysvaltojen kyberjoukkojen luomiseen ja kyberoperaatioihin, joita jatkuvan vastavuoroisuuden (*persistent engage*) doktriinin omaksuminen on kiihdyttänyt.[706] Yhtä lailla Yhdysvaltojen kesällä 2020 esittelemä *Clean Network* -ohjelma on reaktio Kiinan ja Venäjän kyberhyökkäyksiin ja -vakoiluun.[707] Eskalaatiokontrollin pitkä aikajänne liittyy siis suurvaltakilpailuun ja ilmenee näkyvimmin asevarustelukilpailuna, joka voi hetkellisen koetun etulyöntiaseman tai olemassa oloa uhkaavan uhan johdosta riistäytyä tahattomasti ja vahingossa konfliktiksi. Hyökkäystoimet eivät siis aina ole eskalaation ainut lähde tai väline. Kaikenlainen toiminnan muutos tai kiihtyminen muuttaa kybertilaa ja voi johtaa hallitsemattomiin seurauksiin. Kybertoimintaympäristön kehyksessä teknologian kehityksellä on korostunut asema suurvaltojen voimasuhdearvioissa. Jokin uusi teknologia voi mahdollistaa yhdelle osapuolelle eskalaatiodominoinnin, mikä taas synnyttää turvattomuutta potentiaalisissa vastustajissa.[708]

Informaatioturvallisuuden ja -puolustuksen järjestelmän ja rakenteellisen kyberasymmetrian lyhyen aikavälin vaikutukset liittyvät suljettujen ja avoimien verkkojen muutoksiin konfliktin kehyksessä kuukausien, viikkojen ja päivien aikana. Määrätyissä tapauksissa kyse voi olla minuuteista, sekunneista tai alle sekunneistakin, mikäli järjestelmä automatisoidaan riittävälle tasolle. Järjestelmän käyttö eskalaatiodominanssin välineenä perustuu jo deterrenssin tarkastelun kohdalla havaittuun kykyyn uhata vastustajaa suojan takaa. Tämä suoja ja sen takaa ja ulkopuolelta suoritettavat iskut voidaan ottaa käyttöön vähitellen ja osittain tai kerralla, nopeasti ja laaja-alaisesti.

Kansallisen internetsegmentin rajojen säätelyllä on välittömin ja näkyvin vaikutus konfliktin luonteeseen. Se on luonteeltaan poikkitoimintaympäristöllinen, koska se heijastuu kybertilan kautta kaikkiin tilan palveluista riippuvaisiin toimintaympäristöihin. Sillä voidaan pyrkiä uhan ehkäisemiseen ennalta tai tappion välttämiseen akuutissa tilanteessa. Kansallisen verkon sulkeminen ei ole pelkästään

---

[706] Klimburg (2020).

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

[708] James Johnsonin artikkeli kuvaa tahattomasti tai tahallaan tämän logiikan hyvin (Johnson (2018)).

puolustuksellinen toimenpide, vaan sillä voidaan vaikuttaa koko globaalin Internetin toimintaan häiritsemällä globaalin verkkoliikenteen reititystä. Sulkemisella on heijastevaikutuksensa kaikkiin valtion rajojen sisällä toimiviin ulkomaisiin yrityksiin. Jos sulkeminen ulottuu elektromagneettiseen tilaan ja avaruuteen, ovat vaikutukset kertaluokkaa suuremmat. Huomioitavaa on, että näillä vaikutuksilla on lyhyt ajallinen kesto. Dataliikenne reitittyy uudelleen ja alkusekasorron jälkeen vaikutukset voivat kääntyä verkkonsa sulkenutta valtiota vastaan tai johtaa vahingossa tapahtuvaan eskalaatioon heijastevaikutusten takia. Toisaalta verkkonsa sulkenut valtio voi syyttää vastustajiaan siitä, että nämä ”pakottivat” valtion sulkemaan verkkonsa – ja ovat siis tämän logiikan mukaan vähintään yhtä syyllisiä.

Kansallisen verkon sulkeminen muuttaa konfliktin luonnetta ja toimii viestinnän välineenä. Kansallisen segmenttinsä sulkenut valtio osoittaa kykyä ja valmiutta kärsiä taloudelliset ja muut seuraukset, ja voi jopa kiristää omasta informaatioympäristöstään riippuvaisia ulkomaisia toimijoita. Se pakottaa vastustajan suorittamaan seuraavan siirron joko suojaamalla itsensä, osoittamalla suljetun verkon heikkoudet eli hyökkäämällä tai liennyttämällä konfliktia. On täysin mahdollista, että konfliktin seuraava askel otetaan jossain toisessa toimintaympäristössä. Kybertoimintaympäristön muokkaamista ei voi erottaa valtioiden välisestä laajemmasta konfliktista, koska eskalaatiodominanssin onnistumisen kannalta merkittävää on, mikä vastapuolten voimatasapaino on muissa toimintaympäristöissä.

Eskalaatiodominanssiin vaikuttaa myös kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmän vahvistama teknologinen ja henkinen resilienssi. Resilienssi muodostaa eräänlaisen voimankäytön kynnyksen jo rauhan aikana. Se muokkaa kansallisesta kriittisestä informaatioinfrastruktuurista ja kansalaisten sekä valtiojohdon tahdosta kestävämmän verrattuna avoimiin kansallisiin verkkoihin ja näiden asukkaisiin. Hyökkääjän tulee käyttää suurempaa voimaa, uusia keinoja tai moraalisesti kyseenalaisia keinoja voidakseen vaikuttaa suljetun verkon valtioon. Tämä tarkoittaa, että sen tulee olla valmis eskaloimaan konfliktia korkeammalle tasolle. Kaikki valtiot eivät tähän välttämättä kykene mm. sisäpoliittisista syistä.

Informaatioturvallisuuden ja -puolustuksen järjestelmän valvonta- ja hallinta-alajärjestelmät ovat myös eskalaatiodominanssin väline. Ne kykenevät puuttumaan sisäisten uhkien kehitykseen ja ehkäisemään ne. Ne kykenevät myös keräämään tietoa ulkopuolelta tehdyistä kyber- ja informaatiohyökkäyksistä ja sisäisten toimijoiden saamasta ulkopuolisesta

tuesta. Hyökkääjä on pakotettu lisäämään ja laajentamaan tukeaan sisäisille toimijoille sitä mukaa kuin valvontajärjestelmät edesauttavat sisäisen uhan heikentämisessä. Sen on siis pakko eskaloida, mikäli haluaa saavuttaa tavoitteensa. Suljetun verkon valtio voi käyttää kerääntyvää todistusaineistoa attribuutiossa ja sen perusteella eskaloida vuorostaan konfliktia muissa toimintaympäristöissä ja kansainvälisen yhteisön silmissä oikeutetulla tavalla. Hyökkääjä joutuu harkitsemaan, missä vaiheessa se luopuu tuestaan sisäisille kumouksellisille vai haluaako jatkaa konfliktin eskalointia valtioiden väliseksi suoraksi kamppailuksi.

Kansallisen segmentin sulkeuduttua informaatioturvallisuuden ja -puolustuksen vastatoimijärjestelmä mahdollistaa ensi- ja vastaiskun. Suljetun verkon valtio voi iskeä vastustajan kriittistä informaatioinfrastruktuuria tai rajatumpia kohteita vastaan kyberasein sodan alkuvaiheessa. Kyberhyökkäystä voidaan käyttää yllätysedun saamiseksi tai voimannäyttämiseksi ja eskalaatiokynnyksen nostamiseksi. Ensimmäisessä tapauksessa tarkoituksena on käyttää rakenteellista kyberasymmetriaa sodan voittamiseen ja sitä käsitellään seuraavassa luvussa. Jälkimmäisessä tapauksessa ensi-iskun kohde kohde joutuu päättämään, eskaloiko se konfliktia ja missä toimintaympäristössä. Jos informaatioturvallisuuden ja -puolustuksen järjestelmä toimii tehokkaasti, vastustaja joutuu eskaloiman tavanomaisella voimalla tai ydinaseilla, mikä nostaa konfliktin intensiteettiä merkittävästi. Se voi tietenkin myös vastata ei-sotilaallisin toimin, esimerkiksi pakotteilla, tai liennyttää. Jos ensi-iskun kohde on avoimen verkon valtio, nämä ei-sotilaalliset reaktiot eivät poista valtion verkon haavoittuvuuksia ja pelkoa uudesta hyökkäyksestä. Näillä tekijöillä voi olla merkittäviä sisäpoliittisia vaikutuksia päätöksentekoon.

Kansallisen verkon sulkeminen ei välttämättä tarkoita konfliktin intensiteetin tai laajuuden kasvattamista. Eskalaatiodominanssiin liittyy myös kyky olla eskaloimatta tai sietää vastustajan eskaloivat toimet. Kansallinen segmentti voi kiistää hyökkääjältä yhden toimintaympäristön käytön, jolloin se joutuu päättämään jatkaako tilanteen eskalointia jossain toisessa toimintaympäristössä. Vastapuolen kybertoimintaympäristön harmaan vaiheen toiminta, joka ei ylitä rankaisudeterrenssin kynnystä eli niin kutsuttu ”salamitaktiikka” (*salami tactics),*[709] vaikeutuu toimintatilan kaventuessa. On toisaalta myös mahdollista, että hyökkääjä houkuttelee kohteen sulkemaan verkkonsa kasvattamalla hiljalleen hyökkäysten intensiteettiä. Kansallisen verkon sulkeminen voi aiheuttaa kustannuksia,

[709] Schelling (2008), 67–69; Wirtz (2017), s. 107.

jotka pakottavat suljetun verkon valtion muuttamaan toimintaansa tavalla tai toisella.

Informaatioturvallisuuden ja -puolustuksen järjestelmä on kompleksinen ja sitä käytetään erittäin keskinäisriippuvaisessa ja monitasoisessa strategisessa ympäristössä. Tahaton tai vahingossa tapahtuva eskalaatio on hyvin mahdollinen. Kansallisen internetsegmentin sulkeminen ei kuitenkaan kärsi samanlaisesta monitulkintaisuudesta kuin esimerkiksi risteily- tai ballististen ohjusten käyttö. Ohjukset voidaan varustaa joko tavanomaisilla tai ydinkärjillä, joten ilman parempaa tietoa kohteen pitää olettaa pahinta ja toimia sen mukaan.[710] Puolustautumistoimet kybertilassa eivät myöskään ole yhtä monitulkintaisia kuin vastustajan verkkoihin suuntautuvat kyberoperaatiot, joiden tavoitteena voi olla vakoilu, tiedustelu, hyökkäyksen valmistelu tai varsinainen hyökkäys.[711]

Monitulkintaisuus ja epävarmuus voivat kuitenkin liittyä kansallisen verkon sulkemisen syihin. Potentiaaliselle vastustajalle voi olla epäselvää suljetaanko verkko sotaan valmistautumisen vai sisäisen turvallisuuden takia. Verkon sulkeminen voidaan tulkita ensi-iskun valmisteluksi, jossa käytettäisiin jonkinlaista ”tuomiopäivän” kyberasetta.[712] Kansallisen segmentin irrottaminen ja informaatiotilan sulkeminen voi johtaa viestinnän heikkenemiseen osapuolten välillä ja lisätä väärinymmärtämisen mahdollisuutta. Eskalaatioriskiä voivat nostaa tehostetut yritykset saada tiedustelutietoja suljetun verkon sisältä. Kansallisen verkon sulkeminen voi koskettaa myös kolmansia osapuolia, jotka voivat ryhtyä toimenpiteisiin suojatakseen omia etujaan. Tällaisia voivat olla esimerkiksi valtiot, monikansalliset yritykset ja aktivistiryhmät. Niiden intressit ja toiminta voivat pahimmassa tapauksessa olla vastakkaisia konfliktin molemmille osapuolille.

Kybersuvereniteetin normin kehittyessä ja liittyessä entistä tiiviimmin kriittiseen informaatioinfrastruktuuriin kyberhyökkäysten eskalaatiokynnys muuttuu. Nykyisellään on vaikea etukäteen tietää, minkälaista kyberhyökkäystä esimerkiksi Venäjä pitäisi valtion aseellisena voimankäyttönä toista valtiota vastaan. Yhdenlaisen viestin antaa maan

---

[710] Acton, James M.: *Is It a Nuke? Pre-Launch Ambiguity and Inadvertent Escalation*. Carnegie Endowment for International Peace, Washington DC, 2020.
[711] Valeriano, Jensen & Maness (2018), s.31.
[712] Ajatus venäläisten taipumuksesta käyttää ”tuomiopäivän kyberasetta” on Thorntonin ja Mironin ja kuvastaa lähinnä läntistä uhkakuvadiskurssia (Thornton & Miron (2020), s. 12–21).

hallituksen julkaisema kriittisen informaatioinfrastruktuurin kategorialistaus.[713] Pelkkä viestintä ei kuitenkaan riitä. Kansallinen internetsegmentti liittää monia yksityistoimijoiden järjestelmiä ja palveluja valtiovaltaan avoimien verkkojen valtioista poikkeavalla tavalla. Tahattomaan eskalaatioon voivat johtaa esimerkiksi energia- tai sotilasteolliseen kompleksiin kohdistuva vakoiluoperaatio, yritys ujuttaa haavoittuvuus ohjelmisto- tai laitteistotuotantoon tai bottiverkoston luominen älykaupunkien IoT-laitteisiin tukeutuen. Se mikä Lännessä voitaisiin tulkita yksityissektorin kyberturvallisuusasiaksi, voidaan Venäjällä tulkita kansallisen turvallisuuden kysymykseksi.

Kansallisten internetsegmenttien osalta vahingossa tapahtuvan eskalaation riskiä nostavat informaatioturvallisuuden ja -puolustuksen järjestelmän alajärjestelmien keskinäisriippuvuudet. Haittaohjelmat voivat esimerkiksi levitä hallitsemattomasti keskitetyissä hallintajärjestelmissä ja -verkoissa. Vakoilutarkoituksessa tehdyt tietomurtoyritykset voivat päätyä vaikuttamaan kansallisen turvallisuuden kannalta kriittisiin järjestelmiin. Informaatioturvallisuuden ja -puolustuksen järjestelmän automatisointi muodostaa myös riskin.[714] Jos kansallisen segmentin hallinta alistetaan tekoälylle, siirrytään päätöksenteossa konenopeuteen ja päädytään saman ongelman ääreen kuin ydinaseiden kanssa.[715] Miten vältetään vahingossa tapahtuva eskalaatio, kun ihmiset luottavat manipuloitavissa olevien koneiden läpinäkymättömiin päätöksiin toimista ja vastatoimista?[716] Pahimmassa tapauksessa kansallisen puolustuksen järjestelmät on integroitu niin, että hyökkäys kybertoimintaympäristössä aiheuttaa automaattisen vastareaktion jossain toisessa toimintaympäristössä.

---

[713] ПП-127a: Постановление Правительства РФ от 8 февраля 2018 г. N. 127 ”*Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений* (с изменениями от 13 апреля 2019 г.) [http://pravo.gov.ru/proxy/ips/?docbody=&nd=102460750], luettu 22.2.2021.

[714] Kyberturvallisuusjärjestelmien automatisointi ja integrointi esiintyvät Venäjän digitaalisen talouden ohjelman tavoitteissa (Президиум Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам: *Паспорт федерального проекта Информационная безопасность - Национальная программа ”Цифровая экономика Российской Федерации” от 6 мая 2019 года.* [https://files.data-economy.ru/Docs/Pass_Cybersecurity.pdf], luettu 3.1.2021).

[715] Blair (1993), 113–115.

[716] Johnson, James: Delegating Strategic Decision-making to Machines: Dr. Strangelove Redux? *Journal of Strategic Studies*, 2020. DOI: 10.1080/01402390.2020.1759038.

Keskitetty päätöksenteko ja nopeus, joka näyttäytyy suljettujen verkkojen vahvuutena, voikin kääntyä riskitekijäksi.

Asevoimien verkkojen ja järjestelmien osalta kansallisen internetsegmentin suhde tahattomaan tai vahingossa tapahtuvaan eskalaatioon riippuu siviili- ja sotilasverkkojen integraation tasosta. Kuten luvussa 3 todettiin, asevoimilla on pyrkimys pitää verkkonsa erillään siviiliverkoista, jos vain mahdollista. Suljettu kansallinen verkko voi kokonaisuudessaan suojata yhteiskunnallisia kohteita (*countervalue*) ja kaksoiskäyttökohteita kyberhyökkäyksiltä, mutta sotilaskohteiden (*counterforce*) suojaamiseen sillä on konfliktitilanteessa rajattu vaikutus. Koska asevoimien johtamisjärjestelmät on pääsääntöisesti erotettu siviiliverkoista, hyökkäykset kansallista internetsegmenttiä vastaan eivät automaattisesti uhkaa valtion kyber- tai ydinasevastaiskukykyä. Todellisuudessa pyrkimykset niin suljettujen kuin avoimien verkkojen valtioiden turvallisuusalojen integrointiin ja turvallisuustoimijoiden yhteistyön lisäämiseen synnyttävät yhteyksiä asevoimien ja siviilitoimijoiden verkkojen välille. Teknologian kaksoiskäytön lisääntyessä asevoimien ja siviiliteollisuuden välille avautuu yhä enemmän yhteyksiä. Yksittäiset satelliitit voivat palvella niin siviili- kuin sotilasasiakkaita. Suurvaltojen strategiset ilma- ja ohjuspuolustusjärjestelmät luottavat todennäköisesti osiltaan siviilioperaattoreiden palveluihin vähintään sähköntuotannon osalta. Joukkojen mobilisaatio ja ryhmityssiirrot ovat riippuvaisia siviilijärjestelmien tarjoamista lento-, rautatie- sekä laiva- ja satamapalveluista. Minkä tahansa mainitun järjestelmän häiriö voidaan tulkita aseelliseksi hyökkäykseksi.

Toisaalta kansallisen segmentin sulkeutuessa sotilasjärjestelmille saattaa aiheutua odottamatonta haittaa. Kaikkia riippuvuuksia ei ehkä ole huomioitu. Kansallisen verkon hallittukin sirpaloituminen vaikeuttaa päivitysten, konfiguraatiomuutosten, salausavaimien ja sertifikaattien välittämistä teollisuudelta asevoimille, kybertilannekuvan jakamista, yhteistyötä siviiliviranomaisten kanssa ja ulkomailla sijaitsevien joukkojen johtamista. Sama haaste koskee esimerkiksi valtion ulkomailla sijaitsevia edustustoja ja lähetystöjä. Eskalaatioriski kasvaa asevoimien joutuessa toimimaan huonojen johtamisyhteyksien ja epäselvän tilannekuvan varassa. Venäjällä riskiä on yritetty vähentää perustamalla kansallisen puolustuksen johtokeskus, mutta mitä tapahtuu, jos tämä keskus yllättäen katoaa verkosta edes hetkeksi?

Eskalaatiokontrolli on etuun pyrkivänä menetelmänä tai riskien hallintana haasteellinen kyberstrategian osa. Toteutuessaan kansalliset

internetsegmentit muokkaavat kybertoimintaympäristöä ja vaikuttavat muihin toimintaympäristöihin. Syntyvät keskinäisriippuvuudet voivat tukea joustavaa eskalaatiodominointia, mutta myös johtaa ongelmiin etenkin siirryttäessä deterrenssistä sodankäyntiin, jossa sodan kitka lisää epävarmuutta moninkertaisesti.[717] Mikäli esimerkiksi Venäjä päättäisi käyttää eskalaatiokontrollia lisääntyvän kivun aiheuttamiseksi vastustajalle sodan päättämiseksi sille edullisella tavalla tai ulkopuolisten pitämiseksi konfliktin ulkopuolella, kuten Kofman, Fink ja Edmonds ovat esittäneet Venäjän pyrkivän toimimaan[718], hyökkäyksellisten ja puolustuksellisten kybersuorituskykyjen, kaukovaikutteisten tavanomaisten ja ydinaseiden ja muiden keinojen yhteiskäyttö kriittisiä sotilas- ja siviilikohteita vastaan asettaisi vastapuolen erittäin vaikeaan asemaan. Kun samaan vaikutukseen voidaan pyrkiä useilla eri asejärjestelmillä, teknologian käyttöön liittyvät eskalaatioportaat tai kynnykset hämärtyvät. Hyökkääjä ei välttämättä ymmärrä kohteiden arvoja puolustajalle. Esimerkiksi suljetun verkon valtio voi tulkita avoimet kansalliset verkot merkiksi siitä, ettei kohdevaltio aseta kriittiselle informaatioinfrastruktuurille arvoa ja iskee niihin ajatellen, ettei eskaloi tilannetta. Kriittisellä informaatioinfrastruktuurilla voi kuitenkin olla merkittävää arvoa kohdevaltiolle ja näin konflikti eskaloituu tahattomasti. Eskalaatioportaikkojen ongelmat eivät toki ole suljettujen kansallisten verkkojen esiintuoma ongelma, vaan ne on tiedostettu jo alusta alkaen Herman Kahnin eskalaatioportaita kohtaan esitetyssä kritiikissä.[719]

Lopuksi voidaan todeta, että informaatioturvallisuuden ja -puolustuksen järjestelmän toiminta edellyttää useiden kansallisten toimijoiden yhteistoimintaa, koordinointia ja synkronointia. Keskitetyn johtamisen takia yksittäinen taho voi kuitenkin tehdä koko valtion informaatiotilaa koskevia päätöksiä, joilla voi olla tuntemattomia seurannaisvaikutuksia. Tämä ja muut edellä käsitellyt epävarmuustekijät eivät poista sitä tosiasiaa, että suljettu kansallinen verkko on toimiva informaatioylivoiman tavoittelun ja sitä kautta eskalaatioherruuden väline. Se on linnoitus, jonka takaa voidaan joko uhata vastustajaa sen omalla maalla tai pakottaa vastustaja laajentamaan ja kiihdyttämään konfliktia, jos se haluaa vallata linnoituksen.

---

[717] Lindsay & Gartzke (2020).
[718] Kofman, Fink & Edmonds (2020), s. 10.
[719] Paret (1990), 764–766; McDermott, W. Basil: Thinking about Herman Kahn. *The Journal of Conflict Resolution*, Vol. 15, No. 1 (Mar., 1971), s. 55–70.

5.4 Asymmetrian sotilaallinen hyväksikäyttö

Rakenteellisen kyberasymmetrian sotilaallinen hyväksikäyttö tarkoittaa pakottamisen ja raa'an voiman käyttöä kybertilassa ja kykyä aiheuttaa sellaista vaikutusta kybertilassa tai sen kautta, joka pakottaa vastustajan lopettamaan vastarinnan vastoin omaa tahtoaan tai kiistää vastaavan vaikutuksen omiin järjestelmiin. Sotilaallinen hyväksikäyttö liittyy valtiosuhteiden konfliktin ja sodan alkuvaiheen sekä sodan vaiheisiin, jolloin uhkakuvina korostuvat alueellinen sota, kansannousu ja suurvaltasota. Konfliktissa ja sodassa käytössä ovat kaikki ei-sotilaalliset ja sotilaalliset avoimet ja salatut keinot ja menetelmät. Valtion strategisen toimintaympäristön kaikki ulottuvuudet ovat vuorovaikutuksessa keskenään ja voivat muuttua nopeasti. Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä turvaa osittain kansallisen informaatio- ja kybertaistelutilan hallinnan ja puolustajan toiminnan vapauden sekä vastustajan toiminnan vapauden kiistämisen (sotilasverkot toimivat itsenäisesti). Lisäksi se tukee kyberhyökkäyksiä vastustajan järjestelmiä vastaan, sotatoimia muissa toimintaympäristöissä ja edesauttaa kansakunnan selviytymistä sodan eskaloituessa totaaliseksi.

Kansallisen internetsegmentin sulkeminen on välttämätön ehto asymmetrialle, muttei itsessään riittävä. Sotilaallinen hyväksikäyttö edellyttää kykyä käyttää voimaa vastustajan pakottamiseksi, mitä pelkkä kansallisten verkkojen irrottaminen globaalista Internetistä ei takaa. Kansallisen segmentin sulkeminen toimii vastustajan pakottamisen välineenä vain, jos tämä ei kykene suojaamaan samalla tai riittävällä tavalla itseään. Vain tällöin voidaan suojan takaa uhata tai käyttää pakottavaa voimaa asymmetrisellä tavalla.

Rakenteellisen kyberasymmetrian sotilaallinen hyväksikäyttö perustuu suljetun kansallisen verkon aikaisemmin luotuun tieteellisteknologiseen perustaan, teknologiseen ja henkiseen resilienssiin, valvonta- ja hallintajärjestelmiin sekä aktiivisten vastatoimien suorituskykyihin. Suljettu kansallinen verkko voidaan irrottaa globaalista Internetistä ja jakaa hallitusti osiin. Puolustustoimien johtaminen on keskitettyä ja jatkuvaa ja tilannekuva yhteinen ja kattava. Kriittiset järjestelmät voivat tuottaa palveluja tarvittaessa alueellisesti. Kansallinen kybertaistelutila on puolustajan muokattavissa ja ohjelmistot ja laitteistot omin voimin hallittavissa ja päivitettävissä. Informaatiotilan hallinta ylläpitää psykologista resilienssiä, vaikka yhteiskunnan kriittiset palvelut kärsisivät vaurioita. Suljetun kansallisen verkon kyky tuottaa kaikki edellä mainitut edut liittyy tapaan, jolla ulkomaan liityntöjä hallitaan ja kriittisten

järjestelmien resilienssi taataan. Mikäli verkko on rakennettu niin, että valtio voidaan irrottaa globaalista Internetistä hallitsemattomasti ulkopuolelta käsin, on se rakentaminen epäonnistunut.

Verrattuna suljettuihin kansallisiin verkkoihin avoimet verkot ovat sotatilassa todennäköisesti siiloutuneita ja hajaantuneita. Koordinoidut kansalliset puolustustoimet ovat hitaita, jos lainkaan mahdollisia. Teknologinen ja henkinen resilienssi ovat riippuvaisia yksityissektorin liiketaloudellisista tekijöistä sekä poliittisen järjestelmän vahvuudesta ja arvopohjasta. Jos verkkoja ja järjestelmiä ei ole kahdennettu hyvien käytänteiden mukaisesti tai palvelut on kilpailusyistä keskitetty samoihin fyysisiin ja loogisiin järjestelmiin, resilienssi on heikko. Avoimen verkon puolustajilla on verraten heikko näkyvyys kansalliseen verkkoonsa ja täten rajallinen tilannekuva, toiminnan vapaus ja kyky johtaa puolustustoimia. Avoin kansallinen verkko voidaan tilapäisesti lamauttaa, hajottaa osiin ja mahdollisesti eristää laaja-alaisella kyberhyökkäyksellä, joka kohdistuu kriittisiin pisteisiin. Toki nämä kriittiset pisteet tulee pystyä paikantamaan ja tunkeutuminen valmistelemaan hyvissä ajoin ennen iskua. Verkko voi myös sirpaloitua itsekseen eri toimijoiden pyrkiessä suojelemaan omia järjestelmiään. Toisaalta avoin kansallinen verkko ja siihen tukeutuvat järjestelmät voivat juuri sirpaloitumisen takia lamautua yksiltä osin toisten osien toimiessa suhteellisen normaalisti.

Suljettujen ja avoimien kansallisten verkkojen voimasuhteeseen vaikuttaa ennen kaikkea tilannekuvan jakaminen ja täten tilanneymmärryksen muodostuminen sodan alkuvaiheessa, kyky toimia omissa ja vastustajan verkoissa, johtamisen yhtenäisyys, toimenpiteiden nopeus ja ajoitus sekä verkkojen (ja kansakunnan) kyky sietää ja palautua hyökkäyksistä. Valvonnan ja kontrollin keskittäminen ja verkottaminen, massiivinen datan kerääminen ja kansainvälisten teknisten, taloudellisten ja poliittisten yhteyksien rajoittaminen ovat suljettujen kansallisten verkkojen perusta, mutta muodostavat myös haavoittuvuuden. Tämä korostuu, kun viimeistään sodan julistamisen hetkellä avoimen verkon valtion vastatoimijärjestelmän lailliset ja poliittiset rajoitukset poistuvat ja kansainvälinen yhteistyö tiivistyy ja tarjoaa paremman tilannekuvan ja teknologisen tuen. Realismia on todeta, että rajoitukset poistuvat, tai niiden pitäisi poistua, jo jonkin aikaa ennen virallista ja julkista päätöstä. Tämän jälkeen suljettujen ja avoimien verkkojen valtioiden asevoimien ja tiedustelupalveluiden ja kyberjoukkojen käytössä olevan teknologian taso, doktriini, organisaatioiden tehokkuus, kyky yhteistoimintaan ja toimivaltuudet sekä ammattitaito ratkaisevat hyökkäys- ja puolustustoimien onnistumisen.

Kansallisen internetsegmentin sulkemista käytetään kybertaistelutilan muokkaamiseen. Yksittäisten järjestelmien tai verkkojen haavoittuvuudet eivät muutu, mutta kansallisen tason muutoksilla voi olla vaikutusta hyökkääjän harhauttamisen, hidastamisen ja torjumisen kannalta. Suljettu kansallinen segmentti voi parhaimmillaan estää ennalta valmistelemattomien hyökkäysten toteuttamisen, vaikeuttaa joidenkin valmisteltujen hyökkäysten toteuttamista ja vähentää hyökkäyspinta-alaa ja iskettäviä kohteita. Se nostaa tiedusteluun ja valmisteluun kuluvien resurssien määrää ja luo epävarmuutta valmisteltujen hyökkäysten toimivuudesta. Kybertoimintaympäristön käytön kiistäminen hankaloittaa kaikissa toimintaympäristöissä suoritettujen hyökkäysten vaikutusten arviointia etenkin, jos avaruuden ja vapaan elektromagneettisen spektrin käyttö on myös kiistetty.

Kansallisen internetsegmentin valvonta, vapauden rajoittaminen ja irti kytkeminen on mahdollista tehdä alueellisesti ja joustavasti. Tämä on oleellinen ominaisuus aseellista kansannousua tai paikallista konfliktia hallittaessa. Sisäiset turvallisuusuhat vaativat herkempää hallintaa jo pelkästään valtiojohdon legitimiteetin näkökulmasta. Kansallisen internetsegmentin täysi sulkeminen voi olla tehokas toimi epäsuoria ja ei-sotilaallisia keinoja käyttäviä valtiotoimijoita vastaan kiristyvän konfliktin aikana, mutta riskinä ovat tilanteen pitkittyessä taloudelliset vaikeudet. Sodan alkuvaiheessa ja sodassa kansallisen internetsegmentin täysi sulkeminen tarjoaa puolustuksellisen edun niin sisäisiä kuin ulkoisia kyber- ja informaatiohyökkäyksiä vastaan. Pakottavalla voimankäytöllä suljetun verkon valtion hyötykustannuslaskelmiin vaikuttaminen vaikeutuu huomattavasti, kun hyökkääjän mahdollisuudet vaikuttaa puolustajan arvottamiin kohteisiin heikkenee. Kansallinen segmentti toimiikin eräänlaisena ”informaatioajan siviilipuolustuksen” elementtinä kiistäen hyökkääjältä mahdollisuuden vaikuttaa yhteiskunnallisiin (*countervalue*) kohteisiin.

Sodan luonteella on vaikutus siihen, miten kansallista informaatioturvallisuuden ja puolustuksen järjestelmää käytetään. Ymmärrys sodan luonteesta on toki strategiskulttuurinen ilmiö ja näin ollen suljetun verkon käyttökin voi vaihdella valtioittain. Merkittävästi heikompaa vastustajaa vastaan käydyssä sodassa kansallisen verkon sulkeminen ei ole tarpeellista, ellei pelätä kolmannen osapuolten osallistumista sotaan. Verkko voidaan sulkea osittain etenkin sellaisten kohteiden osalta, joihin heikompi valtio saattaisi pyrkiä iskemään. Lisäksi valvontaa voidaan kiristää ja vastatoimien painopiste asettaa kansainvälisen mielipiteen muokkaamisen ja heikomman vastustajan lamauttamiseen ja eristämiseen muusta maailmasta laaja-alaisilla

paikannettuja heikkouksia vastaan suunnatuilla toimenpiteillä. Sodassa vertaisvastustajaa vastaan kansallisen verkon täydellinen sulkeminen mahdollisimman aikaisessa vaiheessa on järkevää. Siten kiistetään laajat suorituskyvyt omaavalta vastustajalta mahdollisuus informaatiovaikuttamiseen, kyberhyökkäysten valmisteluun ja yllätyksen tavoitteluun.

Rakenteellisen kyberasymmetrian vaikutukset poikkeavat puolustus- ja hyökkäystaistelun suhteen. Puolustustaistelussa kansallinen internetsegmentti tukee tavanomaisten ja ydinaseiden käyttöä muissa toimintaympäristöissä. Se suojaa välillisesti asevoimien johtamisjärjestelmiä ja tarjoaa varayhteyksiä, mikäli asevoimien omat järjestelmät lamaantuvat. Mitä joustavammin kansallisen verkon rakennetta voidaan muokata ja sen järjestelmiä päivittää ja vaihtaa, sitä vaikeampi hyökkääjän on tiedustella hyökkäyskohteita tai hyökkäystensä vaikutuksia. Mitä tiiviimmin kansallinen verkko suljetaan, mukaan lukien avaruus[720] ja vapaa elektromagneettinen tila, sitä vaikeampi ulkopuolisen hyökkääjän on tunkeutua asevoimien verkkoihin. Mitä vahvempi resilienssi kansallisella informaatioinfrastruktuurilla on, sitä paremmin se palautuu esimerkiksi ilma-avaruusiskun vaikutuksista ja kykenee tukemaan valtion sotilaallisen voiman mobilisointia vastahyökkäykseen.

Oleellinen tekijä kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmän toiminnan kannalta puolustustaistelussa on sen kokonaisuuden harjoituttaminen ja keskinäisriippuvuuksien hallinnointia jo rauhan aikana. Kybertilan moninaiset keskinäisriippuvuudet aiheuttavat lamauttavia vaikutuksia, mikäli kansallista internetsegmenttiä yritetään säädellä konfliktin tai sodan aikana ilman valmistautumista. Sotateollisen kompleksin, ICT-yritysten, finanssialan, energian tuotannon, jäte- ja vesihuollon, logistiikkajärjestelmien, alue- ja paikallishallinnon tietojärjestelmien, rautateiden, lentoliikenteen ja vesiväylien ohjausjärjestelmien ja verkkojen tulee kyetä toimimaan yhteyksien katkettua globaaliin Internettiin. Muussa tapauksessa kansallisen verkon sulkeminen johtaisi sekasortoon ja asevoimien toimintaedellytysten merkittävään heikkenemiseen. Venäjän vuonna 2020 aloittamat kansalliset

[720] Kommunikaatio- ja tiedustelusatelliittien häirintä laajan maantieteellisen alueen yläpuolella on suurvaltojen suorituskykyjen puitteissa viimeistään 2030-luvulla (Harrison et a. (2020)).

kyberharjoitukset ja vuonna 2021 rakentamat viisi kyberharjoitusaluetta vastaavat juuri tähän haasteeseen.[721]

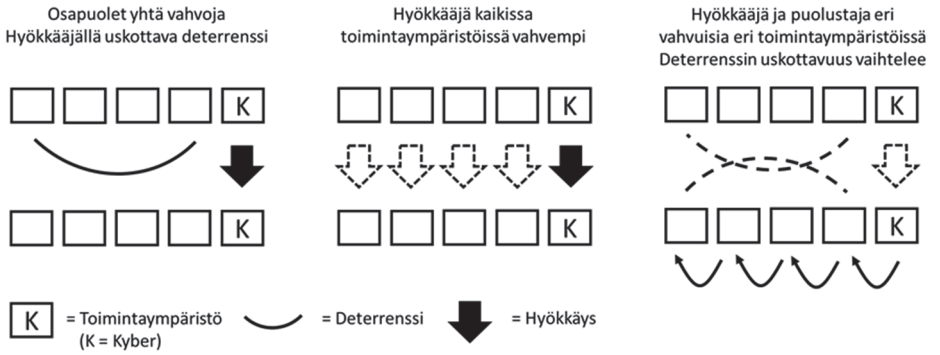
Puolustustaistelun näkökulmasta suljettu kansallinen verkko voidaan nähdä svetšiniläisittäin kulutussodankäynnin mahdollistajana, joka antaa puolustajalle aikaa selustan turvaamiseen ja voiman kasvattamiseen suhteessa vastustajaan.[722] Kansallinen internetsegmentti tuottaa kybertoimintaympäristöön syvyyden, johon tukeutuen valtio perustaa ja ryhmittää sotavoimansa ja joka tukee sotatoimia koko niiden keston ajan. Kyber- ja informaatiotila siis tukevat informaatioyhteiskunnan kansallisen voiman eri komponenttien rakentamista ja niiden käyttöön saamista. Tämä koskee myös kansakunnan psykologista vahvuutta ja valmiutta sotaan. Kansallisen internetsegmentin ollessa suojattu hyökkääjää ja sen tukialuetta kulutetaan muun muassa kyberhyökkäyksillä, kunnes voimaa on koottu tarpeeksi vastahyökkäystä varten. Erona Svetšinin ja hänen aikalaistensa ajatuksiin on sodan aikajänteen merkittävä lyheneminen.

Suljetun ja avoimen kansallisen verkon valtioiden välisessä konfliktissa ja sodassa hyökkäykselliset kyberoperaatiot voivat tukea ja mahdollistaa muissa toimintaympäristöissä tapahtuvia operaatioita tai saavuttaa itsessään strategisia tavoitteita. Luvussa 2 esitetyn kritiikin mukaan kyberhyökkäysten strateginen vaikutus on rajoitettu, koska ne ovat ajalliselta kestoltaan rajoitettuja eivätkä aiheuta pysyvää vahinkoa. Tämä väite tulisi kuitenkin aina asettaa määrätyn konfliktin voimasuhteiden kehykseen. Mikäli osapuolet ovat kaikissa toimintaympäristöissä tasavahvoja, kyberhyökkäysten strateginen vaikutus edellyttää hyökkääjältä uskottavaa deterrenssiä muissa toimintaympäristöissä. Muussa tapauksessa hyökkäyksen kohde eskaloi muissa toimintaympäristöissä ja vaikutus jää puolittaiseksi, jos sitä on laisinkaan. Jos taas hyökkäävä osapuoli on kaikissa toimintaympäristöissä vahvempi, voidaan kyberoperaatioita käyttää itsenäisesti pakottamiseen, sillä heikomman kyky vastata toimiin on rajoitettu. Kyberhyökkäyksen vaikuttavuutta voidaan tukea voimankäytöllä muissa toimintaympäristöissä. Osapuolien vahvuuksien ja deterrenssin

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

[722] Svechin (1992), 298. Svetšinin aikalaisen A. E. Snesarevin ajatuksia mukaillen informaatioturvallisuuden ja -puolustuksen järjestelmä valmistaa valtiota oman aikansa sotaan, jonka käymisen väline valtio on (Снесарев, А. Е. & Керсновский, А. А.: *Философия войны*. Вече, Москва, 2018, s. 291–292).

uskottavuuden ollessa eri toimintaympäristöissä eri määräisiä tai laatuisia kyberhyökkäysten strateginen vaikutus riippuu kybervoimatasapainon ulkopuolisista tekijöistä. Vaikutukseen pääseminen edellyttää maalittamista, jonka tuottaa systemaattisia, poikkitoimintaympäristöllisiä vaikutuksia. Kaikissa tapauksissa maantiede, yhteiskuntien rakenne, yhtenäisyys ja resilienssi, teknologisen osaamisen erot, strateginen kulttuuri ja liittolaisjärjestelmät vaikuttavat merkittävästi hyökkäysten vaikutuksiin ja niiden tulkintaan. Edellä kuvatut tapaukset on esitetty kuvassa 13.



Kuva 13: Kyberhyökkäysten strategiset vaikutusmahdollisuudet vastustajassa

Mikäli kansallinen internetsegmentti kyetään onnistuneesti sulkemaan, on luvussa 4 suoritetun analyysin perusteella suljetun verkon valtiolla rakenteelliseen kyberasymmetriaan pohjautuen puolellaan hyökkäyksellinen etu. Kuten edellä on todettu, tätä etua voidaan käyttää deterrenssin tai eskalaation hallinnan välineenä. Pakottamisen tai raa'an voiman välineenä etua voidaan käyttää yllätykselliseen ensi-iskuun tai vastahyökkäyksen tukemiseen. Yllätyksellinen ensi-isku voi lamaannuttaa osan avoimen verkon valtion kriittisestä informaatioinfrastruktuurista ja johtamisen kyvyistä ja estää taisteluvoiman ryhmittämisen, mobilisoinnin tai kansainvälisen avun vastaanottaminen. Viranomaisyhteistyön perusta voidaan lamauttaa ja kohdevaltio hajottaa käytännössä osiin ja eristää muusta maailmasta. Yhteiskunnan tahto puolustautua voidaan romahduttaa lamauttamalla informaatioyhteiskunnan perusta.

Niin Kiina kuin Yhdysvallat valmistautuvat toteuttamaan kyberensi-iskun, eikä Venäjäkään aio antautua hyökkäyksen kohteeksi.[723] Hyökkäykset voidaan kohdistaa avoimen verkon valtioon kaikkialta kybertoimintaympäristöstä, mikä hidastaa attribuutiota ja vastatoimia. Hyökkäys ja sen valmistelu voidaan aloittaa ennen varsinaista sodan julistamista, jolloin päätöksenteon tapa avoimen verkon valtiossa saattaa johtaa hitaaseen ja epävarmaan reagointiin. Suljetun verkon valtiossa informaatioturvallisuuden ja -puolustuksen järjestelmä kaventaa sitä vastaan hyökkäävän käytössä olevaa aikaa ja tilaa. On toki mahdollista, että parempi yhteinen tilannekuva yhdistettynä keskitettyyn johtamiseen johtavat suljetun verkon osalta hätäilevään ja tempoilevaan päätöksentekoon. Ensi-iskun toteuttamisessa on riskinsä.

Rakenteellinen kyberasymmetria tekee ensi-iskusta tai jopa ennalta ehkäisevästä hyökkäyksestä houkuttelevan. Se minimoi omat kustannukset, koska kyberaseet on voitu kehittää ennalta avoimien verkkojen heikkouksia hyödyntäen ja omat kohteet on suojattu kansallisen verkon sulkeuduttua. Se maksimoi onnistumisen todennäköisyyden, koska avoimen verkon valtio alkaa suojella järjestelmiään tehokkaammin vasta sodan alettua tai uhan ollessa välitön. Suljettu verkko taas minimoi avoimen verkon valtion vastatoimien onnistumisen mahdollisuuden. Vaikka kyberhyökkäyksiä ei käytettäisikään, kansallisen verkon sulkeminen tukee informaatiovaikuttamista. Avoimien verkkojen informaatiotilaa voidaan hyödyntää muissa toimintaympäristöissä käytettävän pakottavan ja raa'an voiman vaikutusten tukemisessa samalla, kun oma tila on hallinnassa. Jos ajatus siitä, että kyberhyökkäykset ovat vaarallisimmillaan joko ensi-iskun tai informaatiovaikuttamisen välineenä, pitää paikkansa niin kansallisen segmentin etupainoisessa sulkemisessa on sotilaallisstrategisesta näkökulmasta järkeä.[724]

---

[723] Sanger (2019) s. xiii; Dossi (2020); Austin, Greg: The Strategic Implications of China's Weak Cyber Defences. *Survival*, Vol. 62, No. 5 (2020), s. 119–138; Колесниченко, Александр: Андрей Крутских: с кибербезопасностью все так же, как с ядерным оружием. *Аргументы и Факты*, 25.5.2017. [https://aif.ru/society/safety/andrey_krutskih_s_kiberbezopasnostyu_vse_tak_zhe_kak_s_yadernym_oruzhiem], luettu 4.1.2021.

[724] Tällaisesta ajattelusta on viitteitä niin venäläisessä kuin kiinalaisessakin sotataidossa. (Pynnöniemi (2019); Kukkola (2020a); McReynolds (2016); Fravel, Taylor M.: *Active Defense: China's Military Strategy since 1949*. Oxford University Press, Oxford, 2019, s. 210; Thomas (2020).

Rakenteellinen kyberasymmetria antaa syvyydelle merkityksen myös hyökkäyksen osana. Avointa kansallista verkkoa vastaan hyökättäessä taistelutilan syvyys alkaa suljetun verkon rajalta. Hyökkäykset voidaan ulottaa kohdevaltiolle kriittisten valtioiden tietoliikennesolmuihin ja merikaapeleihin. Kohdevaltio voidaan pyrkiä eristämään ulkomaailmasta yhdistetyillä kyber-, avaruus-, kineettisillä ja ELSO-hyökkäyksillä. Tämä on mahdollista etenkin, jos kohde on hyökkääjän maantieteellinen naapuri, pinta-alaltaan suhteellisen pieni ja huonosti verkottunut. Hyökkäykset voidaan kohdistaa avoimen verkon valtion kykyyn projisoida voimaa rajojensa ulkopuolelle. Ne voidaan kohdistaa avoimen verkon valtion tilannekuva- ja johtamisjärjestelmiin niin sen rajojen sisä- kuin ulkopuolellakin. Samalla tavoin voidaan iskeä talous-, logistiikka- ja energiatuotantojärjestelmiä vastaan koko taistelualueen, kaikkien avoimen verkon riippuvuuksien syvyydessä. Asevoimia vastaan voidaan iskeä missä päin maailmaa tahansa mukaan lukien avaruus. Kyberhyökkäyksillä voidaan tukea omien asevoimien toimintaa kaikkialla maailmassa. Niillä voidaan tukea informaatiovaikuttamista useita eri kohdeyleisöjä vastaan, sijaitsivat nämä sitten avoimen verkon valtiossa tai sen ulkopuolella. Informaatiovaikuttamista voidaan yhdistää, kaiuttaa ja vahvistaa, koska avoimet verkot eivät estä informaation leviämistä.

Syvyyden lisäksi rakenteellinen kyberasymmetria vaikuttaa hyökkäysten luonteeseen. Kotimaiseen ja vastustajan ratkaisusta poikkeavaan ohjelmisto- ja laitteistoteknologiaan perustuva kansallinen internetsegmentti mahdollistaa kyberhyökkäyksen avoimia verkkoja vastaan käyttäen voimakkaasti leviävää ja yleistä haavoittuvuutta hyödyntävää haittaohjelmaa. Tämä on eräänlainen kybertilan ”biologinen ase”, jota vastaan omat ohjelmistot ja laitteet on rokotettu. Toisaalta kansallinen internetsegmentti voi olla erittäin haavoittuvainen vastaavanlaiselle hyökkäykselle. Mikäli globaali Internet hajoaa kansallisiin osiin, muodostuu kansainvälisen järjestelmän tasolla ongelmaksi kyberaseiden ”kansallinen” räätälöinti. Syntyy ekosysteemejä vastaan kehitettyjä aseita, joiden käyttökynnys madaltuu keskinäisriippuvuuden vähetessä.

Edellä esitetyn perusteella on selvää, että kyberhyökkäysten onnistuneella maalittamisella on tärkeä merkitys hyökkäysten vaikutukselle. Kyberhyökkäykset voivatkin noudattaa ydinaseista johdettua maalittamissuunnitelmaa (*Single Integrated Operation Plan, SIOP tai*

OPLAN 8010)[725], jolloin hyökkäykset on helpompi integroida osaksi erilaisia konflikti- ja sotaskenaarioita ja niiden päämääriä. Suunnitelma voi toimia deterrenssin välineenä rauhan aikana tai pakottamisen ja raa'an voiman välineenä sodassa. Suunnitelma edesauttaa kybersuorituskykyjen integroimista muiden sotilaallisten suorituskykyjen osaksi ja tarjoaa päätöksentekijöille mahdollisuuden valita erilaisista vaikuttamisvaihtoehdoista. Maalittamissuunnitelmien haasteena on kybertoimintaympäristön muuttuva luonne, joka rajoittaa kyberaseiden joustavaa käyttöä.[726] Rakenteellisen kyberasymmetrian kehyksessä maalittamissuunnitelmat voivat tukea pakottamista hyökättäessä ensi-iskun omaisesti avoimiin verkkoihin, mutta niiden hyöty hyökättäessä suljettuihin verkkoihin on rajallinen. Suljetun verkon puolustaja kykenee muuttamaan verkkojensa rakennetta, paikkaamaan haavoittuvuuksia ja rajoittamaa kohde- ja vaikutustiedustelua siinä määrin, että maalittamissuunnitelmat voivat olla vain hyvin yleisluontoisia. Niihin on vaikea liittää nopeassa tilannekehityksessä relevanttia, käytössä olevaa suorituskykyä.

Informaatioturvallisuuden ja -puolustuksen järjestelmän asevoimien verkot ja järjestelmät ovat rakenteellisen kyberasymmetrian sotilaallisen hyväksikäytön erityistapaus. Niin ohjus-, ilma- ja avaruuspuolustusjärjestelmät kuin strategisten ydinaseiden johtamisjärjestelmät ovat haavoittuvia antisatelliittiaseille, pitkän kantaman täsmäaseille ja kyberhyökkäyksille. Järjestelmät on usein hajautettu laajalle maantieteelliselle alueelle. Tästä syystä ne tarjoavat runsaasti maaleja ja hyökkäysvektoreita kyberhyökkäykkäyksille, joita kaikkia on vaikea suojata. Tavanomaisten ja ydinaseiden johtamisjärjestelmien digitalisoituminen ja yhteen kietoutuminen ja siviili- ja sotilasinfrastruktuurin kaksoiskäyttö lisäävät haavoittuvuuksia. Joitain haavoittuvuuksia voidaan kompensoida esimerkiksi estämällä

[725] SIOP käsitteestä ks. Kristensen, Hans M.: *Obama and the Nuclear War Plan. Federation Of The American Scientists Issue Brief, February, 2010.* [https://fas.org/programs/ssp/nukes/publications1/WarPlanIssueBrief2010.pdf], luettu 4.1.2021.

[726] SIOP soveltamisesta kyberaseisiin ks. Long, Austin: A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning. *Journal of Cybersecurity*, Vol. 3, No. 1 (2017), s. 19–28; Mazanec, Brian M.: *Lessons for the Cyber Battlefield from the Early Nuclear Era's Single Integrated Operating Plan*. FDD Press, Washington DC, 2019.

potentiaalista vastustajaa maalittamasta ydinaseita häiritsemällä sen tiedustelujärjestelmiä.[727]

Venäjän tapauksessa maantieteellä on erityinen merkityksensä. Maan koko tarkoittaa, että strategisesti tärkeät johtamisjärjestelmät on hajautettu laajalle alueelle. Satelliittiviestintä on kriittinen eräiden alueiden osalta. Toiset alueet ovat pitkien, rautateitä seuraavien kiinteiden yhteyksien varassa, joiden varrella on suojaamattomia linkkiasemia ja muita yhdyspisteitä. Merikaapeleilla on suuri merkitys etenkin Kaukoidässä. Hyökkäysvektoreita on lukuisia, eikä kansallisen internetsegmentin sulkeminen sulje niitä kaikkia. Lisäksi kansallisten verkkojen sulkeminen voi vaikuttaa Venäjän asevoimien ulkomailla sijaitseviin ohjus- ja ilmapuolustusjärjestelmiin. Ongelmiin voivat joutua myös sotilaspiirit ja sodan aikana strategiset yhteisjohtoportaat omilla suunnillaan, jos paikallishallinnon, turvallisuusviranomaisten ja liittovaltion verkot fragmentoituvat tavalla, joka ei noudata yhteisjohtoportaiden vastuualueita tai taisteluajatusta.[728] Venäjästä tehtyjen havaintojen on tässä tarkoitus osoittaa, että asevoimat on integroitavat kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmään, mikäli siitä ei haluta rakentaa voimanlähteen sijaan kriittistä heikkoutta.

Teknologian kehityksellä on ratkaiseva vaikutus suljettujen kansallisten verkkojen kehitykseen ja täten rakenteellisen kyberasymmetrian sotilaalliseen hyväksikäyttöön. Tekoälyn kehitys johtaa ”sormenjälkien” käytöstä anomaliapohjaiseen jatkuvasti kehittyvään uhkien etsintään ja torjuntaan. Kansallisesta verkosta kerätty tapahtumatietokanta tukee

---

[727] Cimbala, Stephen J.: Nuclear Crisis Management and Deterrence: America, Russia, and the Shadow of Cyber War. *The Journal of Slavic Military Studies*, Vol. 30, No. 4 (2017), 487–505, s. 501; Futter, Andrew: War Games Redux? Cyberthreats, US–Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control. *European Security*, Vol. 25, No. 2 (2016), s. 163–180; Austin, Greg & Sharikov, Pavel: “Pre-emption is victory”: Aggravated Nuclear Instability of the Information Age. *The Nonproliferation Review*, Vol. 23, No. 5-6 (2016), s. 691–704; Blair, Bruce G.: Why Our Nuclear Weapons Can Be Hacked. *The New York Times*, March 14, 2017 [https://www.nytimes.com/2017/03/14/opinion/why-our-nuclear-weapons-can-be-hacked.html?hpw&rref=opinion&action=click&pgtype=Homepage&module=well-region&region=bottom-well&WT.nav=bottom-well&_r=0], luettu 12.1.2021; Аксенов, С.В.: Обеспечение устойчивости группировки стратегических ядерных сил в условиях информационного противоборства. *Вестник академии военных наук*, № 2 (67) (2019), с. 66–68.

[728] Venäjän asevoimista ks. Whisler (2020b); Westerlund, Fredrik & Oxenstierna, Susanne (eds.): *Russian Military Capability in a Ten-Year Perspective – 2019*. FOI, Stockholm, 2019; Puolustusministeriö: *Voiman Venäjä*. Puolustusministeriö, Helsinki, 2019.

puolustuksellisen tekoälyn kehittämistä. Sen pitäisi nopeuttaa päätöksentekoa ja tarjota parempi suoja.[729] Tekoälyn, big datan ja psykologian integraation avulla voidaan ennustaa määrätyllä todennäköisyydellä kybertaistelukentän tapahtumia ja auttaa ohjaamaan yhteiskunnallista informaatioympäristöä.[730] Tekoälyn ja kehittyneiden simulaatioiden käyttö voimasuhdelaskemissa voi mahdollistaa kansallisen internetsegmentin ominaisuuksien liittämisen osaksi kybervoimalaskelmia.[731] Nykyisillään tekoälyissä on rajoituksensa. Silti pienetkin erot voivat tarjota merkittävän edun ja horjuttaa voimatasapainoa.[732] Mikäli suljetun verkon valtio onnistuu kehittämään yleisen tekoälyn (AGI), se saa täysin uudenlaisen edun niin hyökkäyksessä kuin puolustuksessa.[733] Lisäksi kansallisen internetsegmentin suljettu ja omavarainen luonne voi vaikeuttaa sitä vastaan kehitettävän hyökkäyksellisen tekoälyn tarvitseman datan hankkimista.

Hyökkäyksellisen tekoälyn kehittäminen on todennäköisesti vaikeampaa kuin puolustuksellisen.[734] Tekoälyteknologia on kuitenkin periaatteessa hyökkäyspainotteista, koska se hyötyy aloitteellisuudesta, eikä tee arvovalintoja olemassa olevan säilyttämisestä kuten ihmiset.[735] Hyödyistä huolimatta hyökkäyksellisen tekoälyn kehittämisessä strategisen tason käyttötarkoituksiin on vaaransa. Kahden tekoälyn asettaminen vastakkain kybertoimintaympäristössä voi johtaa rajoittamattomaan eskalaatioon nopeudella, johon ihmiset eivät ehdi puuttua. Lisäksi tekoäly voi säädellä suljettua kansallista verkkoa tavalla, joka haittaa sotatoimia muissa toimintaympäristöissä. Tekoälyn luotettavuutta heikentävät prosessien läpinäkymättömyys ja järjestelmään päässeen väärän tiedon potentiaalisesti huomaamaton vaikutus.[736] Ihmiset saattavat luottaa liiaksi

---

[729] Stevens, Tim: Knowledge in the Grey Zone: AI and Cybersecurity. *Digital War* (2020). https://doi.org/10.1057/s42984-020-00007-w.
[730] Dear (2019).
[731] Reach, Clint, Kilambi, Vikram & Cozad, Mark: *Russian Assessments and Applications of the Correlation of Forces and Means*. RAND, Santa Monica, 2020, s. 133.
[732] Payne, Kenneth: Artificial Intelligence: A Revolution in Strategic Affairs? *Survival*, Vol. 60, No. 5 (2018), s. 7–32; Geist, Edward & Lohn, J. Andrew: *How Might Artificial Intelligence Affects the Risk of Nuclear War*. RAND, Santa Monica, 2019.
[733] Ayoub, Kareem & Payne, Kenneth: Strategy in the Age of Artificial Intelligence, *Journal of Strategic Studies*, Vol. 39, No. 5-6 (2016), s. 793–819.
[734] Zouave, Erik, Bruce, Marc, Colde, Kajsa, Jaitner, Margarita, Rodhe, Ioana & Gustafsson, Tommy: *Artificially intelligent cyberattacks*. FOI, Stockholm, 2020.
[735] Payne (2018).
[736] Fitzpatrick, Mark: Artificial Intelligence and Nuclear Command and Control. *Survival*, Vol.61, No.3 (2019), s. 81–92.

tekoälyn suosituksiin etenkin paineen alla ja kiireessä, jolla voi olla traagisia seurauksia strategisessa päätöksenteossa (eli ydinaseiden käyttö).[737]

Koska tekoäly on uusi teknologia, valtioiden tavat hyödyntää sitä todennäköisesti poikkeavat kehityksen alkuvaiheessa. Silti Thortonin ja Mironin väite siitä, että erityisesti venäläiset näkevät tekoälyn tarjoavan hetkellisen etulyöntiaseman suurvaltakilpailussa ja että he ovat taipuvaisia käyttämään tätä etua, on kyseenalainen.[738] Uusien asejärjestelmien käytössä Yhdysvallat on Israelin rinnalla ollut historian todistusaineiston valossa johtovaltio Saksan jälkeen 1900- ja 2000-luvuilla.[739] On varsin todennäköistä, että kaikki suurvallat ja alueelliset johtovaltiot kehittävät hyökkäyksellisiä tekoälysovellutuksia useisiin eri tarkoituksiin. On myös hyvin todennäköistä, että suurvallat tulevat käyttämään näitä sovelluksia tilaisuuden ilmantuessa. Yhdysvaltojen hallinnon Kansallisen turvallisuuden komissio on jo suositellut hyökkäyksellisen tekoälyn käyttöönottoa.[740] Johtuen kybernetiikan perinnöstä Venäjä pyrkinee hyökkäysmenetelmien lisäksi kehittämään tekoälyä sotilaspuolella päätöksenteon tukemiseksi ja talous- ja sosiaalipuolella kohti talousjärjestelmän ja yhteiskunnan toiminnan optimointia mukaan lukien informaatiotilan hallinnan tukeminen. Systeemiajattelu voi ohjata Venäjää kehittämään vastustajien heikentämiseen ja horjuttamiseen tähtäävää informaatiovaikuttamista enemmän kuin kineettiseen vaikuttamiseen rinnastettavia tekoälysovelluksia.[741] Deterrenssin rakentaminen ja suojautuminen Yhdysvaltojen ja Kiinan hyökkäykselliseltä tekoälyteknologialta on Venäjälle vähintään yhtä tärkeää kuin spekulatiivisen ensi-iskukyvyn hankkiminen ja käyttäminen. Väittäessään Venäjän olevan taipuvaisempi käyttämään hyökkäyksellistä tekoälyä, Thorton ja Miron osoittavat enemmän peiliajattelua (*mirror-imaging*) kuin venäläisen strategisen kulttuurin ymmärrystä, joka korostaa oveluutta, luovuutta ja yllätystä.

---

[737] Johnson (2020).
[738] Thornton & Miron (2020).
[739] Ydinaseet (Japani 1945), rypälepommit ja täsmäaseet (Vietnam 1960- ja 1970-luvut), häivepommikoneet (Panama 1989), modernit täsmäristeilyohjukset (Irak 1991), aseistetut UAV:t (Afganistan 2001) ja kineettistä tuhoa aiheuttavat kyberaseet (Iran 2010).
[740] National Security Commission on Artificial Intelligence: *Final Report*, 2021. [https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf], luettu 6.3.2021.
[741] Ks. Thomas (2019); Kari (2019); Kukkola (2020a).

Kvanttikommunikaatio ja -salaus on toinen rakenteelliseen kyberasymmetriaan vaikuttava teknologia. Kvanttiteknologian edut liittyvät tiedusteluun ja uhkien ennaltaehkäisyyn pakottamisen ja raa'an voiman käytön sijaan. Tiedon salaaminen tai vastustajan viestien avaaminen tarjoavat mahdollisuuden yllätykseen ja etuun taistelukentällä.[742] Esimerkiksi kansallisen internetsegmentin tapauksessa jo käytössä oleva QKD-teknologia mahdollistaisi liikkeessä olevan datan suojaamisen. Varsinainen kvanttiviestintä on tosin vielä koeasteella ja teknologia aivan liian kallista toteutettavaksi kansallisella mittakaavalla.[743] Aikanaan siitä tullee kuitenkin olennainen osa kansallisia internetsegmenttejä samoin kuin laajakaistayhteyksiä tarjoavista minisatelliiteista.

Jotta suljetun verkon ja avoimen verkon suhde voi synnyttää sotilaallisesti hyväksikäytettävää rakenteellista kyberasymmetriaa, suljetun verkon tulee sisällyttää itseensä kaikki olevat ja tulevat kommunikaatioteknologiat. Jon Lindsay on todennut osuvasti, ettei teknologia itsessään määrittele strategisia lopputuloksia vaan politiikka ja sosiaaliset käytännöt kuten organisaatiokulttuuri. Ne määrittelevät, miten uusi teknologia omaksutaan ja mihin sitä käytetään. Lisäksi huipputeknologia edellyttää merkittäviä resursseja, eikä kaikilla ole varaa parhaaseen.[744]

Kyberasymmetrian sotilaallisella hyväksikäytöllä voi olla myös laajempia kuin taistelevia osapuolia koskevia vaikutuksia. Kansallisen internetsegmentin sulkemisesta voivat kärsiä esimerkiksi liittolaissuhteet. Puolustusliitot kykenevät todennäköisesti osittain toimimaan asevoimien välisten yhteyksien avulla, mutta taloudelliset, finanssialan, viestinnälliset ja kulttuuriset yhteydet katkeavat. Katkoksen merkitys riippuu tietenkin kyseisestä liittolaissuhteesta. Venäjän tapauksessa monet sen naapurimaista, kuten Valko-Venäjä, Kazakstan, Armenia ja Ukraina, ovat jossain määrin riippuvaisia Venäjän energia-, finanssi- ja talousjärjestelmästä ja olisivat vaikeuksissa tietoliikenneyhteyksien

[742] Lindsay, Jon R.: Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage. *Security Studies*, Vol. 29, No. 2 (2020), s. 335–361.
[743] Ananthaswamy, Anil: The Quantum Internet Is Emerging, One Experiment at a Time. *Scientific American*, June 19, 2019. [https://www.scientificamerican.com/article/the-quantum-internet-is-emerging-one-experiment-at-a-time/], luettu 4.1.2021; Giles, Martin: Explainer: What is Quantum Communication? *MIT Technology Review*, February 14, 2019. [https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/], luettu 4.1.2020.
[744] Lindsay (2020).

katketessa. Tulevaisuudessa Kiinalla on todennäköisesti yhä merkittäviä investointeja Venäjällä, joiden tilapäistäkään menetystä se ei katsoisi hyvällä. Hieman nurinkurisesti suurin menetys yhteyksien katkeamisesta koituisi Venäjän talous- ja finanssiyhteyksille Euroopan Unioniin ja Yhdysvaltoihin.[745] Vaikka kansallisen internetsegmentin sulkeminen ei suurella todennäköisyydellä ole taloudellisesti kannattavaa, pitää taloudellisia menetyksiä aina verrata sodasta koituviin odotettuihin tappioihin (nykypäivänä harvemmin voittoihin). Nykyaikaisessa sodankäynnissä vahinkoja joka tapauksessa koituu informaatioyhteiskunnalle ja -taloudelle ja itsensä parhaiten suojannut kykenee paremmin palaamaan normaalitilaan.

Pakottavalta ja raa'an voiman käytöltä puolustautuminen kybertoimintaympäristössä voi siis johtaa menetyksiin muilla suunnilla. Toisaalta liittolaisista voi olla apuakin, jos jokin niistä valikoituu ylläpitämään suljetun verkon valtion rajattuja yhteyksiä ulkomaailmaan. Voi syntyä niin sanottuja "transit" valtioita tai kokonaisia "kyberblokkeja." Koska tietoverkot eivät ole ainoa datan kulkureitti, blokkiutumisen pitäisi ulottua avaruuteen ja vapaaseen elektromagneettiseen tilaankin. Kansalliset informaatioturvallisuuden ja -puolustuksen järjestelmät voivat itse asiassa johtaa kyber- ja informaatiotilassa tapahtuvaan blokkiutumiseen välttämättömistä markkinataloudellisista, poliittisista ja sotilaallisista syistä. Kansainvälisiin normistoihin, standardeihin ja instituutioihin voi ilmestyä liittokuntakohtaisia ja toisensa poissulkevia resurssijakoja elektromagneettisen spektrin ja dataliikenteen osalta. Blokkien väliset yhteydet karsiutuvat vähimmäismäärään tehokkuuden, yhteensopimattomuuden ja valvonnan tuloksena. Näin kyber- ja informaatiotila muuttuvat valtioiden turvallisuutta tavoittelevan kyberstrategian seurauksena.

Kaikki edellä mainittu huomioiden voidaan todeta, että rakenteellinen kyberasymmetria tukee strategisten päämäärien saavuttamista kybertoimintaympäristössä. Sen vaikutus on kuitenkin suurin toimintaympäristöjen rajat ylittävässä pakottamisessa ja raa'an voiman

---

[745] Центральный банк российской федерации: *Внешняя торговля Российской Федерации услугами - 2019*. Статистический сборник. Банк России, Москва, 2020. [https://www.cbr.ru/statistics/macro_itm/svs/], luettu 12.1.2021; Domínguez-Jiménez, Marta & Poitiers, Niclas: *FDI another day: Russian reliance on European investment*. Policy Contribution 03/2020, Bruegel; Liuhto, Kari: Motivations of Russian Firms to Invest Abroad: How Do Sanctions Affect Russia's Outward Foreign Direct Investment? *Baltic Region*, Vol. 26, No. 4 (2015), s. 4–19.

käytössä. Suljetun kansallisen verkon ja asevoimien turvaamien rajojen suojista tehdyt kyberhyökkäykset, jotka yhdistetään kaukovaikutteisten tavanomaisten ja ydinaseiden käyttöön, takaavat parhaimmat vaikutusmahdollisuudet. Työnjaollisesti kyberhyökkäykset kohdistunevat johtamisen, tiedustelun, valvonnan ja maalittamisen järjestelmiin kaikissa toimintaympäristöissä sekä kriittiseen informaatioinfrastruktuuriin kohteissa, joihin ei haluta tai pystytä käyttämään kineettistä vaikuttamista. Kyberhyökkäyskykyjen käyttö on omiaan lamauttamaan vihollisen päätöksenteon ja johtamiskyvyn tuhoamisen sijaan. Vastapuolen päätöksentekijöitähän tarvitaan sodan poliittisten päämäärien saavuttamiseksi. Lisäksi niin pitkään kuin avoimen verkon valtion verkot ovat toiminnassa hyökkääjän kannattaa hyökätä yhteiskunnallisia kohteita (*countervalue*) vastaan, koska sotilaskohteet ovat huomattavasti vaikeammin saavutettavissa eikä niiden lamauttaminen välttämättä vähennä kohteen vastaiskukykyä muissa toimintaympäristöissä tai laske taistelutahtoa. Vastustajan ollessa sisäinen vihollinen, kybersuorituskyvyillä tuetaan muita turvallisuusviranomaisia vihollisen tuhoamisessa samalla, kun se eristetään ulkopuolisesta tuesta.

Rakenteellisen kyberasymmetrian vaikutus pakottamiselta ja raa'an voiman käytöltä puolustautumiseen on kiistatta hyökkäystä suurempi. Kansallinen internetsegmentti voi ehkäistä niin valtion pitkään jatkuvaa horjuttamista informaation avulla kuin strategisen yllätyksenkin. Kansallinen informaatioinfrastruktuuri ja sen hallinta sekä yhteiskunnan henkinen kestävyys on valmistelu suursotaan. Kansallinen internetsegmentti parhaimmillaan kiistää informaatioylivoiman saavuttamisen vastustajalta, on ylivoima sitten psykologista tai teknologista. Kiistäminen ei perustu pelkästään verkkojen sulkemiseen vaan kansallisiin ohjelmistoihin, laitteisiin, salaukseen, valvontaan, massamaisen datan keräämiseen ja analysointiin, sisäisiin vastatoimiin ja kyber- ja informaatioturvallisuusjärjestelmiin ja lukuisiin toimijoihin. Puolustuksen näkökulmasta kansallinen internetsegmentti suojaa sodassa yhteiskunnan kriittistä infrastruktuuria ja palveluita, talouden ja huoltovarmuuden edellyttämiä logistiikkajärjestelmiä, kansallisia sisäiseen ja ulkomaanviestintään tarkoitettuja järjestelmiä, valtiojohdon päätöksentekoon ja johtamiseen tarvittavia järjestelmiä sekä turvallisuusviranomaisten rikosten, terrorismin ja kumouksellisen toiminnan torjuntaan tarvittavia järjestelmä.

Edellä esitettyyn perustuen voidaan todeta, että rakenteellisesta kyberasymmetriasta saatava merkittävin sotilaallinen hyöty on pakottamisen ja raa'an voimankäytön kestämisessä, ei voiman käytössä. Ensi-iskun mahdollisuus voi vaikuttaa houkuttelevalta, mutta sen

käyttökelpoisuutta rajoittaa konfliktin hyvin nopea todennäköinen laajeneminen muihin toimintaympäristöihin. Kyberhyökkäysten käyttö pakottamisen ja raa'an voiman välineenä on aina asetettava kontekstiinsa. Vahvemman valtion hyökätessä heikompaa vastaan rajoitetussa sodassa kansallisten verkkojen täydellisessä sulkemisessa ei ole taloudellisesti tai sotilaallisesti järkeä. Vahvemman kannattaa säilyttää toiminnanvapautensa kaikissa ympäristöissä. Poikkeuksena on tilanne, jossa heikommalla valtiolla on suhteeton kyberhyökkäyskyky tai se kykenee nopeasti samaan ulkopuolista apua liittokunnalta tai toiselta suurvallalta. Oleelliseksi tekijäksi muodostuu kaikissa tapauksissa konfliktin kesto. Mitä pidempään kansallisten verkkojen sulkutila jatkuu, sitä suuremmat ovat yhteiskunnalliset vaikutukset ja sitä suuremmalla todennäköisyydellä hyökkääjä pääse läpi vahvistetuistakin puolustusjärjestelmistä.[746] Pitkitetyssä kansallisen internetsegmentin sulkemisessa on järkeä vain taisteltaessa sisäistä vihollista vastaan. Silloinkin ulkomaanyhteydet voidaan säilyttää rajoitetusti avoimina.

Lopuksi voidaan todeta, että kansallisen internetsegmentin sulkeminen ei välttämättä liity suoraan verkkonsa sulkevaan valtioon kohdistuvaan aggressioon. Esimerkiksi tulevaisuuden suursodassa Yhdysvaltojen ja Kiinan välillä Venäjä voi olla sivustakatsoja tai yhden suurvallan epäsuora liittolainen. Sen on tällöinkin kyettävä suojaamaan itsensä kybertoimintaympäristön puolella tapahtuvilta sotatoimilta. Sodilla on taipumus levitä toimintaympäristöissä ja niiden välillä. Suljettu ja autonominen verkko auttaisi Venäjää säilyttämään ja palauttamaan kansallisen toimintakykynsä sodassa kärsinyttä muuta maailmaa nopeammin.

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

6 Päätäntä

Tässä luvussa esitellään työn tulokset, pohditaan auki jääneitä kysymyksiä, tarkastellaan kriittisesti tehtyä työtä ja esitetään jatkotutkimusaiheita. Ensimmäinen osio esittelee keskeisimmät käsitteet, alatutkimuskysymyksiin saadut vastaukset ja lopulta itse tutkimusongelmaan saadun vastauksen. Pohdintaosio kritisoi erinäisiä sotatieteellisiä käsitteitä, tarkastelee kulttuuritekijöitä ja kybertoimintaympäristön muutosta. Kriittinen tarkastelu keskittyy työn tekemisen aikana esiin tulleisiin puutteisiin ja määrättyihin valintoihin, joilla on ollut vaikutusta työn tuloksiin. Näiden havaintojen pohjalta esitetään jatkotutkimusaiheita.

6.1 Vastaukset

Tämän työn tavoitteena oli kehittää käsite- ja teoriapohjaa aikaisemman tutkimuksen havaitseman rakenteellisen kyberasymmetrian tutkimiseksi. Lähestymistapana käytettiin teoriasidonnaista selvittävää ja kuvailevaa laadullista tapaustutkimusta, jonka tutkimuskohteena olivat Venäjän kansallisen internetsegmentin strategiset vaikutukset lähitulevaisuudessa 2030-luvulle. Työn tieteenfilosofinen perusta on pragmaattinen ja työn teoreettisena kehyksenä sovellettiin muokattua klassista neorealismia ja systeemiteoriaa. Tutkimusongelma oli, tuottaako Venäjän kansallinen internetsegmentti rakenteellista kyberasymmetriaa, miten se ilmenee ja mitkä ovat sen strategiset vaikutukset? Tutkimusongelmaa lähestyttiin neljän alakysymyksen kautta, joihin on vastattu työn luvuissa 2–5. Tutkimuskysymyksiin vastattaessa pyrittiin vertailemaan Venäjästä tehtyjä havaintoja kahteen muuhun suurvaltaan, Yhdysvaltoihin ja Kiinaan, työn tulosten yleistettävyyden parantamiseksi.

Ensimmäinen alatutkimuskysymys oli, mitä on rakenteellinen kyberasymmetria, miten sen olemassaoloa voidaan tarkastella ja mitä tarkoitetaan strategisilla vaikutuksilla? Kysymykseen vastattiin rakentamalla aikaisempaan kansainvälisen politiikan, strategian ja kyberturvallisuuden tutkimukseen perustuen kybertilan ja -toimintaympäristön, kybervoiman ja kyberstrategian käsitteet. Näiden pohjalta muodostettiin strategisen kybervoiman käytön neljä muotoa, jotka ovat konfliktien ennaltaehkäisy, deterrenssi, konfliktin eskalaation hallinta ja rakenteellisen kyberasymmetrian sotilaallinen hyväksikäyttö eli pakottamisen ja raa'an voiman käyttö. Kybervoiman käsittelyn jälkeen tarkasteltiin aikaisempia käsityksiä asymmetriasta sotilaallisen toiminnan kehyksessä ja muodostettiin niiden pohjalta rakenteellisen

kyberasymmetrian määritelmä. Rakenteellisen kyberasymmetrian tarkastelemiseksi esiteltiin digitaalisen maaston käsite, jonka avulla tutkimus kyettiin kohdistamaan kybertoimintaympäristön määrättyihin piirteisiin. Lopuksi muodostettiin rakenteellisen kyberasymmetrian analyysissä käytetyt toiminnan vapauden, yhteisen tilannekuvan, johtamisen ja resilienssin käsitteet.

Tässä työssä käytetty kybertilan käsitteen määritelmä on Daniel Kuehlia mukaillen 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. Korostettaessa kybertilan luonnetta nimenomaan toiminnan ympäristönä voidaan käyttää käsitettä kybertoimintaympäristö. Tällöin huomio ei ole pelkästään tilassa, sen luonteessa tai ominaisuuksissa vaan myös prosesseissa, tiedonhallinnassa ja ihmisten vuorovaikutuksessa.

Kybervoima määriteltiin työn tarpeita vastaavasti kyvyksi, joka mahdollistaa toimijan vaikutuksen muihin kybertilassa tai sen kautta ja kybertilan hallinnan ja muokkaamisen toimijan preferenssien mukaisesti. Määritelmällä haluttaan korostaa kybertilan muokattavuutta ja muuttuvuutta inhimillisen toiminnan seurauksena. Kybertilan kehyksessä voima perustuu teknologiseen, tieteelliseen, taloudelliseen, normatiiviseen, doktriinilliseen, organisatoriseen ja inhimilliseen (ammatilliseen) potentiaaliin. Kybervoiman resurssit ja keinot eivät ole yksinomaan sotilaallisia vaan ylittävät hallinnonalojen ja sodan ja rauhan rajat. Kybervoimaan liittyen kyberstrategia määriteltiin kybervoiman käytön suunnitteluksi, siihen valmistautumiseksi ja toteuttamiseksi sotilaallisin ja ei-sotilaallisin keinoin kybertilan ja valtioiden välisten suhteiden kontekstissa. Kyberstrategiaa suunnitellaan ja toimeenpannaan valtioiden välisten suhteiden eli rauhanomaisen kilpailun, kiristyneen kilpailun, konfliktin mukaan lukien sodan alkuvaiheen ja sodan aikana.

Strategisen tason voimankäytön muotojen käsitteiden muodostusta ohjasi *bargaining model of war* -malli, joka pohjaa yhdysvaltaiseen kylmän sodan aikaiseen ydinasedeterrenssiteoriaan ja operaatioanalyysiin. Näin ollen konfliktin ennaltaehkäisy perustuu aktiiviseen ja passiiviseen uhan syntymisen estämiseen. Deterrenssi perustuu voimankäytön ehkäisyyn uhkaamalla rankaisulla tai tavoitteiden saavuttamisen kiistämisellä sotilaalliseen voimaan perustuen. Konfliktin eskalaation hallinta liittyy voimankäytön intensiteetin säätelyyn konfliktin jo alettua.

Kyberasymmetrian hyväksikäyttö on perusta sodan päämäärien väkivaltaiselle, tuhoavalle ja pakottavalle saavuttamiselle.

Konfliktin ennaltaehkäisyllä tarkoitetaan potentiaalisen uhan neutralointia kaikilla käytettävissä olevilla toimilla niin, että suoraa aseellisen voiman käyttöä tai sillä uhkaamista ei tarvita. Kybertoiminnan osalta konfliktien ennaltaehkäisyn voi ajatella liittyvän tiedusteluun, ennakkovaroituksen hankkimiseen, taivutteluun, kansainvälisten normien rakentamiseen sekä toimintaympäristön muokkaamiseen potentiaalisten uhkien ehkäisemiseksi.

Kyberdeterrenssillä tarkoitetaan pyrkimystä taivutella potentiaalinen vastustaja pidättäytymään voimankäytöstä kybertilassa, kybertilasta tai muussa tilassa uhkaamalla sietämättömällä rangaistuksella, kiistämällä potentiaaliset hyödyt tai muutoin vaikuttamalla vastustajan hyötykustannuslaskelmiin kybertilaan liittyvillä suorituskyvyillä. Kyberdeterrenssi muodostaa osan valtion yleisestä deterrenssistrategiasta. Kyberdeterrenssi liittyy valtion suojaamiseen uhilta myös laajemmassa informaatio(psykologisessa)ympäristössä ja se on vuorovaikutuksessa muihin toimintaympäristöihin ja keinoihin.

Konfliktin eskalaation hallinnalla tarkoitetaan pyrkimystä säädellä jo käynnistyneen konfliktin intensiteettiä voimankäytöllä tai sillä uhkaamalla kybertilassa tai sen kautta tavoitteena saada vastustaja lopettamaan voimankäyttö itselle hyödyllisellä ja poliittisten päämäärien tavoittelua palvelevalla tavalla sekä samalla estää tahaton ja vahingossa tapahtuva eskalaatio. Rakenteellisen kyberasymmetrian sotilaallinen hyväksikäyttö on pakottamisen ja raa'an voiman käyttöä kybertilassa ja kykyä aiheuttaa sellaista vaikutusta kybertilassa tai sen kautta, joka pakottaa vastustajan lopettamaan vastarinnan vastoin omaa tahtoaan tai kiistää vastaavan vaikutuksen omiin järjestelmiin.

Strateginen vaikutus määriteltiin tässä työssä toimintaympäristön muutoksen kautta. Strateginen vaikutus muuttaa valtioiden toimintaympäristöä niin, että niiden välinen voimasuhde muuttuu potentiaalisen tulevan konfliktin osalta. Strateginen vaikutus liittyy voimankäytön edellytysten muuttumiseen sekä voimankäytön päämäärän tavoittamiseen liittyvään muutokseen kohdejärjestelmässä strategisella tasolla. Strategisia vaikutuksia esiintyy kaikissa valtioiden välisten suhteiden vaiheissa.

Asymmetrialle sotilaallisessa kontekstissa annettiin työssä tehdyn analyysin perusteella seitsemän eri merkitystä, jotka liittyivät

materiaalisten resurssien suhteelliseen epätasapainoon, suhteellisiin perustavanlaatuisiin eroihin ominaisuuksissa, suhteellisiin eroihin käsityksissä konfliktin luonteesta osapuolten välillä, tilaan ja aikaan, informaatioon ja mielikuvitukseen eli luovuuteen. Analyysin perusteella todettiin myös, että sellainen käsitys asymmetriasta, joka liittyy ajatukseen heikommasta, mahdollisesti attribuutiota välttelevästä, ei-valtiollisesta toimijasta, joka käyttää epätavanomaisia keinoja, on liian rajallinen näkemys kybertilan ja valtioiden välisten suhteiden kontekstissa.

Havaintojen perusteella työtä varten jatkokehitettiin aikaisemman tutkimuksen esittelemää rakenteellisen kyberasymmetrian käsitettä. Valtiokeskeisestä näkökulmasta ja aikaisemmin määritellyn kybervoiman käsitteen kautta ymmärrettynä valtio kykenee käyttämään kybervoimapotentiaaliaan muokatakseen ja kontrolloidakseen muuttuvaa, teknologiaperusteista ja ihmisen luomaa kybertilaa haluamaansa suuntaan. Näin se voi muuttaa tilan rakennetta tavalla, joka tuottaa rakenteellista kyberasymmetriaa, mikäli mahdolliset vastustajat pidättäytyvät vastatoimista. Rakenteellinen kyberasymmetria on siis kybertilan ominaisuus, joka syntyy kahden tai useamman toimijan välille, kun kybertilan rakennetta ja sääntöjä muokataan, niin että yksi toimijoista saa epäsuhtaisen ja hyväksikäytettävän puolustuksellinen ja hyökkäyksellisen edun toisiin toimijoihin nähden.

Rakenteellisen kyberasymmetrian havainnoimiseksi ja havainnollistamiseksi esiteltiin digitaalisen maaston käsite. Se mahdollistaa kybertilan kartoittamisen ja sen elementtien tarkastelun. Yksinkertaisimmillaan digitaalinen maasto viittaa ihmisen rakentamaan ja hallitsemaan informaatioinfrastruktuuriin. Monimutkaisimmillaan se viittaa niihin sosiaalisiin ja ei-sosiaalisiin rakenteisiin, jotka tekevät informaatioinfrastruktuurin merkitykselliseksi. Digitaalisen maaston käsite mahdollistaa erilaisten kansallisten tietoliikenneverkkojen ja -järjestelmien tarkastelun eri tavoin koostuvina järjestelminä tai järjestelmien järjestelminä. Digitaalisen maaston järjestelmistä koostuva ”kartta” sisältää teknisiä, funktionaalisia, normatiivisia, taloudellisia, sotilaallisia ja poliittisia elementtejä.

Digitaalinen maasto kuvattiin työn tutkimusongelman ohjaamana ja globaalin kybertilan kehyksessä suljetuiksi ja avoimiksi kansallisiksi verkoiksi (järjestelmien järjestelmäksi) ja niiden väliseksi vuorovaikutukseksi. Suljetut kansalliset verkot ovat globaalista Internetistä irrotettuja sisäisesti toimivia tietoverkkoja. Ne koostuvat valtion alueella sijaitsevasta ja sen suvereenin määräämisvallan alla olevasta Internetin infrastruktuurista ja palveluista sekä muista tietoverkoista- ja

järjestelmistä. Ne määrittelevät valtion rajat kybertilassa. Avoimet kansalliset verkot perustuvat löyhästi tapaan, jolla Internettiä hallinnoitiin teknologisesti kehittyneissä länsimaissa 2010-luvun puolivälissä. Avoin kansallinen verkko sai tutkimuksessa muotonsa suhteessa suljetun kansallisen verkon rakenteeseen.

Suljettujen ja avoimien kansallisten verkkojen kuvauksia käytettiin työssä rakenteellisen kyberasymmetrian analyysiin tarkastelemalla niitä toiminnan vapauden, yhteisen tilannekuvan, johtamisen ja resilienssin käsitteiden kautta. Toiminnan vapaus kybertoiminta- tai taistelutilassa määriteltiin kyvyksi toteuttaa hyökkäyksellisiä ja puolustuksellisia kyberoperaatioita omissa ja vastustajan verkoissa ja kiistää vastustajalta samainen kyky. Toiminnan vapaus liittyy vastustuksen puutteeseen ja kykyyn käyttää hyväksi tätä puutetta. Toiminnan vapauden analyysin kohteena oli suljettujen ja avoimien kansallisten verkkojen rajojen ja sisäisen rakenteen vaikutus toimijoiden kykyyn vaikuttaa kohteisiin tai kiistää tuo vaikutus sekä toimijoiden kyky toimia verkoissa.

Yhteinen tilannekuva määriteltiin Rauno ja Tuija Kuusiston määritelmän mukaisesti yhden tai useamman käyttäjän yhteisesti käytössä olevaksi tiedoksi. Tällaisen tilannekuvan edellyttämiä rakenteita, prosesseja, tietosisältöjä ja -malleja sekä tietovirtoja voidaan tarkastella ulkopäin. Yhteisen tilannekuvan analyysin kohteeksi määrittyivät siis tilannetietojen keräämiseen, tilannekuvan muodostamiseen, analysointiin, jakamiseen ja seurantaan liittyvät tekijät.

Johtaminen määriteltiin prosessien ja rakenteiden kautta organisaation tavoitteen saavuttamiseksi. Kybertoimintaympäristössä johtaminen on lähtökohtaisesti riippuvainen johtamisjärjestelmistä ja verkoista. Työssä keskityttiin johtamisen rakenteisiin, eli missä ja mihin liittyen päätökset tehdään, ja prosesseihin, eli miten päätökset tehdään ja välitetään, sekä teknologiaan, joka mahdollistaa rakenteet ja prosessit. Analyysi keskittyi informaation hallintaan, päätöksenteon tukeen ja toimeenpanon järjestelmiin strategisella, operatiivisella ja taktisella tasolla.

Kyberresilienssin käsite määriteltiin Ross et al. määritelmään perustuen kyvyksi ennakoida, sietää, palautua, ja sopeutua haitallisiin olosuhteisiin, stressiin, hyökkäyksiin tai muutoksiin järjestelmissä, joihin kuuluu kyberresursseja. Kyberresilienssi poikkeaa puolustuksesta, koska se perustuu riskin minimointiin ja palautumiseen, ei kohteen suojeluun haitalliselta vaikutukselta. Resilienssi eroaa turvallisuudesta, jonka perustana on uhkien puute, koska resilienssi hyväksyy riskin jatkuvan läsnäolon valmistautumisen ja mukautumisen perustana. Resilienssin

psykologinen puoli viittaa kykyyn kestää ja palautua ulkopuolisesta informaatiovaikuttamisesta. Resilienssin analyysi keskittyi kriittiseen informaatioinfrastruktuuriin ja sen toiminnan jatkuvuuden edellytyksiin avoimissa ja suljetuissa kansallisissa verkoissa sekä yhteiskunnan kykyyn kestää negatiivisia informaatiovaikutuksia.

Käsitteiden määrittelyn jälkeen työssä vastattiin toiseen alatutkimuskysymykseen eli, mikä on Venäjän kansallinen internetsegmentti ja sen suhde informaatioturvallisuuden ja -puolustuksen järjestelmän ja suljetun kansallisen verkon käsitteisiin? Kansallisen internetsegmentin ymmärtämiseksi valittiin järjestelmäteoreettinen lähestymistapa. Tältä perustalta järjestelmä eli vierasperäisesti systeemi ymmärrettiin vuorovaikutuksessa olevien objektien kokonaisuutena, jolla on rajat suhteessa toisiin järjestelmiin, sisäiset väliset suhteet ja järjestymisen periaatteet, ja jolla on funktio ja päämäärä. Järjestelmäajattelun ja -lähestymistavan valinta perustui osittain sen vahvaan asemaan niin venäläisessä, yhdysvaltalaisessa kuin kiinalaisessa sotatieteellisessä ajattelussa. Tässä työssä informaatioturvallisuuden ja -puolustuksen järjestelmä saa sisältönsä Venäjän kansallisen internetsegmentin hankkeen tavoitetilasta ja Venäjä valtion ominaispiirteistä.

Venäjän kansallisen internetsegmentin tapauksen ymmärtämiseksi työssä tarkasteltiin Venäjän valtion ominaispiirteitä, strategiskulttuurisia ideoita, kybertoimintaympäristöön liittyviä hankkeita ja informaatioturvallisuuteen liittyvää ajattelua. Aikaisemman tutkimuksen, järjestelmäajattelun ja venäläisen informaatioturvallisuusajattelun ja virallisten asiakirjojen ja uutisten pohjalta muodostettiin tutkimuskohdetta kuvaavat käsitteet. Kansallinen internetsegmentti määriteltiin suljetun kansallisen verkon venäläiseksi käytännön ilmenemismuodoksi. Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä määriteltiin yhtenäiseksi kokoelmaksi valtiojohdon välineitä ja keinoja kansallisen segmentin rajaamiseksi, rakentamiseksi ja turvaamiseksi kybertilassa. Se on informaatioturvallisuutta tuottava järjestelmien järjestelmä. Informaatioturvallisuus ymmärretään työssä venäläisittäin ja valtiokeskeisittäin suojaksi ulkoisilta ja sisäisiltä informaatiouhilta, joka turvaa valtion suvereniteetin, alueellisen eheyden, taloudellisen kehityksen, puolustuksen ja turvallisuuden. Informaatioturvallisuuden ja -puolustuksen järjestelmän käsitettä käytettiin työssä keinona kuvata tai ”kartoittaa” inhimillisen toiminnan jälki digitaalisessa maastossa. Se saa sisältönsä Venäjän kansallisen internetsegmentin tapauksesta. RuNetin käsitettä ei käytetty työssä, koska se on liian epämääräinen sosiokulttuurinen konstruktio ja ylittää Venäjän rajat.

Informaatioturvallisuuden ja -puolustuksen järjestelmä koostuu funktionaalisista alajärjestelmistä, jotka tuottavat, muokkaavat, ohjaavat ja kontrolloivat informaatiota, siihen liittyviä rakenteita, prosesseja ja käyttäjiä valtiossa. Järjestelmällä on kahdeksan alajärjestelmää. Ensimmäinen alajärjestelmä on taloudellinen ja tieteellinen järjestelmä eli valtion tieteellisteknologinen perusta. Toinen alajärjestelmä koostuu valtion salaus- ja autentikointipalveluista. Kolmas alajärjestelmä koostuu hallinnollisista ja teknisistä toimenpiteistä, joilla poistetaan ja rajoitetaan pääsy valtion turvallisuuden kannalta epätoivottuun informaatioon. Neljäs alajärjestelmä koostuu kohdennetuista tiedustelujärjestelmistä kuten SORM sekä massiivisesta internetdatan keräämisestä ja lokalisaatiosta. Viides alajärjestelmä koostuu kriittisestä informaatioinfrastruktuurista ja sen säätelystä. Kuudes alajärjestelmä koostuu aktiivisista informaatioteknologisista ja informaatiopsykologisista vastatoimista. Seitsemäs alajärjestelmä koostuu asevoimien verkoista ja järjestelmistä. Kahdeksas alajärjestelmä koostuu hallinta-, kontrolli-, valvonta- ja palautejärjestelmistä.

Suljetun kansallisen verkon, kansallisen internetsegmentin ja informaatioturvallisuuden ja -puolustuksen järjestelmän määrittelyn jälkeen määriteltiin niiden vastinkappale eli teoreettinen avoin kansallinen verkko. Se perustuu tapaan, jolla Internettiä hallinnoitiin teknologisesti kehittyneissä länsimaissa 2010-luvun puolivälissä. Aika- ja aluerajaus perustui siihen, että Venäjä muodosti kansallisen internetsegmenttinsä rakennusohjelman perusperiaatteet suhteessa siihen, miten Internettiä hallinnoitiin Lännessä kyseisellä aikajaksolla. Venäjän hanke on siis vastaus noissa hallintamuodoissa havaittuihin vahvuuksiin ja heikkouksiin. Teoreettiselle avoimelle kansalliselle verkolle rakennettiin sisältö kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmän alajärjestelmien kautta, jotta suljettuja ja avoimia verkkoja voitaisiin vertailla. Mallia rakennettaessa tiedostettiin, että läntinen tapa hallinnoida kansallista kybertilaa on voimakkaan muutoksen kohteena. Kenties juuri työn aihepiiriin liittyen.

Kun Venäjän kansallinen internetsegmentti oli käsitteellistetty kansalliseksi informaatioturvallisuuden ja -puolustuksen järjestelmäksi, vastattiin kolmanteen alatutkimuskysymykseen eli, miten Venäjän kansallinen internetsegmentti vertautuu avoimiin kansallisiin verkkoihin toiminnan vapauden, yhteisen tilannekuvan, johtamisen ja resilienssin osalta ja muodostuuko suhteesta rakenteellista kyberasymmetriaa? Vastauksia etsittiin kolmen eri analyysin avulla.

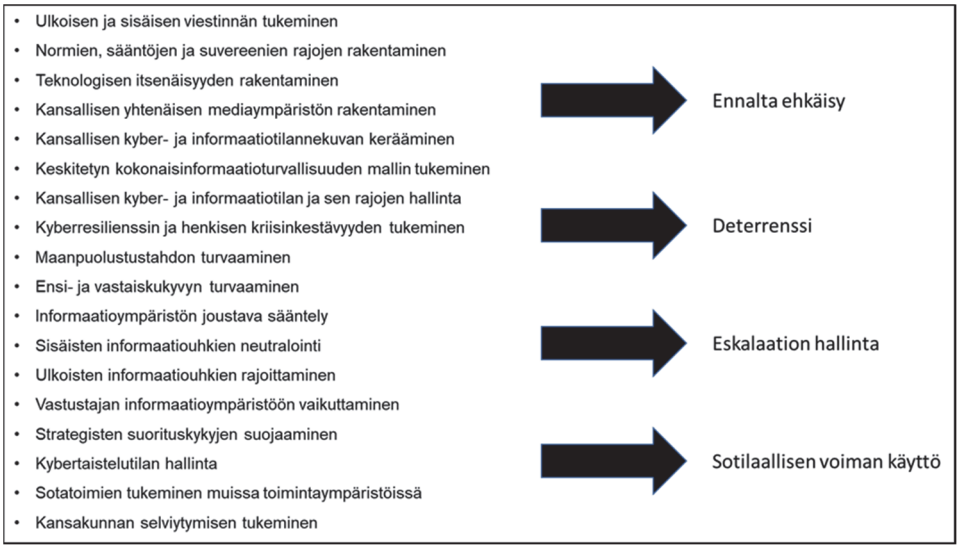
Hyökkäysvektorianalyysissä tarkasteltiin suljetun ja avoimen kansallisen verkon hyökkääjän ja puolustajan kykyjä tunkeutua toistensa verkkoihin ja suojella omiaan. Analyysi vahvisti aikaisemmat havainnot suljetun verkon valtiota hyödyttävän rakenteellisen asymmetrian olemassaolosta. Suljetun kansallisen verkon puolustaja kykenee muokkaamaan omaa verkkoaan ja korjaamaan sen haavoittuvuuksia huomattavasti tehokkaammin kuin avoimen verkon puolustaja ja täten kiistämään hyökkääjän toiminnan vapauden kybertaistelutilassa. Suljetun verkon puolustajalla on parempi toiminnanvapaus omissa verkoissaan, organisaation ja teknologian takaama yhteinen tilannekuva ja keskitetty johtamiskyky ja kriittisen informaatioinfrastruktuurin hallintaan perustuva vahvempi resilienssi kuin avoimen verkon puolustajalla. Avoimen verkon puolustaja ei kykene rajoittamaan hyökkääjän toiminnan vapautta kansallisella tasolla, sen tilannekuva on hajaantunut ja epätarkka ja johtaminen tehotonta ja hidasta johtuen verkon teknisestä ja hallinnollisesta sisäisestä hajanaisuudesta. Avoimen verkon resilienssi on riippuvainen yksityisten toimijoiden kaupallisista riskiarvioista. Toisaalta suljetun verkon puolustajan keskitetty verkonhallintajärjestelmä voi osoittautua haavoittuvuudeksi, mikäli hyökkääjä kykenee manipuloimaan sitä.

Suljetun ja avoimen kansallisen verkon sisäisiä rakenteellisia eroja vertailtiin kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmän alajärjestelmien kautta. Tämäkin analyysi vahvisti rakenteellisen kyberasymmetria olemassaolon suljetun ja avoimen kansallisen verkon välillä. Analyysi tosin osoitti, että avoimen verkon rakenteessa on merkittäviä vahvuuksiakin. Kansainvälinen yhteistyö, verkkojen ja teknologioiden heterogeenisyys ja avoimuus, toimivaltuuksien joustava sääntely, teknologisen ja psykologisen resilienssin monitahoisuus sekä valtionhallinnon ja yksityissektorin yhteistyö voivat vahventaa avoimia kansallisia verkkoja suhteessa suljettuihin. Lisäksi monet suljetun verkon vahvuuksista sisältävät ristiriitaisia elementtejä ja voivat muuttua heikkouksiksi määrätyissä tilanteissa. Tämä johtuu pitkälti kansallisen internetsegmentin taustalla vaikuttavasta autoritaarisesta poliittisesta järjestelmästä, pyrkimyksistä hallinnan keskittämiseen ja yhteiskunnan ohjailuun ja sulkeutuneesta ja innovaatioita tukahduttavasta valtiojohtoisesta autarkisesta taloudellisesta järjestelmästä. Tulosten osalta on huomioitava, että Venäjän valtion ominaisuudet vaikuttavat tarkasteluun, ja mikäli suljettu kansallinen verkko olisi pohjautunut johonkin toiseen valtioon, tulokset olisivat voineet olla erilaiset.

Kolmas analyysi tarkasteli kansallisten verkkojen suhdetta valtioiden välisten suhteiden jatkumolla. Analyysi vahvisti kahden edellisen tavoin

rakenteellisen kyberasymmetrian olemassaolon konfliktin kehityksen ja uhkien muutoksen suhteen. Se osoitti, kuinka suljettu kansallinen verkko perustuu ”Internet shutdown”-käytännön sijaan kansallisen kyber- ja informaatiotilan joustavalle säätelylle. Informaatioturvallisuuden ja -puolustuksen järjestelmä mahdollistaa tilan hallinnan ajallisesti, paikallisesti ja toiminnallisesti uhkiin suhteutetusti. Kansallisen verkon irti kytkeminen globaalista Internetistä on äärimmäinen hallinnan muoto. Suljetun kansallisen verkon etu on ennen kaikkea kyvyssä muokata taistelutilaa kriisin kehittyessä ja kyvyssä ylläpitää teknologisen omavaraisuuden avulla järjestelmien toimintaa kansainvälisten toimitusketjujen katketessa. Mitä pidemmälle valtiosuhteiden kriisi etenee sitä suuremmaksi suljetun verkon etu kasvaa verrattuna avoimiin verkkoihin. Mikäli avoimen kansallisen verkon yhteydet ulkomaailmaan kyetään katkaisemaan tai se sirpaloituu kokonaan, se menettää kaikki mahdolliset edut ja kärsii kaikki mahdolliset haitat. Suljettu kansallinen verkko on lähtökohtaisesti rakennettu juuri tällaista tapahtumaa silmällä pitäen.

Työn neljäs alatutkimuskysymys oli, miten rakenteellinen kyberasymmetria vaikuttaa voimankäyttöön tai sillä uhkaamiseen poliittisten tavoitteiden saavuttamiseksi valtioiden välisten suhteiden eri vaiheissa? Kysymykseen vastattiin tarkastelemalla rakenteellisesta kyberasymmetriasta kolmanteen kysymykseen saatuja vastauksia kybervoiman käytön muotojen ja strategisen ympäristön kehyksessä. Analyysi sidottiin suljetun ja avoimen kansallisen verkon valtion suhteen tarkasteluun niiden strategisessa ympäristössä. Toiminnot, joita informaatioturvallisuuden ja -puolustuksen järjestelmä tukee tai mahdollistaa kuhunkin voiman käytön muotoon liittyen on koottu kuvaan 14.



Kuva 14: Kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmän toiminnot ja voimankäytön muodot

Konfliktin ennaltaehkäisyn osalta todettiin, että suljettu kansallinen verkko edesauttaa sisäistä ja ulkoista tiedustelua ja täten ennakkovaroituksen saamista. Järjestelmä kiistää potentiaalisilta sisäisiltä uhilta ”hapen.” Valtion ulkopuolelle suuntautuvat aktiiviset toimenpiteet pyrkivät muokkaamaan globaalin kyber- ja informaatiotilan vihamielisestä suotuisaksi tai uhkaamiseen kykenemättömäksi. Keinot eivät voi kuitenkaan olla pelkästään vihamielisiä tai salattuja. Kansallinen internetsegmentti ennalta ehkäisee uhkia omavaraisen ja itsenäisen teknologisen kehityksen kautta. Riippuvuudet vähenevät, kriittinen tieto ja infrastruktuuri suojataan ja voimatasapainon teknologinen komponentti vahvistuu. Kansallinen internetsegmentti ei ole pelkästään eristäytymisen väline vaan voi toimia valtion vaikutusvaltaa rakentavana levittäjänä ja täten ennaltaehkäistä uhkia ja konflikteja vetovoiman kautta. Informaatio- ja kybersuvereenisuuden sekä informaatio- ja kyberaseiden kiellon normien kehitys vuorostaan helpottaa suljettujen kansallisten verkkojen rakentamista. Konfliktien ennaltaehkäisy perustuu informaatioturvallisuuden ja -puolustuksen järjestelmän näkökulmasta pitkälti globaalin kybertoimintaympäristön eli valtion strategisen ympäristön muokkaamiseen. Strategisiin vaikutuksiin päästään kontrolloimalla omaa informaatiotilaa, rakentamalla potentiaalista kybervoimaa tasapainon säilyttämiseksi ja muokkaamalla globaalia kybertoimintaympäristöä. Tämä on mahdollista, koska kybertila on helposti muokattavissa ja avoimien kansallisten verkkojen valtiot ovat huonoja torjumaan vaikutusyrityksiä.

Kyberdeterrenssin tarkastelussa todettiin, että suljettu kansallinen verkko perustuu ennen kaikkea kiistämiseen perustuvaan deterrenssiin. Järjestelmä vahvistaa valtion teknologista ja psykologista resilienssiä merkittävästi. Kyber- ja informaatioympäristön käytön kiistämisellä on vaikutusta muidenkin toimintaympäristöjen voimankäytön edellytyksiin. Deterrenssi on poikkitoimintoympäristöllistä. Toimiakseen täydellisesti kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmän tulee ulottua Internetin lisäksi avaruuteen ja koko vapaan tilan sähkömagneettiseen spektriin. Järjestelmä ehkäisee ”aktiivisen deterrenssin” vaikutuksia. Sen päämääränä on luoda rinnakkainen tila ja todellisuus, jossa oleskeleviin ulkopuolisilla taloudellisilla, henkilökohtaisilla tai häpäisemiseen perustuvilla sanktioilla on heikko vaikutus. Jos Internetin perustana olevia reititysprotokollia ei merkittävästi muuteta, kansallinen internetsegmentti ei helpota deterrenssin toimivuuden kannalta tärkeää ulkopuolelta tulevien hyökkäysten attribuutiota.

Rakenteellinen kybersymmetria vaikuttaa deterrenssiin ajan funktiona. Kustannusten ja todennäköisyyden näkökulmasta rakenteellisen kyberasymmetrian vahvistuessa ennaltaehkäisevän tai ensi-iskun toteuttaminen näyttäytyy avoimen verkon valtiolle rationaalisemmalta ratkaisulta kuin odottaminen. Koska kybertoimintaympäristössä on käytännössä mahdotonta ensi-iskulla tuhota kohteen vastaiskukykyä, avoin verkko jää haavoittuvaiseksi kostoiskulle. Avoimen kansallisen verkon valtio ei kykene suojaamaan kriittistä infrastruktuuriaan samalla tavalla kuin suljettu. Avoimen kansallisen verkon valtion osalta syntyy siis deterrenssivaje.

Suljetun kansallisen verkon rakentaminen voidaan tulkita suhteettomana panostuksena ”siviilipuolustukseen”, mikä taas voidaan tulkita ensi-iskuun tai ennalta ehkäisevään iskuun valmistautumiseksi. Tämä voi olla tarkoituskin. Rakenteellinen kyberasymmetria lisää rankaisudeterrenssin uskottavuutta, koska verkkonsa sulkevalla valtiolla on kiistaton kyky iskeä takaisin samaan aikaan, kun sen omat arvokkaat kohteet ovat suhteellisesti paremmassa suojassa kuin avoimien verkkojen valtioiden. Näin ollen kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä voi laskea kynnystä käyttää kyberaseita muiden sotilaallisten suorituskykyjen rinnalla osana rankaisudeterrenssiä. Kansallisen internetsegmentin varsinainen irrottaminen globaalista Internetistä lisää poikkitoimintaympäristöllisen rankaisudeterrenssin uskottavuutta. Toisaalta se voi myös väärin tulkittuna toimia signaalina ensi-iskuun valmistautumisesta. On myös selvää, että kyberdeterrenssin rakentamista ei voi erottaa muista toimintaympäristöistä. Suljetun kansallisen verkon rakentaminen vaikuttaa muiden toimintaympäristöjen toimintalogiikkaan.

Mikäli kansallisesta internetsegmentistä ei kyetä rakentamaan potentiaalisen vastustajan silmissä uskottavaa kiistävän deterrenssin välinettä, se on hyödytön ja mahdollisesti haitallinenkin projekti. Lisäksi, kun järjestelmä on kerran luotu, siitä on vaikea luopua altistumatta merkittäville haavoittuvuuksille siirtymäkauden aikana. Muokkaamalla kybertilaa ja -toimintaympäristöä kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmä vaikuttaa deterrenssin hintakustannus- sekä todennäköisyyslaskelmiin. Laskelmien perusteet muuttuvat jatkuvasti, koska muun muassa teknologian kehitys muuttaa suljettujen ja avoimien verkkojen suhdetta.

Eskalaatiokontrollin tarkastelussa todettiin, että eskalaation hallinnassa tulee erottaa toisistaan yhtäältä rakenteellisen kyberasymmetrian pitkän ja lyhyen aikajänteen vaikutukset ja toisaalta eskalaatiodominointi tahattomien seurausten hallinnasta. Eskalaatiokontrollin pitkä aikajänne liittyy suurvaltakilpailuun ja voimatasapainoon. Kybertoimintaympäristön kehyksessä teknologian kehityksellä on korostunut asema suurvaltojen voimasuhdearvioissa. Jokin uusi teknologia voi mahdollistaa yhdelle osapuolelle eskalaatiodominoinnin, mikä taas synnyttää turvattomuutta potentiaalisissa vastustajissa. Turvattomuuden tunne voi riistäytyä tahattomasti tai vahingossa konfliktiksi.

Kyberhyökkäysten eskalaatiokynnys muuttuu kybersuvereniteetin, ja mahdollisesti kyberaseiden kiellon, normin kehittyessä ja liittyessä entistä tiiviimmin kriittiseen informaatioinfrastruktuuriin. Se mikä Lännessä voitaisiin tulkita yksityissektorin kyberturvallisuusasiaksi, voidaan esimerkiksi Venäjällä tulkita kansallisen turvallisuuden kysymykseksi. Normeja voidaan myös käyttää hyväksi eskalaation kontrolloinnissa. Jos toinen osapuoli on voimakkaamin kiinnittynyt kybersodankäyntiin liittyviin normeihin ja käytössääntöihin kuin toinen, voi jälkimmäinen käyttää liikkumatilaa hyväkseen kiristämällä, painostamalla ja suoranaisilla sopimusrikkomuksilla. Näillä toimilla voi olla niin lyhyen kuin pitkän ajan vaikutuksia.

Rakenteellisen kyberasymmetrian lyhyen aikavälin vaikutukset liittyvät suljettujen ja avoimien verkkojen muutoksiin konfliktin kehyksessä kuukausien, viikkojen, päivien ja jopa sekuntien aikana. Kansallisen verkon sulkeminen ei ole pelkästään puolustuksellinen toimenpide, vaan sillä voidaan vaikuttaa koko globaalin Internetin toimintaan. Kansallisen segmentin sulkeminen toimii vastustajan pakottamisen välineenä vain, jos tämä ei kykene suojaamaan samalla tai riittävällä tavalla itseään. Sulkeminen pakottaa vastustajan suorittamaan seuraavan siirron joko suojaamalla itsensä, osoittamalla suljetun verkon heikkoudet eli

hyökkäämällä tai liennyttämällä konfliktia. On täysin mahdollista, että konfliktin seuraava askel otetaan jossain toisessa toimintaympäristössä. Kansallinen internetsegmentti voi kiistää hyökkääjältä yhden toimintaympäristön käytön, jolloin se joutuu päättämään, jatkaako tilanteen eskalointia jossain toisessa toimintaympäristössä. Eskalaatiodominanssin onnistumisen kannalta merkittävää onkin vastapuolten voimatasapaino muissa toimintaympäristöissä.

Kyberhyökkäystä voidaan käyttää yllätysedun saamiseksi tai voimannäyttämiseksi, rajoitetusti tuhoamiseen ja lamauttamiseen ja eskalaatiokynnyksen nostamiseksi. Jos kuitenkin suljettu kansallinen verkko toimii tehokkaasti, vastustaja joutuu eskaloimaan tavanomaisella voimalla tai ydinaseilla, mikä nostaa konfliktin intensiteettiä merkittävästi. Vastapuolen tulee käyttää suurempaa voimaa, uusia keinoja, uutta toimintaympäristöä tai moraalisesti kyseenalaisia keinoja voidakseen vaikuttaa suljetun verkon valtioon.

Eskalaatiodominointi toimii myös sisäisten uhkien tapauksessa. Ulkopuolinen hyökkääjä joutuu harkitsemaan, missä vaiheessa se luopuu tuestaan sisäisille kumouksellisille liikkeille vai haluaako jatkaa konfliktin eskalointia valtioiden väliseksi suoraksi kamppailuksi. Kumouksellisille itselleen informaatiotilan kaventuminen tarkoittaa toiminnan vapauden ja kansalaisten tuen heikentymistä. Tämä voi pakottaa heidät toimimaan muissa ympäristöissä, mikä voi olla suljetun verkon valtion tavoite alun perin. Valtion toimien legitimiteetti väkivaltaista terrorismia vastaa toimittaessa on suurempi kuin esimerkiksi tukahdutettaessa voimatoimin nettiaktivismia.

Kansallisen verkon sulkeminen ei välttämättä tarkoita konfliktin intensiteetin tai laajuuden kasvattamista. Eskalaatiodominanssiin liittyy kyky olla eskaloimatta tai sietää vastustajan eskaloivat toimet eli konfliktin osapuolien tulkinnoilla ja toimilla on vaikutusta. Kansallisen verkon sulkemisen syihin voi kuitenkin liittyä monitulkintaisuutta ja epävarmuutta. Potentiaaliselle vastustajalle voi olla epäselvää suljetaanko verkko sotaan valmistautumisen vai sisäisen turvallisuuden takia. Lisäksi suljetun verkon puolustaja voi uskoa liikaa järjestelmäänsä ja sortua liialliseen kiristykseen tai uhkailuun (*brinkmanship*).

Kansallisten internetsegmenttien osalta vahingossa tapahtuvan eskalaation riskiä nostavat informaatioturvallisuuden ja -puolustuksen järjestelmän alajärjestelmien keskinäisriippuvuudet. Kansallisen segmentin sulkeutuessa sotilasjärjestelmille saattaa aiheutua odottamatonta haittaa. Kaikkia riippuvuuksia ei ehkä ole huomioitu. Eskalaatioriski kasvaa

asevoimien joutuessa toimimaan huonojen johtamisyhteyksien ja epäselvän tilannekuvan varassa. Eri verkkojen ja toimintaympäristöjen keskinäisriippuvuudet voivat tukea joustavaa eskalaatiodominointia, mutta myös johtaa ongelmiin ja haavoittuvuuksiin etenkin siirryttäessä deterrenssistä sodankäyntiin, jossa sodan kitka lisää epävarmuutta moninkertaisesti

Rakenteellisen kyberasymmetrian sotilaallisen hyväksikäytön tarkastelussa todettiin, että kansallisen internetsegmentin sulkeminen on välttämätön ehto asymmetrialle, muttei itsessään riittävä. Asymmetrian hyödyntämiseksi pakottamisessa ja raa'an voiman käytössä tarvitaan hyökkäyskykyä. Avoin kansallinen verkko voidaankin tilapäisesti lamaannuttaa, hajottaa osiin ja mahdollisesti eristää laaja-alaisella kyberhyökkäyksellä, joka kohdistuu kriittisiin pisteisiin. Hyökkäyksen onnistumisessa kriittisenä tekijä on avoimen verkon resilienssin taso, joka on riippuvainen yksityistoimijoista. Hyökkäys- ja puolustuskyky yhdessä toimintaympäristössä ei kuitenkaan riitä. Jotta rakenteellinen kyberasymmetria tukee suljetun verkon valtion strategisten päämäärien saavuttamista suurimmalla mahdolliselle tavalla, kybersodankäyntiin on liitettävä toimintaympäristöjen rajat ylittävää pakottamisesta ja raa'an voiman käyttöä.

Rakenteellisen kyberasymmetrian vaikutus pakottamiselta ja raa'an voiman käytöltä puolustautumiseen on suurempi kuin vaikutus hyökkäykseen. Kansallinen internetsegmentti voi ehkäistä niin valtion pitkään jatkuvaa horjuttamista informaation avulla kuin laskea kyberasein toteutettavan strategisen yllätyksen todennäköisyyttä onnistua. Suljettu kansallinen verkko voidaan nähdä kulutussodankäynnin mahdollistajana, joka antaa puolustajalle aikaa selustan turvaamiseen ja voiman kasvattamiseen suhteessa vastustajaan. Rakenteellinen kyberasymmetria antaa syvyydelle merkityksen myös hyökkäyksen osana. Avointa kansallista verkkoa vastaan hyökätessä taistelutilan syvyys alkaa suljetun verkon rajalta eli kattaa koko muun kybertoimintaympäristön.

Kansallisen internetsegmentin sulkemista voidaan käyttää kyber- ja informaatiotaistelutilan muokkaamiseen. Yksittäisten järjestelmien tai verkkojen haavoittuvuudet eivät muutu, mutta kansallisen tason muutoksilla voi olla vaikutusta hyökkääjän harhauttamisen, hidastamisen ja torjumisen kannalta. Puolustustaistelussa kansallinen internetsegmentti tukee tavanomaisten ja ydinaseiden käyttöä muissa toimintaympäristöissä. Se suojaa välillisesti asevoimien johtamisjärjestelmiä ja tarjoaa varayhteyksiä, mikäli asevoimien omat järjestelmät lamaantuvat. Kansallisen internetsegmentin valvonta, vapauden rajoittaminen ja irti

kytkeminen on mahdollista tehdä alueellisesti ja joustavasti. Tämä auttaa aseellista kansannousua kukistettaessa tai paikallista aseellista konfliktia käytäessä. Huonosti toteutettuna kansallisen informaatiotilan muokkaaminen voi kuitenkin johtaa asevoimien toimintakyvyn heikkenemiseen.

Oleellinen tekijä puolustustaistelussa suljetun kansallisen verkon toiminnan kannalta on sen kokonaisuuden harjoituttaminen ja keskinäisriippuvuuksien hallinnointia jo rauhan aikana. Asevoimat on integroitava kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmään, mikäli järjestelmästä ei haluta rakentaa voimanlähteen sijaan kriittistä heikkoutta. Teknologian kehitys vaikuttaa rakenteellisen kyberasymmetrian sotilaalliseen hyväksikäyttöön etenkin puolustuksessa. Jotta suljetun verkon ja avoimen verkon suhde voi synnyttää sotilaallisesti hyväksikäytettävää rakenteellista kyberasymmetriaa, suljetun verkon tulee sisällyttää itseensä kaikki olevat ja tulevat kommunikaatioteknologiat.

Pakottamisen tai raa'an voiman käytössä rakenteellisen kyberasymmetrian etua voidaan käyttää yllätykselliseen ensi-iskuun tai vastahyökkäyksen tukemiseen. Yllätyksellinen ensi-isku voi lamauttaa osan avoimen verkon valtion kriittisestä informaatioinfrastruktuurista ja johtamisen kyvyistä ja estää taisteluvoiman ryhmittämisen, mobilisoinnin tai kansainvälisen avun vastaanottamisen. Tämän mahdollisuuden seurauksena ensi-iskusta tai jopa ennalta ehkäisevästä hyökkäyksestä tulee myös avoimen verkkojen valtion osalta houkutteleva vaihtoehto. Suljettu verkko tai sulkemisprosessi voi olla indikaatio hyökkäystä edeltävästä puolustusvalmiuden ja hyökkäyskyvyn kohottamisesta. Vastustajan suljettu kansallinen verkko voi täten toimia perusteena hyökkäyksellisen kyber- ja muun voiman käytölle. Tämä siitä huolimatta, että suljetut verkot eivät hyökkäystoimintaa tai -mahdollisuutta itsessään vahvistaisikaan.

Rakenteellisesta kyberasymmetriasta saatava merkittävin sotilaallinen hyöty on pakottamisen ja raa'an voimankäytön kestämisessä, ei voiman käytössä. Kyberhyökkäysten käyttö pakottamisen ja raa'an voiman välineenä on aina asetettava kontekstiinsa. Esimerkiksi vahvemman valtion hyökätessä heikompaa vastaan rajoitetussa sodassa kansallisten verkkojen täydellisessä sulkemisessa ei ole vahvemman osalta taloudellisesti tai sotilaallisesti järkeä. Poikkeuksena on tilanne, jossa heikommalla valtiolla on suhteeton kyberhyökkäyskyky tai se kykenee nopeasti samaan ulkopuolista apua liittokunnalta tai toiselta suurvallalta. Informaatioteknologian kehityksen johdosta rakenteellisesta kyberasymmetriasta saatava merkittävin etu esiintyy sodan alkuvaiheessa nykyaikaisen sodan luonteen kehittyessä toimintaympäristöjen rajat

ylittäväksi. Pitkitetyssä kansallisen internetsegmentin sulkemisessa on järkeä vain taisteltaessa sisäistä vihollista vastaan, jolloin ulkomaanyhteydet voidaan säilyttää rajoitetusti avoimina.

Työssä suoritetun kolmen analyysin perusteella voidaan väittää, että kybervoiman tarkastelu kybertilan ja -toimintaympäristön muokkaamisen välineenä, muiden voimankäytön muotojen ohella, tarjoaa uuden näkökulman valtioiden kyberstrategioiden kansallisten ja globaalien vaikutusten tutkimiseen. Rakenteellisen kyberasymmetrian käsite kuvaa ilmiötä, joka syntyy, kun yksittäiset valtiot rakentavat suljettuja kansallisia verkkoja niiden potentiaalisten vastustajien pitäessä verkkonsa avoimena. Se antaa uuden näkökulman valtioiden asymmetristen voimasuhteiden tarkasteluun. Olkoonkin, että tämä näkökulma voi menettää merkityksensä, jos kaikki maailman valtiot alkavat sulkea verkkojaan.

Rakenteellinen kyberasymmetria on luonnollisesti riippuvainen suljettujen ja avoimen verkkojen suhteesta. Suljettuja kansallisia verkkoja voidaan tarkastella järjestelmien järjestelminä, joilla on teknologisia, poliittisia, sotilaallisia ja taloudellisia alajärjestelmiä. Ne rakentavat kybervoimaa, rajaavat kansallisen kyber- ja informaatiotilan, turvaavat sen sisäisiltä ja ulkoisilta uhilta sekä muokkaavat globaaleja normeja ja voimatasapainoa. Venäjän kansallinen internetsegmentti on tällaisen järjestelmä tuote ja suljetun kansallisen verkon tosi maailman tapaus. Mikäli Venäjän hanke kansallisen internetsegmentin rakentamiseksi onnistuu ja muut maat eivät muuta tapaansa hallinnoida kansallisia verkkojaan, Venäjän kansallinen internetsegmentti tuottaa rakenteellista kyberasymmetriaa. Jos taas muut maat seuraavat Venäjän mallia, rakenteellinen kyberasymmetria jää syntymättä, mutta kybersodankäynnin ja suurvaltakilpailun luonne muuttuu todennäköisesti merkittävästi.

Rakenteellisen kyberasymmetrian ilmenemismuodot ja strategiset vaikutukset ovat moninaiset. Kansallisen suljetun verkon rakentamista voidaan verrata taistelukentän strategiseen muokkaamiseen ja valmisteluun. Se pakottaa vastustajat reagoimaan. Pitkällä aikavälillä kybersuvereniteetti voi välttämättömistä sotilaallisista syistä laajeta kansainväliseksi normiksi. On mahdollista, että kyberrajoja ei tulevaisuudessa enää ylitetä vapaasti. Uudet kybervoimankäyttöön ja -vakoiluun liittyvät normit voivat asettaa merkittäviä reunaehtoja voimankäytölle ja muokkaavat niiden vaikutuksia. Seurauksena ovat pyrkimykset kansalliseen teknologiseen omavaraisuuteen ja teknologiapohjaisiin liittokuntiin. Kriittisestä informaatioinfrastruktuurista tulee valtion turvallisuuden tärkeä ellei tärkein objekti, ja valtiot alkavat valvoa kybertoimintaympäristön rajoja ja kohteita. Kybertilan ja -

toimintaympäristön militarisoituminen vaikuttaa vääjäämättömältä. Tavoitteena on kansallisen kyber- ja informaatiotilan hallinta, jolla voidaan saavuttaa paikallinen ja ajallinen informaatioylivoima jo rauhan aikana.

Kiristyneessä kilpailutilanteessa ja etenkin konfliktissa ja sodan alkuvaiheessa informaatioylivoima voi tarjota sotilaallisen edun. Tällöin kyberhyökkäykset ovat deterrenssin ja pakottamisen välineinä tehokkaimmillaan. Sodan alkuvaiheessa rakenteellinen kyberasymmetria suosii verkkonsa sulkeneen valtion taistelutoimintaa ja mahdollisuutta dominoida eskalaatiota. Turvallisuuden tunne voi kuitenkin johtaa aggressiiviseen politiikkaan ja riskinottoon. Äkisti alkavan sodan uhka voi kasvaa. Kybertoimintaympäristön hyökkäyspuolustustasapaino muuttuu epävakaaksi. Molemmin puolisen haavoittuvuuden asetelma heikkenee suljettujen verkkojen tuottaman todellisen tai näennäisen turvallisuuden tunteen johdosta. Kansallisen informaatiotilan sääntelystä kehittyy osa strategista viestintää ja ennakkovaroitusanalyysiä, samalla, kun tietoliikenneverkko ja -järjestelmätiedustelu hankaloituu ja epävarmuus lisääntyy. Nämä tekijät voivat johtaa konfliktin leviämiseen muihin toimintaympäristöihin ja tahattomaan eskalaatioon.

Edellä esitetty rakenteellisen kyberasymmetrian tulkinta osoittaa, miksi suljettujen kansallisten verkkojen rakentaminen kiehtoo valtiotoimijoita, ja miksi siinä on vaaransa. Pohjois-Korea ja Iran voivat jo nyt irrottaa itsensä tilapäisesti globaalista Internetistä, mutta tuskin selviäisivät pitkittyneestä ja täydellisestä sulusta. Kiina epäilemättä pystyisi tähän, mikäli olisi pakotettu, mutta kärsisi valtavia taloudellisia tappioita. Suurvaltojen voimatasapainon muuttuessa Yhdysvaltojen intresseissä voi olla vastaavan kyvyn luominen. Väistyvän suurvallan on suojeltava itseään. Mahdollisuus toteuttaa suljettu kansallinen verkko pienissä tai keskikokoisissa demokraattisissa oikeusvaltioissa on olemassa. Mahdollisuuden hyväksikäyttöä on kuitenkin pohdittava tarkkaan, sillä kansallisen internetsegmentin juuret ovat autoritaaristen valtioiden poliittisissa perinteissä ja intresseissä. Täydellisen turvallisuuden ja tehokkuuden tavoittelu ovat demokratian ainaisia uhkia. ICT-sektorin omavaraisuuden tavoittelu voi päättyä kansantaloudellisiin ongelmiin. Lisäksi suljetun kansallisen verkon edellyttämät valvonta- ja hallintajärjestelmät voivat synnyttää uusia ja ennakoimattomia haavoittuvuuksia.

6.2 Pohdinta

Työn aikana on herännyt joitain tutkimiskohteeseen liittyviä pohdittavia ajatuksia, jotka eivät varsinaisesti mahdu tutkimuskysymyksiin

vastaamisen piiriin, mutta esitetään tässä tekijän ja lukijan iloksi, sekä toivottavasti sotatieteellisen keskustelun edistämiseksi.

Käsitteet on rakennettu joskus jotain käyttötarkoitusta varten. Ne eivät ole todellisuuden aitoja tai tosia kuvauksia. Tässä työssä on sivuttu ja käytetty useita käsitteitä, jotka ovat enemmän tai vähemmän haastavia tai jopa harhaan johtavia sotatieteellisen keskustelun kannalta. Holismi ymmärrettynä jonkin maan erityisenä strategisen kulttuurin piirteenä on näistä yksi. Tähän kiinnitettiin huomiota luvussa 2.1. Ensiksikin niin Yhdysvaltojen, Kiinan kuin Venäjänkin sotatieteiden taustalla vaikuttaa entistä voimakkaammin systeemiteoria, jonka pääkäsite holismi on. Vastustajat oppivat toisiltaan.[747] Toiseksi käytettäessä holismin käsitettä Venäjän toiminnan ymmärtämiseksi ajattelumallit, toiminta ja toimijat menevät helposti sekaisin. Tämä johtaa erillisten havaintojen yhdistämiseen kuvitelluksi kokonaisuudeksi. Kolmanneksi sotilaallisen toiminnan selittäminen holistisen ajattelun kautta on riskialtista. Esimerkiksi Dmitri Adamskyn mukaan holistisdialektisella ajattelulla on ollut vahva vaikutus Venäjän asevoimien kehitykseen ja nykyiseen toimintaan. Adamsky selittää tällä ajattelulla niin Venäjän toiminnan epäonnistumista kuin onnistumistakin – kaiken selittävässä tekijässä on ongelmansa.[748] Toiset ovat soveltaneet ajatusta venäläisestä holistisesta ajattelusta Venäjän informaatiosodankäynnin ymmärtämiseen. Taustalla on väite siitä, että Venäjä Neuvostoliiton perillisenä on korostanut informaatiosodankäynnin psykologista puolta.[749] Venäläisten mielestä taas Länsi on nimenomaan syyllistynyt psykologiseen sodankäyntiin tai paremminkin käyttänyt hyväkseen teknologista johtoasemaansa vaikuttamisen välineenä.[750] Holistisen ajattelun käyttö sotataidon selittävänä tekijänä saattaa siis kätkeä taakseen koko joukon muita tekijöitä

[747] Ks. esim. Kilcullen (2020).

[748] Adamsky selittää holismilla osana strategista kulttuuria Venäjän suhdetta RMA:han, informaatiosodankäyntiajattelua ja Syyrian operaation toteutusta. (Adamsky (2010, 54); Adamsky (2015); Adamsky, Dmitry (Dima): Russian Campaign in Syria – Change and Continuity in Strategic Culture. *Journal of Strategic Studies*, Vol. 43, No. 1 (2020), s. 104–125.

[749] Kofman, Fink & Edmonds (2020), s. 5; Giles, Keir: Russia's Public Stance on Cyberspace Issues. Teoksessa *2012 4th International Conference on Cyber Conflict*. C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) NATO CCD COE Publications, Tallinn, 2012, s. 63–75, s. 68; Giles, Keir: *The Next Phase of Russian Information Warfare*. NATO Strategic Communications Centre of Excellence, Riga, 2016, s.2. [https://www.stratcomcoe.org/download/file/fid/5134], luettu 24.2.2021; Thomas (2017), s. 84, s. 150; Robinson et al. (2018); Ajir & Vailliant (2018).

[750] Крутских (2019).

tai tuoda mukanaan kulttuurisia ennakkoasenteita. Holismikäsitteen haasteet eivät tarkoita, että se pitäisi hylätä venäläisen ajattelun tulkkina. Sen määrittelyyn, käyttöalaan ja selitysvoimaan tulee kuitenkin suhtautua kriittisesti.

Asymmetria on toinen käsite, jota on käytetty varsin vapaasti läntisessä sotatieteellisessä keskustelussa. Käsitteen monitahoisuutta on analysoitu luvussa 2.3. Lännessä asymmetria on nähty 1990-luvulla ensin oman teknologisen ylivoiman tuomana etuna, sitten kapinallisten ja terroristien sodankäynnin keinona ja nykyisellään Kiinan ja Venäjän pyrkimyksenä tehdä tyhjäksi Lännen teknologinen ylivoima. Asymmetria on läntisessä diskurssissa vastustajaan liittyvä määre, jonka luonteesta on esitetty ainakin seitsemän erilaista tulkintaa. Venäjällä asymmetriasta on tullut 2010-luvulla sotataidollinen muotikäsite, joka nähdään etenkin heikomman valtion keinoksi haastaa vahvempi valtio kustannustehokkaasti. Kiinalaisessa ajattelussa asymmetria liittyy osapuolten erilaisuuteen tai tilanteen ja ympäristön tarjoamiin mahdollisuuksiin. Niin venäläisessä kuin kiinalaisessakin ajattelussa asymmetrialla on siis positiivinen sävy. Sen sijaan läntisessä ajattelussa asymmetrialla selitetään omaa heikkoutta vastustajan edessä. Lännessä asymmetrian tulkinta jonain mitä vastustaja tekee ”meille” on rajoittanut sen analyysiä. Lisäksi Lännen, Venäjän ja Kiinan erilaiset tulkinnat voivat johtaa ”asymmetrian kierteeseen”, jossa toisen osapuolen asymmetriapyrkimykset nähdään hyökkäyksellisinä ja omia asymmetrisia toimia edellyttävänä.[751] Asymmetria käsite ja sen käyttö edellyttävät jatkotutkimusta.

Deterrenssi on kolmas käsite, joka on tätä työtä tehtäessä herättänyt ajatuksia. Luvussa 2.2 on esitetty jonkin verran kritiikkiä käsitteen nykykäyttöä kohtaan. Yksi deterrenssikäsitteen ongelmista on se, että arkikäytössä yhden deterrenssi voi muuttua toisen pakottamiseksi. Neuvostoliitto kutsui Yhdysvaltojen deterrenssiä kirjaimellisesti pelotteluksi.[752] Tällä hetkellä Lännessä kirjoitetaan aktiivisesta ja poikkitoimintaympäristöllisestä deterrenssistä ja eräät ovat esittäneet Venäjän harrastava poikkitoimintaympäristöllistä pakottamista.[753] Deterrenssistä on tulossa kiertoilmaus pakottamiselle. Koko *bargaining*

[751] Kilcullen (2020), s. 210–211.
[752] Bruusgaard, Kristin Ven: Russian Strategic Deterrence. *Survival*, Vol. 58, No. 4 (2016), s. 7–26.
[753] Adamsky (2015).

model of war -malli menettää analyyttisen merkityksenä, kun sen käsitteet politisoidaan.

Toinen, erillinen ongelma, on deterrenssikäsitteen laajentaminen kaiken politiikan perustaksi, kaikkiin toimintaympäristöihin ja kaiken kokoisille valtioille sopivaksi. Euroopan hybridiuhkien torjunnan osaamiskeskuksen esittelemä hybridiuhkien deterrenssimalli on tästä hyvä esimerkki.[754] Malli sisällyttää itseensä valtiota kohtaavan monimuotovaikuttamisen torjunnan kiistämällä vastustajan tavoitteet, uhkaamalla seurauksilla, aiheuttamalla kustannuksia, jotka muuttavat vastustajan käytöstä, ja eskaloimalla, mikäli käytös ei muutu. Tämä ei ole enää deterrenssiä. Schellingin deterrenssi on määritelmänomaisesti vaikuttamista, jotta kohde ei ryhtyisi toimintaan. Kohteen toiminnan muuttamista kutsutaan alkuperäisessä deterrenssiteoriassa pakottamiseksi. Todettakoon, että venäläinen strategisen deterrenssin käsite ei myöskään noudattele Schellingin käsitteistön määritelmiä. Molemmissa edellä mainituissa tapauksissa deterrenssin käsite toimii ehkä strategian, politiikan tai viestinnän ohjaamisen välineenä, mutta tieteellisen analyysin välineenä se menettää terävyytensä.

Vertaillessani Venäjän, Kiinan ja Yhdysvaltojen näkemyksiä, ottaen huomioon, että Venäjän näkemykset ovat itselleni tutuimmat, olen tullut siihen tulokseen, että suurvaltojen näkemykset kyber- ja informaatioteknologian sotilaallisesta käytöstä ovat lähentymässä. Tämä on pitkällisen, vuorovaikutuksellisen oppimisen tulos, jossa läntisellä ja neuvostoliittolaisella systeemiteorialla ja -tieteillä on merkittävä rooli. Silti suurvaltojen toiminnan muodoissa voidaan havaita eroja. Venäjä harjoittaa laaja-alaista informaatiovaikuttamista, Kiinan toiminnassa on korostunut teknologiavakoilu ja Yhdysvallat on käyttänyt kyberoperaatioita sotilaallisen turvallisuuden takaamiseen, vakoilun ohessa. Toiminnan syitä voi arvailla. Ehkä Venäjää on ohjannut marxismileninistisen jatkuvan kamppailun perinne, Kiinaa pyrkimys saavuttaa ”tianxia-järjestelmän”[755] ja Yhdysvaltoja systeemi- ja taloustieteet, deterrenssiteoria ja

---

[754] Keršanskas, Vytautas: *Deterrence: Proposing a more strategic approach to countering hybrid threats*. Hybrid CoE Paper 2, March 2020. [https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf], luettu 24.2.2021.

[755] Tianxia -käsitteestä ks. Puranen, Matti: Historia poliittisen maailmankatsomuksen palveluksessa: tianxia-teoria ja kiinalainen poliittinen kosmologia. *Ennen ja Nyt*, 28.11.2017. [https://www.ennenjanyt.net/2017/11/historia-poliittisen-maailmankatsomuksen-palveluksessa-tianxia-teoria-ja-kiinalainen-poliittinen-kosmologia/], luettu 7.1.2021.

operaatioanalyysi. Toiminnassa havaitut erot ovat todellisia, mutta niiden pohjalta tehtyjen kulttuuriin, identiteetteihin ja intresseihin liittyvien väittämien kanssa on oltava varovainen. Jos suurvaltoja eivät ohjaa kansainvälisen järjestelmän voimajakauma ja anarkia, ei se tarkoita, että ne olisivat ainutlaatuisia. Suurvaltojen toimintaa voi ohjata jaettu realpolitik -perustainen strateginen kulttuuri, kuten Alastair Johnston on esittänyt.[756]

Vaikka suurvallat olisivat rationaalisia tai kulttuurinsa pääpiirteiltään samanlaisia, strategisen kulttuurin tutkimus voi kertoa meille jotain suurvaltojen valitsemista keinoista ja käytöksen muodoista. Väitöskirjassani esittämän näkemyksen mukaan venäläinen sotatieteellinen ja informaatioturvallisuuteen liittyvä ajattelu antaa vahvan perustan suljetun kansallisen verkon rakentamiselle.[757] Venäläisten tutkijoiden analyysi vahvistaa informaatiotilan ja sen hallinnan merkityksen tärkeyden Venäjän voimatasapainoajattelussa. [758] Venäjän tapauksessa informaatioturvallisuuden ja -puolustuksen järjestelmä sopii strategisen deterrenssin käsitteeseen, joka sisältää voimapolitiikan kaikki muodot ja sotilaalliset ja ei-sotilaalliset keinot. Kansallisen internetsegmentin rakentaminen vaikuttaa taloudellisesti järjettömältä ja toimimattomalta idealta, mutta venäläisen sotilasstrategisen ajattelun näkökulmasta siinä on järkeä. Se on osa modernia ”asymmetrista vastetta” Yhdysvaltojen kyberpuolustuksen alueelliselle komentoportaalle (U.S. Cyber Command) ja Kiinan strategisen tuen puolustushaaralle (Strategic Support Force). ”Vasteen” toinen osa ovat asevoimien ja turvallisuuspalveluiden kyberjoukot, joiden perustamisen, suorituskykyjen ja toiminnan tunnustamista Venäjä on vältellyt.

Vaikuttaa siltä, kuten Timothy Thomaskin on todennut, että venäläiset rinnastavat kyber- ja informaatioaseet ja niiden vaikutukset strategisiin aseisiin.[759] Näin ollen on siis rationaalista, että venäläiset yhtäältä osoittavat valmiutta sopia asioista strategisen kybertoimintaympäristön vakauden turvaamiseksi, mutta toisaalta kehittävät uusia menetelmiä ja keinoja tuon ympäristön hyödyntämiseksi. Näin joko siksi, että vain pariteetti kaikkien toimintaympäristöjen strategisissa suorituskyvyissä takaa valtion turvallisuuden ja Venäjän suurvalta-aseman suhteessa Yhdysvaltoihin ja Kiinaan. Tai siitä syystä, että minimaalinen riittävän

[756] Johnston, Alastair Iain: Thinking about Strategic Culture. *International Security*, Vol. 19, No. 4 (Spring 1995), s. 32–64, s. 61–63.
[757] Ks. Luku 3.2.
[758] Chekov et al. (2019).
[759] Kukkola (2020), s. 368–369; Thomas (2020), 138–139.

rankaiseva vastaiskukyky nähdään kaikille osapuolille riittäväksi varustelun tasoksi, jolloin suorituskykyjen rajoittaminen riittävällä tasolle on kaikkien osalta järkevää.[760] Toisaalta kysymys voi olla vain väärinymmärryksestä ja sen tuottamasta pelosta, kuten eräät ovat väittäneet kylmän sodan aikana tapahtuneen.[761] Informaatioturvallisuuden ja -puolustuksen järjestelmän rationaliteetti riippuu siis pitkälti siitä, miten rationaalisuus ymmärretään, arvotetaan ja mikä on informaation merkitys voimasuhdelaskelmissa. Väitöskirjassani esitin strategiskulttuuristen ideoiden tarjoavan syyn eli tekevän järkeväksi Venäjän kansallisen internetsegmentin rakentamisen määrätyssä strategisessa ympäristössä. Tässä työssä suoritettu strategisten vaikutusten analyysi osoittaa, että rakenteellinen kyberasymmetria tukee informaatioturvallisuuden ja -puolustuksen järjestelmän rakentamisen rationaliteettia, mikäli voimankäyttö ymmärretään *bargaining model of war* -mallin mukaisesti.

Tämä työ on tarkastellut Venäjän kansallisen internetsegmentin hanketta toteutumisen näkökulmasta. Kritiikkiä toteutumisen todennäköisyyttä kohtaan on esitetty työn useassa kohdassa. Syytä skeptisismiin on. Toimiva ja turvallinen kansallinen internetsegmentti voi lopulta olla liian kallis jopa autoritaarisen, energiarikkaan valtion toteutettavaksi. Täydellinen onnistuminen edellyttäisi kansainvälisesti kilpailukykyisen ICT-ekosysteemin luomista mukaan lukien piiri- ja komponenttituotanto sekä käyttöjärjestelmät ja palvelut.

Muitakin syitä skeptisyydelle on löydettävissä. Jos kyberkeinot ovat ainoastaan tukevia tai mahdollistavia sodankäynnin välineitä, rakenteellisella kyberasymmetrialla ei välttämättä ole strategista vaikutusta. Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä voi lopulta luoda sellaisia heikkouksia, jotka neutraloivat hankkeesta saatavat hyödyt. Informaatioteknologian luonne jatkuvine päivityksineen, nollapäivähaavoittuvuuksineen, ja disruptiivisine sovellutuksineen voi muodostaa suljetuista kansallisista verkoista lähinnä kansallisen tason kriittisen haavoittuvuuden. Kansallisen

---

[760] Tästä huomiosta kiitos työn ensimmäiselle ohjaajalle Katri Pynnöniemelle. (Ks. Karaganov, Sergei A. & Suslov, Dmitry V.: *The New Understanding and Ways to Strengthen Multilateral Strategic Stability*. Higher School of Economics, Moscow, 2019; Suslov, Dmitry V.: S – Strategic Stability. *Russia in Global Affairs*, No.1 (2020 January/March), s. 122–128).

[761] CIA:n venäjäasiantuntijan sanoin: ”We didn’t realise just how f***ing scared Soviet leaders were of us.” (Barrass, Gordon: Able Archer 83: What Were the Soviets Thinking? Survival, Vol. 58, No. 6 (2016), s. 7–30, s. 24).

internetsegmentin sulkeminen voi tuottaa paljon suurempia häiriöitä kuin tarjoaa suojaa. Pelkkä resilienssi saattaa tarjota halvemman ja suuremman hyödyn kuin monimutkainen ja kallis turvallisuusjärjestelmä. Sotilaalliset ja taloudelliset liittolaissuhteet todennäköisesti kärsivät kansallisten internetyhteyksien katkaisemisesta. Koko hanke on riippuvainen valtiovallan resursseista ja toimintakyvystä. On todennäköistä, että kansallisen internetsegmentin hallinnan edellyttämä byrokratia lisää kuluja ja korruptiota ja vähentää innovaatioita. Kotimaisten ratkaisujen tietoturva ei ole välttämättä parempi kuin avoimien ratkaisujen tai kansainvälisten yritysten tarjoamat. Poliittinen sensuuri ja kontrolli saattavat kasvattaa kansalaisvastarintaa, heikentää vallan legitimiteettiä ja lisätä sisäpiirihyökkäysten mahdollisuutta. Datan massamainen kerääminen, kansallisen kriittisen infrastruktuurin kartoittaminen ja keskitetyt kyberturvallisuusjärjestelmät muodostuvat hyökkäyskohteiksi. Kyberdiplomatialla on vaikea peittää koko hankkeen autoritaarisuutta. Kansallista informaatiotilaa ei voi täydellisesti valvoa ja kontrolloida. Ja silti, kaikesta edellä mainitusta huolimatta, Venäjä rakentaa kansallista internetsegmenttiä, ja luovat sekä sitoutuneet ihmiset pyrkivät ratkaisemaan yllä esitetyt ongelmat.

Saatavilla olevien lähteiden kautta tarkasteltuna voidaan väittää, että Venäjän Internetin ulkomaan yhteyksien täydellinen katkaiseminen ulkopuolelta tai sen saattaminen sisäisesti toimintakyvyttömäksi on erittäin vaikeaa. Kansallisen internetsegmentin rakentaminen vaikuttaisi näin ollen olevan pikemminkin strategiskulttuuristen ideoiden, uhkakuvien tai poliittisten ja institutionaalisten intressien kuin teknisiin seikkoihin perustuvan rationaalisen päättelyn tulos. *Oman näkemykseni on, että informaatioturvallisuuden ja -puolustuksen järjestelmä ei tule toteutumaan sellaisena kuin eräät venäläiset teoreetikot sen haluaisivat nähdä.*[762] Eli yhtenäisenä valtiollisena informaatiotilana, joka on luonteeltaan järjestelmien järjestelmä ja jota käytetään informaatiokamppailussa toisia vastaavia järjestelmiä vastaan, ja joka on lisäksi keskitetty kansallinen informaatio-, johtamis-, kontrolli- ja hallintajärjestelmä.[763]

En myöskään usko, että ”suvereeni Internet” tulee toteutumaan annetuissa laeissa ja määräyksissä käsketyllä tavalla. Teknologiset haasteet, korruptio ja kansalaisyhteiskunnan ja talouselämän vastustus on liian vahvaa. Toimijakenttä on sirpaloitunut ja liian monella viranomaisella on

[762] Ks. Luku 3.1.
[763] Kukkola (2020a), s. 360.

nykyisellään mahdollisuus hyötyä järjestelmän rakentamisesta. Tämä ei tarkoita, että Venäjän hanke epäonnistuisi. *Poliittinen tahto hankkeen toteuttamiseksi on olemassa*. Keväällä ja kesällä 2021 kansallisen informaatiotilan hallinta ja turvaaminen nousivat uudelleen poliittisen johdon agendalle.[764] Lopullinen toteutus ja muiden suurvaltojen siitä tekemät tulkinnat määrittelevät hankkeen vaikutuksen ja vaikuttavat merkittävästi kybertoimintaympäristön tulevaisuuteen.

Tämä työ antaa uuden näkökulman väitteeseen siitä, että kybervoiman pakottava käyttö kärsii synnynnäisistä heikkouksista. Väite perustuu läntiseen hyökkäykselliseen näkökulmaan. Pakottava käyttö voi saada voimansa myös puolustuksesta. Kuten työssä on todettu, kansallisen segmentin sulkeminen oikea aikaisesti yhdistettynä määrättyyn voimatasapainoon muissa toimintaympäristöissä voi tarjota mahdollisuuden strategisten vaikutusten saavuttamiseen ensi-iskulla tai ennaltaehkäisevällä iskulla. Tämä ei tarkoita, että kybervoima olisi samaistettavissa tavanomaiseen aseelliseen voimaan tai ydinaseisiin. Kyberhyökkäyksillä on kuitenkin sitä suurempi pakottava voima, mitä enemmän yhteiskunnat perustuvat informaatioteknologiaan ja mitä vähemmän ne kykenevät itseään suojelemaan. Esimerkiksi kansainvälisen järjestelmän tasolla ongelmaksi voi muodostua kyberaseiden ”biologinen” räätälöinti. Mikäli globaali Internet hajoaa kansallisiin osiin, syntyy kansallisia ekosysteemejä vastaan kehitettyjä aseita, joiden käyttökynnys madaltuu keskinäisriippuvuuden vähetessä. Keinojen ja vastakeinojen dialektiikka voi toimintaympäristöjen luonteen takia johtaa yllättäviin, ja katastrofaalisiin, seurauksiin.

Kybertoimintaympäristö muuttuu jatkuvasti toimijoiden vuorovaikutuksen seurauksena. ”Aktiivisen deterrenssin”, vakoilun, vaikutusoperaatioiden ja kyberrikollisuuden tuloksena jatkuvasti käynnissä oleva ”kyberkähinä” muokkaa taistelutilaa. Kamppailu voi eskaloitua niin, että kansainvälinen suvereenisuuteen perustuva normisto koetaan lopulta tarpeelliseksi. Chris Demchak onkin väittänyt, että kybertoimintaympäristön luonne muokkaa valtioista luonnostaan ”kaupunkivaltioita”. Ne varautuvat piiritykseen ja yrittävät torjua kyberuhat rajojensa ulkopuolella.[765] Mutta mitä tapahtuu, jos kaikki maailman valtion sulkevat verkkonsa? Onko edessä niin

---

[764] РИА Новости: Матвиенко призвала более четко регулировать интернет-пространство. *РИА Новости*, 19.4.2021 [https://ria.ru/20210419/matvienko-1728942339.html], luettu 29.7.2021.
[765] Demchak (2011), s. 50.

kutsutun liberaalin maailmanjärjestyksen perikato vai onko niin, ettei tätä järjestystä ikinä ollutkaan?[766] Tietävätkö ne, jotka vaativat Euroopan Unionille digitaalista suvereniteettia, mitä haluavat ja ovat tekemässä?

Työn johdannossa todettiin, että teoreettisten avoimien verkkojen malli perustuu vanhentuneeseen näkemykseen läntisten valtioiden tavasta hallinnoida kansallisia tietoliikenneverkkojaan. Näin siksi että, 2010-luvun puolivälistä lähtien, osittain Yhdysvaltojen NSA:n vakoilutoiminnan paljastumisen, osittain Venäjän informaatiovaikuttamisen, osittain Kiinan teollisuusvakoilun ja osittain kyberterrorin uhan takia, monet läntiset valtiot alkoivat suhtautua epäilevästi vapaaseen ja avoimeen Internetiin. Lisäksi suurvaltojen kyberdeterrenssinäkemykset lähentyvät toisiaan. Kiina ja Iran rakentavat jossain määrin samanlaista kyberdeterrenssiä kuin Venäjä.[767] Yhdysvaltojen Cyber Solarium Commission esitys USA:n kyberdeterrenssiksi sisältää samoja elementtejä kuin Venäjän ”aktiivinen kyberdeterrenssi.”[768] Jopa Euroopassa isolationistisen kybersuvereniteetin idea on vahvistumassa.[769] Aika on armoton kybertoimintaympäristön tutkimuksen tuloksille.

---

[766] Ikenberry, John: The End of Liberal International Order? *Foreign Affairs*, Vol. 94, No. 1 (2018), s. 7–23; Duncombe, Constance & Dunne, Tim: After Liberal World Order. *International Affairs*, Vol. 94, No. 1 (2018), s. 25–42; Porter, Patrick: *A World Imagined: Nostalgia and Liberal Order*. Policy Analysis 843, Cato Institute, June 5, 2018. [https://www.cato.org/publications/policy-analysis/world-imagined-nostalgia-liberal-order], luettu 12.1.2021.

[767] Jiang, Tianjiao: From Offense Dominance to Deterrence: China’s Evolving Strategic Thinking on Cyberwar. *Chinese Journal of International Review*, Vol. 1, No. 2 (2019); Kolton (2017); Kausch, Kristina: *Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East*. German Marshall Fund of the United States, Policy Brief, November 24, 2017. [https://www.gmfus.org/publications/cheap-havoc-how-cyber-geopolitics-will-destabilize-middle-east], luettu 10.1.2021; Musiani et al. (2016).

[768] Cyberspace Solarium Commission: *End Report,* March 2020. [https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view], luettu 1.7.2020.

[769] Burwell, Frances G. & Propp, Kenneth: *The European Union and the Search for Digital Sovereignty: Building “Fortress Europe” or Preparing for a New World?* Atlantic Council, 2020. [https://www.atlanticcouncil.org/wp-content/uploads/2020/06/The-European-Union-and-the-Search-for-Digital-Sovereignty-Building-Fortress-Europe-or-Preparing-for-a-New-World.pdf], luettu 21.10.2020; European Commission: *Joint Communication To The European Parliament And The Council: The EU's Cybersecurity Strategy for the Digital Decade*. Brussels, 16.12.2020 JOIN(2020) 18 final. [https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade], luettu 18.12.2020.

Avoimien kansallisten verkkojen luonne on muuttumassa ja tulee muuttumaan radikaalisti 2030-luvulle tultaessa. Suurvallat kehittävät omia, suojattuja tuotantoketjujaan. Koska pienien valtioiden tai alueellisten suurvaltojen resurssit eivät riitä omiin ratkaisuihin, syntyy ohjelmisto- ja laitetuotantoblokkeja – suurvaltojen ja niiden strategisten liittolaisten ympärille kehittyviä informaatioteknologisia saarekkeita. Informaatioinfrastruktuurista tulee Lännessäkin kriittinen kansallisen turvallisuuden kohde, joka asetetaan turvallisuusviranomaisten, asevoimien tai liittokuntien valvontaan. Yhteiskunnallisia toimijoita mobilisoidaan mukaan siviilipuolustuksen hengessä. Syntyy kybersiviili- ja kansalaispuolustusjoukkoja. Datan liikkuvuutta säännellä liittokuntien ja valtioiden välillä. Valtiot ja liittokunnat perustava avaruus- ja kyberjoukkoja ja informaatiovaikuttamiseen keskittyviä organisaatioita. Kansalliset tai ”luotettavien kumppaneiden” kanssa toteutetut salausratkaisut ohittavat kansainvälisten yritysten tarjoamat ratkaisut.

Edellän mainitut kehityskulut eivät voi olla vaikuttamatta rakenteellisen kyberasymmetrian muotoutumiseen. On hyvin todennäköistä, että kyber- ja informaatiotila tulee jakautumaan tavalla, joka heijastaa sen kanssa vuorovaikutuksessa olevia valtasuhteita. Avaruus, kyber- ja informaatiotila voivat sirpaloitua ennustamattomilla tavoilla. Lopputuloksena rakenteellinen kyberasymmetria sellaisessa muodossa kuin sitä tässä työssä on tarkasteltu saattaa jäädä syntymättä tai hiipuu hiljaa pois. Sen sijasta syntyy valtaan ja maantieteeseen perustuva uusi maailmanjärjestys – niin kuin aina ennenkin on tapahtunut.

6.3 Kritiikki ja jatko

Tämä työ on jatkoa väitöskirjalleni, jossa rakenteellisen kyberasymmetrian analyysille ei ollut tilaa. Näin ollen työssä on päällekkäisyyksiä aikaisemman tutkimuksen kanssa. Tutkimusraportissa esiintyvä aikaisemman tutkimuksen toisto on ollut välttämätöntä ymmärrettävän raportin kirjoittamiseksi. Työstä on tarkoituksella jätetty pois venäläisen strategisen kulttuurin laajempi esittely ja siihen on viitattu vain, kun strategiskulttuuristen ideoiden käsittelyllä on nähty olevan lisäarvoa. Samoin neoklassisen realismin teoria on esitelty vain niiltä osin kuin se auttaa ymmärtämään työn ongelmanasettelua ja lähestymistapaa.

Tätä työtä on ohjannut pyrkimys tuottaa uutta ja relevanttia sanottavaa kybertoimintaympäristöstä. Tässä on toivottavasti onnistuttu. Työn aikana kävi kuitenkin selväksi, että läntisten voimankäyttöön liittyvien käsitteiden soveltamisessa kybertoimintaympäristön tarkasteluun on rajoitteensa. Olen muokannut joitain käsitteitä työhön paremmin soveltuviksi, mutta laajempi

käsitteiden uudelleen tarkastelu ja terminologinen käsiteanalyysi olisivat otollinen jatkotutkimusaihe. Esimerkiksi syvempi Venäjän, Yhdysvaltojen ja Kiinan käyttämien pääkäsitteiden ja strategisen tason käyttäytymisen vertailu olisi varmasti hyödyllistä kybertoimintaympäristön kehityksen ymmärtämiseksi. Ainakin se auttaisi ymmärtämään sitä, miten suurvaltojen, ja miksei pienien maidenkin, deterrenssikäsitykset ovat keskenään vuorovaikutuksessa.

Työn laadullinen analyysi on abduktiivisuutensa johdosta varsin subjektiivista. Eri lähtökohdista ponnistava analyysi voi hyvinkin tuottaa toisenlaisia päätelmiä kansallisista internetsegmenteistä ja rakenteellisesta kyberasymmetriasta. Työssä esitetty kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmä perustuu pehmeän systeemiteorian mukaisesti tutkijan tulkintaan havaitusta ilmiöstä.[770] Mielestäni malli auttaa hahmottamaan valtiollista kybertilaa ja -toimintaympäristöä. Se ei välttämättä ole nykyisessä muodossaan täydellinen ja on jo nyt kehittynyt ensimmäisestä versiostaan. Se on kuvaus sosiaalisesta todellisuudesta, joten se ei koskaan tule olemaan valmis. Informaatioturvallisuuden ja -puolustuksen järjestelmän ja tätä kautta tässä työssä esitetyn suljetun kansallisen verkon mallin suurin rajoitus on sen yhteys 2010-luvun Venäjän valtioon ja yhteiskuntaan. Tästä syystä luvussa 4 toteutetun analyysin tuloksia ei voi kaikilta osin yleistää vaan rakenteellista kyberasymmetriaa tarkasteltaessa informaatioturvallisuuden ja -puolustuksen järjestelmän alajärjestelmien sisältö tulee muodostaa tapauskohtaisesti. Lisäksi Venäjän tapaustakin tulee aika ajoin tarkastella uudelleen.

Kansallinen informaatioturvallisuuden ja -puolustuksen järjestelmän nimi viestii itsessään ongelmasta, joka liittyy informaatiosodankäyntiin yleisesti. Teknologinen ja psykologinen puoli ovat tiiviissä vuorovaikutuksessa keskenään. Olen työssä pyrkinyt keskittymään teknologiseen puoleen. Venäjän kansallista internetsegmenttiä ei voi kuitenkaan ymmärtää ilman sen informaatiopsykologista puolta. Tämä johtuu osiltaan siitä, että kansallinen internetsegmentti on primaarisesti tarkoitettu informaation hallintaan ja vasta sekundaarisesti valtion kriittisten toimintojen turvaamiseen. Lisäksi informaatioturvallisuuden ja -puolustuksen järjestelmän vastatoimien alajärjestelmä perustuu osiltaan informaatiovaikuttamiseen, jolloin Venäjän internetsegmentti on myös ulospäin suuntautuvan vaikuttamisen väline. Luvussa 5 esitetty analyysi

[770] Checkland (1993), s. 100–101.

osoittaa useaan otteeseen, että vastapuolen tulkinta verkkonsa sulkevan valtion toiminnasta on ratkaiseva voimankäytön tekijä. Näin ollen teknologinen ja psykologinen kietoutuvat toisiinsa tavalla, jossa niiden erottaminen ei ole yksinkertaista eikä kenties tarkoituksenmukaistakaan. Yhden tai toisen lähestymistavan valinnan sijaan monitieteellinen suljettujen kansallisten verkkojen tutkimus voisi tarjota hedelmällisemmän näkökulman.

Teoreettisen avoimen verkon käyttäminen suljetun verkon vastaparina oli vaikea ratkaisu. Niiden vertailu on saattanut tuoda keinotekoista vastakkainasettelua ilmiöön, joka on paljon monisyisempi kuin kahden objektin suhde. Avoimen verkon rakentaminen ”eurooppalaisen teknologisesti kehittyneen 2010-luvun valtion” pohjalle olisi voinut hyötyä laajemmasta taustatutkimusta. Lisäksi, kuten edellä on todettu, avoimet kansalliset verkot ovat muutoksen kohteena. Toisaalta mallin kiinnittämisestä yhteen määrättyyn valtioon olisi seurannut omat ongelmansa. Tällaisenaan ”teoreettinen avoin kansallinen verkko” korostaa suljetun kansallisen verkon erityispiirteitä. Kolme eri näkökulmista tehtyä analyysiä todistaa rakenteellisen kyberasymmetrian olemassaolosta, vaikka avoimen verkon yksittäisiä piirteitä muutettaisiinkin.

Käytössä ollut tila rajoitti voimankäytön muotojen analyysia ja sitä voisi hyvinkin syventää tulevaisuudessa. Kuvassa 14 esitetyt kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmän toiminnot ja voimankäytön muodot olisivat hyvä lähtökohta jatkotutkimukselle. Rauhan ja sodan rajat ylittävä toimintopohjainen tarkastelu voisi selkeyttää kybervoiman käytön erityispiirteitä.

Olen koko työn läpi käyttänyt käsitettä Länsi kuvaamaan määrättyä poliittista, sotilaallista, kulttuurista ja taloudellista valtioiden kokonaisuutta. Lännelle on annettu työn alussa määritelmä, joka perustuu englanninkieliseen käsitteeseen *the West*. Sen käyttö sitoo työn määrättyyn tapaa jäsentää kansainvälinen järjestelmä ja niin on tarkoituskin. Venäjän voimassa olevan ulkopoliittisen konseptin mukaan ”Läntisten valtioiden halu säilyttää asemansa, esimerkiksi painostamalla näkemyksiään globaaleihin prosesseihin ja harjoittamalla vaihtoehtoisten valtakeskusten saarrostuspolitiikkaa, johtaa lisääntyneeseen epävakauteen kansainvälisissä suhteissa, lisääntyneeseen turbulenssiin globaalilla ja

alueellisella tasolla."[771] Venäjää tutkittaessa Lännestä ei pääse eroon. Vaihtoehtona olisi ollut käyttää viime aikoina suosioon tullutta samanmieliset maat (*like-minded countries*) käsitettä. Käsite on kuitenkin liian epämääräinen ja poliittisesti tarkoituksenmukainen ollakseen tutkimusmielessä hyödyllinen.

Tätä työtä tulisi jatkaa vertailemalla Venäjän, Kiinan ja esimerkiksi Iranin kansallisia verkkoja informaatioturvallisuuden ja -puolustuksen järjestelmän mallin kehittämiseksi. Samoin tulisi kehittää avoimen kansallisen verkon käsitettä vertailemalla useita valtioita ja päivittämällä käsite 2020-luvulle. Kun käsitteitä on jalostettu, olisi hyvä palata rakenteellisen asymmetrian käsitteeseen ja tarkastella sitä uudelleen. Etenkin Lännessä tapahtuvat muutokset digitaalisen tai kybersuvereniteetin osalta tulevat varmasti vaikuttamaan tässä työssä esitettyihin havaintoihin. Olisi myös hyödyllistä tarkastella Suomen "kansallisen verkon" ja Venäjän kansallisen informaatioturvallisuuden ja -puolustuksen järjestelmän suhdetta. Sotatieteiden kehittymisen kannalta olisi ennen kaikkea perustelua tutkia kybertoimintaympäristöä pienen, liittoutumattoman valtion näkökulmasta geopoliittiset ja historialliset seikat huomioiden.

Tämä työ tarjoaa pohjan yhteiskuntatieteelliselle tutkimukselle. Kybertoimintaympäristön muodostuessa yhä keskeisemmäksi osaksi ihmisten ja valtioiden kanssakäymistä sen rakenteellisilla muutoksilla on hyvin todennäköisesti vaikutuksia ihmissuhteisiin, yhteisöjen muodostumiseen, valtioiden kanssakäymiseen ja suurvaltojen nousuun ja tuhoon. Kybertoimintaympäristön muutos heijastaa syviä sosiaalisia, taloudellisilla ja moraalisia muutoksia. Suurvaltojen voimatasapainon muutos voi vaikuttaa siihen, kuka pääsee määrittelemään tavan, jolla kansallisia verkkoja tulevaisuudessa hallitaan. Valtioiden tapa järjestää kansallinen kybertoimintaympäristönsä voi kertoa yllättäviä asioita kansainvälispoliittisista voimasuhteista. Näiden aiheiden tutkiminen voisi palvella ihmiskuntaa pitkällä tähtäimellä enemmän kuin keskittyminen yksittäisten kyberoperaatioiden tekijöiden ja vaikutusten tarkasteluun.[772]

---

[771] Указ-640: Указ Президента РФ от 30.11.2016 N 640 "*Об утверждении Концепции внешней политики Российской Федерации*". [http://www.consultant.ru/document/cons_doc_LAW_207990/], luettu 8.1.2021.

[772] Näistä ideoista kiitos työn toiselle ohjaajalle komentaja (evp.) Topi Tuukkaselle.

LÄHTEET

1 SUOMENKIELINEN JA ENGLANNINKIELINEN MATERIAALI

1.1 Tutkimukset ja opinnäytteet

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

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

Hartikainen, Riku: *Johtamista vai ohjausta? Puolustusvoimien moninaiset johtamis- ja ohjausmallit*. Yleisesikuntaupseerikurssi 57:n opinnäytetyö, Maanpuolustuskorkeakoulu, 2015.

Hollanti, Juha: *Alivoimaisen taktiikka. Suomalaisen taktisen ajattelun tarkastelu*. Akateeminen väitöskirja, Maanpuolustuskorkeakoulu, julkaisusarja 1: tutkimuksia No. 38. Maanpuolustuskorkeakoulu, Helsinki, 2019.

Hölttä, Niko: *Yhtymän esikunnan tilanneymmärryksen kehittäminen operaatioiden johtamisessa*. Yleisesikuntaupseerikurssi 54:n opinnäytetyö, Maanpuolustuskorkeakoulu, 2009.

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

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

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

Kuusisto, Rauno: *Aspects on availability: a teleological adventure of information in the lifeworld*. Doctoral Dissertation. Series / National Defence College, Department of Tactics and Operations Art. 1, Julkaisusarja / Maanpuolustuskorkeakoulu, taktiikan laitos. 1, Taktiikan tutkimuksia, 2004.

Lalu, Petteri: *Syvää vai pelkästään tiheää: neuvostoliittolaisen ja venäläisen sotataidollisen ajattelun lähtökohdat, kehittyminen, soveltaminen käytäntöön ja nykytilanne. Näkökulmana 1920- ja 1930-luvun syvän taistelun ja operaation opit*.

Akateeminen väitöskirja, Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 1 Nro 3/2014, Helsinki, 2014.

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

Siukonen, Veikko: *APT-Operaation inhimilliset tekijät: Operaation tarkastelu päätöksenteon näkökulmasta*. Jyväskylän yliopisto, Tietojenkäsittelytiede, pro gradu – tutkielma, 2019.

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

1.2 Kirjallisuus

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

Acton, James M.: *Is It a Nuke? Pre-Launch Ambiguity and Inadvertent Escalation*. Carnegie Endowment for International Peace, Washington DC, 2020.

Adamsky, Dima: *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the USA, and Israel*. Stanford University Press, Stanford, 2010.

Alberts, David S. & Papp, Daniel S. (eds.): *Information Age Anthology – Volume III: The Information Age Military – Volume III*. CCRP Publication Series, 2001.

Alberts, David S. & Papp, Daniel S. (eds.): *The Information Age Anthology – Volume I: An Anthology on Its Impact and Consequences – Volume I*. CCRP Publication Series, 1997.

Alberts, David S. & Papp, Daniel S. (eds.): *The Information Age Anthology – Volume II: National Security Implications of the Information Age – Volume II*. CCRP Publication Series, 2000.

Alberts, David S., Garstka, John J., Hayes, Richard E. & Signori, David A.: *Understanding Information Age Warfare*. CCRP. Washington, DC., 2001.

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

Andress, Jason & Winterfeld, Steve: *Cyber Warfare. Techniques, Tactics and Tools for Security Practitioners. (*2nd ed*.)* Syngress, Waltham. 2014, s. 169–171.

Angström, Jan & Widen J. J.: *Contemporary Military Theory: The Dynamics of War*. Routledge, New York, 2015.

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

Arquilla, John and Ronfeldt, David: *In Athena's Camp.* RAND, Santa Monica, 1997.

Ashby, Ross W.: *An Introduction to Cybernetics*. London, Chapman & Hall, 1956. [http://pespmc1.vub.ac.be/ASHBBOOK.html], luettu 23.9.2019.

Barkin, Samuel J.: *Realist constructivism: Rethinking International Relations Theory*. Cambridge University Press, Cambridge, 2010, s. 66–71.

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

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

Berger, Heidi: *Venäjän informaatio-psykologinen sodankäyntitapa terrorismin torjunnassa ja viiden päivän sodassa*. Maanpuolustuskorkeakoulu, Johtamisen ja sotilaspedagokiikan laitos, Julkaisusarja 1. Nro 5/2010, Edita Prima Oy, Helsinki, 2010.

Biddle, Stephen: *Military Power - Explaining Victory and Defeat in Modern Battle.* Princeton University Press, Princeton, 2004.

Biddle, Tami Davis: *Air Power And Warfare: A Century Of Theory And History*. Strategic Studies Institute, US Army War College, 2019.

Black, Jeremy: *The Cold War. A Military History*. Bloomsbury, London, 2015, s. 156–160.

Blair, Bruce G.: *Strategic Command and Control: Redefining the Nuclear Threat*. The Brookings Institution, Washington, D.C., 1985.

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

Blombergs, Fred (toim.): *Suomen turvallisuuspoliittisen ratkaisun lähtökohtia*. Maanpuolustuskorkeakoulu, Julkaisusarja 1, No. 4. Maanpuolustuskorkeakoulu, Helsinki, 2016.

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

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

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

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

Buzan, Barry: *People, States and Fear. An agenda for international security studies in the post-cold war era*. ECPR Press, Colchester, 2007.

Byman, Daniel & Waxman, Matthew: *The Dynamics of Coercion: American Foreign Policy and the Limits of Military Might*. Cambridge University Press, Cambridge, 2002.

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

Candolin, Catharina: *Securing Military Decision Making in a Netwok-Centric Enviroment*. Helsingin Teknillinen korkeakoulu, väitöskirja, Picaset Oy, Helsinki, 2005.

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

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

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

Cimbala, Stephen J.: *The New Nuclear Disorder: Challenges to Deterrence and Strategy*. Routledge, London & New York, 2015.

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

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

Clegg, Stewart R., Hardy, Cynthia & Nord, Walter R. (eds.): *Handbook of Organization Studies*. SAGE, London, 1996.

Coram, Robert: *Boyd. The Fighter Pilot Who Changed the Art of War*. Back Bay Books, New York, 2002.

Corbett, Julian: *Some Principles of Maritime Strategy*. Longmans, Green and Company, London, 1911. [http://onlinebooks.library.upenn.edu/webbin/gutbook/lookup?num=15076], luettu 27.4.2020.

Davis, Paul K. & Stan, Peter J.: *Concepts and Models of Escalation*. RAND, Santa Monica CA, 1984.

Davis, Paul K., Kulick, Jonathan & Egner, Michael: *Implications of Modern Decision Science for Military Decision-Support Systems*. RAND, Santa Monica, 2005.

de Rosnay, Joël: *The Macroscope A new world scientific system*. Harper & Row, Publishers, New York, 1975. [http://pespmc1.vub.ac.be/macroscope/], luettu 23.9.2019.

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

Demchak, Chris: *Wars of disruption and resilience: cybered conflict, power, and national security*. University of Georgia Press, Athens, 2011.

DeNardis, Laura: *The Global War for Internet Governance*. Yale University Press, New Haven, 2014.

Deptula, D.*: Effects Based Operations, Change in the Nature of Warfare*. Aerospace Education Foundation, Arlington, VA, 1996.

Deutsch, Karl W.: *The Nerves of Government: Models of Political Communication and Control*. Collier-Macmillan, New York & London, 1963.

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

Donnelly, Christopher: *Red Banner. The Soviet Military System in Peace and War*. Jane's Information Group, Coulsdon, 1988.

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

Easton, David: *A Framework for Political Analysis*. University of Chicago Press, Chicago & London, 1979.

Easton, David: *A Systems Analysis of Political Life*. John Wiley & Sons, New York, 1965.

Engström, Jeffrey: *Systems Confrontation and System Destruction Warfare. How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*. RAND, Santa Monica, 2018.

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

Fall, Kevin R. & Stevens, Richard W.: *TCP/IP Illustrated, Volume 1: The Protocols (2nd ed.)* Addison-Wesley, Upper Saddle River NJ, 2012.

Forrester, Jay W.: *Industrial Dynamics*. Productivity Press, Cambridge, MA, 1961.

Fravel, Taylor M.: *Active Defense: China's Military Strategy since 1949*. Oxford University Press, Oxford, 2019.

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

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

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

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

Galeotti, Mark: *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right*. Mayak Intelligence, Prague, 2016.

Galeotti, Mark: *The Vory: Russia's Super Mafia*. Yale University Press, New Haven and London, 2018.

Garstka, John: *Network Centric Operations Conceptual Framework Version 1.0*. Evidence Based Research, Inc, Vienna, VA, 2003.

Garthoff, Raymond L.: *Deterrence and the Revolution in Soviet Military Doctrine*. The Brookings Institution, Washington, D.C., 1990.

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

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

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

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

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

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

Giddens, Anthony: *The Nation State and Violence: Volume Two of A Contemporary Critique of Historical Materialism*. Polity, Cambridge, 1985.

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

Glantz, David M.: *The Role of Soviet Intelligence in Soviet Military Strategy in WWII*. Presidio Press, Novato, CA, 1990.

Glantz, David M.: *The Soviet Conduct of Tactical Maneuver*. Frank Cass, New York, 1991.

Godwin III, J. B., Kulpim, A., Rauscher, K. F. & Yaschenko, V. (eds.): *Critical Terminology Foundations 2. Russia-U.S. Bilateral on Cybersecurity*. Policy Report 2/2014. EastWest Institute and the Information Security Institute of Moscow State University, 2014.

Golts, Aleksandr: *Military Reform and Militarism in Russia*. The Jamestown Foundation, Washington, D.C., 2019.

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

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

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

Green, James A (ed.): *Cyber Warfare: A multidisciplinary analysis*. Routledge, New York, 2015.

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

Gritsenko, Daria, Wijermars, Mariëlle & Kopotev, Mikhail (Eds.): *The Palgrave Handbook of Digital Russia Studies*. Palgrave Macmillan, London, 2021.

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

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

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

Hammond, Debora: *The Science of Synthesis. Exploring the Social Implications of General Systems Theory*. The University Press of Colorado, Boulder, 2003.

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

Handel, M.: *Masters of War: Classical Strategic Thought*. Frank Cass, London, 1996.

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

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

Heginbotham, E. (ed.): *The U.S. - China Military Scorecard: Forces, Geography, and the Evolution of Balance of Power 1996-2017*. RAND, Santa Monica, 2017.

Herspring, Dale R.: *The Kremlin and the High Command: Presidential Impact on the Russian Military from Gorbachev to Putin*. University Press of Kansas, Lawrence, KS, 2006.

Hitchens, Theresa & Goren, Nilsu: *International Cybersecurity Information Sharing Agreements*. University of Maryland Center for International & Security Studies, Maryland, 2017.

Hoffman, David E.: *The Dead Hand. The Untold Story of the Cold War Arms Race and Its Dangerous Legacy*. Anchor Books, New York, 2009.

Hollis, Martin and Smith, Steve: *Explaining and Understanding International Relations*. Clarendon Press, Oxford, 1990.

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

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

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

Huhtinen, Aki Mauri & Rantapelkonen, Jari: *Imagewars: Beyond the mask of information warfare*. Gummerus, Saarijärvi, 2002.

Hutchins, Susan G.: *Principles for Intellihent Decision Aiding*. Technical Report 1718. Naval Command, Control and Ocean Surveillance Center, San Diego SA, 1996.

Huttunen, Mika: *Monimutkainen taktiikka*. Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 1, Nro 1/2010.

Inkster, Nigel: *China's Cyber Power*. IISS. Routledge, New York, 2016.

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

Jamshihi, Mo (ed.): *Systems of Systems Engineering: Principles and Applications*. CRC Press, New York, 2008.

Jantunen, Saara: *Strategic Communication: practise, communication and dissonance*. Maanpuolustuskorkeakoulu, Johtamisen ja sotilaspedagogiikan laitos, Julkaisusarja 1, No. 11, Juvenes, Helsinki, 2013.

Johnson, G., Scholes, K. & Whittington, R.: *Exploring Corporate Strategy. Text and Cases*. FT Prentice Hall Financial Times, Harlow, 2005.

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

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

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

Joseph, Jonathan & Wight, Colin (eds.): *Scientific Realism and International Relations*. Palgrave, Basingstoke, 2010.

Kahn, Herman: *On Thermonuclear War*. Princeton University Press, Princeton, 1960.

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

Kallio, Jyrki: *Xi Jinping Thought And China's Future Foreign Policy Multipolarity With Chinese Characteristics*. FIIA Briefing Paper 243, August 2018. FIIA, Helsinki, 2018.

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

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

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

Kaplan, Fred: *The Wizards of Armageddon*. Stanford University Press, Stanford, California, 1983.

Karaganov, Sergei A. & Suslov, Dmitry V.: *The New Understanding and Ways to Strengthen Multilateral Strategic Stability*. Higher School of Economics, Moscow, 2019.

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

Kelly, Alan & Christopher, Paul: *Decoding Crimea. Pinpointing The Influence Strategies Of Modern Information Warfare*. NATO Strategic Communications Centre of Excellence, Riga, 2020.

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

Kline, Ronald R.: *The Cybernetics Moment, Or Why We Call Our Age the Information Age*. Johns Hopkins University Press, Baltimore, 2015.

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

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

Kosola, Jyri & Solante, Tero: *Digitaalinen taistelukenttä: Informaatioajan sotakoneen tekniikka*. Maanpuolustuskorkeakoulu, Sotatekniikan laitos, Julkaisusarja 4, No. 35, Helsinki, 2013.

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

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

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

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

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

Kuusisto, Rauno & Kuusisto, Tuija (toim.): *Yhteinen tilanneymmärrys - Strategis-operatiivisten päätösten tukipalvelujen perusteet*. Edita Prima Oy, Helsinki, 2005.

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

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

Kuusisto, Tuija: Tiedonhallinta päätöksenteossa kybertoimintaympäristössä. Teoksessa *Kybertaistelu 2020*. Kuusisto, Tuija (toim.) Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2, No. 1/2014, Juvenes Print, Helsinki, 2014.

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

Laine, Markus, Bamberg, Jarkko & Jokinen, Pekka (toim.): *Tapaustutkimuksen taito*. Gaudeamus Helsinki University Press, Helsinki, 2007.

Lamont, Christopher: *Research Methods in International Relations*. SAGE Publications Ltd., London, 2015.

Lasconjarias, Guillaume & Marrone, Alessandro: *How to Respond to Anti-Access/Area Denial (A2/AD)? Towards a NATO Counter-A2/AD Strategy*. Research Division - NATO Defense College, Rome, 2016.

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

Lehto, Martti: *Kybermaailman ilmiöitä ja määrittelyjä*. Jyväskylän yliopisto, Informaatioteknologian tiedekunta, 2019. [https://www.jyu.fi/it/fi/hae-opiskelemaan/hakukohteet/kyberturvallisuuden-seka-turvallisuus-ja-strateginen-analyysi-maisteriohjelmien-yhteisvalinta/kybermaailma_v10-0.pdf], luettu 16.3.2020.

Leonhard, Robert R.: *The Art of Maneuver: Maneuver Warfare Theory and Airland Battle*. Ballantine Books, New York, 1991.

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

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

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

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

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

Lillianfeld, Robert: *The Rise of Systems Theory: an Ideological Analysis*. John Wiley and Sons, New York, 1978.

Lindsay, Jon R., Cheung, Tai Ming & Reveron, Derek S.: *China and Cybersecurity. Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press, Oxford, 2015.

Lobell, S. E., Ripsman, N. M. & Taliaferro, J. W.: *Neoclassical Realism, the State, and Foreign Policy*. Cambridge University Press, Cambridge, 2009.

Luhmann, N.: *Essays on self-reference*. Columbia University Press, New York, 1990.

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

Luhmann, Niklas: *The Differentation of Society*. Columbia University Press, New York, 1981.

Lukes, Steven: Power: *A Radical View* (2nd ed.) Palgrave Macmillan, Basingstoke, 2005.

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

Mahan, Alfred T.: *The Influence of Sea Power upon History 1660-1783*. Dover edition. Little, Brown and Company, Boston, 1890.

Maness, R. C. & Valeriano, B. *Conflict in Cyber Space: Theoretical, strategic and legal perspectives*. Routledge, New York, 2016.

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

Mann, Edward C., Endersby, Gary & Searle, Thomas R.: *Thinking Effects: Effects-Based Methodology for Joint Operations*. Air University Press, Alabama, 2002.

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

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

Mets, David R.: *The Air Campaign. John Warden and the Classical Airpower Theorists*. Air University Press, Maxwell Air Force Base, Alabama, 1999.

Michel, Leo & Pesu, Matti: *Strategic Deterrence Redux. Nuclear Weapons and European Security*. FIIA Report, September 2019/60, Helsinki, 2019.

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

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

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

Morgan, Patrick M. (Ed.): *Deterrence Now*. Cambridge University Press, Cambridge, UK, 2003.

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

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

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

Mätäsniemi, Teemu (ed.): *Operational decision making in the process industry Multidisciplinary approach*. VTT Tiedotteita - Research Notes 2442. VTT, Helsinki, 2008.

Nuopponen, Anita: *Käsiteanalyysia käsiteanalyysista – kohti systemaattista käsiteanalyysia. Käännösteoria, ammattikielet ja monikielisyys*. VAKKI:n julkaisut, N:o 36. Vaasa, 2009.

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

Nye, Joseph: *Cyber Power*. Harvard Kennedy School, Cambridge, 2010.

Näsi, Antti: *Ajatuksia käsiteanalyysista ja sen käytöstä yrityksen taloustieteessä*. Yrityksen taloustieteen ja yksityisoikeuden laitoksen julkaisuja. Sarja A2: Tutkielmia ja raportteja 11. Tampere, 1980.

Ó Tuathail, Gearoid & Dalby, Simon (eds.): *Rethinking Geopolitics*. Routledge, London, 1998.

O´Rourke, Lindsay: *Covert Regime Change: America´s Secret Cold War*. Cornell University Press, Ithaca, 2018.

O'Brien, James A. & Marakas, George, M.: *Management Information Systems* (10th ed.) McGraw-Hill, Irwin, New York, 2011.

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

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

Owens, Bill: *Lifting the Fog of War*. The Johns Hopkins University Press, Baltimore, 2001.

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

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

Parsons, Talcott: *The Social System*. Routledge, London, 1991.

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

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

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

Piiroinen, Mika (toim.): *Verkkotaistelu 2020: Taustatutkimus Maavoimien Taistelun kuvat 2020 tutkimukseen*. Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2, No. 2/2003, Edita Prima Oy, Helsinki, 2003.

Pomerantsev, Peter & Weiss, Michael: *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Institute of Modern Russia, Inc., New York, 2014.

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

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

Posen, B.: *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars*. Cornell University Press, Ithica, 1984.

Puolustusministeriö: *Voiman Venäjä*. Puolustusministeriö, Helsinki, 2019.

Pynnöniemi, Katri (toim.): *Russia´s Critical Infrastructures - Vulnerabilities and Possibilities*. FIIA Report 35, Helsinki, 2012.

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

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

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

Rantapelkonen, Jari & Koistinen, Lotta: *Pohdintoja sotatieteellisistä käsitteistä*. Maanpuolustuskorkeakoulu, Sotataidon laitos, Julkaisusarja 2: Tutkimusselosteita nro 1, Helsinki, 2016.

Rantapelkonen, Jari & Salminen Mirva (Eds.): *The Fog of Cyber Defence*. Maanpuolustuskorkeakoulu, Johtamisen ja pedagogiikan laitos, Julkaisusarja 2, No: 10, Juvenes Print Oy, Tampere, 2013.

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

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

Rekkedal, Nils Marius: *Nykyaikainen sotataito. Sotilaallinen voima muutoksessa*. Maanpuolustuskorkeakoulu, Helsinki, 2013.

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

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

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

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

Robinson, Linda, Helmus, Todd C., Cohen, Raphael S., Nader, Alizera, Radin, Andrew, Magnuson, Madeline & Migacheva, Katya: *Modern Political Warfare: Current Practices and Possible Responses*. RAND, Santa Monica, Calif., 2018.

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

Saarelainen, Jorma: *Näkemyksiä Venäjän Informaatiosodankäynnistä*. Maanpuolustuskorkeakoulu Taktiikan laitos, Julkaisusarja 1 Taktiikan tutkimuksia, N:o1/1999. Hakapaino, Helsinki, 1999.

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

Salminen, Ari: *Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin*. Vaasan yliopiston julkaisusarja opetusjulkaisuja 62, julkisjohtaminen 4, Vaasa, 2011.

Sanastokeskus TSK: *Kokonaisturvallisuuden sanasto TSK 50*. Sanastokeskus TSK, Helsinki, 2017.

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

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

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

Schmitt, Michael N. (ed.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, Cambridge, 2017.

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

Shlapak, D. A. and Johnson, M. W.: *Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of Baltics*. RAND, Santa Monica, 2016.

Sirén, Torsti (toim.): *Strateginen kommunikaatio ja informaatio-operaatiot 2030*. Maanpuolustuskorkeakoulu, Johtamisen ja sotilaspedagogiikan laitos, Juvenes Print Oy, Helsinki, 2011.

Sivonen, Pekka: *Suomalaisia näkökulmia strategian tutkimukseen*, Maanpuolustuskorkeakoulu, Julkaisusarja 1: Strategian tutkimuksia No. 33. Juvenes Print, Tampere, 2013.

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

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

Snyder, Glenn: *Deterrence and Defence*. Princeton University Press, Princeton, 1961.

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

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

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

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

Terrill, Andrew W.: *Escalation And Intrawar Deterrence During Limited Wars In The Middle East*. Strategic Studies Institute, U.S. Army War College, Carlisle, PA, 2009.

Thomas, Timothy: *Cyber Silhouettes. Shadows Over Information Operations*. Foreign Military Studies Office, Fort Leavenworth, KS, 2005.

Thomas, Timothy: *Kremlin Kontrol: Russia's Political-Military Reality*. Fort Leavenworth, KS: FMSO, 2017.

Thomas, Timothy: *The Chinese Way of War: How Has it Changed*? MITRE, McLean, VA, 2020.

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

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

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

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

Tuomi, Jouni & Sarajärvi, Anneli: *Laadullinen tutkimus ja sisällönanalyysi*. Tammi, Helsinki, 2018.

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

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

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

Vankka, Jouko (ed.): *Critical Infrastructure Protection against Cyber Threats*. National Defence University, Report Series 1, No 36. Juvenes Print, Tampere, 2014.

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

Von Bertalanffy, Ludvig: *General System Theory*. George Braziller, New York, 1968.

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

Wardak, Ghulam Dastagir, Turbiville, Graham Hall Jr. & Garthoff, Raymond L.: *The Voroshilov Lectures. Materials from the Soviet General Staff Academy. Volume I: Issues of Soviet Military Strategy*. National Defense University Press, Washington, DC, 1989.

Ware, Willis, H. & Holland, Wade B.: *Soviet Cybernetics Technology: I. Soviet Cybernetics 1959-1962*. RAND Corporation, Santa Monica, 1963.

Westerlund, Fredrik & Oxenstierna, Susanne (eds.): *Russian Military Capability in a Ten-Year Perspective – 2019*. FOI, Stockholm, 2019.

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

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

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

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

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

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

Yin, Robert K.: *Case Study Research: Design and Methods*, 4th ed. CA Sage Publications, Newbury Park, California, 2009.

Zhang, Nan, Krishna, Kant & Sajal K.: *Handbook on Securing Cyber-Physical Critical Infrastructure*. Elsevier, Amsterdam, 2012.

Zouave, Erik, Bruce, Marc, Colde, Kajsa, Jaitner, Margarita, Rodhe, Ioana & Gustafsson, Tommy: *Artificially intelligent cyberattacks*. FOI, Stockholm, 2020.

1.3 Artikkelit ja Internet-lähteet

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

Acton, James M.: Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War. *International Security*, Vol. 43, No. 1 (Summer 2018), s. 56–99.

Adamsky, Dmitry (Dima): Cross-Domain Coercion: The Current Russian Art of Strategy. *Proliferation Papers*, No. 54, November 2015. [https://www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf], 8.1.2021.

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

Adamsky, Dmitry (Dima): Russian Campaign in Syria – Change and Continuity in Strategic Culture. *Journal of Strategic Studies*, Vol. 43, No. 1 (2020), s. 104–125.

Adamsky, Dmitry: Deterrence à la Ruse: Its Uniqueness, Sources and Implications. Teoksessa *NL ARMS Netherlands Annual Review of Military Studies 2020: Deterrence in the 21st Century—Insights from Theory and Practice*. Osinga, Frans & Sweijs, Tim (Eds.) Springer, Berlin, 2020, s. 161–175

Adler, Emmanuel: Seizing the Middle Ground: Constructivism in World Politics. *European Journal of International Relations*, Vol. 3, No. 3 (1997), s. 319–363.

Ajir, Media & Vailliant, Bethany: Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*, Vol. 12, No. 3 (Fall 2018), s. 70–89.

Albert, Mathias & Buzan, Barry: Securitization, Sectors and Functional Differentiation. *Security Dialogue*, Vol. 42, No. 4/5, Special issue on The Politics of Securitization (August-October 2011), s. 413–425.

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

Alker, Hayward R.: The Powers and Pathologies of Networks: Insights from the Political Cybernetics of Karl W. Deutsch and Norbert Wiener. *European Journal of International Relations*, Vol.17, No. 2 (2011), s. 351–378.

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

Anderson, Ruth A., Crabtree, Benjamin F., Steele, David J. & McDaniel, Reuben R, Jr.: Case Study Research: The View From Complexity Science. *Qualitative Health Research*, Vol. 15, No. 5 (May 2005), s. 669–685.

Anteroinen, Jukka: The Systems Concepts in Military Operations - Discussion of critique. *Systems Conference (SysCon), 2013 IEEE International*, s. 102–108.

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

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

Art, Robert J.: Force and Fungibility Reconsidered. *Security Studies*, Vol. 8, No. 4 (1999), s. 183–189.

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

Asmolov G. & Kolozaridi P.: Run Runet Runaway: The Transformation of the Russian Internet as a Cultural-Historical Object. Teoksessa *The Palgrave Handbook of Digital Russia Studies*. Gritsenko D., Wijermars M., Kopotev M. (eds.) Palgrave Macmillan, Cham, 2021, s. 227–296.

Assaad, Mohamad Ali, Talj, Reine & Charara, Ali: A view on Systems of Systems (SoS). *20th World Congress of the International Federation of Automatic Control (IFAC WC 2017) - special session, Jul 2016, Toulouse, France*.

Aström, Karl J. & Kumar, P.R. Control: A Perspective. *Automatica*, Volume 50, Issue 1, (January 2014), s. 3-43.

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

Austin, Greg & Sharikov, Pavel: "Pre-emption is victory": Aggravated Nuclear Instability of the Information ge. *The Nonproliferation Review*, Vol. 23, No. 5-6 (2016), s. 691–704.

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

Austin, Greg: The Strategic Implications of China's Weak Cyber Defences. *Survival*, Vol. 62, No. 5 (2020), s. 119–138.

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

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

Bacon, Edwin: Security Council and Decision-making. Teoksessa *Routledge Handbook of Russian Security*. Kanet, Roger E. (ed.) Routledge, London and New York, 2019, s. 119–130.

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

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

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

Barnett, Michael: Culture, Strategy and Foreign Policy Change: Israel's Road to Oslo. *European Journal of International Relations*, Vol. 5, No. 1 (1999), s. 5–36.

Barrass, Gordon: *Able Archer 83*: What Were the Soviets Thinking? *Survival*, Vol. 58, No. 6 (2016), s. 7–30.

Barrinha, André & Renard, Thomas: Cyber-diplomacy: The Making of an International Society in the Digital Age. *Global Affairs*, Vol.3, No.4-5 (2017), s. 353–364.

Baumann, Mario: 'Propaganda Fights' and 'Disinformation Campaigns': The Discourse on Information Warfare in Russia-West relations. *Contemporary Politics*, Vol. 26, No. 3 (2020), s. 288–307.

Bebber, Robert: Cyber Power and Cyber Effectiveness: An Analytic Framework. *Comparative Strategy*, Vol. 36, No. 5 (2017), s. 426–436.

Becker, Uwe & Vasileva, Alexandra: Russia's Political Economy Re-conceptualized: A Changing Hybrid of Liberalism, Statism and Patrimonialism. *Journal of Eurasian Studies*, Vol. 8, No. 1 (January 2017), s. 83–96.

Benbow, Tim: Talking 'Bout Our Generation? Assessing the Concept of "Fourth-Generation Warfare". *Comparative Strategy*, Vol. 27, No. 3 (2008), s. 148–163.

Bendett, Samuel & Kania, Elsa B.: *A new Sino-Russia high-tech partnership. Authoritarian innovation in an era of great-power rivalry*. ASPI Policy brief Report No. 22/2019. [https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership], luettu 7.5.2021.

Bennett, Andrew & Elman, Colin: Case Study Methods in the International Relations Subfield. *Comparative Political Science*, Vol. 40, No. 2 (February 2007), s. 170–195.
Betz, David & Stevens, Tim: Cyberspace and the State: Toward a Strategy for Cyberpower. *Adelphi Series* Vol. 51, No. 424 (2011).

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

Biddle, Stephen: Military Power: A Reply. *Journal of Strategic Studies*, Vol. 28, No. 3 (2005), s. 453–469.

Biddle, Tami Davis: Coercion Theory: A Basic Introduction for Practitioners. *The Strategist*, Vol. 3, No. 2 (Spring 2020). [https://tnsr.org/2020/02/coercion-theory-a-basic-introduction-for-practitioners/], luettu 1.5.2020.

Björck, Fredrik, Henkel, Martin, Stirna, Janis & Jelena Zdravkovic: Cyber Resilience - Fundamentals for a Definition. *Advances in Intelligent Systems and Computing*, Vol. 353 (2015), s. 311–316.

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

Blair, Bruce G.: Why Our Nuclear Weapons Can Be Hacked. *The New York Times*, March 14, 2017 [https://www.nytimes.com/2017/03/14/opinion/why-our-nuclear-weapons-can-be-hacked.html?hpw&rref=opinion&action=click&pgtype=Homepage&module=well-region&region=bottom-well&WT.nav=bottom-well&_r=0], luettu 12.1.2021.

Blank, Stephen: Cyber War and Information War à la Russe. Teoksessa *Understanding Cyber Conflict: Fourteen Analogies*. Perkovich, George & Levite, Ariel E. (Eds.) Georgetown University Press, Washington, D.C., 2017, s. 81–98.

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

Blasko, Dennis J.: China's Evolving Approach to Strategic Deterrence. Teoksessa *China's Evolving Military Strategy*. McReynolds, Joe (ed.) The Jamestown Foundation, Washington, D.C., 2016, s. 279–297.

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

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

Borghard, Erica D. & Lonergan, Shawn W.: The Logic of Coercion in Cyberspace. *Security Studies*, Vol. 26, No. 3 (2017), s. 452–481.

Boulding, Kenneth: General Systems Theory. The Skeleton of Science. *Management Science*, Vol. 3, No. 2 (1956), s. 197–208. [http://pespmc1.vub.ac.be/books/Boulding.pdf], luettu 15.10.2019.

Bousquet, Antoine & Curtis, Simon: Beyond Models and Metaphors: Complexity Theory, Systems Thinking and International Relations. *Cambridge Review of International Affairs*, Vol. 24, No. 1 (March 2011), s. 43–62.

Bousquet, Antoine: Cyberneticizing the American War Machine: Science and Computers in the Cold War. *Cold War History*, Vol. 8, No. 1 (February 2008), s. 77–102.

Bowen, Glenn: Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, Vol. 9, No. 2 (2009), s. 27–40.

Brangetto, Pascal, Veenendaal, Matthijs A.: Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. Teoksessa *8th International Conference on Cyber Conflict: Cyber Power*. Pissanidis N., Rõigas H. ja Veenendaal, M. (Eds.) CCD COE, Tallinn, 2016, s. 113–126.

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

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

Bratton, Patrick: A Coherent Theory of Coercion? The Writings of Robert Pape. *Comparative Strategy*, Vol. 22, No. 4 (2003), s. 355–372.

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

Bruusgaard, Kristin Ven: Russian Strategic Deterrence. *Survival*, Vol. 58, No. 4 (2016), s. 7–26.

Bruusgard, Kristin Ven: *Russian Concept of Deterrence*. Russia Seminar 2021, 26.2.2021, National Defence University, Helsinki [https://www.youtube.com/watch?v=PURKPOeskBk&t=33s], luettu 21.2.2021.

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

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

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

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

Carpenter, Paul & Andrews, William F.: Effect-based Operations: Combat Proven. *Joint Forces Quarterly*, Vol. 52, No. 1, s. 78–81.

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

Cebrowski, A. K. & Garstka, J. J.: Network-Centric Warfare: Its Origin and Future. *Proceedings Magazine*, Vol. 124, No. 1 (1998), s. 28–35.

Central Intelligence Agency: *General Staff Academy Lectures: Principles of the Automation and Mechanization of Troop Control*. Document VII-211. Prepared 6 September 1968, published October 1969. CIA/DO Intelligence Information Special Report, 11 November 1976 [https://www.cia.gov/library/readingroom/docs/1976-11-11.pdf], luettu 6.7.2020.

Centre for International Governance Innovation & IPSOS: *2014 CIGI-Ipsos Global Survey on Internet Security and Trust*. [https://www.cigionline.org/sites/default/files/documents/internet-survey-2014-factum.pdf], luettu 12.1.2021.

Centre for Strategic and International Studies: *Significant Cyber Incidents, September 2018.* [https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity], luettu 7.5.2020.

Chandel, Sonali, Jingji, Zang, Yunnan, Yu, Jingyao, Sun & Zhipeng, Zhang: The Golden Shield Project of China: A Decade Later An in-depth study of the Great Firewall. *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 17-19 October, Guilin, China.*

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

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

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

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

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

Chen, Jim: Effectively Exercising Deterrence in the Cyber Domain. Teoksessa *Proceedings of the 13th International Conference on Cyber Warfare and Security 8-9 March 2018*. Chen, Jim Q. & Hurley, John S. (ed.) National Defense University, Washington D.C., 2018, s. 120–125.

Chernobrov, Dmitry & Briant, Emma L.: Competing Propagandas: How the United States and Russia Represent Mutual Propaganda Activities. *Politics*, 2020, s. 1–17. [https://doi-org.mp-envoy.csc.fi/10.1177/0263395720966171], luettu 29.1.2021.

Christine, D. Irene & Thinyane, M.: Comparative Analysis of Cyber Resilience Strategy in Asia-Pacific Countries. Teoksessa *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress* (DASC/PiCom/CBDCom/CyberSciTech), Calgary, AB, Canada, 2020, s. 71–78.

Christou, George, Croft, Stuart, Ceccorulli, Michela & Lucarelli, Sonia: European Union Security Governance: Putting the 'Security' Back In. *European Security*, Vol. 19, No. 3 (2010), s. 341–359.

Chuanying, Lu: Forging Stability in Cyberspace. *Survival*, Vol. 62, No. 2 (2020), s. 125–136.

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

Cimbala, Stephen J.: Nuclear Crisis Management and Deterrence: America, Russia, and the Shadow of Cyber War. *The Journal of Slavic Military Studies*, Vol. 30, No. 4 (2017), 487–505.

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

Cioffi-Revilla, Claudio: Origins and Age of Deterrence: Comparative Research on Old World and New World Systems. *Cross-Cultural Research*, Vol. 33 No. 3 (August 1999), s. 239–264.

Claessen, Eva: Reshaping the Internet – The Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU. *Journal of Cyber Policy*, Vol.5, No.1 (2020), s. 140–157.

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

Correll, John T.: The Assault on EBO. The cardinal sin of Effects-Based Operations was that it threatened the traditional way of war. *Air Force Magazine*, Vol. 96, No. 1 (January 2013), s. 50–53.

Council on Foreign Relations: *Cyber Operations Tracker, September 2018.* [https://www.cfr.org/interactive/cyber-operations], luettu 7.5.2020.

Crane, Keith W., Joneckis, Lance G., Acheson-Field, Hannah, Boyd, Iain D., Corbin, Benjamin A., Han, Xueying & Rozansky, Robert N.: *Assessment of the Future Economic Impact of Quantum Information Science*. Institute for Defense Analyses, 2017 [https://www.ida.org/-/media/feature/publications/a/as/assessment-of-the-future-economic-impact-of-quantum-information-science/p-8567.ashx], luettu 12.1.2021.

Cuihong, Cai: Cybersecurity in the Chinese Context. Changing Concepts, Vital interests, and Prospects for Cooperation. *China Quarterly of International Strategic Studies*, Vol. 1, No. 3 (2015), s. 471–496.

Czerwinski, Thomas J.: Command and Control at the Crossroads. *Parameters*, Autumn 1996, s. 121–132.

Dahmann, Judith S., Rebovich, George Jr. & Lane, Jo Ann: Systems Engineering for Capabilities. *CROSSTALK The Journal of Defense Software Engineering*, November 2008, s. 4–9.

Daucé, Françoise & Musiani, Francesca (eds.): Infrastructure-Embedded Control, Circumvention and Sovereignty in the Russian Internet. *First Monday*, 26(5), special issue, 3 May 2021 [https://firstmonday.org/ojs/index.php/fm/issue/view/693], luettu 28.7.2021.

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

Demchak, Chris & Dombrowski, Peter: Cyber Westphalia: Asserting State Prerogatives in Cyberspace. *Georgetown Journal of International Affairs*, Volume International Engagement on Cyber III, 2013, s. 29–38.

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

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

Digiser, Peter: Fourth Face of Power. *The Journal of Politics*, Vol. 54, No. 4 (1992), s. 977–1007.

Domínguez-Jiménez, Marta & Poitiers, Niclas: *FDI another day: Russian reliance on European investment*. Policy Contribution 03/2020, Bruegel.

Dossi, Simone: On the Asymmetric Advantages of Cyberwarfare. Western Literature and the Chinese Journal Guofang Keji. *Journal of Strategic Studies*, Vol. 43, No. 2 (2020), s. 281–308.

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

Duncombe, Constance & Dunne, Tim: After Liberal World Order. *International Affairs*, Vol. 94, No. 1 (2018), s. 25–42.

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

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

Dyndal, Gjert Lage: Airborne Intelligence, Surveillance and Reconnaissance. Teoksessa *Routledge Handbook of Air Power*. Olsen, John Andreas (ed.) Routledge, Abingdon, Oxon, 2018, s. 107–117.
Echevarria II, Antulio J.: Strategic Culture Is Not a Silver Bullet. *Naval War College Review*, Vol. 70, No. 4, (Autumn 2017), s. 121–124.

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

Echevarria, Antulio J.: *Operational Concepts and Military Strength, 2017 Index of U.S. Military Strength*. [https://www.heritage.org/military-strength-topical-essays/2017-essays/operational-concepts-and-military-strength], luettu 14.4.2020.

Ejimabo, O. N.: An Approach to Understanding Leadership Decision Making in Organization. *European Scientific Journal*, Vol. 11, No. 1 (2015), s. 2–24.

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

Elder-Vass, Dave: Luhmann and Emergentism Competing Paradigms for Social Systems Theory? *Philosophy of the Social Sciences*, Vol. 37, No. 4 (December 2007), s. 408–432.

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

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

Endsley, Mica R.: Situation Awareness Misconceptions and Misunderstandings. *Journal of Cognitive Engineering and Decision Making*, Vol. 9, No. 1, (March) 2015, s. 4–32.

Endsley, Mica: Situation Awareness: Operationally Necessary and Scientifically Grounded. *Cognition, Technology & Work*, Vol. 17, No. 2 (May 2015), s. 163–167.

Endsley, Mica: Theoretical Underpinnings of Situation Awareness: A Critical Review. Teoksessa *Situation Awareness Analysis and Measurement*. Endsley, M. R. and Garland, D. J. (Eds.). Lawrence Erlbaum Associates, Mahwah, NJ, 2000, s. 3–32.

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

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

Evans, M.: Elegant Irrelevance Revisited: A Critique of Fourth-Generation Warfare. *Contemporary Security Policy*, Vol. 26, No. 2 (2005), s. 242–249.

Fischerkell, Michael P. & Harknett, Richard J.: Deterrence Is Not a Credible Strategy for Cyberspace (and What Is). *Orbis,* Vol. 61, No. 3 (2017), s. 381–393.

Fischerkeller, Michael P. & Harknett, Richard J.: Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation. *The Cyber Defense Review*, Special Edition: International Conference on Cyber Conflict (CYCON U.S.), November 14-15, 2018: Cyber Conflict During Competition (2019), s. 267–287.

Fischerkeller, Michael: Incorporating Offensive Cyber Operations into Conventional Deterrence Strategies. *Survival*, Vol.59, No.1 (February-March 2017), s. 103–134.

Fischer-Lescano, Andreas: Critical Systems Theory. *Philosophy and Social Criticism*, Vol. 38, No. 1 (2012), s. 3–23.

Fitzgerald, Mary: Russian Views on IW, EW, and Command and Control: Implications for the 21st Century. *Command & Control Research & Technology Symposium, 1999. U.S. Naval War College, Rhode Island. June 29 - July 1, 1999.* [http://www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/089fitzg.pdf], luettu 5.8.2018.

Fitzpatrick, Mark: Artificial Intelligence and Nuclear Command and Control. *Survival*, Vol.61, No.3 (2019), s. 81–92.

Fitzsimmons, Michael: The False Allure Of Escalation Dominance. *War on the Rocks*, November 16, 2017. [https://warontherocks.com/2017/11/false-allure-escalation-dominance/], luettu 27.11.2020.

Fjäder, Christian: The Nation-state, National Security and Resilience in the Age of Globalisation. *Resilience*, Vol.2, No.2 (2014), s. 114–129.

Flonk, Daniëlle, Jachtenfuchs, Markus & Obendiek, Anke S.: Authority Conflicts in Internet Governance: Liberals vs. Sovereigntists? *Global Constitutionalism*, Vol. 9, No. 2 (2020), s. 364–386.

Flynn, Matthew J.: Strategic Cyber: Responding to Russian Online Information Warfare. *Cyber Defence Review*, Special Edition 2019, s. 193–207.

Flyvbjerg, Bent: Five Misunderstandings About Case-Study Research. *Qualitative Inquiry* Vol. 12, No. 2 (April 2006), s. 219–245.

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

Fravel, M. Taylor.: China's "World-Class Military" Ambitions: Origins and Implications. *The Washington Quarterly*, Vol.43, No.1 (2020), s. 85–99.

Freedman, Lawrence: Asymmetric War. *The Adelphi Papers*, Vol. 45, No. 379 (2006), s. 49–60.

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

Freedom House: *Freedom on the Net 2017: Russia, 2017*. [https://freedomhouse.org/report/freedom-net/2017/russia], luettu 11.1.2018.

Freedom House: *Nations in Transit 2020: Russia*. [https://freedomhouse.org/country/russia/freedom-world/2020], luettu 19.2.2021.

Freudenstein, Roland: Facing up to the Bear: Confronting Putin's Russia. *European View*, Vol. 13 (2014) s. 225–232.

Friedrichs, J. and Kratochwil, F.: On Acting and Knowing: How Pragmatism Can Advance International Relations Research and Methodology. *International Organization*, Vol. 63, No. 4 (Fall, 2009), s. 701–731.

Futter, Andrew: War Games Redux? Cyberthreats, US–Russian Strategic Stability, and New Challenges for Nuclear Security and Arms Control. *European Security*, Vol. 25, No. 2 (2016), s. 163–180.

GAN: *Russia Corruption Report*, June 2020. [https://www.ganintegrity.com/portal/country-profiles/russia/], luettu 29.1.2021.

Gardiner, Joseph, Cova, Marco & Nagaraja, Shishir: *Command & Control. Understanding, Denying and Detecting*. University of Birmingham, February 2014. [https://arxiv.org/ftp/arxiv/papers/1408/1408.1136.pdf], luettu 2.7.2020.

Gare, Arran: Aleksandr Bogdanov and Systems Theory. *Democracy & Nature*, Vol. 6, No. 3, 2000, s. 341–359.

Gartzke, Erik & Lindsay, John: *Cybersecurity and Cross-Domain Deterrence: The Consequences of Complexity* [http://deterrence.ucsd.edu/_files/LindsayGartzke_ConsequencesofComplexity_Draft.pdf], luettu 16.8.2018.

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

Gartzke, Erik: Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth. *International Security*, Vol. 38, No. 2 (Fall 2013), s. 41–73.

Gat, Azar: So Why Do People Fight? Evolutionary Theory and the Causes of War. *European Journal of International Relations*, Vol. 15, No. 4 (2009), s. 571–599.

Gatlan, Sergiu: SolarWinds Victims Revealed after Cracking the Sunburst Malware DGA. *Bleeping Computer*, December 22, 2020. [https://www.bleepingcomputer.com/news/security/solarwinds-victims-revealed-after-cracking-the-sunburst-malware-dga/], luettu 28.12.2020.

Geers, Kenneth: The Cyber Threat to National Critical Infrastructures: Beyond Theory. *Information Security Journal*: A Global Perspective, Vol. 18, No. 1 (2009), s. 1–7.

Geist, Edward: Deterrence Stability in the Cyber Age. *Strategic Studies Quarterly*, Vol. 9, No. 4 (Winter 2015), s. 44–61.

Gerasimov, Valery: The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. Originally published in Military-Industrial Kurier, 27 February 2013.1 Translated from Russian 21 June 2014 by Robert Coalson, editor, Central News, Radio Free Europe/Radio Liberty. *Military review*, January-February 2016, s. 23–29.

Gerring, John: What Is a Case Study and What Is It Good for? *The American Political Science Review*, Vol. 98, No. 2 (May, 2004), s. 341–354.

Gibson, Irving M.: The Maginot Line. *The Journal of Modern History*, Vol. 17, No. 2 (June, 1945), s. 130–146.

Giles, Keir: Russia's Public Stance on Cyberspace Issues. Teoksessa *2012 4th International Conference on Cyber Conflict*. C. Czosseck, R. Ottis, K. Ziolkowski (Eds.) NATO CCD COE Publications, Tallinn, 2012, s. 63–75.

Giles, Keir: *The Next Phase of Russian Information Warfare*. NATO Strategic Communications Centre of Excellence, Riga, 2016. [https://www.stratcomcoe.org/download/file/fid/5134], luettu 24.2.2021.

Giles, Keir: *The Russian Information Warfare Construct. Contract Report*. Defence Research and Development Canada, 2020.

Giles, Martin: Explainer: What is Quantum Communication? *MIT Technology Review*, February 14, 2019. [https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/], luettu 4.1.2020.

Gioe, David V., Lovering, Richard & Pachesny, Tyler: The Soviet Legacy of Russian Active Measures: New Vodka from Old Stills? *International Journal of Intelligence and CounterIntelligence*, Vol. 33, No. 3 (2020), s. 514–539.

Glaser, Charles L.: The Security Dilemma Revisited. *World Politics*, Vol. 50, No. 1 (1997), s. 171–201.

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

Goel, Sanjay: How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race. *Connections*, Vol. 19, No. 1 (Winter 2020), s. 87–95.

Gold, Josh: *The Five Eyes and Offensive Cyber Capabilities: Building a 'Cyber Deterrence Initiative'*. NATO CCD COE, Tallinn, 2020. [https://ccdcoe.org/uploads/2020/10/2020-Josh-Gold-Five-Eyes-and-Offensive-Cyber-Capabilities.pdf], luettu 19.2.2021.

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

Goldman, Emily O.: From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy. *Texas National Security Review*, Vol. 3, No. 4 (Fall 2020), s. 84–101.

Goldsmith, Jack: *Living Inside Adversary Networks*. Lawfare blog, 16th March 2018. [https://www.lawfareblog.com/living-inside-adversary-networks], luettu 5.5.2020.

Gompert, David C. & Libicki, Martin: Cyber War and Nuclear Peace. *Survival*, Vol.61, No.4 (2019), s. 45–62.

Gray, Colin S.: What Rand Hath Wrought. *Foreign Policy* No. 4 (Autumn, 1971), s. 111–129.

Green, Brendan R. & Long, Austin: The MAD Who Wasn't There: Soviet Reactions to the Late Cold War Nuclear Balance. *Security Studies*, Vol. 26, No. 4 (2017), s. 606–641.

Greiman, Virginia: Cyber Security and Global Governance. Teoksessa *Proceedings of the 14th European Conference on Cyber Warfare & Security*. Abouzakher, Nasser (ed.) University of Hertfordshire, Hattfield, 2015, s. 71–78.

Grey, Christopher: Security Studies and Organization Studies: Parallels and Possibilities. *Organization*, Vol. 16, No. 2 (2009), s. 303–316.

Grier, Peter: The First Offset. *Air Force Magazine*, Vol. 99, No. 6 (June 2016), s. 56–60.

Guerlac, H.: Vauban: The Impact of Science of War. Teoksessa Paret, Peter (ed.): *Makers of Modern Strategy from Machiavelli to the Nuclear Age*. Clarendon Press, Oxford, 1990, s. 64–90.

Guitton, Clement: Cyber insecurity as a national threat: overreaction from Germany, France and the UK? *European Security*, Vol. 22, No. 1 (2013), s. 21–35.

Gutzwiller, Robert S., Ferguson-Walter, Kimberly J. & Fugate, Sunny J.: Are Cyber Attackers Thinking Fast and Slow? Exploratory Analysis Reveals Evidence of Decision-Making Biases in Red Teamers. *Proceedings of the Human Factors and Ergonomics Society 2019 Annual Meeting*, Vol. 63, No. 1 (2019), s. 217–221.

Gutzwiller, Robert S., Fugate, Sunny, D. Sawyer Benjamin D. & Hancock, P. A.: The Human Factors of Cyber Network Defense. *Proceedings of the Human Factors and Ergonomics Society 59th Annual Meeting – 2015*, Vol. 59, No. 1, s. 322–326.

Guzzini, Stefano: The Limits of Neorealist Power Analysis. *International Organization*, Vol. 47, No. 3 (1993), s. 443–478.

Habermas, Jürgen: Talcott Parsons: Problems of Theory Construction. *Social Inq*. Vol 51, No. ¾ (1981), s. 173–196.

Hamati-Ataya, Inanna: Beyond (Post)Positivism: The Missed Promises of Systemic Pragmatism. *International Studies Quarterly*, Vol. 56 (2012), s. 291–305.

Hanska, Jan: Pelotetta vai pidäkettä? Deterrenssiteorian käytäntöä pienen valtion näkökulmasta. *Tiede ja Ase*, Vol 2019, No. 1, s. 42–70, s. 58–59.

Hare, F.: The Significance of Attribution to Cyberspace Coercion: A Political Perspective. In *4th International Conference on Cyber Conflict*. C. Czosseck, R. Ottis & K. Ziolkowski (Eds.) NATO CCD COE Publications, Tallinn, 2012, s. 125–140.

Harknett, Richard J. & Nye, Joseph S. Jr.: Correspondence – Is Deterrence Possible in Cyberspace. *International Security*, Vol. 42, No. 2 (2017), s. 196–199.

Harknett, Richard J. & Smeets, Max: Cyber Campaigns and Strategic Outcomes. *Journal of Strategic Studies*, 2020 DOI: 10.1080/01402390.2020.1732354.

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

Hasík, James: Beyond the Briefing: Theoretical and Practical Problems in the Works and Legacy of John Boyd. *Contemporary Security Policy*, Vol. 34, No. 3 (2013), s. 583–599.

Healey, Jason & Jervis, Robert: The Escalation Inversion and Other Oddities of Situational Cyber Stability. *Texas National Security Review*, Vol. 3, No. 4 (Fall 2020), s. 30–53.

Heath, Timothy R.: An Overview of China's National Military Strategy. Teoksessa *China's Evolving Military Strategy*. McReynolds, Joe (ed.) The Jamestown Foundation, Washington, D.C., 2016, s. 12–45.

Hellmann, Gunther (ed.): Pragmatism and International Relations: Beliefs as Rules for Action: Pragmatism as a Theory of Thought and Action. *International Studies Review* (2009) 11, s. 638–662.

Henson, S. A., Henshaw, M.J.D., Barot, V., Siemieniuch, C.E., Sinclair, M.A., Dogan, H., Lim, S.L., Ncube, C., Jamshidi, M. & DeLaurentis, D.: Towards a Systems of Systems Engineering EU Strategic Research Agenda. *2013 8th International Conference on System of Systems Engineering, Maui, HI, 2013*, s. 99–104.

Heylighen, Francis, Joslyn Cliff & Turchin Valentin: What are Cybernetics and Systems Science? *Principia Cybernetica Web (Principia Cybernetica, Brussels), 1999.* [http://pespmc1.vub.ac.be/CYBSWHAT.html], luettu 7.7.2020.

Heylighen, Francis: *Web Dictionary of Cybernetics and Systems*. [http://pespmc1.vub.ac.be/ASC/INDEXASC.html], luettu 23.9.2019.

Hitchins, D. K.: A General Theory of Command and Control. *1989 Third International Conference on Command, Control, Communications and Management Information Systems, Bournemouth, UK, 1989*, s. 111–126.

Hobbs, Carla (ed.): *Europe's Digital Sovereignty: From Rulemaker To Superpower In The Age Of Us-China Rivalry*. European Council on Foreign Relations, July 2020. [https://www.ecfr.eu/page/-/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry.pdf], luettu 17.10.2020.

Hodgson, Quentin E.: Understanding and Countering Cyber Coercion. Teoksessa *10th International Conference on Cyber Conflict CyCon X: Maximising Effects*. Minárik, T., Jakschis, R. and Lindström, L. (eds.) NATO CCD COE, Tallinn, 2018, s. 73–88.

Hoffman, Frank G.: Hybrid Warfare and Challenges. Teoksessa *Strategic Studies: A Reader*. Mahnken, Thomas G. & Maiolo, Joseph A. (eds.) Routledge, New York, 2014, s. 329–337.

Hoffman, Frank G.: *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies, Arlington, Virginia, 2007. [http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf], luettu 14.4.2020.

Hoffmann, Stacie, Lazanski, Dominique & Taylor, Emily: Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet. *Journal of Cyber Policy*, Vol. 5, No. 2 (2020), s. 239–264.

Honig, Or Arthur & Zimskind, Sarah: Not Completely Blind: What Dictators Do to Improve Their Reading of the World. *Comparative Strategy*, Vol. 36, No. 3 (2017), s. 241–256.

Humbert, Clemence & Joseph, Jonathan: Introduction: The Politics of Resilience: Problematising Current Approaches. *Resilience*, Vol. 7, No. 3 (2019), s. 215–223.

Hutchens, Michael E., Dries, William D., Perdew, Jason C., Bryant, Vincent D. & Kerry E. Moores: Joint Concept for Access and Maneuver in the Global Commons: A New Joint Operational Concept. *Joint Forces Quarterly*, Vol. 84 (Jan. 27, 2017), s. 134–139.

Hutchins, Eric M., Cloppert, Michael J. & Amin, Rohan M.: *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* [https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf], luettu 29.6.2020.

Hyvönen, Ari-Elmeri, Juntunen, Tapio, Mikkola, Harri, Käpylä, Juha, Gustafsberg, Harri, Nyman, Markku, Rättilä, Tiina, Virta, Sirpa & Liljeroos, Johanna: *Kokonaisresilienssi ja turvallisuus: tasot, prosessit ja arviointi*. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 17/2019. Valtioneuvoston kanslia, Helsinki, 2019.

ID Quantique: *Understanding Quantum Cryptography*, White paper, May 2020. [https://marketing.idquantique.com/acton/attachment/11868/f-020d/1/-/-/-/-/Understanding%20Quantum%20Cryptography_White%20Paper.pdf], luettu 24.11.2020.

Ikenberry, John: The End of Liberal International Order? *Foreign Affairs*, Vol. 94, No. 1 (2018), s. 7–23.

Inglis, John C., Lumpkin, Michael D., Waltzman, Rand & Watts, Clint: *Cyber-enabled Information Operations*. Subcommittee on Cybersecurity, Committee on Armed Services, United States Senate, One Hundred Fifteenth Congress, First Session, April 27, 2017. [https://www.hsdl.org/?view&did=802817], luettu 21.2.2021.

Inozemtsev, Vladislav: The Yandex Affair: Insider Trading and Institutionalized State Control. *Eurasia Daily Monitor* Volume: 16 Issue: 174 [https://jamestown.org/program/the-yandex-affair-insider-trading-and-institutionalized-state-control/], luettu 28.7.2021.

Jackson, Patrick Thaddeus & Nexon, Daniel H.: Paradigmatic Faults in International-Relations Theory. *International Studies Quarterly* Vol. 53, No. 4, (December 2009), s. 907–930.

Jackson, Patrick Thaddeus: Situated Creativity, or, the Cash Value of a Pragmatist Wager for IR. *International Studies Review*, Vol. 11, No. 3 (September 2009), s. 638–662, s. 656–659.

Jaitner, Margarita & Rantapelkonen, Jari: Russian Struggle for Sovereignty in Cyberspace. *Tiede ja Ase*, Vol. 71 (2013), s. 64–89, 83.

Jensen, Benjamin & Valeriano, Brandon: *What Do We Know about Cyber Escalation? Observations from Simulations and Surveys*. Atlantic Council, 2019. [https://www.atlanticcouncil.org/wp-

content/uploads/2019/11/What_do_we_know_about_cyber_escalation_.pdf], luettu 12.1.2021.

Jensen, Benjamin, Valeriano, Brandon & Maness, Ryan: Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies*, Vol. 42, No. 2 (2019), s. 212–234.

Jervis, R.: Dilemmas About Security Dilemmas. *Security Studies*, Vol. 20, No. 3 (2011), s. 416–423.

Jervis, Robert: Complexity and the Analysis of Political and Social Life. *Political Science Quarterly*, Vol. 112, No. 4 (Winter, 1997-1998), s. 569–593.

Jervis, Robert: Review: Deterrence Theory Revisited. *World Politics*, Vol. 31, No. 2 (January 1979), s. 289–324.

Jiang, Tianjiao: From Offense Dominance to Deterrence: China's Evolving Strategic Thinking on Cyberwar. *Chinese Journal of International Review*, Vol. 1, No. 2 (2019).

Johnson, James S.: China's Vision of the Future Network-centric Battlefield: Cyber, Space and Electromagnetic Asymmetric Challenges to the United States. *Comparative Strategy*, Vol. 37, No. 5 (2018), s. 373–390.

Johnson, James: Delegating Strategic Decision-making to Machines: Dr. Strangelove Redux? *Journal of Strategic Studies*, 2020. DOI: 10.1080/01402390.2020.1759038.

Johnson, Robert: Hybrid War and Its Countermeasures: A Critique of the Literature. *Small Wars & Insurgencies*, Vol. 29, No. 1 (2018), s. 141–163.

Johnston, Alastair Iain: Thinking about Strategic Culture. *International Security*, Vol. 19, No. 4 (Spring 1995), s. 32–64.

Jones Day: Implementing China's Cybersecurity Law, August 2017. [https://www.jonesday.com/files/upload/Implementing%20Chinas%20Cybersecurity%20Law.pdf], luettu 28.4.2020.

Jonsson, Oscar and & Seely, Robert: Russian Full-Spectrum Conflict: An Appraisal After Ukraine. *Journal of Slavic Military Studies*, Vol. 28, No. 1 (2015), s. 1–22.

Joseph, Jonathan: Resilience as embedded neoliberalism: a governmentality approach. *Resilience*, Vol. 1, No. 1 (2013), s. 38–52.

Junio, Timothy J.: Military History and Fourth Generation Warfare. *Journal of Strategic Studies*, Vol. 32, No. 2 (2009), s. 243–269.

Kagan, Frederick W.: The Rise and Fall of Soviet Operational Art, 1917-1941. Teoksessa *The Military History of the Soviet Union*. Higham, Robin & Kagan, Frederick W. (eds) Palgrave, New York, 2002, s. 79–92.

Kallberg, Jan & Cook, Thomas S.: The Unfitness of Traditional Military Thinking in Cyber. Four Cyber Tenets That Undermine Conventional Strategies. *IEEE Access*, Vol. 5, 2017, s. 8126–8130.

Kania, Elsa B & Costello, John: Seizing the Commanding Heights: The PLA Strategic Support Force in Chinese Military Power. *Journal of Strategic Studies*, 2020, DOI: 10.1080/01402390.2020.1747444.

Kantola, Harry, Huttunen, Mika & Kiviharju, Mikko: Taistelun elementit kybertoimintaympäristössä. Teoksessa *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, s.142–152, s. 143.

Kärkkäinen, Anssi: Kyberpuolustuksen taistelukenttä nyt ja tulevaisuudessa. Teoksessa *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, s.72–83.

Kausch, Kristina: *Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East*. German Marshall Fund of the United States, Policy Brief, November 24, 2017. [https://www.gmfus.org/publications/cheap-havoc-how-cyber-geopolitics-will-destabilize-middle-east], luettu 10.1.2021.

Kavanagh, Camino: *The United Nations, Cyberspace and International Peace and Security – Responding to Complexity in the 21st Century. UNIDIR, 2017.* [https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf], luettu 17.10.2019.

Keating, Charles B., Padilla, Jose J. & Adams, Kevin: System of Systems Engineering Requirements: Challenges and Guidelines. *Engineering Management Journal*, Vol. 20, No. 4 (December 2008), s. 24–31.

Kello, Lucas: The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, Vol. 38, No. 2 (Fall 2013), s. 7–40.

Keizer, Gregg: Garden-variety DDoS Attack Knocks North Korea Off The Internet. Experts Cite the Fragility of North Korea's Connection, Note That Routine DDoS Attacks Could Have Easily Forced the Country Offline. *Computerworld*, 23.12.2014. [https://www.computerworld.com/article/2862652/garden-variety-ddos-attack-knocks-north-korea-off-the-internet.html], luettu 29.7.2021.

Kern, Sean & Gaines, Charles: Expanding Combat Power Through Military Cyber Power Theory. *Joint Forces Quarterly*, Vol. 79, No. 4 (Quartet 2015), s. 88–95.

Keršanskas, Vytautas: *Deterrence: Proposing a More Strategic Approach to Countering Hybrid Threats*. Hybrid CoE Paper 2, March 2020. [https://www.hybridcoe.fi/wp-content/uploads/2020/07/Deterrence_public.pdf], luettu 24.2.2021.

Kerttunen, Mika: Ydinaseet 2000-luvun maailmanjärjestyksessä. Teoksessa *Sota – Teoria ja todellisuus. Näkökulmia sodan muutokseen*. Raitasalo, Jyri & Sipilä, Joonas (toim.) Maanpuolustuskorkeakoulu, Strategian laitos, Julkaisusarja 1, No. 24. Maanpuolustuskorkeakoulu, Helsinki, 2008, s. 11–41, s. 24–25.

Kim, Hyeob, Kwon, HyukJun & Kim, Kyung Kyu: Modified Cyber Kill Chain Model for Multimedia Service Environments. *Multimedia Tools and Applications*, Vol. 78 (2019), s. 3153–3170.

Kipp, Jacob W.: ‘Smart’ Defense From New Threats: Future War From a Russian Perspective: Back to the Future After the War on Terror. *The Journal of Slavic Military Studies*, Vol. 27, No. 1 (2014), s. 36–62.

Kiviharju, Mikko & Huttunen, Mika: Kybertaktiikkaa – Yleisten periaatteiden soveltuvuudesta kybertoimintaympäristössä. Teoksessa *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018, s.161–180.

Klare, Michael T.: Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation. *Arms Control Today*, November 2019. [https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new-pathways-escalation], luettu 30.4.2020.

Klimburg, Alexander: Mixed Signals: A Flawed Approach to Cyber Deterrence. *Survival*, Vol.62, No.1 (2020), s. 107–130.

Klimburg, Alexander: Mobilising Cyber Power. *Survival*, Vol. 53, No. 1 (2011), s. 41–60.

Knight, Ben: German Data Storage Laws 'threaten free trade'. *DW*, 12.1.2017. [https://www.dw.com/en/german-data-storage-laws-threaten-free-trade/a-37110699], luettu 12.1.2021.

Knopf, Jeffrey W.: The Fourth Wave in Deterrence Research. *Contemporary Security Policy*, Vol. 31, No. 1 (2010), s. 1–33.

Kofman, Michael, Fink, Anya & Edmonds, Jeffrey: *Russian Strategy for Escalation Management: Evolution of Key Concepts*. CNA, 2020. [https://www.cna.org/centers/cna/sppp/rsp/escalation-management], luettu 25.1.2021.

Kolodziej, E. A.: French Strategy Emergent: General Andre Beaufre: A Critique. *World Politics*, Vol. 19, No. 3 (1967), s. 417–444.

Kolton, Michael: Interpreting China’s Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence. *The Cyber Defense Review*, Vol. 2, No. 1 (Winter 2017), s. 119–154.

Konyshev, Valery & Sergunin, Alexander: Military. Teoksessa *Tsyganov, Andrei P. (ed.) Routledge Handbook of Russian Foreign Policy*. Routledge, London and New York, 2018, s. 168–181.

Korhonen, Suvi: Valtorin pelko osui oikeaan: katkenneet ”kahdennetut” kaapelit samassa kourussa – TietoEvryltä saatetaan vaatia korvauksia. *Tivi*, 22.7.2021 [https://bit.ly/3C7Hxce], luettu 30.7.2021.

Kosola, Jyri: Teknologia 2030+. Vaikutukset tulevaisuuden sodankäyntiin. Teoksessa *Tuleva sota. Tulevaisuuden sodan tulevaisuus*. Rantapelkonen, Jari (toim.) Edita, Helsinki, 2018, s. 44–83.

Kristensen, Hans M. & Korda, Matt: United States Nuclear Forces, 2020. *Bulletin of the Atomic Scientists*, Vol. 76, No. 1 (2020), s. 46–60.

Kristensen, Hans M.: *Obama and the Nuclear War Plan. Federation Of The American Scientists Issue Brief, February, 2010.*

[https://fas.org/programs/ssp/nukes/publications1/WarPlanIssueBrief2010.pdf], luettu 4.1.2021.

Kuehl, Daniel T.: *From Cyberspace to Cyberpower - Defining the Problem*. Teoksessa *Cyberpower and National Security*. Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K., National Defence University Press, Washington, D.C., 2009, s. 24–42.

Kukkola, Juha & Ristolainen, Mari: Projected Territoriality: A Case Study of the Infrastructure of Russian 'Digital Borders'. *Journal of Information Warfare*, Vol. 17, No. 2 (2018), s. 83–100.

Kukkola, Juha, Nikkarila, Juha-Pekka & Ristolainen, Mari: Asymmetric frontlines of cyber battlefields. *Presented at International Command and Control Research and Technology Symposium (ICCRTS), Los Angeles, USA, November 6.-8., 2017*.

Kukkola, Juha, Ristolainen, Mari & Nikkarila, Juha-Pekka: Confrontation with a closed network nation: Open network society's choices and consequences. *Presented at Military Communications (MILCOM) conference, Baltimore, USA, October 23.-25, 2017*.

Kukkola, Juha: Cyber asymmetry – Towards new strategic thinking? Teoksessa *Game Changer: Structural Transformation of Cyberspace*. Kukkola, Juha, Ristolainen, Mari & Nikkarila, Juha-Pekka. Finnish Defence Research Agency, Riihimäki, 2017, s. 131–188.

Kukkola, Juha: Civilian and Military Information Infrastructure and the Control of the Russian Segment of Internet. *Presented at The International Conference on Military Communications and Information Systems (ICMCIS) Varsova, Puola, Toukokuu 22.-23., 2018*.

Kukkola, Juha: The Russian National Segment of the Internet as a Source of Structural Cyber Asymmetry. Teoksessa *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Ertan, A., Floyd, K., Pernik, P. & Stevens, T. (Eds.) CCD COE, Tallinn, 2020b, s. 9–30.

Kuusisto, Tuija: Tiedonhallinta päätöksenteossa kybertoimintaympäristössä. Teoksessa *Kybertaistelu 2020*. Kuusisto, Tuija (toim.), Maanpuolustuskorkeakoulu, Taktiikan laitos, Julkaisusarja 2, No. 1/2014, Juvenes Print, Helsinki 2014, s. 33–61.

Lalu, Petteri & Puistola, Juha: *On the concept of hybrid warfare*. Finnish Defence Research Agency, Research Bulletin 01 – 2015. [https://puolustusvoimat.fi/documents/1951253/2815786/PVTUTKL+TUTKIMUSKATSAUS+2015_1+engl.pdf/12fd458c-aa76-4ed6-a402-b19c13fb18c3/PVTUTKL+TUTKIMUSKATSAUS+2015_1+engl.pdf.pdf], luettu 14.4.2020.

Lambakis, Steven, Kiras, James & Kolet, Kristin: Understanding "Asymmetric" Threats to the United States. *Comparative Strategy*, Vol. 21, No. 4 (2002), s. 241–277.

Lantis, Jeffrey S.: Strategic Culture and Tailored Deterrence: Bridging the Gap between Theory and Practice. *Contemporary Security Policy*, Vol. 30, No. 3 (2009), s. 467–485.

Lassila, Jussi: Aivovuoto Venäjältä: Kremlin kaksiteräinen miekka. *FIIA Comment 6*, Toukokuu 2019. [https://www.fiia.fi/wp-content/uploads/2019/05/comment6_emigration_from_russia_fi.pdf], luettu 29.7.2021.

Laszlo, Ervin: Systems Philosophy. *Ultimate Reality and Meaning* January, Vol. 1, No. 3 (1978), s. 223–230.

Lawlor Russell, Alison: Strategic Anti-Access/Area Denial in Cyberspace. Teoksessa Maybaum, M., Osula, A. & Lindström, L. (Eds.): *7th International Conference on Cyber Conflict: Architectures in Cyberspace*. NATO CCD COE Publications, Tallinn, 2015, s. 153–168.

Lawson, Sean: Cold War Military Systems Science and the Emergence of a Nonlinear View of War in the US military. *Cold War History*, Vol. 11, No. 3 (August 2011), s. 421–440.

Lee, Tony S., Ghosh, Sumit & Nerode, Anil: Asynchronous, Distributed, Decision-Making Systems with Semi-Autonomous Entities: A Mathematical Framework. *IEEE Transactions On Systems, Man, And Cybernetics—Part B: Cybernetics*, Vol. 30, No. 1, February 2000, s. 206–212.

Legro, Jeffrey & Moravcsik, Andrew: A. Is Anybody Still a Realist. *International Security*, Vol. 24, No. 2 (1999), s. 5–55.

Lehto, Martti & Limnéll, Jarno: Kybersodankäynnin kehityksestä ja tulevaisuudesta. *Tiede- ja Ase*, Vol. 75 (2017), s. 179–212.

Lehto, Martti: *Kybermaailman ilmiöitä ja määrittelyjä*. Jyväskylän yliopisto, Informaatioteknologian tiedekunta, 2019. [https://www.jyu.fi/it/fi/hae-opiskelemaan/hakukohteet/kyberturvallisuuden-seka-turvallisuus-ja-strateginen-analyysi-maisteriohjelmien-yhteisvalinta/kybermaailma_v10-0.pdf], luettu 16.3.2020.

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

Leuprecht, Christian, Szeman, Joseph & Skillicorn, David B.: The Damoclean sword of offensive cyber: Policy uncertainty and collective insecurity. *Contemporary Security Policy*, Vol. 40, No. 3 (2019), s. 382–407.

Lewis, James A.: National Perceptions of Cyber Threats. *Strategic Analysis*, Vol. 38, No. 4 (2014), s. 566–578.

Libicki, Martin C.: The Conversion of Information Warfare. *Strategic Studies Quarterly*, Vol. 11, No. 1, (Spring 2017), s. 49–65.

Libicki, Martin C.: *What Is Information Warfare?* National Defense University, Institute for National Strategic Studies, Washington, D.C., 1995.

Lider, Julian: The Correlation of World Forces: The Soviet Concept. *Journal of Peace Research*, Vol. 17, No. 2 (1980), s. 151–171.

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

Lilly, Bilyana & Cheravitch, Joe: The Past, Present, and Future of Russia's Cyber Strategy and Forces. Teoksessa 2020 *12th International Conference on Cyber Conflict 20/20 Vision: The Next Decade*. T. Jančárková, L. Lindström, M. Signoretti, I. Tolga, G. Visky (Eds.) NATO CCDCOE Publications, Tallinn, 2020, s. 129–155.

Limnéll, Jarno: *Holistic Approach is Necessary to Solve Security Issues of This Decade*. Cyberwarch Finland, 1/2021, s. 14–15.

Limnéll, Jarno: Kyber rantautui Suomeen. *Aalto-yliopiston julkaisusarja Tiede + Teknologia* 12/2014.

Lin, Herbert: Attribution of Malicious Cyber Incidents: From Soup to Nuts. *Journal of International Affairs*, Vol. 70, No. 1 (Winter 2016), s. 75–137.

Lin, Herbert: Doctrinal Confusion and Cultural Dysfunction. *The Cyber Defense Review*, Vol. 5, No. 2 (2020), s. 89–108.

Lind, William S.: *Maneuver Warfare Handbook*. Westview Press, Boulder, Colorado, 1985, s. 6–7.

Lindsay, Jon R. & Gartzke, Erik: Politics by Many Other Means: The Comparative Strategic Advantages of Operational Domains. *Journal of Strategic Studies*, 2020 DOI: 10.1080/01402390.2020.1768372.

Lindsay, Jon R.: Demystifying the Quantum Threat: Infrastructure, Institutions, and Intelligence Advantage. *Security Studies*, Vol. 29, No. 2 (2020), s. 335–361.

Lindsay, Jon R: Stuxnet and the Limits of Cyber Warfare. *Security Studies*, Vol.22, No.3 (2013), s. 365–404.

Liuhto, Kari: Motivations of Russian Firms to Invest Abroad: How Do Sanctions Affect Russia's Outward Foreign Direct Investment? *Baltic Region*, Vol. 26, No. 4 (2015), s. 4–19.

Long, Austin: A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning. *Journal of Cybersecurity*, Vol. 3, No. 1 (2017), s. 19–28.

Lubin, Asaf: A New Era of Mass Surveillance is Emerging Across Europe. *Just Security*, January 9, 2017 [https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe/], luettu 12.1.2021.

Lucas, Edward & Pomeranzev, Peter: *Winning the Information War Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe*. CEPA, 2016. [https://li.com/wp-content/uploads/2016/08/winning-the-information-war-full-report-pdf.pdf], luettu 28.1.2021.

Lucas, Edward: Trump Has Become Putin's Ally in Russia's War on the West. *CNN*, February 7, 2017. [https://www.cnn.com/2017/02/07/opinions/trumps-moral-relativism-lucas-opinion/index.html], luettu 28.1.2021.

Luhn, Alec & Harding, Luke: Putin dismisses Panama Papers as an attempt to destabilise Russia. *Guardian*, April 7th, 2016. [https://www.theguardian.com/news/2016/apr/07/putin-dismisses-panama-papers-as-an-attempt-to-destabilise-russia], luettu 1.5.2019.

Lundberg, Jonas: Situation Awareness Systems, States and Processes: A Holistic Framework. *Theoretical Issues in Ergonomics Science*, Vol. 16, No. 5 (2015), s. 447–473.

Lykke, Arthur F.: Toward an Understanding of Military Strategy. *Military Review* Vol. LXIX, No. 5, (May 1989), s. 2–8.

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

Magd, Noora: Kybertaistelutila kybertoimintaympäristön sotilaallisena ulottuvuutena. Teoksessa *Kyberajan viestitaktiikkaa*. Hirvonen, Pauliina (toim.) Viestiupseeriyhdistys ry ja Maanpuolustuksen viestisäätiö, Seinäjoki, 2018.

Magnanti, Thomas L.: Networks as an Aid in Transportation and Contingency Planning. *Proceedings of Workshop Held 28–30 March 1982*. George Horwich (ed.), Pergamon, 1983, s. 703–723.

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

Mahnken, Thomas G.: The Future of Strategic Studies. *The Journal of Strategic Studies*, Vol. 26, No. 1 (2003), s. x–xviii.

Maier, Mark W.: Research Challenges for Systems-of-Systems. *IEEE International Conference on Systems, Man and Cybernetics Waikoloa, HI, USA, October 10-12, 2005,* s. 3149–3154.

Main, Steven J.: 'You Cannot Generate Ideas by Orders': The Continuing Importance of Studying Soviet Military History—G. S. Isserson and Russia's Current Geo-Political Stance. *The Journal of Slavic Military Studies*, Vol. 29, No.1 (2016), s. 48–72.

Maker, Simran R.: Mutually Assured Disruption: *Framing Cybersecurity In Nuclear Terms A National Committee on American Foreign Policy Report*, January 2018. [https://www.ncafp.org/2016/wp-content/uploads/2018/01/Mutually-Assured-Disruption-S.-Maker.pdf], luettu 5.1.2021.

Mälkki, Juha: Vaikutusperusteisen operatiivisen ajattelun (EBAO) sotataidolliset lähtökohdat. *Tiede ja Ase*, Vol 69 (2010), s. 7–31.

Mälksoo, Maria: Countering Hybrid Warfare as Ontological Security Management: The Emerging Practices of the EU and NATO. *European Security*, Vol. 27, No. 3 (2018), s. 374–392.

Mancilla, Roberto Gustavo: Introduction to Sociocybernetics (Part 1): Third Order Cybernetics and a Basic Framework for Society. *Journal of Sociocybernetics*, Vol. 36, No. 9 (2011), s. 35–56.

Mandiant: *APT1 Exposing One of China's Cyber Espionage Units*. [https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf], luettu 29.6.2020.

Maness, R. C. & Valeriano, B.: Cyber spillover conflicts: Transition from cyber conflict to conventional foreign policy disputes. Teoksessa *Conflict in Cyber Space: Theoretical, strategic and legal perspectives*. Routledge, New York, 2016, s. 45–64.

March, James G. & Olsen, Johan P.: The Institutional Dynamics of International Political Orders. *International Organization*, Vol. 52, No. 4 (Autumn 1998), s. 943–969.

Marten, Kimberly: The 'KGB State' and Russian Political and Foreign Policy Culture. *Journal of Slavic Military Studies*, Vol. 30, No. 2 (2017), s. 131–151.

Matthews, Earl D., Arata, Harold J. III & Hale, Brian L.: Cyber Situational Awareness. *The Cyber Defense Review*, Vol. 1, No. 1 (Spring 2016), s. 35–46.

Mazanec, Brian M.: *Lessons for the Cyber Battlefield from the Early Nuclear Era's Single Integrated Operating Plan*. FDD Press, Washington DC, 2019.

Mazarr, Michael J.: Virtual Territorial Integrity: The Next International Norm. *Survival*, Vol. 62, No. 4 (2020), s. 101–118.

McCarthy, J. A., Burrow, C., Dion, M. & Pacheco, O.: Cyberpower and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts. Teoksessa *Cyberpower and National Security*. Kramer, F. D., Starr, S. H. and Wentz, L. (eds.). National Defence University Press, Washington D.C., 2009, s. 543–556.

McDermott, Basil W.: Thinking about Herman Kahn. *The Journal of Conflict Resolution* , 1971, Vol. 15, No. 1 (Mar., 1971), s. 55–70.

McDermott, Roger N. & Bartles, Charles K.: *The Russian Military Decision-Making Process & Automated Command and Control*. GIDS research 02/2020, 29. October 2020. [https://gids-hamburg.de/wp-content/uploads/2020/10/GIDSresearch2020_02_McDermott_Bartles.pdf], luettu 26.12.2020.

McGraw, Gary & Fick, Nathaniel: Separating Threat from the Hype: What Washington Needs to Know about Cyber Security. Teoksessa *America's Cyber Future Security and Prosperity in the Information Age volume II*. Lord, Kristin M. & Sharp, Travis (ed.) Center for New American Security, 2011, s. 43–53.

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

McVicar, Michael: Decisions in Crisis—An Examination. *Comparative Strategy*, Vol. 34, No. 1 (2015), s. 14–43.

Meakins, Joss: *Living in (Digital) Denial: Russia's Approach to Cyber Deterrence*. Euro-Atlantic Security Report. European Leadership Network, 2018. [https://www.europeanleadershipnetwork.org/report/living-in-digital-denial-russias-approach-to-cyber-deterrence/], luettu 29.4.2020.

Meentemeyer, Scott M., Sauser, Brian & Boardman, John: Analysing a System of Systems Characterisation to Define System of Systems Engineering Practices. *International Journal of System of Systems Engineering*, Vol. 1, No. 3, 2009, s. 329–346.

Metz, S. & Johnson, D. I.: *Asymmetry and U.S. Military Strategy L Definition, Background, and Strategic Concepts*. U. S. Army Strategic Studies Institute: Carlisle, 2001, s. 3–4 [https://apps.dtic.mil/sti/pdfs/ADA387381.pdf], luettu 20.8.2017.

Mikoyan, Sergo A.: Eroding the Soviet "Culture of Secrecy". *Studies in Intelligence*, Vol. 45, No. 5 (2001) [https://www.cia.gov/static/b8834854dbda7fb29d04ee27e368b3e7/Eroding-the-Soviet-Culture.pdf], luettu 29.1.2021.

Milevski, Lucas: Asymmetry is Strategy, Strategy is Asymmetry. *JFQ*, Vol. 75, No. 4 (2014), s. 77–83.

Miller, Benjamin: The Concept of Security: Should it be Redefined? *The Journal of Strategic Studies*, Vol. 24, No. 2 (2001), s. 13–42.

Mingers, John & Standing, Craig: What is Information? Toward a Theory of Information as Objective and Veridical. *Journal of Information Technology*, Vol. 33 (2018), s. 85–104.

Mitchell, P.: Network Centric Warfare: Coalition Operations in the Age of US Military Primacy. IISS, *The Alelphi Papers* Vol. 6, No. 385 (2006).

MITRE: *ATT&CK Matrix for Enterprise.* [https://attack.mitre.org/matrices/enterprise/], luettu 29.6.2020.

Molloy, Steve & Schwenk, Charles R.: The Effects of Information Technology on Strategic Decision Making. *Journal of Management Studies*, Vol. 32, No. 3 (1995), s. 283–311.

Myers, Nicholas J.: Radio Exercises and Trends in Russian C2 Capabilities. *Eurasia Daily Monitor*, Vol. 17, No. 65. [https://jamestown.org/program/radio-exercises-and-trends-in-russian-c2-capabilities/], luettu 14.5.2020.

Nagelhus Schia, Niels & Gjesvik, Lars: The Chinese Cyber Sovereignty Concept (Part 1). *The University of Nottingham's Asia Research Institute*, September 7, 2018. [https://theasiadialogue.com/2018/09/07/the-chinese-cyber-sovereignty-concept-part-1/], luettu 28.1.2021.

Nikkarila, J-P., Åkesson, B., Kuikka, V., & Hämäläinen, J.: Modelling Closed National Networks: Effects in Cyber Operation Capabilities. Teoksessa *Proceedings of the 17th European Conference on Cyber Warfare and Security (ECCWS), Oslo, Norway, 2018 June, 28.-29*, s. 323–329.

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

Noble, Ben & Schulmann, Ekaterina: Not Just a Rubber Stamp. Parliament and Lawmaking. Teoksessa *The New Autocracy: Information, Politics, and Policy in Putin's Russia*. Treisman, Daniel (ed.) Brookings Institution Press, Washington, D.C., 2018, s. 47–78.

Nocetti, Julian: Contest and Conquest: Russia and Global Internet Governance. *International Affairs*, Vol. 91, No. 1 (2015), s. 111–130.

Nocetti, Julian: Cyber Power. Teoksessa *Routledge Handbook of Russian Foreign Policy*. Tsygankov, Andrei P. (Ed.) Routledge, London and New York, 2018.

Nye, Joseph S. Jr.: *ISSF Roundtable 10-6 on The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*. Discussion published by George Fujii on Friday, January 19, 2018. [https://networks.h-net.org/node/1252924/pdf], luettu 23.11.2020.

Nye, Joseph: Deterrence and Dissuasion in Cyberspace. *International Security*, Vol. 41, No. 3 (2016/2017), s. 44–71.

Nye, Joseph: Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly*, Vol. 5, No. 4 (Winter 2011), s. 18–38.

O'Neill, Patrick Howell: The $1 billion Russian cyber company that the US says hacks for Moscow. *MIT Review*, April 15, 2021 [https://www.technologyreview.com/2021/04/15/1022895/us-sanctions-russia-positive-hacking/], luettu 28.7.2021.

Oehmen, Christopher & Multari, Nicholas: *AiR: Asymmetry in Resilience: Report on the First Meeting on Asymmetry in Resilience for Complex Cyber Systems*, U.S. Department of Energy, 2014. [https://cybersecurity.pnnl.gov/documents/AiR_1.0_Final_Report.pdf], luettu 15.4.2020.

Oehmen, Christopher & Multari, Nicholas: *AiR2: Second Meeting on Asymmetry in Resilience Report on the Second Meeting on Asymmetry in Resilience for Complex Cyber Systems*, U.S. Department of Energy, 2016. [https://cybersecurity.pnnl.gov/documents/AiR_2.0_Final_Report.pdf], luettu 15.4.2020.

Oliker, Oleg: Putinism, Populism and the Defence of Liberal Democrazy. *Survival*, Vol.59, No. 1 (February – March 2017), s. 7–24.

Oliker, Olga: *New Document Consolidates Russia's Nuclear Policy in One Place. Russia Matters*, June 4, 2020. [https://www.russiamatters.org/analysis/new-document-consolidates-russias-nuclear-policy-one-place], luettu 6.1.2021.

Oliker, Olga: *Russia's Nuclear Doctrine. What We Know, What We Don't, and What That Means*. Center for Strategic & International Studies, May 2016. [https://www.csis.org/analysis/russia%E2%80%99s-nuclear-doctrine], luettu 6.1.2021.

Olsen, John A.: Boyd Revisited: A Great Mind with a Touch of Madness. *Air Power History*, Vol. 64, No. 4 (2012), s. 7–16.

Osinga, Frans: 'Getting' A Discourse on Winning and Losing: A Primer on Boyd's 'Theory of Intellectual Evolution'. *Contemporary Security Policy*, Vol. 34, No. 3 (2013), s. 603–624.

Owens, William A.: The Emerging System of Systems. *Proceedings*, Vol. 121, No. 5 (1995), s. 36–39.

Pahi, T., Leitner, M & Skopik, F.: Preparation, Modelling, and Visualisation of Cyber Common Operating Pictures for National Cyber Security Centres. *Journal of Information Warfare*, Vol. 16, No. 4 (Fall 2017), s, 26-4.

Paul, Christopher, Clarke, Colin P., Schwille, Michael, Hlavka, Jakub P., Brown, Michael A., Davenport, Steven, Porche, Isaac R. III & Harding, Joel: *Lessons from Others for Future U.S. Army Operations in and Through the Information Environment*. RAND, Santa Monica, 2018. [https://www.rand.org/pubs/research_reports/RR1925z1.html], luettu 21.2.2021.

Payne, Kenneth: Artificial Intelligence: A Revolution in Strategic Affairs? *Survival*, Vol. 60, No. 5 (2018), s. 7–32.

Pernik, Piret: National Cyber Commands. Teoksessa *Routledge Handbook of International Cybersecurity*. Tikk, Eneken & Kerttunen, Mika (eds.) Routledge, London, 2020.

Person, Robert: Balance of Threat: The Domestic Insecurity of Vladimir Putin. *Journal of Eurasian Studies,* Vol. 8, No. 1 (January 2017), s. 44–59.

Piedrahita, Murillo, Andrés F., Gaur, Vikram, Giraldo, Jairo, Cárdenas, Álvaro A. & Rueda, Sandra Julieta: Leveraging Software-Defined Networking for Incident Response in Industrial Control Systems. *IEEE Software*, Vol. 35, No. 1 (January/February 2018), s. 44–50.

Pigeau, Ross, & McCann, Carol: Re-conceptualizing Command and Control. *Canadian Military Journal*, Vol. 3, No 1. (Spring 2002), s. 53–63.

Pirolli, Peter & Russell, Daniel M.: Introduction to this Special Issue on Sensemaking. *Human–Computer Interaction*, Vol. 26, No. 1-2 (2011), s. 1–8.

Plopsky, G.: Russia's Big Plans for Air Defense in Eurasia: Big plans, indeed, but will they materialize? *The Diplomat* (2017, Apr, 7). [https://thediplomat.com/2017/04/russias-big-plans-for-air-defensein-eurasia/], luettu 8.7.2020.

Popescu, Ionut C: Grand Strategy vs. Emergent Strategy in the conduct of foreign policy. *The Journal of Strategic Studies*, Vol. 41, No. 3, (2018), s. 438–460.

Porter, Patrick: *A World Imagined: Nostalgia and Liberal Order*. Policy Analysis 843, Cato Institute, June 5, 2018. [https://www.cato.org/publications/policy-analysis/world-imagined-nostalgia-liberal-order], luettu 12.1.2021.

Potomac Institute for Policy Studies: *Netherlands Cyber Readiness at a Glance*, 2017. [http://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf], luettu 15.4.2020.

Pratt, S.: Pragmatism as Ontology, Not (Just) Epistemology: Exploring the Full Horizon of Pragmatism as an Approach to IR Theory. *International Studies Review* (2016) 18, s. 508–527.

Principia Cybernetica Project: *Principia Cybernetica Web.* [http://pespmc1.vub.ac.be/DEFAULT.html], luettu 4.10.2019.

Puranen, Matti: Historia poliittisen maailmankatsomuksen palveluksessa: tianxia-teoria ja kiinalainen poliittinen kosmologia. *Ennen ja Nyt*, 28.11.2017. [https://www.ennenjanyt.net/2017/11/historia-poliittisen-maailmankatsomuksen-palveluksessa-tianxia-teoria-ja-kiinalainen-poliittinen-kosmologia/], luettu 7.1.2021.

Pynnöniemi, Katri & Busygina, Irina: Critical Infrastructure Protection and Russia's Hybrid Regime. *European Security*, Vol.22, No.4 (2013), s. 559–575.

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.

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

Ramesh, Reethika et al.: Decentralized Control: A Case Study of Russia. *Network and Distributed Systems Security (NDSS) Symposium 2020 23-26 February 2020, San Diego, CA, USA*.

Raska, Michael: The sixth RMA wave: Disruption in Military Affairs? *Journal of Strategic Studies*, 2020, DOI: 10.1080/01402390.2020.1848818.

Rathbun, Brian: A Rose by Any Other Name: Neoclassical Realism as the Logical and Necessary Extension of Structural Realism. *Security Studies*, Vol. 17, No. 2 (2008), s. 294–321.

Rattray, Gregory J.: An Environmental Approach to Understanding Cyberpower. Teoksessa *Cyberpower and National Security*. Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K. (Eds.) National Defence University Press, Washington, D.C., 2009.

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

Renz, Bettina: Russia and 'Hybrid Warfare'. *Contemporary Politics*, Vol. 22, No. 3 (2016), s. 283–300.

Rice, Condoleezza: The Party, the Military, and Decision Authority in the Soviet Union. *World Politics*, Vol. 40, No. 1. (October 1987), s. 55–81.

Rid, T. & Buchanan, B.: Attributing Cyber Attacks. *Journal of Strategic Studies*, Vol. 35, No. 1 (2015), s. 4–37.

Rid, T. & McBurney, P.: Cyber-Weapons. *The RUSI Journal*, Vol. 157, No. 1 (2012), s. 6–13.

Ristolainen, Mari: Should 'RuNet 2020' be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West. Teoksessa *Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS) Dublin, Ireland, June 29.-30., 2017. Scanlon, Mark & Le-Khac, Nhien-An (eds.) 2017*, s. 370–379.

Ristolainen, Mari: Should "RuNet 2020" be Taken Seriously? Contradictory Views about Cybersecurity between Russia and the West. *Journal of Information Warfare*, Vol. 16, No. 4 (2017), s. 113–131.

Rivera, J.: Achieving Cyberdeterrence and the Ability of Small States to Hold Large States at Risk. Teoksessa *7th International Conference on Cyber Conflict: Architectures in Cyberspace*. M. Maybaum, O. &. A.-M. & L. Lindström (eds.) NATO CCD COE Publications, Tallinn, 2015, s. 7–24.

Robinson, Neil & Milne, Sarah: Populism and Political Development in Hybrid Regimes: Russia and the Development of Official Populism. *International Political Science Review*, Vol. 38, No. 4, s. 412–425.

Rose, Gideon: Neoclassical Realism and Theories of Foreign Policy. *World Politics*, Vol. 51, No. 1 (1998), s. 144–172, s. 146.

Rowley, Jennifer: The Wisdom Hierarchy: Representations of the DIKW Hierarchy. *Journal of Information Science*, Vol. 33, No. 2 (2007), s. 163–180.

Rudner, Martin: Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge. *International Journal of Intelligence and CounterIntelligence*, Vol.26, No.3 (2013), s. 453–481.

Russell, S.L. & Jackson, S.C.: Operating in the Dark: Cyber Decision-Making from First Principles. *Journal of Information Warfare*, Vol. 17, No. 1 (Winter 2018), s. 1–15.

Ryan, Maria: Full Spectrum Dominance: Donald Rumsfeld, the Department of Defense, and US Irregular Warfare Strategy, 2001–2008. *Small Wars & Insurgencies*, Vol. 25, No. 1 (2014), s. 41–68.

Sakwa, Richard. Dualism at Home and abroad: Russian Foreign Policy Neo-Revisionism and Bicontinentalism. Teoksessa *Russia's Foreing Policy. Ideas, Domestic Politics and External Relations*. Cadier, David and Light, Margot (eds.) Palgrave Macmillan, Basingstoke, 2015, s. 65–79.

Sanjian, Andrea Stevenson: Constraints on Modernization: The Case of Administrative Theory in the U. S. S. R. *Comparative Politics*, Vol. 18, No. 2 (Jan., 1986), s. 193–210.

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.

Schneider, Volker & Bauer, Johannes M.: Governance: Prospects of Complexity Theory in Revisiting System Theory. *Conference paper, presented at the annual meeting of the Midwest Political Science Association. Panel 33.26 Political Theory and Theories of Political Science. Chicago, Illinois, 14 April 2007.*

Schoen, Fletcher & Lamb, Christopher J.: *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*. Center for Strategic Research Institute for National Strategic Studies National Defense University, Washington D.C., 2012.

Schörnig, Niklas: Neorealism. Teoksessa *Theories of International Relations*. Schieder, Siegfried & Spindler, Manuela (ed.) Routledge, New York, 2015, s. 37–55.

Schreier, Fred: *On Cyberwarfare*. DCAF Horizon 2015 Working Paper No. 7. [https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf], luettu 27.4.2020.

Schwartz, Donald V.: Information and Administration in the Soviet Union: Some Theoretical Considerations. *Canadian Journal of Political Science / Revue canadienne de science politique*, Vol. 7, No. 2 (Jun., 1974), s. 228–247.

Schwartz, Stephen I.: *The Costs of U.S. Nuclear Weapons*. Nuclear Threat Initiative, October 1, 2008. [https://www.nti.org/analysis/articles/costs-us-nuclear-weapons/], luettu 22.2.2021.

Scott, Mark: Welcome to New Era of Global Digital Censorship. It's Dangerous to Ask Tech Companies to Decide What's Legitimate Free Speech. *Politico*, January 14, 2018. [https://www.politico.eu/article/google-facebook-twitter-censorship-europe-commission-hate-speech-propaganda-terrorist/], luettu 12.1.2021.

Sengupta, Sailik, Chowdhary, Ankur, Sabur, Abdulhakim, Alshamrani, Adel, Huang, Dijiang & Kambhampati, Subbarao: A Survey of Moving Target Defenses for Network Security. *IEEE Communications Surveys & Tutorials 2020*, [https://arxiv.org/abs/1905.00964v2], luettu 11.1.2021.

Shahbaz, Adrian: *Freedom on the Net 2018. The Rise of Digital Authoritarianism*. Freedom House, 2019. [https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism], luettu 29.12.2020.

Sharp, Travis: Theorizing Cyber Coercion: The 2014 North Korean Operation against Sony. *The Journal of Strategic Studies*, Vol. 40, No. 7 (2017), s. 898–926.

Sheldon, John B.: The Rise of Cyberpower. Teoksessa *Strategy in the Contemporary World* (4th ed.) Baylis, John, Wirtz, James J. & Gray, Colin S. (Eds.) Oxford University Press, Oxford, 2013, s. 301–319.

Simon, H. A.: Theories of Decision-making in Economic and Behavioral Science. *American Economic Review*, Vol. 49 (1959), s. 253–283.

Simon, H.: *The New Science of Management Decision*. Prentice Hall, Englewood Cliffs, NJ, 1997.

Simon, Luis: A European Perspective on Anti-Access/Area Denial and the Third Offset Strategy. *War on the Rocks*, May 3rd 2016. [https://warontherocks.com/2016/05/a-european-perspective-on-anti-accessarea-denial-and-the-third-offset-strategy/], luettu 14.4.2020.

Simon, Luis: Demystifying the A2/AD Buzz. *War on the Rocks*, 2017. [https://warontherocks.com/2017/01/demystifying-the-a2ad-buzz/], luettu 15.4.2020.

Singh, Madan G.: Tactical Decision Making for the Firm in a Competitive Environment. *Conference Proceedings 1991 IEEE International Conference on Systems, Man, and Cybernetics, University of Virginia*, 13-16 Oct. 1991, 2003-2008.

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

Smeets, Max & Lin, Herbert S.: Offensive Cyber Capabilities: To What Ends? Teoksessa *10th International Conference on Cyber Conflict CyCon X: Maximising Effects*. Minárik, T., Jakschis, R. and Lindström, L. (eds.) NATO CCD COE, Tallinn, 2018, s. 55–72.

Smeets, Max & Work, J.D.: Operational Decision-Making for Cyber Operations: In Search of a Model. *The Cyber Defense Review*, Vol. 5, No. 1 (2020), s. 95–112.

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

Smith, Steve: The Increasing Insecurity of Security Studies: Conceptualizing Security in the Last Twenty Years. *Contemporary Security Policy*, Vol. 20, No. 3 (1999), s. 72–101.

Snodgrass, Anthony W., Gallagher, Mark A. & Gregory A. McIntyre: Modeling Military Strategic Effects with an Input-Output Metamodel. *Military Operations Research*, Vol. 9, No. 1 (2004), s. 19–32.

Sokhey, Sarah Wilson: What Does Putin Promise Russians? Russia's Authoritarian Social Policy. *Orbis*, Vol. 64, No. 3 (2020), s. 390–402.

Solanko, Laura*: From reforms to stagnation – 20 years of economic policies in Putin's Russia*. BOFIT Policy Brief 2020 No. 1. [https://helda.helsinki.fi/bof/bitstream/handle/123456789/16548/bpb0120.pdf?sequence=1&isAllowed=y], luettu 31.1.2021.

Soldatov, Andrei & Rochlitz, Michael: The Siloviki in Russian Politics. Teoksessa *The New Autocracy: Information, Politics, and Policy in Putin's Russia*. Treisman, Daniel (ed.) Brookings Institution Press, Washington, D.C., 2018, s. 79–103.

Soldatov, Andrei: From the "New Nobility" to the KGB. *Russian Politics and Law*, Vol. 55, No. 2 (2017), s. 133–146.

Son, Kyong-Min: Cybernetic Freedom: David Easton, Systems Thinking, and the Search for Dynamic Stability. *American Political Thought: A Journal of Ideas, Institutions, and Culture*, Vol. 7 (Fall 2018), s. 614–645.

Stevens, Tim: A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy*, Vol. 33, No. 1 (2012), s. 148–170.

Stevens, Tim: Knowledge in the Grey Zone: AI and Cybersecurity. *Digital War* (2020). https://doi.org/10.1057/s42984-020-00007-w.

Stone, Christopher: The Implications of Chinese Strategic Culture and Counter-intervention upon Department of Defense Space Deterrence Operations. *Comparative Strategy*, Vol. 35, No. 5 (2016), s. 331–346.

Stone, John: Cyber War Will Take Place! *Journal of Strategic Studies*, Vol. 36, No. 1 (2013), s. 101–108.

Strachan, Hew: Strategy in Theory, Strategy in Practice. *Journal of Strategic Studies*, Vol. 42, No. 2 (2019), s. 171–190.

Strange, Joe: *Centres of Gravity & Critical Vulnerabilities*. Marine Corps University Perspectives on Warflghting Number Four Second Edition [https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/3B_COG_and_Critical_Vulnerabilities.pdf], luettu 14.4.2020.

Suslov, Dmitry V.: S – Strategic Stability. *Russia in Global Affairs*, No.1 (2020 January/March), s. 122–128.

Sweijs, Tim & Zilincik, Samo: *Cross Domain Deterrence and Hybrid Conflict*. The Hague Centre for Strategic Studies, Hague, 2019. [https://hcss.nl/sites/default/files/files/reports/Cross%20Domain%20Deterrence%20-%20Final_0.pdf], luettu 11.1.2021.

Taillat, Stéphane: Disrupt and Restraint: The Evolution of Cyber Conflict and the Implications for Collective Security. *Contemporary Security Policy*, Vol. 40, No. 3 (2019), s. 368–381.

Takala, Tuomo & Lämsä, Anna-Maija: Tulkitseva käsitetutkimus organisaatio- ja johtamistutkimuksen tutkimusmetodologisena vaihtoehtona. *Liiketaloudellinen aikakauskirja* 50, 3 (2001), s. 371–390.

Tangredi, Sam J. CNO vs A2AD: Why Admiral Richardson is Right about Deconstructing the A2/AD Term. *The Navalist,* January 2017. [https://thenavalist.com/home/2017/1/8/dissecting-the-buzz-words-that-control-the-defense-debates], luettu 15.4.2020.

Thomas, Timothy L.: Russian Views on Information-Based Warfare. *Airpower Journal* – Special Edition 1996, s. 26–35.

Thomas, Timothy: Nation-state Cyber Strategies: Examples from China and Russia. Teoksessa *Cyberpower and National Security*. Kramer, Franklin D., Starr, Stuart H. and Wentz, Larry K. (Eds.) National Defence University Press, Washington, D.C., 2009, s. 465–488.

Thomas, Timothy: Creating Cyber Strategists: Escaping the 'DIME' Mnemonic. *Defence Studies*, Vol. 14, No. 4 (2014), s. 370–393, s. 373.

Thomas, Timothy: The Evolution of Russian Military Thought: Integrating Hybrid, New-Generation, and New-Type Thinking. *The Journal of Slavic Military Studies*, Vol. 29, No. 4 (2016), s. 554–575.

Thomas, Timothy: Russian Military Thought: Concepts and Elements. MITRE Corporation, McLean VA, 2019. [https://www.mitre.org/publications/technical-papers/russian-military-thought-concepts-and-elements], luettu 4.5.2020.

Thomas, Timothy: Information Weapons: Russia's Nonnuclear Strategic Weapons of Choice. *The Cyber Defense Review*, Vol. 5, No. 2 (2020), s. 125–144.

Thornton, Rod & Miron, Marina: Towards the 'Third Revolution in Military Affairs'. *The RUSI Journal*, Vol. 165, No. 3 (2020), s. 12–21.

Tikk, Eneken & Kerttunen, Mika: *Parabasis. Cyber-diplomacy in Stalemate*. Norwegian Institute of International Affairs, 2018. [https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2569401/NUPI_Report_5_18_Tikk_Kerttunen.pdf?sequence=1&isAllowed=y], luettu 6.5.2019.

Tomes, Robert: The Cold War Offset Strategy: Assault Breaker And The Beginning Of The RSTA Revolution. *War on the Rocks*, November 20, 2014. [https://warontherocks.com/2014/11/the-cold-war-offset-strategy-assault-breaker-and-the-beginning-of-the-rsta-revolution/], luettu 14.4.2020.

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

Tóth, Gábor Attila: Authoritarianism. *Oxford Constitutional Law*, February 2017. [https://oxcon.ouplaw.com/view/10.1093/law-mpeccol/law-mpeccol-e205], luettu 12.1.2021.

Tran, Huy T., Domercxant, Jean Charles & Mavris, Dimitri N.: Evaluating the Agility of Adaptive Command and Control Networks from a Cyber Complex Adaptive Systems Perspective. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, Vol. 12, No. 4 (2015) s. 405–422.

Trevithick, Joseph: No, The United States Doesn't Have An Automatic "Dead Hand" Trigger For Its ICBMs. *The Drive: The Warzone*, February 7, 2020. [https://www.thedrive.com/the-war-zone/32114/no-the-united-states-doesnt-have-an-automatic-dead-hand-trigger-for-its-icbms], luettu 8.7.2020.

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

Van Bezooijen, B. J. A., Essens, P. J. M. D. & Vogelaar, A. L. W.: Military Self-synchronization: An Exploration of the Concept. *11TH ICCRTS, Coalition Command And Control In The Networked Era 27 September 2006*.

Van Evera, Stephen: Offense, Defense, and the Causes of War. *International Security*, Vol. 22, No. 4 (Spring 1998), s. 5–43.

Van Rijmenam, Mark & Logue, Danielle: Revising the 'Science of the Organisation': Theorising AI Agency and Actorhood. *Innovation*, 2020 DOI: 10.1080/14479338.2020.1816833.

Vego, Milan: Effects-Based Operations: A Critique. *Joint Forces Quarterly,* Vol. 41, No. 2 (2006), s. 51–57.

Vego, Milan: On Operational Art. *Strategos*, Vol. 1 No. 2 (2017), s. 15–39.

Vendil Pallin, Carolina: Internet Control Through Ownership: The Case of Russia. *Post-Soviet Affairs*, Vol. 33, No. 1 (2017), s. 16–33.

Vendil Pallin, Carolina: Russian Information Security and Warfare. Teoksessa Kanet, Roger E.: *Routledge Handbook of Russian Security*. Routledge, London and New York, 2019, s. 203–213.

Vendil, Carolina: The Russian Security Council. *European Security*, Vol.10, No.2 (Summer 2001), s. 67–94.

Vidmer, Richard F.: Management Science in the USSR: The Role of "Americanizers". *International Studies Quarterly,* Vol. 24, No. 3 (Sep., 1980), s. 392–414.

Vidmer, Richard F.: Soviet Studies of Organization and Management: A "Jungle" of Competing Views. *Slavic Review*, Vol. 40, No. 3 (Autumn, 1981), s. 404–422.

Votel, Joseph, Cleveland, Charles, Connett, Charles & Irwin, Will: Unconventional Warfare in the Gray Zone. *Joint Forces Quarterly*, Vol. 80 (1st Quarter) 2016, s. 101–109.

Wang, G., Yang, Y., Ren, Q. & Ma, R.: Efficiency of Command and Control in Cyberspace: Visit from the Perspective of Complexity Theory. *2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery,* Beijing 10-12 October 2013, s. 398–401.

Warden, John A. III: Success in Modern War: A Response to Robert Pape's Bombing to Win. *Security Studies*, Vol. 7, No. 2 (1997), s. 172–190.

Warden, John: The Enemy as a System. *Airpower Journal*, Vol. 9, No. 1 (1995), s. 40–55.

Warren, Tom: Microsoft Bids Farewell to Windows 7 and the Millions Of PCs That Still Run It: An End of the Traditional Windows Era. *The Verge*, 14.1.2020. [https://www.theverge.com/2020/1/14/21065122/microsoft-windows-7-end-of-support-lifecycle-millions-pcs], luettu 5.1.2021.

Welt, Cory & Nelson, Rebecca M.: *Russia: Domestic Politics and Economy, September 9, 2020*. Congressional Research Service, R46518 – Version 4. [https://fas.org/sgp/crs/row/R46518.pdf], luettu 28.7.2021.

Wheeler, N. J.: British Nuclear Weapons and Anglo-American Relations 1945-54. *International Affairs*, Vol. 62, No. 1 (Winter, 1985-1986), s. 71–86.

Whisler, Greg (2020a): Strategic Command and Control in the Russian Armed Forces: Untangling the General Staff, Military Districts, and Service Main Commands (Part Two). *The Journal of Slavic Military Studies*, Vol. 33, No. 1 (2020), s. 89–112.

Whisler, Greg (2020b): Strategic Command and Control in the Russian Armed Forces: Untangling the General Staff, Military Districts, and Service Main Commands (Part Three). *The Journal of Slavic Military Studies*, Vol. 33, No. 2 (2020), s. 237–258.

Whisler, Greg: Strategic Command and Control in the Russian Armed Forces: Untangling the General Staff, Military Districts, and Service Main Commands (Part One). *The Journal of Slavic Military Studies*, Vol. 32, No. 4 (2019), s. 463–484.

White, Ralph K.: Social Science Research in the Soviet Bloc. *The Public Opinion Quarterly*, Vol. 28, No. 1 (Spring, 1964), s. 20–26.

Whyte, Christopher: Beyond Tit-for-tat in Cyberspace: Political Warfare and Lateral Sources of Escalation Online. *European Journal of International Security*, Vol. 5, No. 2 (2020), s. 195–214.

Whyte, Christopher: Dissecting the Digital World: A Review of the Construction and Constitution of Cyber Conflict Research. *International Studies Review*, Vol. 20, No. 3 (2018), s. 520–532.

Willett, Marcus: Assessing Cyber Power. *Survival*, Vol.61, No.1 (2019), s. 85–90.

Williams, Martyn: How the Internet Works in North Korea. *Slate*, November 28, 2016. [https://slate.com/technology/2016/11/how-the-internet-works-in-north-korea.html], luettu 28.1.2021.

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

Wirtz, J. J.: Life in the "Gray Zone": Observations for contemporary strategists. *Defense & Security Analysis*, Vol. 33, No. 2 (2017), s. 106–114.

Wither, James K.: Making Sense of Hybrid Warfare. *Connections*, Vol. 15, No. 2 (Spring 2016), s. 73–87.

Young, Thomas-Durell: Legacy Concepts: A Sociology of Command in Central and Eastern Europe. *Parameters*, Vol. 47, No. 1 (Spring 2017), s. 31–42.

Zins, Chaim: Conceptual Approaches for Defining Data, Information, and Knowledge. *Journal of the American Society for Information Science and Technology*, Vol. 58, No. 4 (2007), s. 479–493.

1.4 Viralliset julkaistut asiakirjat

Congressional Research Service: *Defense Primer: Information Operations, Updated December 15, 2020*. [https://fas.org/sgp/crs/natsec/IF10771.pdf], luettu 21.2.2021.

Cyberspace Administration of China: *National Cyberspace Security Strategy*, 27.12.2016. [https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/], luettu 23.12.2020.

Cyberspace Solarium Commission: *End Report,* March 2020. [https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view], luettu 1.7.2020.

Davis, Susan: NATO in The Cyber Age: Strengthening Security & Defence, Stabilising Deterrence. NATO Parliamentary Assembly, Science And Technology Committee (STC) 13 August 2019. [https://www.nato-pa.int/download-file?filename=sites/default/files/2019-09/148%20STC%20Davis%20-%20NATO%20IN%20THE%20CYBER%20AGE%20-%20fall%20revision%20-%20clean%2011.9.19.pdf], luettu 12.1.2021.

Defence Intelligence Agency: *Russia Military Power: Building a Military to Support Great Power Ambitions*, 2017. [http://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Russia%20Military%20Power%20Report%202017.pdf], luettu 8.7.2020.

ENISA: *An overview on enhancing technical cooperation between CSIRTs and LE*, May 07, 2020. [https://www.enisa.europa.eu/publications/support-the-fight-against-cybercrime-tools-for-enhancing-cooperation-between-csirts-and-le], luettu 10.7.2020.

ENISA: *Critical Information Infrastructures Protection approaches in EU*, July 2015. [https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf], luettu 15.9.2020.

ENISA: *CSIRTs by Country - Interactive Map.* [https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map], luettu 10.7.2020.

ENISA: *Definition of Cybersecurity: Gaps and overlaps in standardisation Version 1.0, December 2015.* [https://www.enisa.europa.eu/publications/definition-of-cybersecurity], luettu 28.4.2020.

ENISA: *EU Member States incident response development status report*, November 27, 2019 [https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report], luettu 10.7.2020.

ENISA: *National Cyber Security Strategies - Interactive Map* [https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map], luettu 12.1.2021.

ENISA: *Study on CSIRT landscape and IR capabilities in Europe 2025*, February 2019 [https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025/at_download/fullReport], luettu 12.1.2021.

ENISA: *Supply Chain Integrity. An overview of the ICT supply chain risks and challenges, and vision for the way forward*, Version 1.1, August 2015 [https://www.enisa.europa.eu/publications/sci-2015/at_download/fullReport], luettu 12.1.2021.

ENISA: *Threat Landscape and Good Practice. Guide for Internet Infrastructure, January 2015.* [https://www.enisa.europa.eu/publications/iitl/at_download/fullReport], luettu 7.5.2020.

European Commission: *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Brussels, 13.9.2017 JOIN(2017) 450 final.* [https://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cyber-security_ec.pdf], luettu 7.7.2020.

European Commission: *Building Resilience: The EU's approach – Factsheet, 2018.* [http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/resilience_en.pdf], luettu 1.5.2020.

European Commission: *A European strategy for data*. COM(2020) 66 final, 19.2.2020. [https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066], luettu 12.1.2021.

European Commission: *Digital Economy and Society Index (DESI) 2020).* [https://ec.europa.eu/digital-single-market/en/digital-economy-and-society-index-desi], luettu 14.7.2020.

European Commission: *Joint Communication To The European Parliament And The Council: The EU's Cybersecurity Strategy for the Digital Decade*. Brussels, 16.12.2020 JOIN(2020) 18 final. [https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade], luettu 18.12.2020.

European Commission: *Reports and Studies about Digital Economy and Society Index*, 2020. [https://ec.europa.eu/digital-single-market/en/reports-and-studies/76018/3650], luettu 14.7.2020.

European Parliament: *Cyber defence in the EU Preparing for cyber warfare?* Briefing, October 2014. [https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf], luettu 21.2.2021.

European Union: *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 "NIS Directive".* [https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN], luettu 7.7.2020.
European Union: *Joint Communication to the European Parliament and the Council:*
International Telecommunication Union (ITU): *Global Cybersecurity Index & Cyberwellness Profiles*, April 2015. [https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf], luettu 15.9.2020.

International Telecommunications Union (ITU): *Global Cybersecurity Index (CGI) 2017.* [https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf], luettu 28.4.2020.

Madiega, Tambiama: *Digital sovereignty for Europe*. European Parliament, July 2020. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf], luettu 17.10.2020.

Ministère des Armées: *Droit International Appliqué Aux Opérations Dans Le Cyberespace*, 2019. [https://www.defense.gouv.fr/content/download/565895/9750877/file/Droit+internat+appliqu%C3%A9+aux+op%C3%A9rations+Cyberespace.pdf], luettu 8.10.2020.

Ministry of Defence of the Great Britain: *Joint Operations Execution. Joint Warfare Publication 3-00*. (2nd ed.) The Joint Doctrine & Concepts Centre, Shrivenham 1-11, 2004. [https://dokumen.tips/documents/jwp-3-00-jt-ops-execution-2004.html], luettu 11.1.2021.

Ministry of Foreign Affairs of the People's Republic of China: *China's Policies on Asia-Pacific Security Cooperation, January 2017.* [https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1429771.shtml], luettu 4.5.2020.

Multinational Experiment 7: *Outcome 3 – Cyber Domain Objective 3.4 Cyber Situational Awareness Standard Operating Procedure. Version 1.0, 1 December 2012.* [https://www.hsdl.org/?view&did=760553], luettu 6.7.2020.

National Institute of Standards and Technology (NIST): *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0, February 12, 2014.* [https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf], luettu 29.6.2020.

National Security Commission on Artificial Intelligence: *Final Report*, 2021. [https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf], luettu 6.3.2021.

NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE): *Strategy and Governance* (verkkosivu). [https://ccdcoe.org/library/strategy-and-governance/], luettu 14.7.2020.

NATO: *AJP-3.3 Allied Joint Doctrine for Air and Space Operations. Edition B Version 1, April 2016*, 1-1. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/624137/doctrine_nato_air_space_ops_ajp_3_3.pdf], luettu 11.1.2021.

NATO: *Allied Command Operations Comprehensive Operations Planning Directive COPD Interim V2.0 04 October 2013, NATO Unclassified.* [https://www.cmdrcoe.org/download.cgf.php?id=9], luettu 13.5.2020.

NATO: *Allied Joint Doctrine For Cyberspace Operations, AJP-3.20, Edition A Version 1, January 2020*. NATO Standardization Office (NSO), 2020a. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf], luettu 13.7.2020.

NATO: *Brussels Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July 2018.* [https://www.nato.int/cps/en/natohq/official_texts_156624.htm], luettu 24.8.2020.

NATO: *Military Strategic Level Decision Making within a (Future) Framework of Cyber Resilience*. STO-TR-SAS-116, 24.8.2020. NATO Unclassified Rel To PFP, 2020b. DOI: 10.14339/STO-TR-SAS-116.

NATO: *Wales Summit Declaration*. Press Release (2014) 120, Issued on 05 Sep. 2014. [https://www.nato.int/cps/en/natohq/official_texts_112964.htm], luettu 19.2.2021.

New York State Department Of Financial Services: *Cybersecurity Requirements For Financial Services Companies, 23 NYCRR 500.* [https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf], luettu 29.6.2020.

NIS Cooperation Group: *EU coordinated risk assessment of the cybersecurity of 5G networks*, 9 October 2019 [https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132], luettu 12.1.2021.

OECD: *Digital Security Risk Management for Economic and Social Prosperity*. OECD Recommendation and Companion Document, 2015. [https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf], luettu 12.1.2021.

Office of the Deputy Under Secretary of Defense for Acquisition and Technology, Systems and Software Engineering: *Systems Engineering Guide for Systems of Systems, Version 1.0*. ODUSD(A&T)SSE, Washington, DC, 2008.

PVOHJEK-PE: *Puolustusvoimien toiminta*. HN707/23.11.2017, liite 1.

PVOHJEK-PE: *Puolustusvoimien toiminta*. HN707/23.11.2017, liite 6.

Pääesikunta.: *Sotilaallisen suorituskyvyn käsitemalli*. Asiakirja HO46, 31.5.2018.

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

Suomen Valtioneuvosto: *Valtioneuvoston puolustusselonteko*. Valtioneuvoston kansalian julkaisusarja 5/2017, Helsinki, 2017.

The Department of the Army of the United States of America: *ADP 6-0 31 July 2019. Mission Command: Command and Control of Army Forces*. Headquarters Department of the Army, Washington D.C., 2019.

The President of the United States: *National Security Strategy of the United States of America*, December 2017. White House, Washington, DC., 2017.

The State Council Information Office of the People's Republic of China: *China's National Defense in the New Era*. Foreign Languages Press Co. Ltd., Beijing, 2019.

The State Council Information Office of the People's Republic of China. *China's Military Strategy*. Beijing, May 2015. [http://eng.mod.gov.cn/Press/2015-05/26/content_4586805.htm], luettu 27.4.2020.

The United States Army Combined Arms Doctrine Directorate: *FM 100-5 Operations*, May 1986, s.180. [http://cgsc.cdmhost.com/utils/getdownloaditem/collection/p4013coll9/id/893/filename/894.pdf/mapsto/pdf/type/singleitem], luettu 14.4.2020.

The United States Department of Defense (U.S. DoD) (2018a): *Cyber Strategy – Summary, 2018.* [https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF], luettu 5.5.2020.

The United States Department of Defense (U.S. DoD), Chairman of the Joint Chiefs of Staff: *Joint Vision 2010, 1996.* [http://drseres.com/tavoktatas/irodalom/stb/jv2010.pdf], luettu 8.5.2020.

The United States Department of Defense (U.S. DoD), Chairman of the Joint Chiefs of Staff: *Concept for Future Operations. Expanding Joint Vision 2010, May 1997.* [http://web.archive.org/web/20040225022332/http://www.dtic.mil/jointvision/history/cfjoprn1.pdf], luettu 8.5.2020.

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

The United States Department of Defense (U.S. DoD): *DOD Dictionary of Military and Associated Terms, December, 2020*. [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2020-06-18-073638-727], luettu 11.1.2021.

The United States Department of Defense (U.S. DoD): *Joint Publication 3-13: Information Operations*; 27 November 2012 Incorporating Change 1 20 November 2014. [https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf], luettu 11.1.2021.

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

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

The United States Department of Defense (U.S. DoD): *Joint Vision 2020*, printed in Joint Force Quarterly, Summer 2000. [http://www.dtic.mil/dtic/tr/fulltext/u2/a526044.pdf], luettu 14.4.2020.

The United States Department of Defense (U.S. DoD): *Military and Security developments involving the People´s Republic of China, Annual report to congress 2020*. The Office of the Secretary of Defence, 2020.

The United States Department of Defense (U.S. DoD): *Network Centric Warfare, Report to Congress*, 27 July 2001. [http://www.dodccrp.org/files/ncw_report/report/ncw_appendix.pdf], luettu 14.4.2020.

The United States Department of Defense (U.S. DoD): *Summary of the 2018 National Defense Strategy: Sharpening the American Military's Competitive Edge.*

[https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf], luettu 5.1.2021.

The United States Department of Defense (U.S. DoD): *Systems Engineering Guide for Systems of Systems, version 1.0, 2008.* [http://acqnotes.com/wp-content/uploads/2014/09/DoD-Systems-Engineering-Guide-for-Systems-of-Systems-Aug-2008.pdf], luettu 17.10.2019.

The United States Department of Homeland Security: *Cybersecurity Strategy, 15th May 2018* [https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf], luettu 7.7.2020.

The United States Department of Justice: *U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage*, May 19, 2014. [https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor], luettu 30.12.2020.

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

The White House: *National Security Strategy of the United States of America, December 2017.* [https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf], luettu 4.5.2020.

Ulkoministeriö: *Kansainvälinen oikeus kyberympäristössä - Suomen kansallisia kantoja*. Ulkoministeriö, 15.10.2020. [https://um.fi/documents/35732/0/Suomennos+Kansainv%C3%A4linen+oikeus+kyberymp%C3%A4rist%C3%B6ss%C3%A4.pdf/26706a43-4d7e-07da-8c4f-7c53b6ca51ab?t=1602581216672], luettu 16.10.2020.

Valtioneuvosto: *Ehdotus valtioneuvoston periaatepäätökseksi kyberturvallisuuden kehittämisohjelmasta*. Lausuntopyynnön diaarinumero: VN/ 797/2021. [https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=e09805fc-83a1-4207-8f16-55a991363d0d], luettu, 12.3.2021.

Valtioneuvoston kanslia: *Valtioneuvoston puolustusselonteko*. VNS 3/2017 vp. Valtioneuvoston kanslia, Helsinki, 2017.

Valtiovarainministeriö: *Tietoturvapoikkeamatilanteiden hallinta. Valtiovarainministeriön julkaisuja 8/2017.* [https://www.suomidigi.fi/sites/default/files/2020-06/VM_8_2017.pdf], luettu 29.6.2020.

Vlacheas, Panagiotis T., Stavroulaki, Vera, Demestichas, Panagiotis, Cadzow, Scott & Slawomir Gorniak: *Ontology and taxonomies of resilience*. ENISA, 2011. [https://www.enisa.europa.eu/publications/ontology_taxonomies/at_download/fullReport], luettu 1.5.2020.

World Bank: *World Bank Open Data.* [https://data.worldbank.org], luettu 14.7.2020.

1.5 Arkistot

Hagel, Chuck: *Secretary of Defense Speech: Reagan National Defense Forum Keynote*, November 15th 2014. [https://www.defense.gov/Newsroom/Speeches/Speech/Article/606635/], luettu 14.4.2020.

Kennan, George: *George F. Kennan on Organizing Political Warfare*, April 30th 1948. [https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=941dc9ee5c6e51333ea9ebbbc9104e8c], luettu 15.4.2020.

2 VENÄJÄNKIELINEN MATERIAALI

2.1 Kirjallisuus

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

Комов, С.А. (под общ. редакцией). *Международная информационная безопасность: дипломатия мира*. Сборник статей. Военинформ, Москва, 2009.

Коцыняк М.А., Кулешов И.А., Кудрявцев А.М. & Лаута О.С.: *Киберустойчивость Информационнотелекоммуникационной Сети*. Бостон-спектр, Санкт-Петербург, 2015.

Крутских, А.В. (Под общ. ред.): *Международная информационная безопасность: Теория и практика: В трех томах. Том 1: Учебник для вузов*. Издательство «Аспект Пресс», Москва, 2019.

Медриш, М.А. (ред.): *Стабильность, безопасность, отказоустойчивость глобальной инфраструктуры Интернета: технические и правовые вопросы*. ПИР-Цеитр, Москва - Лос Анджелес, 2016.

Подвиг, П. Л.: *Стратегическое ядерное вооружение России*. ИздАТ, Москва, 1998.

Рипенко, Ю. Б.: *Управление войсками*. Gorizont, Москва, 2016.

Рогозин, Дмитрий (под общ.ред.): *Война и мир в терминах и определениях*. Вече, Москва, 2011.

Снесарев, А. Е. & Керсновский, А. А.: *Философия войны*. Вече, Москва, 2018.

Торгованова, Ю. Б. (под общ. ред.): *Управление подразделениями в мирное время*. Сиб. федер. ун-т, Красноярск, 2015.

Тюшкевич, С. А.: *О законах войны вопросы военной теории и методологии*. Проспект, Москва, 2017.

2.2 Artikkelit ja Internet-lähteet

Агора: *Свобода интернета 2018: делегирование репрессий.* [https://meduza.io/static/0001/Свобода-интернета-2018.pdf], luettu 1.3.2019.

Агора: *Свобода интернета 2019: план «Крепость»*. [https://2019.runet.report/assets/files/Internet_Freedom%202019_The_Fortress.pdf], luettu 17.3.2020.

Аксенов, С.В.: Обеспечение устойчивости группировки стратегических ядерных сил в условиях информационного противоборства. *Вестник академии военных наук*, № 2 (67) (2019), с. 66–68.

Андреев, В.: 5 Этапов развития АСУ. *Воздушно-космическая оборона*, №2, 2011 г.

Воейков, Денис: «Цифровая экономика» исполнила бюджет хуже всех нацпроектов. *CNews.ru*, 13.1.2020. [https://www.cnews.ru/news/top/2020-01-13_tsifrovaya_ekonomika_provalila], luettu 5.1.2020.

Воейков, Денис: МВД потратит 270 миллионов на серверы с «Эльбрусами» «не хуже» Intel и AMD. *CNEWS*, 7.7.2020. [https://www.cnews.ru/news/top/2020-07-07_mvd_potratit_270_millionov], luettu 8.7.2020.

Воейков, Денис: Власти хотят признавать «железо» российским за деньги. В этой идее нашлись «коррупциогенные факторы». *CNEWS*, 16.7.2021. [https://cnews.ru/link/n532505], luettu 28.7.2021.

Военный энциклопедический словарь *(ВЭС)*. Воениздат, Москва, 2007. [https://encyclopedia.mil.ru/encyclopedia/dictionary/list.htm], luettu 11.1.2021.

Гаврилюк, Анастасия & Шестоперов, Дмитрий: Отступный интернет Законопроект о бесплатном доступе к значимым сайтам предложено доработать. *Коммерсантъ* №38 от 05.03.2021. [https://www.kommersant.ru/doc/4713549], luettu 28.7.2021.

Гаврилюк, Анастасия: «Суверенный рунет» сочли угрозой стабильности. Операторы критикуют новые требования Роскомнадзора. *Коммерсантъ* №132, 29.07.2021. [https://www.kommersant.ru/doc/4919761?from=main_9], luettu 29.7.2021.

Герасимов, В.В.: Организация обороны Российской Федерации в условиях применения противником «традиционных» и «гибридных» методов ведения войны. *Вестник Академии военных наук*, № 2 (55) 2016, с. 19–23

Герасимов, Валерий: Развитие военной стратегии в современных условиях. Задачи военной науки. *Вестник Академии военных наук*, № 2 (67) 2019, с. 6–1.

Герасимова, В.В.: Основные тенденции развития форм и способов применения вооруженных сил, актуальные задачи военной науки по их совершенствованию. *Вестник Академии военных наук*, № 1 (42) 2013, с. 24-29.

Гордеев, Владислав: Счетная палата не увидела прорывного эффекта от особых экономических зон. *РБК*, 9.4.2020. [https://www.rbc.ru/economics/09/04/2020/5e8eb2679a79477a36b61c5f], luettu 8.7.2020.

Дылевский И. Н., Запивахин, В. О., Комов С. А., Петрунин, А. В. & Эльяс, В. П.: Военно-политические аспекты государственной политики Российской Федерации в

области международной информационной безопасности. *Военная мысль* № 1/2015, с. 11–17.

Картаполов, А.В.: Уроки военных конфликтов, перспективы развития средств и способов их ведения. Прямые и непрямые действия в современных международных конфликтах. *Вестник Академии военных наук*, № 2 (51) 2015, с. 26–36.

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

Колесниченко, Александр: Андрей Крутских: с кибербезопасностью все так же, как с ядерным оружием. *Аргументы и Факты*, 25.5.2017. [https://aif.ru/society/safety/andrey_krutskih_s_kiberbezopasnostyu_vse_tak_zhe_kak_s_yadernym_oruzhiem], luettu 4.1.2021.

Корченкова, Наталья & Тишина, Юлия: Суверенный рунет вышел на связь С критикой законопроекта выступила РСПП. *Коммерсантъ,* №23 08.02.2019. [https://www.kommersant.ru/doc/3875941?from=main_4], luettu 28.7.2021.

Криворучко, Владимир: Вооружение в лабиринтах программ. *Военно-промышленный курьер*, 18.06.2020. [https://vpk.name/news/411648_vooruzhenie_v_labirintah_programm.html], luettu 8.7.2020.

Лукацкий, Алексей: *Бизнес без опасности*. Blogi. [https://lukatsky.blogspot.com/], luettu 28.7.2021.

Махутов, Н. А., Балановский, В.Л. & Подъяконов, В.М.: Обеспечение безопасности высокорисковых критически и стратегически важных объектов городской инфраструктуры в условиях появления новых видов угроз. *Вестник Академии Военных Наук*, № 1 (70) 2020, с. 31–36.

Махутов, Н.А., Резников, Д.О., Петров, В.П. Особенности обеспечения безопасности критических Инфраструктур. *Безопасность в техносфере*, №1 (январь–февраль 2014), с. 3–14.

Полякова, Виктория: СМИ узнали о возможном росте цен на домашний интернет и ТВ на 15–20%. *РБК* 26 июл 2020. [https://www.rbc.ru/technology_and_media/26/07/2020/5f1cd34d9a79471490c2fa3e], luettu 5.1.2021.

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

РИА Новости: Матвиенко призвала более четко регулировать интернет-пространство. *РИА Новости*, 19.4.2021 [https://ria.ru/20210419/matvienko-1728942339.html], luettu 29.7.2021.

РИА новости. Шойгу рассказал, как прозападная оппозиция "лезет" на военные объекты. *РИА новости*, 25.3.2020. [https://ria.ru/20200325/1569119235.html], luettu 6.5.2020.

Роскомсвобода: «Китаизация» Рунета входит в активную фазу и начнётся с точек обмена трафиком. *Роскомсвобода*, 18.8.2017. [https://roskomsvoboda.org/31224/], luettu 17.5.2019.

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

Селиванов, А.А. & Чварков, С.В.: О стратегии и концепции ассиметричных действий. *Вестник академии военных наук*, № 3 (72) 2020, с. 57–63.

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

Суровикин, С.В. & Кулешов, Ю.В.: Особенности организации управления межвидовой группировкой войск (сил) в интересах комплексной борьбы с противником. *Военная мысль*, № 8 (2017), с. 5–8.

Суровикин, С.В.: Формы применения и организация управления межвидовой группировкой войск (сил) на театре военных действий. *Вестник Академии военных наук*, №. 1 (46) 2014, с. 40–43.

Тадтаев, Георгий: Путин заявил об угрозе разрушения общества из-за интернета. *РБК*, 4.3.2021. [https://www.rbc.ru/politics/04/03/2021/6040c97c9a7947263f812b1c?from=from_main_6], luettu 28.7.2021.

Фадеев, А. С. & Ничипор, В. И.: Военные конфликты современности, перспективы развития способов их ведения. прямые и непрямые действия в вооруженных конфликтах XXI века. *Военная Мысль*, № 9 2019, с. 33–41.

Хабибрахимов, Альберт: «Сбербанк» стал совладельцем Mail.ru Group и Rambler Group, Андрей Андреев продал Badoo: заметные сделки 2019 года. *VC.ru*, 2.1.2020 [https://bit.ly/377BTby], luettu 28.7.2021.

Шаламберидзе Е.Г.: Теоретические вопросы развития политики национальной обороны России в условиях мирного времени с использованием системы мер невоенного и военного характера. *Вестник Академии военных наук*, № 4 (37) 2011, с. 35–43.

Шаламберидзе Е.Г.: Национальная оборона Российской Федерации: стратегические задачи и возможные перспективы. *Вестник Академии военных наук*, № 4 (41) 2012, с. 30–37.

Чекинов, С. Г. & Богданов, С. А.: Асимметричные действия по обеспечению военной безопасности России. *Военная Мысль*, № 3 2010, с. 13–22.

Черненко, Елена: «Без договоренностей глобального характера эту проблему не решить» Глава нового департамента МИД РФ Андрей Крутских о конфронтации в интернете. *Коммерсантъ*, №33 от 25.02.2020. [https://www.kommersant.ru/doc/4267456], luettu 8.7.2020.

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

Шувертков, Валерий: Систему ПВО ОДКБ еще предстоит создавать. *Воздушно-космическая сфера*, 2015, No. 3, с. 46–49.

2.3 Viralliset julkaistut asiakirjat

ГОСТ: *ГОСТ 28806-90. Качество программных средств. Термины и определения.* [https://meganorm.ru/Data2/1/4294825/4294825913.pdf], luettu 7.7.2020.

ГОСТ: *ГОСТ Р 51897-2011. Менеджмент риска. Термины и определения. Дата введения 2012-12-01.* [http://docs.cntd.ru/document/gost-r-51897-2011], luettu 7.7.2020.

ГОСТ: *ГОСТ Р 56111-2014. Интегрированная логистическая поддержка экспортируемой продукции военного назначения.* [http://cals.ru/sites/default/files/downloads/56111_.pdf], luettu 7.7.2020.

ПП-127a: Постановление Правительства РФ от 8 февраля 2018 г. N. 127 ”*Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений* (с изменениями от 13 апреля 2019 г.) [http://pravo.gov.ru/proxy/ips/?docbody=&nd=102460750], luettu 22.2.2021.

ПП-127b: Постановление Правительства РФ от 12 февраля 2020 г. N 127 ”*Об утверждении Правил централизованного управления сетью связи общего пользования*”. [http://www.consultant.ru/document/cons_doc_LAW_345574/], luettu 14.5.2020.

Президент России: Указ о национальных целях развития России до 2030 года. *Kremlin.ru* 21.7.2020. [http://kremlin.ru/events/president/news/63728], luettu 31.7.2020.

Президиум Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам: *Паспорт федерального проекта Информационная безопасность - Национальная программа ”Цифровая экономика Российской Федерации” от 6 мая 2019 года.* [https://files.data-economy.ru/Docs/Pass_Cybersecurity.pdf], luettu 3.1.2021

РП-1632: Распоряжение Правительства РФ от 28.07.2017 N 1632-р *“Об утверждении программы "Цифровая экономика Российской Федерации"*. [http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf], luettu 23.01.2018.

РП-788: Распоряжение Правительства Российской Федерации от 30 апреля 2015 г. N 788-р ”*О подписании Соглашения между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности*”. [http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=620700#046323 5836450268], luettu 27.4.2020.

Указ-203: Указ Президента РФ от 09.05.2017 N 203 “*О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы*”. [https://www.garant.ru/products/ipo/prime/doc/71570570/], luettu 15.5.2019.

Указ-2976: Указ Президента РФ 25 декабря 2014 г., № Пр-2976. *Военная доктрина Российской Федерации.* [http://base.garant.ru/70830556/], luettu: 21.3.2019

Указ-355: Указ Президента РФ от 2.6.2019 N 355 “Об основах государственной политика Российской Федерации в области ядерного сдерживания”. [http://www.kremlin.ru/acts/bank/45562], luettu 30.12.2020.

Указ-490: Указ Президента РФ от 10.10.2019 N 490 “*О развитии искусственного интеллекта в Российской Федерации (вместе с ”Национальной стратегией развития искусственного интеллекта на период до 2030 года*”. [http://www.consultant.ru/document/cons_doc_LAW_335184/], luettu 11.1.2021.

Указ-640: Указ Президента РФ от 30.11.2016 N 640 “*Об утверждении Концепции внешней политики Российской Федерации*”. [http://www.consultant.ru/document/cons_doc_LAW_207990/], luettu 8.1.2021.

Указ-646: Указ Президента РФ от 05.12.2016 N 646 *“Об утверждении Доктрины информационной безопасности Российской Федерации*”. [http://www.consultant.ru/document/cons_doc_LAW_208191/], luettu 5.5.2020.

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

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

ФЗ-5485-1: Федеральный закон от 21.07.1993 N 5485-1 "*О государственной тайне*" [http://www.consultant.ru/document/cons_doc_LAW_2481/], luettu 29.1.2021.

ФЗ-90: Федеральный закон от 01.05.2019 № 90-ФЗ *"О внесении изменений в Федеральный закон ”О связи” и Федеральный закон ”Об информации, информационных технологиях и о защите информации”*. [http://www.consultant.ru/document/cons_doc_LAW_323815/], luettu 8.5.2019.

Центральный банк российской федерации: *Внешняя торговля Российской Федерации услугами - 2019*. Статистический сборник. Банк России, Москва, 2020. [https://www.cbr.ru/statistics/macro_itm/svs/], luettu 12.1.2021.

Puolustusvoimien tutkimuslaitos

Ylöjärven toimipiste
Esikunta, asetekniikkaosasto, räjähde- ja suojelutekniikkaosasto
PL 5, 34111 Lakiala

Riihimäen toimipiste
Doktriiniosasto, informaatiotekniikkaosasto, tutkimussuunnitteluyksikkö
PL 10, 11311 Riihimäki

Tuusulan toimipiste
Toimintakykyosasto
PL 5, 04401 Järvenpää

Puh. 0299 800

puolustusvoimat.fi > Tietoa meistä > Tutkimuslaitos

ISBN 978-951-25-3211-7 (painettu)
ISBN 978-951-25-3212-4 (verkkojulkaisu)
ISSN 2342-3129 (painettu)
ISSN 2342-3137 (verkkojulkaisu)