VENÄJÄN KYBERVAIKUTTAMINEN UKRAINAN SODASSA 2014–2021

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Tieto- ja viestintätekniikan insinööri (AMK)

Kevät 2023

Jere Tani

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tieto- ja viestintätekniikan insinööri (AMK) Tiivistelmä
Tekijä Jere Tani Vuosi 2023
Työn nimi Venäjän kybervaikuttaminen Ukrainan sodassa 2014–2021
Ohjaaja Ismo Turve

Venäjä suoritti Krimin niemimaan laittoman miehityksen helmikuussa 2014, joka laajeni myöhemmin samana keväänä Ukrainan itäosissa käynnistyneeseen sotaan. Tätä sotaa on jatkunut nyt yhdeksän vuotta, ja sitä on käyty kineettisen sodankäynnin ohella aktiivisesti myös kybertoimintaympäristössä. Tämän tutkimuksen tarkoituksena oli selvittää, millaista kybervaikuttamista Venäjä suoritti Ukrainan sodassa vuosina 2014–2021.

Tämä tutkimus on luonteeltaan kvalitatiivinen eli laadullinen, jossa käytettiin tutkimusmenetelminä kahta erityyppistä sisällönanalyysiä. Tutkimus toteutettiin mukautetun IMRD-mallin mukaisesti, jossa tutkijan omaa pohdintaa kuljetettiin vuoropuhelun omaisesti tutkimusaineiston mukana koko tutkimuksen läpi. Keskeisin aineisto koostui avoimesti saatavilla olevista tutkimuksista ja kirjallisuudesta, Venäjän valtion virallisasiakirjoista, sekä tilastoista ja ajatushautomoiden julkaisuista.

Tutkimuksen yhteydessä kybervaikuttaminen määriteltiin tarkoittavan kybertoimintaympäristössä toteutettavaa, kohdetietojärjestelmiin ja -verkkoihin kohdistettavaa sellaista toimintaa, jolla pyritään häiritsemään tai rajoittamaan niiden käyttöä. Venäjän laaja kybertoiminnan koulutusjärjestelmä luo pohjan Venäjän kybervaikuttamiskyvylle. Valtion strategisen tason asiakirjoissa luodaan toimintaedellytykset rajat ylittäville hyökkäyksellisille toimille. Kyberuhkatoimijoiden keskinäinen valtataistelu sekä yhteiskoordinoinnin puute vaikuttavat kuitenkin negatiivisesti operaatioiden menestykseen.

Venäjän kyberuhkatoimijoiden kohteet sekä käytetyt menetelmät poikkesivat toimijoiden ja virastojen kesken vuosina 2014–2021. Venäjän sotilastiedustelu GRU:n kybervaikuttamisen kohteena oli ensisijaisesti kriittinen infrastruktuuri, jolla pyrittiin todennäköisesti edesauttamaan Venäjän asevoimien kineettistä sodankäyntiä. Turvallisuuspalvelu FSB keskitti kybervaikuttamisen Ukrainan poliittisen järjestelmän horjuttamiseen, jolla luotiin yhteiskunnallista epävakautta. Tutkimuksen yhteydessä ei havaittu ulkomaan siviilitiedustelupalvelu SVR:n alaisiin kyberuhkatoimijoihin linkittyviä kyberoperaatioita.

Kyberhyökkäykset käynnistyvät usein tietojenkalasteluoperaatioilla. Näin ollen kyberhyökkäyksiltä suojautumisen keskiössä ovat laitteiden, palveluiden ja tietojärjestelmien käyttäjät sekä heidän tietoturvallisuustietoisuutensa lisääminen.

Avainsanat Venäjä, Ukrainan sota, kybervaikuttaminen, kybersodankäynti
Sivut 81 sivua ja liitteitä 0 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Information and Communication Technology (BEng) Abstract
Author Jere Tani Year 2023
Subject Cyber Influence in the Russo-Ukrainian War in 2014-2021
Supervisor Ismo Turve

Russia conducted an illegal occupation of the Crimean Peninsula, Ukraine in February 2014, which later in the spring expanded into war in eastern Ukraine. This war has now been ongoing for nine years, and it has been fought, not only through kinetic warfare, but also actively in the cyber domain. The purpose of this study is to examine the nature of the cyber influence operations in the Russo-Ukrainian War between 2014 and 2021?

This study is qualitative in nature, using two different types of content analysis as research methods. The research was conducted according to a modified IMRD model, where the researcher's own reflections were carried along in a dialogue-like manner throughout the entire study. The data consisted of openly available research and literature, official documents and doctrines from the Russian government, as well as statistics and publications from think tanks.

Cyber influence was defined in this study as a form of activity that takes place in the cyberspace, with the aim of causing disruption or hindrance to the usage of targeted information systems and networks. Russia has an extensive system for training and recruiting cyber professionals, which serves as the foundation for their cyber influence capabilities. The official governmental documents provide a framework for aggressive cross-border actions. However, the success of Russian cyber operations is negatively impacted by the internal power struggle among state authorities and a lack of joint coordination.

Russian cyber threat actors utilized various targets and methods, depending on the specific agency and actor involved. The Military Intelligence Agency (GRU) primarily targeted critical infrastructure, which was likely intended to support Russia's kinetic military operations. The Federal Security Service (FSB) focused on undermining Ukraine's political system, leading to social instability. The study did not detect any cyber threat activity associated with the Foreign Intelligence Service (SVR).

Cyberattack usually start with phishing operations, which is why users of devices, services, and information systems play a critical role in preventing such attacks. Therefore, it is recommended to enhance users' guidance on information security.

Keywords Russian Federation, Russo-Ukraine War, cyber influence, cyber warfare
Pages 81 pages and appendices 0 pages

Sisällys

1 Johdanto 1

2 Tutkimusasetelma 4

2.1 Tutkimuskysymykset 5

2.2 Tutkimuksen aiherajaus 6

2.3 Tutkimuksen rakenne 6

2.4 Tutkimuksen metodiikka 7

2.5 Tutkimuksen käsitteet 8

2.6 Tutkimuksen lähdeaineisto 10

2.7 Tutkimusasetelman kritiikki 10

2.8 Aikaisempi tutkimus 13

3 Kybervaikuttaminen osana kybersodankäyntiä 14

3.1 Kybertoimintaympäristö 15

3.2 Kyberturvallisuus 19

3.3 Kybersodankäynti 22

3.4 Kybervaikuttaminen 26

3.5 Kybersuojautuminen ja kybertiedustelu 29

4 Venäjän valtiollinen kyky kybervaikuttamisoperaatioihin 30

4.1 Venäjän kybertoiminta osana turvallisuus- ja tiedustelupalveluita Neuvostoliiton hajoamisesta tähän päivään 31

4.2 Venäläinen kyberkoulutus ja rekrytointi Neuvostoliiton hajoamisesta tähän päivään 37

4.3 Venäläiset kyberuhkatoimijat (APT-ryhmät) 39

4.3.1 Gamaredon (FSB) 40

4.3.2 Turla (FSB) 41

4.3.3 Dragonfly (FSB) 43

4.3.4 APT29 (SVR) 44

4.3.5 APT28 (GRU) 45

4.3.6 Sandworm (GRU) 47

4.3.7 Ember Bear 48

4.4 Kybervaikuttaminen venäläisissä virallisasiakirjoissa 48

4.4.1 Venäjän federaation ulkopolitiikan konsepti (2016) 49

4.4.2 Venäjän federaation kansallinen turvallisuusstrategia (2021) 51
4.4.3 Venäjän federaation tietoturvallisuuden doktriini (2016) 54
4.4.4 Venäjän federaation kansainvälisen tietoturvallisuuden kenttää koskevat valtionpolitiikan perusperiaatteet (2021) 57
4.4.5 Venäjän federaation sotilasdoktriini (2014) 58
4.4.6 Luonnos Venäjän federaation kyberturvallisuuden strategisesta konseptista (2014) 60
5 Venäjän kybervaikuttamisoperaatiot Ukrainan sodassa 2014–2021 62
5.1 Kyberuhkatoimijoiden käyttämät kybervaikuttamisen menetelmät 63
5.2 Kybervaikuttamisen kohteet 66
5.3 Venäläiset kyberuhkatoimijat Ukrainan sodassa 2014–2021 68
5.4 Yhteenveto 75
6 Johtopäätökset 76
Lähteet 82

1 Johdanto

> *”Ennakkovaroituksista huolimatta tämä aamu on ollut meille kaikille järkytys. Venäjä on massiivisesti laajentanut sotatoimia Ukrainassa ja nyt naamiot on riisuttu, vain sodan kylmät kasvot näkyvät. Suomi tuomitsee jyrkästi Venäjän toimenpiteet, ja sodankäynnin ja vaatii sotaisten toimien pikaista lopettamista. Me olemme tilanteen tasalla, ja myöskin pysymme.”*
>
> Suomen tasavallan presidentti Sauli Niinistö, Helsingissä 24.2.2022,
> Ukrainan laajamittaisen sodan ensimmäisen päivän aamuna.

Näillä sanoilla tasavallan presidentti ja Puolustusvoimien ylipäällikkö Sauli Niinistö kuvasi Venäjän aloittamaa laajamittaista hyökkäyssotaa valtioneuvoston tiedotustilaisuudessa (2022), vain tunteja aggressiivisten hyökkäystoimien alkamisen jälkeen. Tätä samaista hetkeä Venäjän federaation presidentti Vladimir Putin muotoili myöhemmin sotilaallisen erityisoperaation *(ven. Специальная военная операция)* alkamiseksi, jonka tarkoituksena on Ukrainan demilitarisointi ja denatsifiointi (BBC News Russia, 2022).

Huolimatta presidentti Niinistön ja koko läntisen maailman vaatimuksesta sotatoimien pikaiseksi lopettamiseksi, sota jatkuu edelleen tätä tutkimusta tehdessä huhtikuussa 2023. Sota on myös saavuttanut ensimmäisen vuosipäivänsä. Ensimmäisen juuri siksi, koska välittömiä merkkejä sodan päättymisestä ei ole nähtävissä. Naton pääsihteeri Jens Stoltenberg totesi maaliskuussa 2023 Helsingissä, että Vladimir Putin ei ole valmistautumassa rauhanneuvotteluihin, vaan ennemminkin entistä julmempaan sodankäyntiin (NATO, 2023). Venäjän ja presidentti Putinin tavoitteena oli suorittaa nopea, päivistä viikkoihin kestävä erikoisoperaatio tarkoituksenaan horjuttaa Ukrainaa siten, että sen valtionjohto saataisiin syrjäytettyä vallasta ja vaihdettua hallinto venäläismieliseksi. Tässä tavoitteessa epäonnistuminen ja hyökkäyssodan pitkittyminen ovat myötävaikuttaneet lännen asettamien pakotteiden johtamaan Venäjän talouden heikkenemiseen, liikekannallepanoon ja sen myötä sodanjulistukseen. Laajamittaisen sodan pitkittymisen seurauksena ilman rauhanomaista ratkaisua Venäjä ja presidentti Putin ovat menettäneet sellaisen selkeästi osoitettavan ulospääsyn tästä tilanteesta, jolla sekä presidentti että Venäjän valtio pystyisivät säilyttämään kasvonsa. Tämä yhtälö tekee Venäjän aggressiosta entistäkin vaarallisemman.

Ukrainassa helmikuussa 2022 käynnistynyt laajamittainen sota juontaa juurensa jo vuodesta 2014, kun Venäjä miehitti Krimin niemimaan sekä Ukrainan itäosat. Siitä lähtien Venäjä on tukenut alueille jääneitä venäläismielisiä joukkoja niin sotilaallisesti kuin myös taloudellisesti. Ukraina ei ollut tuolloin vastaavalla tavalla sotilaallisesti valmistautunut, kuin mitä se oli helmikuussa 2022. Tämä puolestaan johti keväällä 2014 alueiden lähes välittömään menetykseen ja puolustavien joukkojen aseista riisumiseen.

Globaalisti nouseva trendi datamäärien kasvamisesta, tieto- ja viestintäjärjestelmien integroinnista, avointen tietoverkkojen käytöstä sekä niiden rinnalla lisääntyneestä energiariippuvuudesta ovat muodostaneet uudenlaisen, digitaalisessa ympäristössä vaikuttavan uhkapotentiaalin. Kineettisen sodankäynnin lisäksi vuodesta 2014 Ukrainan maaperällä käytyä sotaa ovat leimanneet myös kybersodankäynnin muodot. Kyberhyökkäysten suorittajia on yleisesti haastavaa, ellei miltei mahdotonta faktuaalisesti identifioida. Joissain tapauksissa yksi taho tai organisaatio astuu esiin ja ilmoittautuu hyökkäyksen suorittajaksi. On kuitenkin tavallista, että kukaan ei suoranaisesti ota vastuuta, erityisesti valtiollisisten kyberhyökkäysten osalta. Näissä tapauksissa operaatio on voinut olla omiaan palvelemaan jonkun tietyn tahon poliittisia, taloudellisia, yhteiskunnallisia tai sotilaallisia tavoitteita.

Yksi lähihistorian tunnetuimmista kybervaikuttamisoperaatioista kohdistui Yhdysvaltojen vuoden 2016 presidentinvaaleihin. Tuolloin kilpailu käytiin republikaanien ehdokkaan Donald Trumpin sekä demokraattien Hillary Clintonin välillä. Pitkin vaalikampanjointia yhdysvaltalaisilla keskustelualustoilla käytiin Clintonia alentavaa, ja toisaalta myös Trumpia ylistävää keskustelua hyvin monipuolisilla väittämillä. Tämän kybervaikuttamisoperaation taustalla oli kaksi Venäjän sotilastiedustelusta vastaavan tiedustelupäähallinnon GRU:n *(ven. ГРУ, Главное разведывательное управление)* alaisuudessa toimivaa valtiollista kyberuhkatoimijaa, eli APT-ryhmää. (Yhdysvaltain liittovaltion hallinto, 2018)

Toinen ryhmistä lähestyi Hillary Clintonin vaalikampanjassa mukana olleita henkilöitä erilaisilla tietojenkalasteluviesteillä. Näiden avulla ryhmä onnistui varastamaan useiden henkilöiden käyttäjätunnukset ja salasanat, ja käyttämään niitä edelleen sähköpostiviestien varastamiseen sekä muihin tietojärjestelmiin murtautumiseen. Kaapattuja sähköposteja sekä

niissä olleita asiakirjoja hyödynnettiin myös demokraattisen puolueen tietoverkkoihin murtautumiseen. Näin pystyttiin käyttäjien huomaamatta seuraamaan tietojärjestelmien käyttöä sekä asentamaan satoja haittaohjelmia, joiden avulla pystyttiin varastamaan lisää salasanoja sekä ylläpitämään pääsy näihin verkkoihin. Toinen ryhmä puolestaan murtautui Yhdysvaltain osavaltioiden vaalilautakuntien, ulkoministeriön sekä ohjelmistoja ja teknologiaa toimittavien yritysten tietojärjestelmiin. Tämän tarkoituksena oli varastaa näihin järjestelmiin tallennettuja äänestäjätietoja. (Yhdysvaltain liittovaltion hallinto, 2018b)

Ryhmät perustivat yhdessä verkkosivuston, jossa julkaistiin tietomurtojen yhteydessä hankittuja asiakirjoja ja sähköpostiviestejä. Toiminta yritettiin peitellä siten, ettei sitä voisi yhdistää Venäjälle. Yhtenä peittelyn keinona kyberuhkatoimijat muun muassa ilmoittivat luomallaan verkkosivulla olevansa yhdysvaltalaisia yksityishenkilöitä. Tämän narratiivin tukemiseksi he käyttivät kuvitteellisia Facebook- ja Twitter-tilejä verkkosivunsa mainostamiseen. Kun Venäjän hallitusta alettiin julkisesti syyttää hyökkäysten organisoinnista, kyberuhkatoimijat loivat uuden kuvitteellisen identiteetin. Tällä identiteetillä julkaistiin englanninkielinen blogipostaus, jossa sen väitettiin olevan romanilainen yksityishenkilö. Kävi kuitenkin ilmi, että näitä blogikirjoituksessa olleita englanninkielisiä sanoja, fraaseja ja lauseita oli hetkeä aiemmin haettu kansainvälisestä hakukoneesta, Moskovassa sijaitsevalla ja GRU:n palvelimella toimivaa tietokonetta käyttäen. (Yhdysvaltain liittovaltion hallinto, 2018b)

Yhdysvaltojen keskeisimmät tiedustelu- ja turvallisuusviranomaiset National Security Agency (NSA), Central Intelligence Agency (CIA) ja Federal Bureau of Investigation (FBI) suorittivat yhteistutkinnan, jonka seurauksena Yhdysvalloissa nostettiin heinäkuussa 2018 syytteet 12 Venäjän sotilastiedustelusta vastaavan tiedustelupäähallinto GRU:n tiedustelu-upseeria vastaan. Tämä informaatio- ja kybervaikuttamisen kokonaisuus edesauttoi osaltaan sitä, että Donald Trump eteni vaalivoittoon ja Yhdysvaltain 45. presidentiksi. (FBI, 2017)

Ukrainan sodassa on vuodesta 2014 lähtien havaittu vastaavia operaatioita. Sotaan on sisältynyt muun muassa palvelunestohyökkäyksiä, tietojenkalasteluoperaatiota sekä merkittäviä datan tuhoamiseen pyrkineitä operaatioita. Tässä, Venäjän kybervaikuttamista Ukrainan sodassa käsittelevän tutkimussarjan ensimmäisessä osassa lukija perehdytetään

kybervaikuttamisen kokonaisuuteen, Venäjän valtiollisiin kyberuhkatoimijoihin, Venäjän kybertoimintaa ohjaaviin virallisasiakirjoihin sekä Ukrainan sodassa vuosina 2014–2021 havaittuihin kybervaikuttamisoperaatioihin. Tutkimussarjan seuraava osa käsittelee Venäjän kybervaikuttamista Ukrainan sodassa vuodesta 2022 lähtien.

Tällä tutkimuksella on pyritty tuottamaan lukijalle yhteen kokoava ja helposti ymmärrettävä kokonaisuus ajankohtaisesta ilmiöstä – Venäjän suorittamasta kybervaikuttamisesta Ukrainan sodassa vuosina 2014–2021. Tutkimus päätettiin tehdä suomen kielellä, koska se on kohdistettu ennen kaikkea kotimaiselle kohderyhmälle. Tutkija tiedostaa myös, että suomenkielistä, kybersodankäyntiä käsittelevää tutkimusta on tarjolla varsin rajallinen määrä. Tutkimuksen sijoittuessa akateemisesti alemman korkeakoulun tutkimustasolle, ei kielivalintaa ollut tarpeen tarkastella mahdollisen kansainvälisen näkyvyyden ja vaikuttavuuden näkökulmasta. Aihetta ei ole sellaisenaan aiemmin tutkittu opinnäytetöissä tai tutkielmissa. Tälle tutkimukselle ei ole ulkopuolista kolmannen osapuolen tilaajaa.

Tutkimuksen käännökset ovat lähdekielestä riippumatta tutkijan tekemiä. Alkuperäinen lähdeteksti avataan tarvittaessa sulkeissa käännöksen jälkeen. Sekä venäjän- että ukrainankielisessä translitteroinnissa noudatetaan SFS 4900 -standardin mukaista merkintätapaa. Mahdollisten muiden vieraskielisten käännösten osalta käytetään yksinkertaisuuden ja tunnistettavuuden vuoksi suomen kielen mukaista kirjoitusasua.

2 Tutkimusasetelma

Tutkimuksen tutkimusasetelma on keskeinen osa tutkimusta, sillä se auttaa tutkijaa suunnittelemaan tutkimuksen toteutuksen ja kertoo, miten tutkimuskysymykset pyritään ratkaisemaan. Tässä luvussa käsitellään tutkimuksen tutkimusasetelman eri osa-alueet.

Ensimmäisenä käsiteltävänä osa-alueena ovat tutkimuskysymykset. Alaluvussa 2.1 esitellään tutkimuksen päätutkimuskysymys sekä alakysymykset, joihin tutkimus pyrkii vastaamaan. Tutkimuskysymykset ohjaavat tutkimuksen suunnittelua sekä tutkijaa pitäytymään tutkimuksen kannalta keskeisissä asioissa.

Toisena osa-alueena käsitellään aiherajaus, jossa kuvaillaan tutkimuksen ajallinen ja temaattinen rajaus, sekä niiden merkitys tutkimuksen kannalta. Aiherajaus auttaa tutkijaa kohdistamaan tiedonhankinta tutkimuskysymysten ratkaisun kannalta oleelliseksi koettuihin teemoihin. Lisäksi huolellisesti ja harkiten tehty aiherajaus auttaa tutkijaa tuottamaan tiiviin ja tutkimuksen kannalta temaattisesti asiassa pitäytyvän tutkimusraportin.

Kolmantena osa-alueena käsitellään tutkimuksen rakennetta ja menetelmiä. Alaluvuissa 2.3 ja 2.4 esitellään tutkimuksen rakenne sekä siinä käytetyt tutkimusmenetelmät ja miksi ne on valittu. Valittavat tutkimusmenetelmät määräytyvät tutkimusaineiston ja tutkimuksen luonteen perusteella, jonka vuoksi niiden valinta on keskeinen osa tutkimuksen suunnittelua.

Alaluvussa 2.5. lukijalle esitellään tutkimuksen kannalta keskeiset käsitteet. Käsitteiden määrittely auttaa tutkijaa ymmärtämään tutkimuskohdetta ja sen merkitystä, sekä luo osaltaan myös lukijalle ymmärrystä käsiteltävästä aihealueesta. Alaluvussa 2.6. käsitellään tutkimuksen lähdeaineisto, jonka yhteydessä lukijalle esitellään tutkimusteemoittain sen aineiston alkuperä.

Itsereflektion kautta muodostettua tutkimusasetelman kritiikkiä ja pohdintaa esitellään alaluvussa 2.7. Siinä tutkija arvioi kriittisesti omaa tutkimusasetelmaansa sekä tunnistaa ympäristön tai tutkijan omien taustojen muodostavat erityispiirteet, jotka voivat mahdollisesti johtaa kognitiivisiin vinoumiin, ja joilla saattaa olla näin ollen vaikutusta tutkimukseen sekä sen tuloksiin. Lopuksi käsitellään tämän tutkimuksen tematiikkaan liittyvää aikaisempaa tutkimusta, joka auttaa tutkijaa ymmärtämään, mitä aiheesta on jo tutkittu ja millaisia tuloksia on saatu. Toisaalta tällä tutkija myös osoittaa perehtyneensä laaja-alaisesti omaa tutkimustaan käsittelevään aihealueeseen.

2.1 Tutkimuskysymykset

Tämän tutkimuksen tutkimuskysymykset muodostuvat yhdestä päätutkimuskysymyksestä sekä kolmesta alatutkimuskysymyksestä. Alatutkimuskysymyksiin vastaamalla saadaan vastaus myös tutkimuksen päätutkimuskysymykseen.

Tutkimuksen päätutkimuskysymys:

1. *Millaista kybervaikuttamista Ukrainan sodassa havaittiin vuosina 2014–2021 ja mitkä kyberuhkatoimijat vastasivat kybervaikuttamisoperaatioista?*

Alatutkimuskysymykset:

1. *Mitä on kybervaikuttaminen?*
2. *Millainen on Venäjän valtiollinen kyky kyberoperaatioiden suorittamiseen?*
3. *Millaisia kybervaikuttamisen menetelmiä käytettiin ja millaisiin kohteisiin Venäjän valtiolliset kyberuhkatoimijat vaikuttivat Ukrainan sodassa vuosina 2014–2021?*

2.2 Tutkimuksen aiherajaus

Tämä tutkimus käsittelee Venäjän kybervaikuttamista Ukrainan sodassa vuosina 2014–2021. Tutkimus haluttiin rajata selkeästi helmikuussa 2022 käynnistyneen laajamittaisen hyökkäyssodan ja sitä tukeneiden kybervaikuttamisoperaatioiden ulkopuolelle. Näin ollen tutkimuksen ajallinen rajaus on tammikuusta 2014 heinäkuuhun 2021 saakka. Tämä tutkimus on rajattu käsittelemään Venäjän suorittamia, Ukrainan valtionhallintoon, sotilaskohteisiin, kriittiseen infrastruktuuriin sekä merkittäviin yrityksiin kohdistuneita hyökkäyksellisiä toimia, eli kybervaikuttamista.

Tästä tutkimuksesta on rajattu pois muut vaikuttamisen muodot sekä pienempiin yrityksiin, yksittäisiin kansalaisiin tai muuten strategisesti vähäisemmän merkityksen kohteisiin kohdistettu kybervaikuttaminen. Tutkimuksessa ei käsitellä Venäjän kybersuojautumista eikä Ukrainan tai länsivaltioiden kybertoimia.

2.3 Tutkimuksen rakenne

Tämä tutkimus on toteutettu mukautetun IMRD-mallin (*Introduction, Methods, Results, Discussion*) rakenteella: johdanto, tutkimusasetelma, tutkimustulokset vuoropuhelussa teorian kanssa sekä pohdinta ja johtopäätökset (Vilkka, 2021, s. 158). Tyypillisestä IMRD-mallista poiketen pohdintaa kuljetetaan vuoropuhelun omaisesti mukana koko tutkimuksen

läpi. Pohdinnat ja eri lukujen yhteydessä tehdyt yhteenvedot yhdistyvät tutkimuksen lopussa tehtävissä pohdinnoissa ja johtopäätöksissä. Tutkimuksen rakenteeksi on valittu IMRD-malli, jotta lukijalla on mahdollisuus löytää haluamansa tieto ilman koko tutkimuksen läpikäymistä. Rakennemallin valinnalla osoitetaan aihealueen aukottomuus sekä se, että tutkija aikoo ratkaista esittämänsä tutkimusongelman.

Tutkimus voidaan teemallisesti jakaa kolmeen osaan ja sen rakenne seuraa alatutkimuskysymysten järjestystä. Kolmannessa pääluvussa tarkastellaan kybervaikuttamista teoreettisesta näkökulmasta. Kybervaikuttamisen sekä yleisesti vaikuttamisen käsitteitä on julkisten keskustelujen yhteyksissä käytetty kovin värikkäästi. Tästä johtuen kybervaikuttamisen termi koettiin oleelliseksi käsitellä tutkimuksen aluksi.

Neljännessä pääluvussa analysoitavan Venäjän valtiollisen kyberoperointikyvyn käsittely alkaa Venäjän virallisasiakirjoja tutkimalla. Näin saadaan hahmotettua lukijalle Venäjän asevoimia ja turvallisuusviranomaisia ohjaavista asiakirjoista muodostettu teoreettinen viitekehys. Jotta suorituskykyä kyetään määrittelemään, on olennaista kuvata myös potentiaaliset kyberoperaatioiden suorittajat. Näin ollen neljännessä pääluvussa esitellään myös Venäjän tietoturvallisuuden ja kybertoiminnan lähihistorian kehitys, sekä aktiivisina olevat Venäjän valtiolliset kyberuhkatoimijat.

Tutkimuksen viidennessä pääluvussa perehdytään Ukrainan sodassa vuosina 2014–2021 havaittuun kybervaikuttamiseen. Kuudennessa pääluvussa esitellään tutkijan omaa, aiemmat luvut yhteen kokoavaa pohdintaa tutkitusta ilmiöstä. Tässä yhteydessä lukijalle esitetään tutkimuksen perusteella saadut vastaukset kuhunkin tutkimuskysymykseen, sekä tämän tutkimuksen muodostamiin jatkotutkimusaiheisiin.

2.4 Tutkimuksen metodiikka

Metodologia on oppijärjestelmä hyväksi havaituista metodeista, kuten tieteenfilosofian, teoriapohjan, aineistonhankintamenetelmän ja tutkimusmenetelmän muodostamasta kokonaisuudesta (Vilkka, 2021, s. 34). Tämä tutkimus on luonteeltaan laadullinen, eli kvalitatiivinen ja kuuluu metodologisesti aristoteeliseen tutkimusperinteeseen. Niin

kybervaikuttamisen käsitteen muodostus, kuin myös venäläisistä virallisasiakirjoista tulkittava valtiollinen kybertoiminnan ohjaus ovat tutkijan subjektiivisia tulkintoja todellisuudesta, ja tutkimus pyrkii näin ollen niiden osalta ymmärtämään tutkittavaa ilmiötä.

Tutkimuksen aineisto perustuu pääosin kirjallisiin dokumentteihin sekä mediajulkaisuihin. Tämänkaltaisen aineiston pohjalta tehtävässä tutkimuksessa on tyypillistä tehdä useiden eri lähteiden kautta hankittavien tietojen vertailua ja lähdekriittistä arviointia, tietojen yhdistelemistä sekä tarvittaessa muokkaamista. Tähän tutkimukseen kerättiin julkisesti saatavalla olevista asiakirjoista ja mediajulkaisuista mahdollisimman laaja aineisto, jolla pyrittiin vastaamaan asetettuihin tutkimuskysymyksiin.

Analyysimenetelminä käytettiin kahta erityyppistä sisällönanalyysiä. Sisällönanalyysi on laadullisen tutkimuksen menetelmä, jolla tutkittavasta ilmiöstä pyritään esittämään tiivis ja selkeä kuvaus. Sisällönanalyysiä on kaikkiaan kolmea eri tyyppiä, joista jokainen luo analyysin tekoon erilaiset lähtökohdat. Luonteeltaan induktiivisessa, eli *aineistolähtöisessä sisällönanalyysi*ssä aineisto ohjaa analyysin tekoa ja tulokset syntyvät tutkimusaineiston perusteella. *Teoriaohjaava sisällönanalyysi*, eli abduktiivisen analyysi on aineistolähtöistä, jossa teoriaa käytetään analyysin apuna. (Vilkka, 2021, ss. 132–136)

Tutkimuksen neljännessä luvussa haetaan osavastauksia Venäjän valtiolliselle kybervaikuttamiskyvylle analysoimalla venäläisiä virallisasiakirjoja sekä valtiollisia kyberoperointi- ja -koulutusrakenteita induktiivisesti, eli aineistolähtöisellä sisällönanalyysilla. Venäjän suorittamia kybervaikuttamisoperaatioita analysoidaan viidennessä luvussa teoriaohjaavan sisällönanalyysin periaattein, eli abduktiivisesti.

2.5 Tutkimuksen käsitteet

Kineettisellä sodankäynnillä tarkoitetaan tässä tutkimuksessa tavanomaisen sodankäynnin muotoja, jossa sotaa käydään kahden tai useamman valtion välillä ja joissa kohteeseen vaikutetaan suoraa aseellista voimaa käyttäen.

Kriittisellä infrastruktuurilla tarkoitetaan niitä järjestelmiä, palveluita ja toimintoja, jotka ovat elintärkeitä yhteiskunnan toimivuudelle ja turvallisuudelle. Tällaisia ovat esimerkiksi sähkö- ja vesihuolto, tietoliikenneverkot, terveydenhuoltojärjestelmät, liikennejärjestelmät, pankki- ja rahoitusjärjestelmät, elintarvikehuolto sekä turvallisuusviranomaisten ja valtionhallinnon toiminta.

Länsivallat ja *länsimaat* käsitteiden määritellään Maïchen (2015) mukaan alkaneen historiallisesti antiikin kreikkalais-roomalaisesta sivilisaatiosta ja kristinuskon synnystä, jonka myötä sen koetaan liittyvän suoraan Euroopan historiaan. Länsimaalainen kulttuuri on sittemmin levinnyt Euroopasta muun muassa Australiaan ja Pohjois-Amerikkaan. Tässä tutkimuksessa *länsimailla* tarkoitetaan eurooppalaisten valtioiden lisäksi länsimaalaisen ja eurooppalaisen kulttuurin omaksuneita maita, kuten Yhdysvaltoja. Vaikka Venäjä, Valko-Venäjä sekä Ukraina kuuluvat maantieteellisesti osaksi Eurooppaa, ei niitä käsitellä tässä tutkimuksessa länsimaina, vaan kutakin valtiota kuvataan omina yksilöinään.

Venäjämielisellä tarkoitetaan sellaista valtiota tai ryhmittymää, jotka tukevat venäläistä ideologiaa ja sitä kautta Venäjän hyökkäyssotaa Ukrainassa. Tässä tutkimuksessa käsiteltäviä tällaisia toimijoita ovat Ukrainan itäosissa toimineet separatistijoukot, Valko-Venäjä sekä erilaiset hacktivist-ryhmät. Vaikka esimerkiksi Pohjois-Korean ja Iranin tunnistetaan tukeneen Venäjää muun muassa asetoimituksilla, eivät kyseiset valtiot sisälly tämän tutkimuksen *Venäjämielisen* määritelmän piiriin, tutkimuksen kyber-aiherajauksen vuoksi.

Venäjän APT-ryhmillä eli *kyberuhkatoimijoilla* tarkoitetaan Venäjän valtiollisessa ohjauksessa toimivia, suunnitelmallista valtiollista kybervakoilua ja -operaatioita suorittavia toimijoita.

Venäjän tiedustelu- ja turvallisuuspalveluilla tarkoitetaan Venäjän federaation puolustusministeriön alaista ja sotilastiedustelusta vastaavaa tiedustelupäähallinto GRU:ta *(ven. ГРУ, Главное разведывательное управление*), ulkomaan siviilitiedustelupalvelu SVR:ää *(ven. СВР*, *Служба внешней разведки)* sekä turvallisuuspalvelu FSB:tä *(ven. ФСБ, Федера́льная слу́жба безопа́сности)*. Tiedustelupäähallinnosta käytetään globaalisti GRU:n lisäksi myös nimitystä GU. Tässä tutkimuksessa tiedustelupäähallintoa kuvataan kuitenkin yksiselkoisuuden vuoksi lyhenteellä GRU.

Ukrainan sodalla tarkoitetaan tämän tutkimuksen yhteydessä keväällä 2014 Ukrainan itäosissa ja Krimin niemimaalla käynnistynyttä Venäjän hyökkäyssotaa. Puhuttaessa helmikuussa 2022 käynnistyneestä laajamittaisesta hyökkäyssodasta, esitetään se selkeästi esimerkiksi ajankohtaan tai laajamittaisuuteen sitoen.

2.6 Tutkimuksen lähdeaineisto

Kybervaikuttamisen käsite vaihtelee erikielisten julkaisujen kesken. Tutkittaessa kybervaikuttamista suomalaisesta näkökulmasta ja tutkimuksen suuntautuessa ensisijaisesti suomalaiseen käyttöön, on kolmannen pääluvun käsitemäärittelyssä valittu lähdeaineistoiksi suomalainen kirjallisuus ja käsitemääritelmät. Näin saadaan varmistettua tutkimuksessa muodostuvien käsitteiden yhteensopivuus ja vertailtavuus Suomessa yleisesti käytössä olevan terminologian kanssa.

Tutkimuksen neljännessä pääluvussa käsiteltävän Venäjän kyberoperaatioiden suorittamiskyvyn pääasiallisena lähdeaineistona toimii Venäjän valtionhallinnon virallisasiakirjat sekä eri ajatushautomoiden ja viranomaisten tutkimusartikkelit. Tämän tutkimuksen viidennessä pääluvussa käsiteltävien Venäjän vuosina 2014–2021 Ukrainassa suorittamien kybervaikuttamisoperaatioiden pääasiallisena aineistona käytetään avoimista lähteistä saatavilla olevia, Venäjän kybervaikuttamista käsitteleviä tutkimusartikkeleita, kansainvälisiä viranomaislähteiden ja ajatushautomojen julkaisuja.

Tämän tutkimuksen aineisto on suomen, englannin, venäjän sekä ukrainan kielistä. Tutkimukseen mahdollisesti liittyvää muuta vieraskielistä aineistoa ei tutkijan kielitaidon takia kyetä hyödyntämään.

2.7 Tutkimusasetelman kritiikki

Tutkimuksessa tulisi aina arvioida tutkimusasetelman rakenne, aineiston riittävyys ja kattavuus, tutkimusmenetelmien kuvaus, menetelmien valinta tutkimukseen nähden, tutkimuskohteen määrittely sekä päättelyketjujen läpinäkyvyys. Yhtä lailla tärkeässä osassa on perusteellinen argumentaatio sekä sen teoriasidonnaisuus. (Toikko & Rantanen, 2009, ss.

121–129) Tässä tutkimuksessa luotettavuutta arvioidaan *riippuvuuden*, *varmistettavuuden*, *siirrettävyyden* sekä *luotettavuuden* käsitteiden kautta.

Riippuvuudessa on kyse tutkimusprosessin sekä käytettyjen menetelmien kuvaamisesta, kuten Sarajärvi ja Tuomi (2011) toteavat. Tämän tutkimuksen toisessa pääluvussa on esitelty tutkimuksessa käytetyt menetelmät sekä miten niitä on käytetty. Tutkimuksen kieliasua ja rakennetta on viimeistelty usean tarkastelun myötä, jotta saavutettaisiin mahdollisimman selkeästi tulkittavissa oleva ja eheä kokonaisuus.

Luotettavuudella tarkoitetaan Sarajärven ja Tuomen (2011) mukaan muun muassa syiden ja seurausten selkeää kuvaamista, joka muodostaa tutkimuksen sisäisen validiteetin. Tämän tutkimuksen kriittistä arviointia luotettavuuden näkökulmasta hankaloittaa se, että Venäjän toteuttamasta kybervaikuttamisesta ei kyetä varmuudella osoittamaan, että se on johtunut virallisasiakirjoissa esitetyistä syistä. Kybertoimintaympäristö itsessään luo eräänlaisen harmaan alueen, joka mahdollistaa hyökkääjälle periaatteellisesti täydellisen anonymiteetin. Tämä asettaa luotettavuuden näkökulmasta arvioinnin hankalaan tilanteeseen, sillä faktuaalisesti on miltei mahdoton osoittaa, että Venäjän kyberuhkatoimijat olisivat Ukrainaan kohdistettujen kyberhyökkäysten takana. Tässä tutkimuksessa tukeudutaankin globaalisti vallitseviin olettamuksiin sekä luotettaviksi osoittautuneiden asiantuntijoiden sekä asiantuntijaorganisaatioiden lausuntoihin.

Siirrettävyydellä tarkoitetaan tutkimustulosten yleistettävyyttä sekä siirrettävyyttä eri konteksteihin ja tilanteisiin, eli toisin sanoen ulkoista validiteettia. Koska laadullisessa tutkimuksessa tutkimusaineisto kerätään usein rajoitetulta joukolta henkilöitä tai yhdestä kontekstista, tulosten yleistettävyyteen liittyy erityisiä haasteita. Siirrettävyydellä pyritään varmistamaan, että tutkimustulokset ovat sovellettavissa myös muihin vastaaviin konteksteihin. On tärkeää, että tutkimuksen ulkopuolinen henkilö pystyy hahmottamaan ne raja-arvot, joiden sisällä tutkimustulokset on saavutettu. Tutkimustulokset tulee myös esittää selkeästi ja perustellusti, jotta niiden soveltuvuus muihin konteksteihin on helpompi arvioida. On kuitenkin huomioitava, että laadullisen tutkimuksen tulokset eivät välttämättä ole yleistettävissä samalla tavalla kuin kvantitatiivisen tutkimuksen tulokset, ja siirrettävyyteen liittyy aina tiettyjä rajoituksia. (Vilkka, 2021, ss. 155–156) Tämän

tutkimuksen osalta siirrettävyyteen on pyritty kuvaamalla mahdollisimman selkeästi tutkimuksessa käytetty aineisto, menetelmät sekä rajaukset. Huomionarvoista on, että tutkijan mahdollisten ennakko-odotusten sekä laadullisen tutkimuksen ominaispiirteitten vuoksi tutkimustulokset saattavat olla osittain puolueellisia. Tämä korostuu erityisesti induktiivisella lähestymistavalla toteutetussa sisällönanalyysissä, jossa tutkijan subjektiivinen rooli näyttelee isoa osaa. Tutkimuksen päättelyketjut on pyritty kuvaamaan mahdollisimman tarkasti, jotta toisella tutkijalla on mahdollisuus tulla samalla aineistolla eri johtopäätöksiin.

Varmistettavuudella tarkoitetaan sitä, että lähteet sekä tutkimusaineisto ovat läpinäkyviä sekä jäljitettävissä olevia, jotta ulkopuoliset tutkijat voivat arvioida tutkimuksen laatua sekä sen validiteettia. Tämä tutkimus noudattaa Hämeen ammattikorkeakoulun viittauskäytäntöjä, joka mahdollistaa ulkopuolisen henkilön tutustumisen lähdeaineistoon ja sen pohjalta tehtyihin analyyseihin.

Näiden neljän luotettavuutta arvioitavan käsitteen lisäksi on tärkeää huomioida myös se, että tutkijan kielitaito on mahdollistanut venäläisen sekä osittain ukrainalaisen aineiston rajoitetun hyödyntämisen. Vaikka käännökset käsittelevät tutkijan kielitaidon kannalta tunnettua aihepiiriä ja käännösten yhteydessä on hyödynnetty alaan soveltuvia tieteellisiä sanakirjoja, tulee tutkimusta tarkasteltaessa kuitenkin tiedostaa mahdolliset käännösvirheet, koska kyseessä ei ole tutkijan äidinkieli tai natiivilla tasolla puhuttu vieraskieli.

Virallisasiakirjojen osalta on tiedostettava, että ne ovat osaltaan myös valtion viestintäkeino, jolla kyetään niin halutessaan luomaan disinformaatiota toisille valtioille. Vaikkakin ne toimivat virallisina Venäjän valtion ja turvallisuusviranomaisten ohjausasiakirjoina, niin niitä ei niiden julkisuusleimansa vuoksi tule pitää absoluuttisena totuutena.

Ukrainan sodassa vuosina 2014–2021 esiintyneen Venäjän kybervaikuttamisen tutkimusaineisto on kerätty vahvistetuista, kansainvälisesti luotettaviksi todetuista lähteistä. Tutkimuksen osalta on kuitenkin tiedostettava se, että Ukrainan sodan saama medianäkyvyys ja siitä seurannut globaali mielenkiinto oli huomattavasti matalammalla tasolla vuosien 2014 ja 2021 välillä, verrattuna helmikuussa 2022 käynnistyneen laajamittaisen hyökkäyksen jälkeiseen aikaan. Tämä on osaltaan vaikuttanut myös

kybervaikuttamisoperaatioista julkisesti saatavilla olevan aineiston määrään ja laatuun. Aineistoa on ollut suhteellisesti vähemmän saatavilla ja se on ollut vähemmän yksityiskohtaista verrattuna helmikuun 2022 jälkeiseen aikaan. Toisaalta 2014–2021 välinen aineisto on saatavilla pääosin virallisista lähteistä ja näin ollen laadullisesti eheämpää, eikä tiedonhankintaa häirinnyt epävirallisten lähteiden muodostama disinformaation ja misinformaation mahdollisuus. Tutkimustulosten esittelyn yhteydessä on tuotu selkeästi esille sellaiset tapaukset, joissa on vahvistamattomia yksityiskohtia. Tällaisia ovat esimerkiksi kybervaikuttamisoperaatiot, joiden tekijää ei ole kyetty faktuaalisesti identifioimaan. Nämä tekijät on kuvattu tulosten yhteydessä olevissa taulukoissa tuntemattomina toimijoina. Lähteiden julkisuusleima mahdollistaa tietojen värittämisen sodan osapuolten toimesta. Venäjän toteuttamaan kybervaikuttamiseen liittyvät arviot tulee ymmärtää siis suuntaa antaviksi. Tämän tutkimuksen tutkimuskysymyksiin peilaten tiedon ja analyysin tarkkuus on kuitenkin riittävän laatuunkäypää, jotta lukija kykenee muodostamaan sen pohjalta oikeansuuntaisen käsityksen.

2.8 Aikaisempi tutkimus

Venäjän kybervaikuttamisesta Ukrainan sodassa ei tämän tutkimuksen ajanjaksolla ole aiempaa tutkimusta. Jari Juutilainen on tutkinut omassa, syyskuussa 2022 julkaistussa ylemmän ammattikorkeakoulun opinnäytetyössään *”Cyber Warfare: A Part of the Russo-Ukrainian War in 2022”* Venäjän kybervaikuttamista Ukrainan sodassa helmikuun 2022 ja heinäkuun 2022 välisenä aikana. Juutilaisen käsittelee opinnäytetyössään läpileikkaavasti kybertoiminnan teoriaa, venäläisiä kyberuhkatoimijoita sekä eri tiedustelulajeja. Helmikuun 2022 ja heinäkuun 2022 välisen ajan käsittelyn lisäksi hän myös sivuaa vuosina 2010–2021 käytyä kybersotaa, mutta sitä käsitellään vain pintapuolisesti taustoittamaan hänen tutkimusongelmaansa.

Giorgadze ym. ovat laatineet aiheesta vuonna 2022 julkaistun tieteellisen artikkelin *”Geopolitics of the Russia-Ukraine War and Russian Cyber Attacks on Ukraine-Georgia and Expected Threats”*. Artikkelissa käsitellään aiempien konfliktien yhteydessä Venäjän kybertoimintaympäristössä aiheuttamia uhkia Ukrainaa ja Georgiaa vastaan. Giorgadze ym. käsittelee myös länsimaiden roolia Ukrainan kyberosaamisen kehittämisessä.

Venäjän valtiollista kybertoimintaa on tutkittu laajasti sekä kotimaisissa että kansainvälisissä tutkimuksissa. Sotatieteiden tohtori Juha Kukkola on käsitellyt Venäjän kansallisen internetsegmentin strategisia vaikutuksia Maanpuolustuskorkeakoululle vuonna 2021 laatimassa diplomityössään *”Rakenteellinen kyberasymmetrian strategiset vaikutukset Venäjän kansallinen internetsegmentti sotilasstrategisena ilmiönä”.* Kukkola toteaa aiheen tärkeäksi jo siitä syystä, että kybertila on yksi sodankäynnin ulottuvuuksista. Kukkola on laatinut myös vuonna 2020 julkaistun Venäjän internetsegmenttiä käsittelevän väitöskirjan *”Digital Soviet Union: The Russian national segment of the Internet as a closed national network shaped by strategic cultural ideas”.* Väitöskirjassaan Kukkola käsittelee Venäjän kehittelemää kansallista internetsegmenttiä, joka toimii suljettuna ympäristönä ja joka voidaan tarvittaessa irrottaa globaalista internetistä. Kukkolan väitöskirjassa käsitellään kattavasti myös Venäjän digitaaliseen ympäristöön liittyviä virallisasiakirjoja.

Myös filosofian tohtori Martti J. Kari käsitteli Venäjän strategisen tason kybertoimintaa omassa väitöskirjatutkimuksessaan *”Russian Strategic Culture in Cyberspace: Theory of Strategic Culture – a tool to Explain Russia’s Cyber Threat Perception and Response to Cyber Threats”*. Kari toteaa vuonna 2019 julkaistussa, kuudesta artikkelista koostuvassa tutkimuksessaan, että Venäjän kyberuhkaskenaarioista on olemassa rajoitettu määrä julkaistua tietoa. Väitöskirjatutkimuksessaan Kari toteaa, että yksi Venäjän historian perusoletuksista on, että Neuvostoliitto on vihollisten ympäröimä ja lännen jatkuvan hyökkäysuhan alla oleva linnake. Hän toteaa tämän narratiivin olevan myös osa Venäjän kyberuhkakuvaa.

3 Kybervaikuttaminen osana kybersodankäyntiä

> *”Käsitteistä voidaan keskustella loputtomiin, mutta tärkeämpiäkin keskustelunaiheita digitalisoituvassa maailmassa riittää. Kyber tarkoittaa bittien maailmaa.”*
> Kyberturvallisuuden professori Jarno Limnéll ym. (2014)

Tämän luvun tarkoitus on luoda terminologinen viitekehys tälle tutkimukselle. Luvussa keskitytään erityisesti määrittelemään kybervaikuttamisen käsite siten, kun se on etymologisesti ja suomen kielessä ymmärretty. Luvussa esitellään myös

kybertoimintaympäristö ja kybersodankäynti, joiden ymmärtäminen on tutkimuksen kannalta oleellista.

3.1 Kybertoimintaympäristö

Niin kyber kuin sen myötä myös kyber-alkuiset sanat ovat ottamassa paikkaansa suomen kielen ja kulttuurin kivijalasta. Ei ole tavatonta, että kyber jo pelkästään käsitteenä herättää yhteiskunnallista keskustelua ja jakaa mielipiteitä. Suomen kielen sana kyber pohjautuu englanninkieliseen vastineeseensa *cyber.* Globaalisti sana kyber on kuitenkin peräisin kreikankielisestä sanasta *kybereo*, joka tarkoittaa ohjata, opastaa ja hallita (Limnéll ym., 2014, s. 29).

Kyber-termi teki oman läpimurtonsa viimevuosituhannen lopulla ensin sotilasympäristössä, josta se sitten adaptoitiin osaksi globaalia turvallisuuspoliittista keskustelua ja yhteiskuntaa. Tuolloin oltiin historiallisen digitalisaation murroksen kynnyksellä, jonka seurauksena toimintaympäristömme oli muuttumassa merkittävästi. Tämän kuvaamiseksi kaivattiin uutta käsitettä, koska jo olemassa olevat käsitteet, kuten *tietoturva* ja *informaatio* eivät tähän täysin sopineet. Tarvittiin käsitettä, joka kuvastaisi tallennetun tiedon (*informaatio*) turvallista siirtämistä ei vain toimijan omissa järjestelmissä (*tietoturva*), vaan myös niiden ulkopuolisissa tietoverkoissa. (Limnéll ym., 2014, ss. 30–31) Tästä huolimatta kyberkäsitteiden tarkka määrittely ja ymmärtäminen on yhä vaikeaa, sillä ne ovat osin päällekkäisiä ja niiden väliset rajat hämäriä.

Tämän tutkimuksen viitekehyksessä on oleellista tarkastella tätä muuttunutta toimintaympäristöä hieman tarkemmin. Kybertoimintaympäristölle ei ole kansainvälisesti yhtä vakiintunutta määritelmää, vaan eri lähteissä käytetään määritelmiä ja termistöjä lomittain keskenään. Kyberympäristöstä tehtyjä englanninkielisiä käännöksiä voidaan niiden määritelmien mukaan tulkita olevan muun muassa *cyber world (kybermaailma), cyber space (kyberavaruus) sekä cyber domain / cyber environment (kybertoimintaympäristö).* Kaikissa näitä termejä kuvaavissa määritelmissä on yhteistä sähköisessä muodossa oleva, tiedon käsittelyyn tarkoitettu, yhdestä tai useammasta tietoverkosta ja laitteesta koostuva

ympäristö. Määritelmillä on lähteistä riippuen keskinäisiä eroavaisuuksia lähinnä fyysisen maailman osalta.

Suomalaisissa kyberalaa käsittelevissä tutkimuksissa muun muassa Laari (2017) ja Flyktman ym. (2019) ovat esittäneet *kybertoimintaympäristön* englanninkieliseksi vastineeksi *cyber space.* Myös Suomen Puolustusvoimat käyttää vastaavaa määrittelyä, jossa *kybertoimintaympäristö (eng. cyber space)* mielletään tilaksi, joka sisältää sähköisten tietoverkkojen ja -järjestelmien lisäksi myös fyysisen infrastruktuurin sekä loppukäyttäjät (Flyktman ym., 2019, ss. 9–15). Yhdysvaltain puolustushaarakomentajien neuvosto, eli Yhdysvaltain asevoimien pääesikunta on määritellyt *cyber space*:n ilman fyysistä infrastruktuuria tai loppukäyttäjiä (Yhdysvaltain asevoimat, 2018, s. 100). Yhdysvaltojen kanssa samaan määrittelyyn on luonnollisesti päätynyt myös Naton Cooperative Cyber Defence Centre of Excellence (NATO, 2017). Toisaalta Yhdysvalloilla ei ole olemassa myöskään mitään kilpailevaa määritelmää kyberulottuvuudelle, vrt. *cyber domain* tai *cyber world.* Tämän pohjalta voidaankin tulla siihen johtopäätökseen, että Yhdysvallat mieltää fyysisen ulottuvuuden osaksi informaatioympäristöä, eikä sitä ole näin ollen ollut tarpeen tuoda kybertoimintaympäristöön. Suomen Natojäsenyyden myötä jää nähtäväksi, tullaanko tässä vielä kovin vakiintumattomassa kybertermistön määrittelyssä siirtymään lähemmäs Naton ja Yhdysvaltojen käytössä olevia määrittelyjä. Toisaalta on huomioitava se, että kybertermistöjä käytetään yhteiskunnassa laaja-alaisesti, eikä pelkästään sotilasympäristössä. Näin ollen Natojäsenyyden ei voida ajatella suoraan ohjaavan meidän terminologista määrittelyämme. Hankalimmassa tilanteessa Puolustusvoimat ja poliisiviranomaiset adaptoituvat Naton terminologiaan ja muu yhteiskunta jatkaa kansallisesti kehitetyn terminologian varassa, jolloin väärinymmärrysten vaara on ilmeinen.

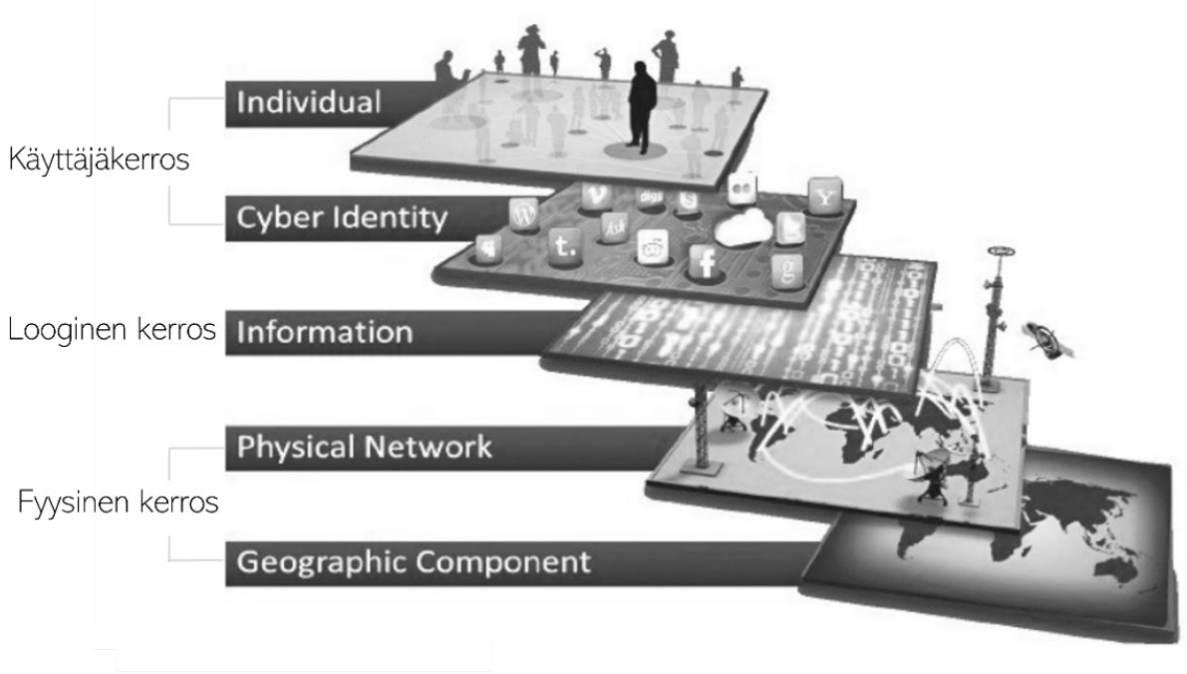
Tämän tutkimuksen näkökulmasta koettiin oleelliseksi käyttää terminologisessa määrittelyssä Suomalaisessa tutkimus- ja ammattilaisympäristöissä laajasti käytössä olevia määritelmiä. Määrittelyn valintaa tukee myös Sanastokeskuksen julkaisema kyberturvallisuuden sanasto, jossa *kybertoimintaympäristö* ja *kyberavaruus* yhdistetään toisiinsa (Sanastokeskus, 2018, s. 21). Toisena valintaa tukevana seikkana oli se, että Suomen kyberturvallisuusstrategiassa ei tehdä eroa kyberavaruuden ja kybertoimintaympäristön välillä, vaan puhutaan vain kybertoimintaympäristöstä (Turvallisuuskomitea, 2013).

Tutkimuksen käsitellessä Venäjän kybervaikuttamista Ukrainan sodassa, on mukana aina myös informaatioulottuvuus, jonka vuoksi tämä määritelmän valinta on erityisen perusteltu. Kuten Limnéll ym. toteavat (2014, s. 5), fyysisen ja bittien sisältämän maailman välillä ei voi, eikä kannatakaan yrittää tehdä yksiselitteistä jakoa, koska kyberulottuvuuden tapahtumilla on selkeitä fyysisiä seurauksia.

Kybertoimintaympäristö poikkeaa muista toimintaympäristöistä siten, että siellä ei tunnisteta valtioiden rajoja, jonka johdosta muutokset ovat nopeita ja vaikutukset hankalasti ennakoitavissa (Turvallisuuskomitea, 2013). Voidaan myös mieltää, että kybertoimintaympäristöä ei sen verkottuneisuuden vuoksi voi omistaa kukaan, mutta toisaalta taas sen voi ajatella omistavan kaikki sen käyttäjät yhdessä.

Nyky-yhteiskunnassa kyberoimintaympäristöjä on lähes kaikkialla. Esimerkiksi jokaisella ihmisellä on oma kybertoimintaympäristönsä, johon muun muassa puhelimet, sosiaalinen media ja verkossa olevat kodinkoneet lukeutuvat. Näiden lisäksi eräässä ääripäässä on valtion kriittinen infrastruktuuri, johon lukeutuvat muun muassa ydinvoimaloiden, sähkö- ja vesilaitosten sekä valtionhallinnon tietojärjestelmiin perustuvat ohjausjärjestelmät. (Flyktman ym., 2019, s. 10) Kybertoimintaympäristö on keskinäisriippuvainen ja moninainen ympäristö, jonka ymmärtämistä voidaan helpottaa jakamalla se osiin. Yksi tapa on jakaa se kolmeen osaan: *fyysiseen-*, *loogiseen-* sekä *käyttäjäkerrokseen* kuvan 1 mukaisesti. Flyktman ym. mukaan (2019) *Fyysinen kerros* muodostuu kosketeltavissa olevista fyysistä asioista, kuten kaapeleista ja päätelaitteista. Tähän kerrokseen kuuluvat eri laitteistot sekä infrastruktuurit, joista muodostuvat fyysiset verkostot. Heidän mukaansa *looginen kerros* muodostuu verkon sekä verkkoon kytketyn laitteen välisestä yhteydestä. Niin ikään Flyktman ym. määrittelevät (2019) *käyttäjäkerroksen* puolestaan tarkoittavan nimensä mukaisesti kybertoimintaympäristössä olevia käyttäjiä.

Kuva 1. Kybertoimintaympäristön kolme kerrosta (mukaillen U.S. Marine Corps Forces & Cyberspace Command, 2018)



Kybertoimintaympäristö on ollut merkittävänä osana viime vuosina koettua globaalia digitalisaation kehitystä, jonka seurauksena niin kriittistä infrastruktuuria kuin myös valtionhallintoa vastaan kohdistuvat uhkat ovat muodostuneet entistä vaarallisemmiksi. Hyökkääjät sekä heidän käyttämät hyökkäysmetodit ovat yhä ammattimaisempia, eivätkä hyökkääjät rajoitu vain yksittäisiin hakkereihin tai hakkeriryhmiin, vaan profiiliaan ovat nostaneet ennen kaikkea valtiolliset kyberuhkatoimijat, eli APT-ryhmät. Tämä on osaltaan asettanut valtioille uusia uhkakuvia perinteisen sotilaallisen vaikuttamisen, kineettisen voimankäytön rinnalle. (Turvallisuuskomitea, 2013, s. 1)

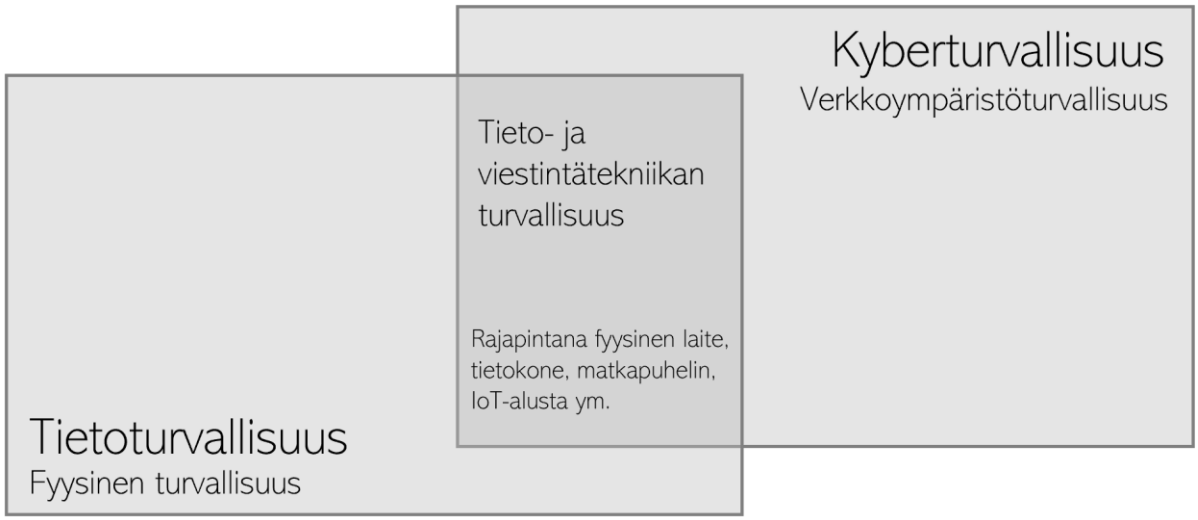
Tämän tutkimuksen yhteydessä käytettävän kybertoimintaympäristön määritelmä on muodostettu viimeisimpien Suomenkielisten, kyberalaa käsittelevien tutkimusten pohjalta. Näin ollen tässä tutkimuksessa kybertoimintaympäristö ymmärretään *fyysiset rakenteet sekä käyttäjät sisältävänä, digitaalisista tietojärjestelmistä muodostuvana toimintaympäristönä.*

3.2 Kyberturvallisuus

Kyber on tuonut luonnollisesti mukanaan myös tarpeen sen turvallisuuden takaamiseksi. Kyberturvallisuus on tullut osaksi jokaisen valtion, yrityksen ja yksittäisen kansalaisen arkea. Valtiollisia kyberturvallisuuskeskuksia alettiin perustamaan runsaasti 2010-luvun aikana, jolloin myös sotilaallista kybertilannekuvaa luovat sekä kyberoperaatioita suorittavat asevoimien kyberpuolustuskeskukset yleistyivät (Lehto & Limnéll, 2017, s. 199). Turvallisuuskomitea julkaisi tammikuussa 2013 Suomen kyberturvallisuusstrategian, joka määrittelee kyberturvallisuuden tavoitetilaksi, jossa sähköisessä muodossa olevan tiedon käsittelyyn tarkoitettuun toimintaympäristöön voidaan luottaa ja sen toiminta turvataan (Turvallisuuskomitea, 2013, s. 13). Eli toisin sanoen kyberturvallisuus kattaa kaiken sellaisen toiminnan ja laitteiston, joilla pyritään turvaamaan sekä laitteita että tietoa mahdollisilta hyökkäyksiltä.

Arkikielessä kyberturvallisuus sekoitetaan usein myös tietoturvallisuuden käsitteeseen. Tietoturvallisuus kattaa tiedon turvaamisen laajasti, painottuen tiedon fyysisen pääsyn rajoittamisen sekä tiedon fyysisen tallentamisen. Kyberturvallisuus sen sijaan painottuu nimenomaan verkkoympäristössä suoritettavaan tiedon, tietojärjestelmien sekä laitteiden turvallisuuden varmistamiseen. Näin ollen on myös luonnollista, että näiden kahden muodostamat uhkakuvat ovat myös osin erilaisia. (F-Secure, n.d.) Kyberturvallisuutta voidaankin ajatella yhtenä tietoturvan osa-alueena. Toisaalta nämä kaksi voidaan mieltää myös rinnakkaisina, toisiaan täydentävinä ja tukevina digitaalisen turvallisuuden muotoina, joiden rajapintana on jokin fyysinen laite. Tämä jäljempänä esitetty keskinäinen suhde on esitetty kuvassa 2.

Kuva 2. Tieto- ja kyberturvallisuuden keskinäinen suhde (mukaillen von Solms & van Niekerk, 2013)



Puhuttaessa valtiollisesta kybertoiminnasta, ei valtioiden välistä keskinäistä luottamusta sekä sen lisäämistä voida liikaa korostaa. Tässä tavoiteltavaan lopputulokseen pyritään avoimella keskustelu- ja toimintakulttuurilla sekä olemalla ennakoitavissa oleva. (Lehto & Limnéll, 2017, s. 205) Tähän tilaan ei kuitenkaan välttämättä kaikkien toimijoiden kanssa päästä, kuten muun muassa Ukrainan sota on osoittanut.

Valtiollinen kybertoiminta, kuten tiedustelu ja hyökkäykset, on monin tavoin kovin samankaltaista kyberrikollisten toiminnan kanssa. Joissain tapauksissa voi olla hyvin vaikeaa määritellä näiden kahden välisiä eroja. Molemmat tahot tunkeutuvat kohdejärjestelmän arkkitehtuuriin vaihtelevilla menetelmillä, tavoitteenaan hankkia omia tarkoitusperiä ja motiivejaan palvelevaa tietoa. Euroopan unioni laati vuonna 2001 niin kutsutun *”Budapestin sopimuksen”* – eli kyberrikollisuutta koskevan yleissopimuksen. Siinä määritellään kyberrikollisuuden ydinalueeksi tietoon tai tietojärjestelmään kohdistuvat luottamuksellisuutta, eheyttä sekä saatavuutta vaarantavat toimet (Euroopan neuvosto, 2001, ss. 1–16). Esimerkkejä tällaisista ovat muun muassa tietoon tai tietojärjestelmiin tunkeutuminen, järjestelmien tai niissä olevien tietojen ulkopuolinen muokkaaminen sekä järjestelmien tiedustelu. Nämä kolme EU:n yleissopimuksessakin mainittua periaatetta: *luottamuksellisuus (eng. confidentiality), eheys (eng. integrity)* ja *saatavuus (eng. availability)* muodostavat myös niin kutsutun tietoturvallisuuden ytimen – CIA:n. Kansainvälinen

tietoturvallisuuden hallintajärjestelmästandardi ISO/IEC 27001 määrittelee periaatteet seuraavasti:

Luottamuksellisuudella tarkoitetaan ja varmistetaan, että tiedot ovat vain niiden henkilöiden saatavilla, joilla on tiedon käsittelyyn määritelty oikeus. Esimerkiksi siis sitä, että valtionhallinnon sekä kriittisen infrastruktuurin kohteissa oleva tieto on ainoastaan siihen virallisesti oikeutettujen henkilöiden saatavilla. Tällöin näissä järjestelmissä liikkuva turvaluokiteltu sähköposti- ja dataliikenne ei ole kenen tahansa saatavilla.

Eheydellä tarkoitetaan tietojen sekä järjestelmien oikeellisuutta ja täydellisyyttä. Toisin sanoen, esimerkiksi valtionjohdon tai asevoimien käsittelemät turvaluokitellut asiakirjat ovat varmasti halutun sisältöisiä sekä halutulle vastaanottajalle osoitettuja ilman, että jokin ulkopuolinen taho olisi manipuloinut tietoa.

Saatavuudella tarkoitetaan ja varmistetaan, että valtuutetuilla käyttäjillä on käytettävissään oikea tietoa oikea aikaisesti. Esimerkiksi siis sitä, että päätöksentekijöillä, kuten valtion tai asevoimien johdolla on käytössään päätöksentekoon vaikuttavat oikeat ja ajantasaiset tiedot.

Näiden kolmen edellä mainitun elementin englanninkielisistä termeistä muodostuu niin sanottu tietoturvallisuuden kolmio *(eng. Cyber Security Triangle, CIA Triad).* Sen avulla kyetään visuaalisesti havainnollistamaan näiden kolmen elementin keskinäistä, kyberturvallisuuden näkökulmasta keskeistä riippuvuussuhdetta. Mikäli jokin näistä kolmesta elementistä vaarantuu, niin turvallisuusjärjestelyjen voidaan todeta pettäneen, joka on puolestaan johtanut tietovuotoon *(eng. Data Breach).* Tietoturvallisuuden kolmio on kehittynyt aikojen saatossa, eikä sen tarkkaa alkuperää tai ajanjaksoa ole tiedossa. Sen taustalla olevat käsitteet olivat kuitenkin sotilaallisessa kontekstissa käytössä jo vuosituhansia sitten. Tietoturvallisuuden kolmio on esitetty alla olevassa kuvassa 3.

Kuva 3.Tietoturvallisuuden CIA-kolmio (mukaillen ISCOOP, 2021)

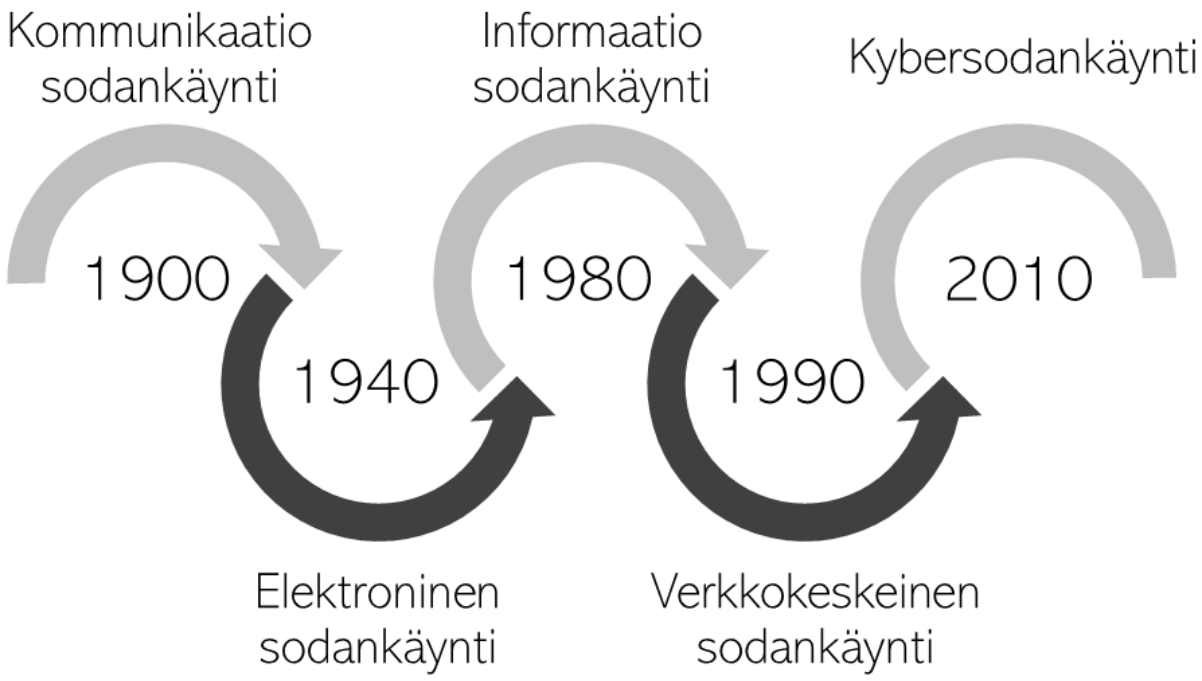
3.3 Kybersodankäynti

Kybersodankäynti on informaatiosodankäynnin lähikäsite, ja sen yhdyssanan määriteosa kyber muodostaa siitä synonyymin tietoverkkosodankäynnille (Flyktman, 2017, s. 25). Kybersodankäynnille ei siitä huolimatta ole yksiselitteistä, yleisesti käytössä olevaa määritelmää, joka puolestaan mahdollistaa sen varsin vaihtelevan käytön eri asiayhteyksissä (Lehto & Limnéll, 2017, s. 194). Lehto ja Limnéll esittävätkin (2017), että sodan ollessa aina laaja-alainen kokonaisuus, tulisi kybersodankäynnin määrittelyn perustua ennemminkin sodan tavoitteisiin ja motiiveihin, eikä niinkään kyberoperaatioiden muotoihin.

Sodankäynnin yleiskäsite voidaan jakaa sekä kineettisen että ei-kineettisen sodankäynnin muotoihin. Kineettisellä sodankäynnillä tarkoitetaan kaikkia perinteisiä sodankäynnin muotoja, joissa kohteeseen vaikutetaan suoraa aseellista voimaa käyttäen (Saressalo, 2012, s. 3). Ei-kineettisellä puolestaan tarkoitetaan sellaista sodankäyntiä, jossa vastustajaan ei kohdisteta suoraa aseellista voimaa, vaan vaikuttaminen toteutetaan esimerkiksi psykologisin tai teknisin keinoin missä tahansa ei-kineettisen sodankäynnin ympäristössä (Lehto & Henselmann, 2020, ss. 318–319). Voidaankin ajatella niin, että Ukrainan sodassa suoritettavat ohjusiskut ja asevoimien joukkojen rintamataistelut ovat kineettistä sodankäyntiä. Aivan yhtä lailla voidaan myös todeta, että sodan molempien osapuolten toteuttamat propagandistiset, kansalaisten mielipiteisiin kohdistetut mediakampanjat ovat osa ei-kineettistä sodankäyntiä.

Kybersodankäynti on ei-kineettisten sodankäynnin muotojen evoluution viimeisin vaihe, ja sen koetaankin kehittyneen viime vuosisadan aikana neljän sodankäynnin muodon seurauksena: *kommunikaatio-, elektroninen-, informaatio- ja verkkokeskeinen sodankäynti* – kuten kuvassa 4 on esitetty (Lehto, 2021, s. 77). Kybersodankäynnin käsitteellinen käyttö on yleistynyt 2000-luvun alusta lähtien, jolloin sillä alettiin osittain korvaamaan 1990-luvulla käyttöönotettua informaatiosodankäynnin käsitteen käyttöä (Lehto & Limnéll, 2017, s. 174).

Kuva 4. Ei-kineettisen sodankäynnin evoluutio (mukaillen Lehto & Limnéll, 2017)



Ei-kineettisen sodankäynnin historian voidaan katsoa ulottuvan 1800- ja 1900-lukujen taitteeseen, kun asevoimat alkoivat ottaa käyttöön ensimmäisiä sähköisiä viestivälineitä ja näin ollen implementoimaan, eli ottamaan käyttöön kommunikaatiosodankäynnin muodon. (Lehto, 2021, s. 72) Tiettävästi ensimmäinen sähköinen viestiväline, viestien lähettämiseen käytetty lennätin sai alkunsa Lontoossa vuonna 1838, jolloin siitä muodostui luonnollisesti myös tiedustelun ja häirinnän kohde. Se oli ensimmäistä kertaa mukana sodankäynnissä Krimin sodassa vuosina 1853–1856. (Distant Writing, n.d.)

Lennättimen käyttöä seurasi 1900-luvun alkupuolella alkanut radioviestintä, joka oli laajassa käytössä erityisesti suurvaltojen laivastojoukkojen keskuudessa, aivan kuten siitä kehitetty

kuuntelutiedustelu. Englannin kuninkaallisen laivaston risteilijä HMS Diana teki tiettävästi historian ensimmäisen kuuntelutiedusteluhavainnon ollessaan Suezin kanavassa tammikuussa 1904. Kaapattu sanoma sisälsi tietoa venäläislaivaston mobilisoinnista, joka oli tuolloiselle Englannin liittolaiselle Japanille erityisen arvokasta tietoa. Sodan edetessä Japani kykeni omalla kuuntelutiedustelukyvyllään kaappaamaan lisää tärkeää, Venäjän laivastojoukkoihin liittyvää tietoa, joka puolestaan näytteli suurta roolia sodan päättyessä Japanin voittoon. (Global Defence Technology, n.d.)

Elektroninen sodankäynti otti ensimmäisen maailmansodan myötä isoja kehitysaskeleita, ja toisessa maailmansodassa sitä kyettiin hyödyntämään aivan uudella tavalla, kun tutkajärjestelmät tulivat laajasti operatiiviseen käyttöön erityisesti ilmasodankäynnin osana. Elektroninen sodankäynti ja vaikuttaminen perustuu siihen, että vastustajan johtamis-, valvonta- ja tulenjohtojärjestelmiin pyritään vaikuttamaan siten, että niiden tuottaman tiedon luotettavuus alenee ja tulkittavuus hankaloituu. (Lehto, 2021, ss. 73–74) Elektronisen sodankäynnin myötä alettiin ymmärtämään vaikuttamisen, suojautumisen ja tiedustelun merkitykset, joka on kantanut myös kybertoimintaympäristöön aina tähän päivään saakka.

Yhdeksi vanhimmaksi ei-kineettisen sodankäynnin muodoksi voitaneen todeta informaatiosodankäynti, jonka juuret ulottuvat 1700- ja 1800-luvuille, kun Preussin kuningas Fredrik Suuri (Fredrik II) ymmärsi informaatiosodankäynnin merkityksen osana vihollisen päätöksentekoon vaikuttamista. Fredrik suuri käytti tuolloin hyvin samankaltaisia keinoja vastustajan harhauttamiseksi, kuin mitä esimerkiksi Venäjän hyökkäyssodassa on sodan molempien osapuolten toimesta nähty. Hän muun muassa korjautti tiestöjä ikään kuin valmistautuakseen vetääntymään, vaikka todellisuudessa hänellä ei ollut mitään aikeita sellaiseen. (Bastian, 2019, s. 33) Vastaava esimerkki löytyy kesältä 2022 Ukrainasta, kun Ukrainan joukot tekivät valmisteluja ja tiedottivat valmistautuvansa vastahyökkäykseen maan eteläosassa sijaitsevan H’ersonin takaisinvaltaukseen, jonka myötä venäläisjoukkoja siirrettiin Ukrainan pohjoisosasta vahventamaan H’ersonin aluetta. Todellisuudessa Ukraina olikin kaikessa hiljaisuudessa valmistellut vastahyökkäystä maan pohjoisosassa sijaitsevaan Harkovan kaupunkiin ja sen lähialueisiin, joiden takaisinvaltauksessa se onnistui menestyksekkäästi 11.9.2022.

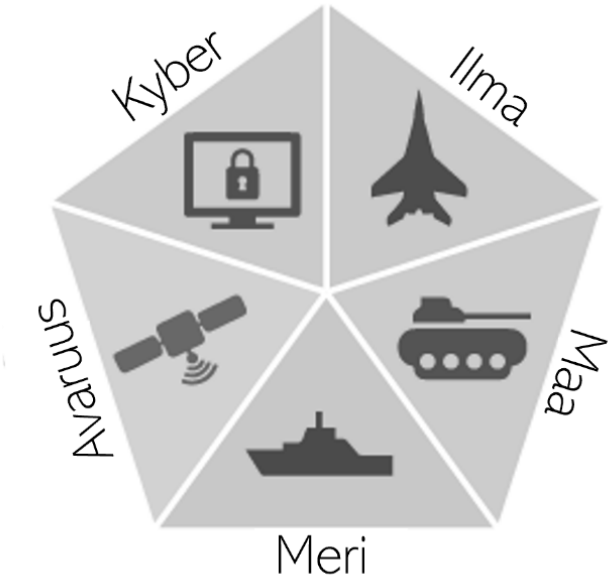
Toinen esimerkki informaatiosodankäynnin historiasta sijoittuu 1800-luvun Ranskaan, keisari Napoleonin aikakauteen. Myös Napoleon osasi käyttää informaatiosodankäyntiä sen ajan mittakaavassa erittäin taitavasti. Hän muun muassa esitti kansalleen omien hyökkäystoimiensa oikeuttamiseksi, kuinka Ranska on ulkovaltojen hyökkäyksen kohteena. Hän piti huolen siitä, että tätä virheellistä sanomaa julkaistaan sanomalehdissä, kaduilla olevissa kylteissä ja että tieto myös levisi naapurimaiden kansalaisille. Napoleon käytti tiettävästi naapurimaissa peitetehtävissä toimivia upseereita näihin tehtäviin, jonka ohella pyrittiin myös vaikuttamaan ulkomaisiin johtajiin sekä heidän mielipiteisiinsä. (Bastian, 2019, ss. 33–34) Tämän kaltaiset operaatiot kuulostavat melko tutuilta, vielä 200 vuoden jälkeenkin. Eräänä esimerkkinä todettakoon Venäjän presidentin Vladimir Putinin voimakas viestintä, jolla on pyritty oikeuttamaan ja saamaan omien kansalaisten hyväksyntä Ukrainan sotaan liittyen. Presidentti Putinin narratiivissa on esiintynyt muun muassa omien kansalaisten suojeleminen Itä-Ukrainassa, fasismin poiskitkeminen sekä Naton hyökkäysvalmistelujen estäminen.

Näiden esimerkkien myötä voidaankin todeta, että jo 1700- ja 1800-luvuilla Fredrik Suuri sekä Napoleon vaikuttivat vastustajiensa informaatio- ja kognitiivisiin prosesseihin, johtamalla vastustajien päätöksentekijöitä harhaan omien joukkojensa suorituskyvyistä sekä aikomuksista. Vaikka informaatiosodankäynnin historia ulottuukin vuosisatojen taakse, on siitä tullut laaja-alaista ja ammattimaisesti hyödynnettyä vasta 1990-luvulla. Aikakaudet ja johtajat ovat vaihtuneet, mutta toimintatavat ovat säilyneet ennallaan.

Asevoimissa on globaalisti ollut jo pitkään käytössä neljä selkeää toimintaympäristöä *(eng. domain)*; *maa*, *meri*, *ilma* sekä näistä tuoreimpana *avaruus*. Kaikki ei-kineettisen sodankäynnin muodot ovat sen koko evoluution ajan olleet kiinteä osa näitä kaikkia edellä mainittuja neljää toimintaympäristöä. Toimittiin sitten maalla, merellä, ilmassa tai avaruudessa, niin elektromagneettisen spektrin piirissä toimivia järjestelmiä käytetään jatkuvasti muun muassa tiedustelu-, valvonta-, maalinosoitus- ja viestintätarkoituksiin. Yhtä lailla kyberoperaatioilla on poikkitieteellinen vaikutus näihin kaikkiin neljään toimintaympäristöön.

Kybertoimintaympäristössä käytävä sodankäynti on kokenut merkittävän kasvun kuluneen vuosikymmenen aikana, jonka seurauksena muun muassa Euroopan Unioni tunnusti kybertoimintaympäristön yhdeksi sotilaalliseksi toimintaympäristöksi omassa kyberpuolustuspolitiikan kehysasiakirjassaan 2014 (Euroopan Unionin neuvosto, 2014), ja NATO Varsovan huippukokouksen yhteydessä 2016 (NATO, 2016, s. 128). Sotilasliiton ohella kybertoimintaympäristö on tunnustettu sotilaalliseksi toimintaympäristöksi myös sotilaallisen voiman läntisissä suurvalloissa, kuten Yhdysvalloissa ja Isossa-Britanniassa. Kybertoimintaympäristö koetaan globaalisti nopeimmin kehittyvänä sotilaallisena toimintaympäristönä, jonka vuoksi suurvallat kokevat erityistä painetta sen kehittämisestä sekä integroinnista yhä tiiviimmin osaksi neljää muuta sotilaallista toimintaympäristöä (Yhdysvaltain liittovaltion hallinto, 2017, ss. 2–10; Iso-Britannian hallinto, 2022a, ss. 18–30). Nämä viisi sotilaallisen toimintaympäristön elementtiä on esitetty kuvassa 5.

Kuva 5. Viisi sotilaallisen toimintaympäristön elementtiä (mukaillen Yhdysvaltain liittovaltion hallinto, 2019)



3.4 Kybervaikuttaminen

Kybervaikuttamisen käsitteen määrittely on tarpeellista, koska tätä sanaparia käytetään varsin kirjavasti eri asianyhteyksissä, jonka vuoksi ei voida olettaa, että lukijoilla olisi

yhteneväinen käsitys sen määritelmästä. Vaikuttamista käytetään terminä myös muissa yhteyksissä, jolloin siitä muodostuu myös toisenlaisia merkityksiä. Määritelmän laatiminen on oleellista myös siitä syystä, että sitä käytetään pohjana neljännessä pääluvussa, kun analysoidaan Venäjän federaation kykyä kyberoperaatioiden suorittamiseen ja siten kybervaikuttamiseen. Tämän tutkimuksen perustuessa suomalaisesta näkökulmasta tehtävään tarkasteluun, koettiin oleelliseksi tarkastella myös kybervaikuttamisen määritelmiä pääosin kotimaisen lähdeaineiston pohjalta.

Sana *vaikuttaminen* muodostuu verbistä ”*vaikuttaa*”. Vaikuttamista kuvaavia verbejä käytetään laajasti muun muassa lääketieteessä, kuvaten lääkkeen vaikuttavuutta ja vaikuttamisaikaa (Kotimaisten kielten keskus, n.d.), sekä esimerkiksi puhuttaessa kansalaisten mahdollisuudesta äänioikeuden myötä vaikuttaa demokraattiseen järjestelmään (Suomen perustuslaki 731/1999 § 14). Sitä käytetään myös epäsuoremmin kuvaamaan esimerkiksi sitä, kuinka toisen henkilön toiminta vaikuttaa toisen mielialaan (Kotimaisten kielten keskus, n.d.). Näitä kaikkia esimerkkejä yhdistää se, että jokin mekanismi tai teko on omiaan aiheuttamaan muutosta sen kohteessa. Esimerkiksi Cambridgen yliopiston sanaston mukaan vaikuttamisen englanninkielinen käännös *influence* kuvaa kykyä vaikuttaa ihmisiin tai asioihin, sekä muuttamaan sitä, miten joku tai jokin kehittyy, käyttäytyy tai ajattelee (Cambridge University, n.d.). Esimerkiksi sosiaalisen median vaikuttajat (*eng. Social Media Influencer)* pyrkivät omalla toiminnallaan vaikuttamaan oman kohderyhmänsä käyttäytymis- ja ajattelumalleihin käsittelemällä ajankohtaisia asioita, tai vaihtoehtoisesti markkinoimalla jonkin yhteistyökumppanin tuotteita (British Council, 2019). Edellä kuvatut määritelmät pätevät myös sotilaallisesta näkökulmasta tarkasteltaessa. Esimerkiksi kineettisillä asejärjestelmillä vaikutetaan johonkin elävään tai elottomaan kohteeseen, jolla pyritään saavuttamaan haluttu vaikutus. Vaihtoehtoisesti voidaan myös tuottaa tietoa, muokata sitä tai rajoittaa sen saatavuutta, jolla pyritään vaikuttamaan ihmisten mielipiteisiin (Sanastokeskus, 2018).

Kybervaikuttaminen yhdyssanan *Kyber* osalle ei ole globaalisti hyväksyttyä määritelmää, ja sen mielletäänkin yleensä liittyvän tietotekniikkaan, tietojärjestelmiin sekä digitaalisessa ympäristössä tehtävään tiedonkäsittelyyn (Lehto & Limnéll, 2017). *Kyber* esiintyy yleensä yhdyssanan määriteosana, jonka johdosta voidaankin geneerisesti ajatella, että määriteosan

avulla voidaan mikä tahansa käsite tuoda osaksi digitaalista ympäristöä. Esimerkkinä todettakoon ulkoministeriössä toimiva, kybertoimintaympäristön kokonaisuudesta poliittisella tasolla vastaava kybersuurlähettiläs (Ulkoministeriö, n.d.). Toisena esimerkkinä voidaan mieltää perinteisen *turvallisuus* käsitteen liitettävyys osaksi digitaalista toimintaympäristöä määriteosansa avulla, jolloin muodostuu termi *kyberturvallisuus*.

Kybervaikuttamisella kyetään suhteellisen alhaisilla kustannuksilla suorittamaan hyökkäyksellisiä operaatioita vastustajan hallussa olevaan informaatioon ja informaatiojärjestelmiin, sekä epäsuorasti myös ihmiselämään (Lehto & Limnéll, 2017, s. 195). Hyökkäyksillä pyritään häiritsemään vastustajan tietojärjestelmiä ja -verkkoja, rajoittamaan tai tuhoamaan käytössä olevaa informaatiota sekä saavuttamaan yleinen kyberylivoima (Lehto & Limnéll, 2017, s. 197). Hyökkääjän eduksi todettakoon vielä se, että sen faktuaalinen identifiointi on haastavaa.

Kybervaikuttamisessa on keskeistä systeeminen ajattelu. Kohteita valittaessa niitä tulisi tarkastella osana kokonaisuutta, jolloin mahdollistetaan sekä suora että epäsuora vaikutus. Kohteiden vallinnassa tulisi suosia sellaisia kohteita, joilla saadaan nopeimmin, pitkävaikutteisimmin sekä tehokkaimmin aikaan haluttu muutos osana strategista kokonaisuutta. Sotilaallisissa operaatioissa ensisijaisia kohteita ovat vastustajan kriittiset rakenteet ja toiminnot sekä niiden haavoittuvuudet. Operaatioiden onnistuminen edellyttää myös tarkkaa operaatiota edeltävää analyysia ja suunnittelua. (Lehto & Limnéll, 2017, s. 197) Kybersodankäynnissä kybervaikuttamisen tulisi olla yhdessä kineettisen sodankäynnin kanssa keskitetysti johdettua yhteisoperaatiotoimintaa (Kuusisto, 2014, s. 172). Ilman näiden kahden yhdistämistä kybervaikuttamisen tulokset jäävät vähäisiksi.

Tässä tutkimuksessa *kybervaikuttamisella* tarkoitetaan kybertoimintaympäristössä toteutettavaa, vastustajan tietojärjestelmiin ja -verkkoihin kohdistettavaa sellaista toimintaa, jolla pyritään häiritsemään tai rajoittamaan niiden, sekä niissä olevan tiedon käyttöä. Tähän lukeutuu myös tietojärjestelmien ja -verkkojen tuhoaminen.

3.5 Kybersuojautuminen ja kybertiedustelu

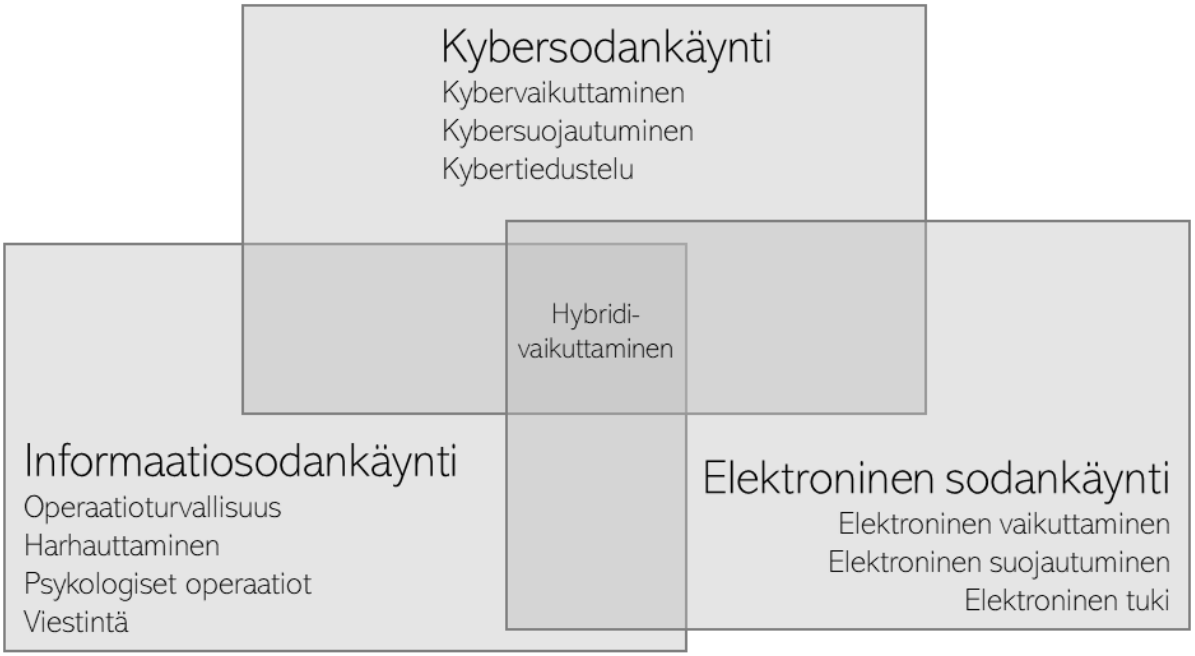
Kyberhyökkäyksen puolustava osapuoli pyrkii kybersuojautumisen toimenpitein estämään, rajaamaan sekä lieventämään eri järjestelmiin ja verkkoihin kohdistuvia kyberhyökkäyksen vaikutuksia. Tällaisia käytännön toimenpiteitä ovat muun muassa tietoverkoissa toteutettava valvonta, havainnointi, vastatoimien toteuttaminen sekä tapahtumien jälkianalysointi. *Kybersuojautumisen* keskeisin tavoite on suojata omia järjestelmiä sekä niissä olevaa tietoa siten, että kyetään säilyttämään riittävä johtamiskyky. (Lehto & Limnéll, 2017, s. 196)

Kybertiedustelu on sellaista laillista tiedonhankintaa, jolla pyritään kartoittamaan ja lisäämään yleistä tilanneymmärrystä erilaisista uhka- sekä riskitekijöistä, niin kotimaassa kuin ulkomaillakin. *Kybervakoilussa* tiedonhankinta toteutetaan laittomin menetelmin, se on kohdekeskeistä ja se kohdistuu esimerkiksi yksityishenkilöihin, yrityksiin, valtionhallintoon sekä sotilaskohteisiin. (Lehto, 2021, s. 59) Puolustusvoimien tietohallintopäällikön ja kyberpuolustuksen erityisasiantuntija Catharina Candolinin mukaan (2022) nämä voidaan jakaa kahteen alaryhmään: tiedusteluun tietoverkoissa sekä tiedusteluun tietoverkoista.

Tietoverkoissa toteutettavalla tiedustelulla kerätään tietoa osana muuta tiedustelutoimintaa. *Tietoverkoista* tehtävällä tiedustelulla puolestaan pyritään keräämään tietoa kohteen tietoverkoista sekä niiden kokoonpanoista, kuten salasanoja ja järjestelmätietoja. (Candolin, 2022) Näiden muodostamalla kokonaisuudella kyetään tuottamaan tietoa kohdejärjestelmien haavoittuvuuksista, sekä arvioita kohteen kyvystä hyökkäyksellisten operaatioiden suorittamiseen. *Kybertiedustelun* tavoitteena on ennen kaikkea ennakkovaroituskyvyn sekä kybervaikuttamisen ja kybersuojautumisen vaatiman tilannetietoisuuden saavuttaminen. (Lehto & Limnéll, 2017, s. 196)

Kybertiedustelu ja *kybersuojautuminen* yhdessä *kybervaikuttamisen* kanssa muodostavat kybersodankäynnin kokonaisuuden osana verkkokeskeistä toimintaympäristöä kuvan 6 mukaisesti.

Kuva 6. Verkkokeskeinen toimintaympäristö (mukaillen Lehto & Limnéll, 2017, s. 198)



4 Venäjän valtiollinen kyky kybervaikuttamisoperaatioihin

> *”Tulisi yksinkertaisesti aina pitää mielessä, että tällainen on todellisuus, jonka amerikkalaiset ovat luoneet. He ovat ne, jotka sen tekivät. Kaikki tämä alkoi alun perin, kun internet ilmestyi ensikertaa – CIA:n salaisena projektina. Ja tällä tavalla kehitys tulee jatkumaan.”*
> Venäjän federaation presidentti Vladimir Putin, Pietarissa 24.4.2014

Suorituskyvyn muodostumiseen voidaan yleisesti katsoa vaikuttavan henkilöstö (tahto), poliittisen johdon asettamat mahdollisuudet ja rajoitteet (käyttö- ja toimintaperiaatteet) sekä käytettävissä olevat välineet. Kyberympäristössä välineet, eli toisin sanoen kyberaseet ovat edullisesti eri toimijoiden valmistettavissa, eikä niiden voida katsoa muodostavan merkittävää eroavaisuutta eri toimijoiden välillä. Sen sijaan kybersuorituskykyyn voidaan katsoa keskeisesti vaikuttavan henkilöstön ammattitaitoisuus ja tahtotila. Henkilöstön ammattitaitoisuutta voidaan luonnollisesti kasvattaa koulutuksella, kun tahto ja motivaatio muodostuvat ennemmin ideologioiden, historian ja opitun perusteella. Näissä molemmissa on vahvasti läsnä toimintaa ohjaavat eri virallisasiakirjat, kuten sotilasdoktriinit. Tämän

tutkimuksen kannalta onkin oleellista tarkastella Venäjän valtiollista kybersuorituskykyä henkilöstön ja tahdon perspektiiveistä.

Venäläisten kyberuhkatoimijoiden luettelo on pitkä ja johtosuhteet monimutkaiset. Niiden väliset suhteet ovat muuttuneet varsin merkittävästi Neuvostoliiton hajoamisesta tähän päivään. Yhtä lailla kybertoimintaa ohjaavien doktriinien sekä muiden virallisasiakirjojen kirjo on kovin moninainen. Tässä luvussa lukijalle pyritään luomaan ymmärrys Venäjän varsin pirstaloisesta kyberkokonaisuudesta, joka muodostuu kyberuhkatoimijoista, niiden johtosuhteista ja keskinäisistä kilpailuasetelmista sekä Venäläistä kybertoimintaa ohjaavista virallisasiakirjoista ja määräyksistä.

4.1 Venäjän kybertoiminta osana turvallisuus- ja tiedustelupalveluita Neuvostoliiton hajoamisesta tähän päivään

Nyky-Venäjän kybersodankäynnin rakenteet ovat peruja Neuvostoliiton signaalitiedustelusta. Kaksi keskeisintä signaalitiedustelun muotoa ovat kuuntelutiedustelu (COMINT) sekä elektroninen mittaustiedustelu (ELINT). Näitä tiedustelumuotoja toteutti Neuvostoliitossa kaksi tiedusteluviranomaista: tiedustelu- ja turvallisuuspalveluna toiminut valtion turvallisuuskomitea KGB *(ven. КГБ, Комите́т госуда́рственной безопа́сности)* sekä sotilastiedustelusta vastannut tiedustelupäähallinto GRU. Molemmat tiedustelupalvelut seurasivat ulkomaista viestiliikennettä ja purkivat salauksia erillisiltä tiedusteluasemilta käsin. KGB:n ja GRU:n osittain yhteisiäkin tiedusteluasemia sijaitsi Neuvostoliiton lisäksi myös ulkomailla, kuten Kuubassa ja Vietnamissa (Heickerö, 2020, ss. 27–31).

Neuvostoliiton hajottua joulukuussa 1991 myös KGB lakkautettiin, ja sen toimintoja varten perustettiin kolme uutta organisaatiota – ulkomaan siviilitiedustelupalvelu SVR, vastatiedustelupalvelu FSK *(ven. ФСК РФ, Федеральная служба контрразведки Российской Федерации)* sekä viestinnän ja informaation virasto FAPSI *(ven. ФАПСИ, Федеральное агентство правительственной связи и информации).* Vastatiedustelupalvelu FSK koki nopean uudelleenjärjestelyn, kun vuonna 1995 siitä muodostettiin Venäjän federaation turvallisuuspalvelu FSB. Tällä muutoksella pyrittiin luomaan useita tiedustelumenetelmiä hallitseva, korkean profiilin turvallisuus- ja

tiedustelupalvelu. (Kari, 2019, ss. 149–150) Viestinnän ja informaation virasto FAPSI:in siirrettiin KGB:ssa valtionhallinnon viestijärjestelmistä vastannut 8. päähallinto sekä signaalitiedustelusta vastannut 16. päähallinto. (Kari, 2019, s. 64) FAPSI:ssa 16. päähallinto nimettiin uudelleen 3. päähallinnoksi, ja sen tehtäviin lisättiin tietoliikenneyhteyksiin kohdistettava elektroninen tiedustelu (Iso-Britannian hallinto, 2022b). Tällä pyrittiin luomaan eräänlainen venäläinen vastine Yhdysvaltojen kansallisesta turvallisuuspalvelu NSA:sta. (Heickerö, 2020, s. 27).

Vuonna 1995 3. päähallinnon johtajaksi nimettiin yksi Venäjän sittemmin tapahtuneen kyberkehityksen merkittävimmistä henkilöistä, Moskovan valtionyliopiston fysiikan tiedekunnasta valmistunut, ja vuodesta 1966 lähtien KGB:n upseerina toiminut Vladislav Sherstjuk. Hän johti FAPSI:n taisteluosastoa ensimmäisessä Tšetšenian sodassa, vastaten tšetšenijoukkojen viestiliikenteen tiedustelusta. Sodan jälkeen vuonna 1998 Sherstjuk nimitettiin FAPSI:n johtajaksi. (Venäjän puolustusministeriö, n.d.) Myöhemmin samana vuonna myös turvallisuuspalvelu FSB käynnisti oman kybertoimintansa, uuden johtajansa, Vladimir Putinin toimesta (Venäjän turvallisuuspalvelu FSB, n.d.-a). FSB:n vastatiedusteluosaston alaisuuteen perustettiin vuonna 1998 sen ensimmäinen varsinainen kyberyksikkö: tietokone- ja tietoturvallisuuden päähallinto UKIB *(ven. УКИБ, Управление компьютерной и информационной безопасности)* (Venäjän turvallisuuspalvelu FSB, 2001).

Venäjällä alettiin 1990-luvun alkupuolella perustamaan myös ensimmäisiä yksityisiä tietoturva- ja kyberalan yrityksiä. Yhtenä, myöhemmin kansainvälisestikin tunnettuna ja menestyneenä esimerkkinä on Kaspersky Lab. Yrityksen perustaja ja toimitusjohtaja Jevgeni Kasperski valmistui KGB:n korkeakoulusta 1987, ja palveli valmistumisensa jälkeen sovellusinsinöörinä KGB:n alaisessa tutkimuslaitoksessa. KGB-taustansa ansiosta Kasperski pystyi luomaan läheiset suhteet turvallisuus- ja tiedustelupalveluiden kanssa. (Bing, 2022; FCC, 2022) Yksityisten kyberyritysten perustaminen oli merkittävää aikaa myös FAPSI:lle, joka pystyi hyödyntämään yrityksiä omassa toiminnassaan, rekrytoinneissaan sekä kyberoperaatioissaan (Kari, 2019, s. 65).

Viestinnän ja informaation virasto FAPSI:n johtaja Vladislav Sherstjuk nimitettiin vuonna 1999 Venäjän turvallisuusneuvoston apulaisjohtajaksi. Myöhemmin samana vuonna Sherstjuk oli mukana perustamassa turvallisuusneuvostoon uutta tietoturvaosastoa, jonka johtajaksi hänet niin ikään nimettiin. (Venäjän turvallisuusneuvosto, n.d.) Tietoturvaosastosta muodostui vastuuorganisaatio Venäjän kyber- ja tietoturvakonseptien suunnittelulle, sekä myöhemmin myös kybertoiminnan poliittiselle ohjaukselle. Sherstjukin toimesta Moskovan valtionyliopistoon perustettiin kyberpoliittisia aiheita käsittelevä tietoturvallisuuden tutkimusinstituutti, joka muodostui tietoturvallisuuden näkökulmasta Venäjän ulkopolitiikkaa määrittelevästi ajatushautomoksi. (Venäjän kansainvälisen tietoturvallisuuden järjestö, 2019) Sherstjukin johtama turvallisuuskomitean tietoturvallisuusosasto valmisteli Venäjän Federaation ensimmäisen tietoturvallisuuden doktriinin, jonka presidentiksi noussut Vladimir Putin hyväksyi vuonna 2000. Doktriini oli samalla Venäjän ensimmäinen kybertoimintaa käsittelevä virallisasiakirja. (Kreml, 2000)

Entinen turvallisuuspalvelu FSB:n johtaja, ja ensimmäisen presidenttikautensa aloittanut Vladimir Putin jatkoi aktiivisesti FSB:n profiilin nostoa ja toimintojen keskittämistä yhden turvallisuus- ja tiedustelupalvelun alaisuuteen. Maaliskuussa 2003 presidentti Putin lakkautti viestinnän ja informaation viraston FAPSI:n, ja jakoi sen keskeisimmät toiminnot osaksi turvallisuuspalvelu FSB:tä sekä ulkomaan siviilitiedustelupalvelu SVR:ää (Venäjän puolustusministeriö, n.d.). FAPSI:ssa signaali- ja tietoliikennetiedustelusta vastannut 3. päähallinto siirrettiin osaksi FSB:tä, jolloin se nimettiin viestitekniikan keskukseksi, toiselta nimeltään 16. keskukseksi. Niin ikään sekä kotimaahan että ulkomaille sijoitetut mittaustiedusteluasemat liitettiin osaksi FSB:tä. (Agentura, n.d.-a) FSB:n hallinnon uudistus jatkui vuonna 2004, kun sen vastatiedusteluosaston alaisuudessa toiminut FSB:n ensimmäinen varsinainen kyberyksikkö, tietokone- ja tietoturvallisuuden päähallinto UKIB muutettiin nykyiseksi tietoturvakeskukseksi, eli 18. keskukseksi. 18. keskus osallistuu tietoverkkojen suojaamiseen sekä salaiseen, ulkomaisiin tietoverkkoihin kohdistuvaan tiedustelutoimintaan. (Agentura, n.d.-b) Tämä 2000-luvun alkupuolen ajanjakso voidaankin nähdä tuoreen turvallisuuspalvelu FSB:n merkittävän laajentumisen aikana, jonka taustalla oli sen entinen johtaja ja nykyinen Venäjän presidentti – Vladimir Putin.

Kybertoimintaa kehitettiin myös yleisesikunnan alaisessa tiedustelupäähallinto GRU:ssa, johon muodostui 2000-luvulla kaksi keskeistä kyberuhkatoimijaa: 85. Erikoispalvelukeskus *(alias: APT28)* sekä Erikoisteknologian pääkeskus *(alias: Sandworm).* GRU liitti myös signaali- ja elektronisen mittaustiedustelun tutkimus- ja kehittämistoimintaa suorittaneen 18. Tieteellisen tutkimuslaitoksen osaksi viraston kybertoimintaa. (CISA, 2022)

Seuraava Venäjän kyberkulttuurin käännekohta koettiin vuonna 2012, kun Sergei Shoigu nimitettiin puolustusministeriksi. Ilman perinteistä KGB-taustaa olevalla Shoigulla oli sotilaspoliittinen tarve osoittaa isänmaallisuuttaan sekä asevoimahenkisyyttään. Korkeassa nosteessa ollut kybertoiminta tarjoutui sopivaksi sotilaallisen vaikutusvallan kasvattamisen työkaluksi, jonka seurauksena hän halusikin perustaa asevoimien omat kyberjoukot. Venäjän asevoimien ensimmäiset kyberjoukot perustettiin rekrytointien jälkeen vuonna 2013. (Brooks & Lysenko, 2018)

Puolustusministeriö asetti kybervelvoitteita myös kemian ja mekaniikan tutkimuslaitos TsNIIKhM:lle *(ven. Государственный научный центр Российской Федерации федеральное государственное унитарное предприятие Центральный научно-исследовательский институт химии и механики).* TsNIIKhM on koko sen lähes 130 vuotisen historian ajan osallistunut sotateolliseen yhteistyöhön, kehittäen asevoimille ruutia, ammuksia sekä räjähteitä. Myöhemmin sille on tiettävästi asetettu myös tiedustelullisia tehtäviä. TsNIIKhM on muun muassa rakentanut kyberaseita sen omaan sekä myös muiden venäläisten toimijoiden käyttöön. Lisäksi TsNIIKhM on tiettävästi suorittanut yhteisoperaatioita muiden kyberuhkatoimijoiden, eli APT-ryhmien kanssa. (CISA, 2022) Yhtenä esimerkkinä TsNIIKhM:n kyberaseiden kehitystyöstä on muun muassa Triton-haittaohjelma, jolla hyökättiin Saudi-Arabialaiseen öljy-yhtiön toiminnanohjausjärjestelmiin vuonna 2017 (Yhdysvaltain liittovaltion hallinto, 2022). TsNIIKhM tunnetaan MITRE:n (2019) määrittelyn mukaisesti myös ”TEMP.Veles” APT-ryhmänä.

Vuoden 2014 Krimin miehityksen jälkeen Venäjän valtiollinen kyky kybersodankäyntiin kasvoi merkittävästi, joka osaltaan kiihdytti eri virastojen keskinäistä kilpailua. Venäjän asevoimat laajensi kyberkoulutustaan entisestään, ulottaen sen myös niihin sotakorkeakouluihin, jotka olivat aiemmin erikoistuneet signaalitiedusteluhenkilöstön

kouluttamiseen. Puolustusministeriön alaisten kyberuhkatoimijoiden ohjauksesta ja valvonnasta vastaa kolme eri asevoimien yleisesikunnan alaista toimijaa: yleisesikunnan 8. päähallinto, GRU:n 6. päähallinto sekä tiedetekninen komitea. Venäjän entinen varapääministeri Dimitri Rogozin ilmaisi jo vuonna 2012 tarpeen sotilaallisen kybertoimintakeskuksen perustamisesta. Alkuvuodesta 2013 Venäjän puolustusministeri Sergei Shoigu ilmoitti kybertoimintakeskuksen perustamisaikeista, ja asetti keskuksen käynnistymisen takarajaksi vuoden 2014 lopun. (Borogan & Soldatov, 2022) Venäjän sotilaallista kybertoimintakeskusta ei ole kuitenkaan vielä vuoden 2023 kevääseen mennessä perustettu.

FSB:n sisällä keskeisimpinä kyberuhkatoimijoina jatkoivat 16. sekä 18.keskus. Yhdysvaltojen vuoden 2016 presidentinvaaleihin sekaantumisen ja sen paljastumisen seurauksena virastot syyttelivät kiinnijäämisestä toisiaan, jonka seurauksena FSB:n alainen 18. keskus koki osittaisen likvidoinnin. (Congressional Research Service, 2022) 18. keskuksen upseereita pidätettiin maanpetoksesta, keskuksen johto joutui eroamaan sekä entinen FSB:n 16. keskuksen johtaja Sergei Buravljov erotettiin turvallisuusneuvostosta. Länsimaiden kanssa suoritettava yhteistyö siirrettiin FSB:n sisällä 18. keskuksesta 8. keskukseen, joka toimii myös Venäjän kansallisena kyberturvallisuuskeskuksena. (Borogan & Soldatov, 2022) FSB:n 18. keskuksen ajauduttua eräänlaiseen paitsioon, toisena FSB:n keskeisenä kyberuhkatoimijana tunnettu 16. keskus nosti profiiliaan ja siitä muodostuikin FSB:n ensisijainen kyberhyökkäyksiä toteuttava yksikkö, joka tunnetaan muun muassa nimellä Dragonfly. (CISA, 2022)

Venäjän tiedustelu- ja turvallisuuspalvelut sekä asevoimat tukeutuvat merkittävissä määrin yksityisen sektorin toimijoihin niin kyberaseiden kehityksessä, kuin myös kyberoperaatioiden suorittamisessa. (Ulkopoliittinen instituutti, 2021) Virastot ja asevoimat luottavat jo Neuvostoliiton aikana rakennettuun tutkimuslaitosten kokonaisuuteen ja sotilaallisteolliseen yhteistyöhön. Jo neuvostoaikana oli tyypillistä, että todellisuudessa KGB:n alainen toiminta pyrittiin piilottamaan osaksi tieteellistä tutkimus- ja opetustoimintaa. Vastaava toimintamalli on tiettävästi yhä käytössä ainakin FSB:llä ja SVR:llä, sekä todennäköisesti myös GRU:lla. Muun muassa neuvostoaikana KGB:lle tietokoneita kehittänyt tieteellinen tutkimusinstituutti Kvant kehittää nykyään, yhdessä alihankkijana toimivan teknologia-alan yrityksen SyTech:n

kanssa, kyberaseita FSB:n 16. keskukselle – eli APT-ryhmä Dragonflylle. (Lilly, 2022, ss. 28–30) Molemmat yritykset ovat sittemmin asetettu Yhdysvaltojen pakotelistalle. (Yhdysvaltain liittovaltion hallinto, 2018) Toinen niin ikään Yhdysvaltojen pakotelistalle asetettu yritys on Positive Technologies, joka tuottaa muun muassa erilaisia tietoturvaratkaisuja niin Venäjän hallinnolle, kuin myös ulkomaisille valtionhallinnoille ja kansainvälisille yrityksille. Tämän lisäksi Positive Technologies järjestää myös ”Positive Hack Days”-hakkerointitapahtumia, joita tiettävästi käytetään FSB:n ja GRU:n rekrytointitapahtumina. (Sherman, 2023) Kolmas, myös Yhdysvaltojen pakotelistalla oleva yritys on kybertutkimusta suorittava, sekä niin ikään hakkerointitapahtumia järjestävä ”Digital Security” (Yhdysvaltain liittovaltion hallinto, 2018).

Venäjän turvallisuus- ja tiedustelupalveluiden kybertoiminnasta tiedetään FSB:n ja GRU:n osalta verrattain paljon. Kuitenkin kolmas valtion tiedusteluviranomainen, ulkomaan siviilitiedustelupalvelu SVR:n on pitänyt toimintansa hyvin hienostuneena ja diskreettinä, eikä siihen olla vielä toistaiseksi pystytty varmuudella liittämään mitään kyberuhkatoimijaa. Läntiset tiedustelupalvelut pitävät kuitenkin todennäköisenä, että muun muassa vuoden 2020 SolarWinds-tapauksen takana ollut APT29 on SVR:n alainen toimija. Vuodesta 2008 lähtien tunnettu APT29, eli ”Cozy Bear”, arvioitiin sen alkuaikoina kuuluvan osaksi FSB:tä, mutta muun muassa Yhdysvallat yhdessä kyberyhteistyökumppaneidensa kanssa ovat viime vuosina yhdistäneet APT29 osaksi SVR:ää. (Lilly, 2022, s. 28) Tämän tutkimuksen yhteydessä koetaan tarkoituksenmukaisesti seurata globaalisti vallitsevaa ymmärrystä, ja tulkita APT29 olevan SVR:n alainen kyberuhkatoimija.

Venäjällä on kaikkiaan kolme keskeistä kybertoiminnasta vastaavaa viranomaista – valtion keskeisimmät turvallisuus- ja tiedustelupalvelut: FSB, GRU ja SVR. Kaikkien edellä mainittujen organisaatioiden kybertoimintaa johdetaan ristiin myös virastojen sisällä, eikä selkeitä yksiselitteisiä johtosuhteita ole yhdelläkään näistä. Puhumattakaan koko valtion kattavasta, keskitetystä kyberjohtosuhteesta. Sen sijaan suoraan presidentin alaisuudessa olevilla turvallisuusjoukoilla on myös oma pienimuotoisempi kybertoiminto, joka osallistuu myös turvallisuus- ja tiedustelupalveluiden kybertoiminnan ohjaukseen. Voidaan siis todeta, että Venäjän valtiollinen kybertoiminta on varsin repaleisesti organisoitu ja johdettu, eikä se voi olla vaikuttamatta kyberoperaatioiden käytännön toteutukseen.

4.2 Venäläinen kyberkoulutus ja rekrytointi Neuvostoliiton hajoamisesta tähän päivään

Siinä missä Venäjän eri turvallisuus- ja tiedusteluviranomaiset kilpailevat keskenään operatiivisella kentällä, niin samaa keskinäistä kilpailua on havaittavissa myös koulutus- ja rekrytointitoiminnassa. Neuvostoliiton aikana upseereille annettiin keskenään kilpailevaa tietoturvakoulutusta kahden eri viranomaisen toimesta: GRU Mustanmeren rannalla Krasnodarin kaupungissa sijaitsevassa sotakorkeakoulussa ja KGB Moskovassa sijaitsevassa korkeakoulussaan. (Venäjän turvallisuuspalvelu FSB, n.d.-b; Global Security, n.d.) Näistä kahdesta, keskenään kilpailleesta kryptografiaa ja koodinmurtoa opettaneesta oppilaitoksesta Moskovassa sijaitsevalla KGB:n korkeakoululla oli huomattavasti parempi maine. Sekä KGB että GRU rekrytoivat henkilöstöään matematiikan ja fysiikan opetuksesta tunnetuista siviilioppilaitoksista, kuten Moskovan valtionyliopistosta, Moskovan insinöörifysiikan instituutista sekä Moskovan fysiikan ja teknologian instituutista. Moskovan valtionyliopisto oli aikoinaan myös tiiviisti mukana KGB:n teknisen osaston perustamisessa. (Borogan & Soldatov, 2022; Meduza, 2018) Vaikka kyseessä olikin virallisesti tarkastellen siviilioppilaitokset, voidaan niiden kuitenkin todeta toimineen erittäin todennäköisesti tiedusteluviranomaisten ohjauksessa.

Neuvostoliiton hajottua joulukuussa 1991 myös KGB:n signaalitiedustelun koulutus- ja rekrytointitoiminnot siirrettiin samassa yhteydessä perustettuun viestinnän ja informaation virasto FAPSI:in. Samalla Moskovassa sijaitseva, entinen KGB:n korkeakoulu nimettiin kryptografian, tietoliikenteen ja tietojenkäsittelytieteiden instituutiksi – IKSI:ksi (*ven. ИКСИ, Институт криптографии, связи и информатики).* (Venäjän turvallisuuspalvelu FSB, n.d.-a) FAPSI jatkoi KGB:n aikaista, Moskovan alueen oppilaitoksiin suuntautunutta henkilöstörekrytointia. FAPSI myös rahoitti IKSI:n alaisuuteen perustetun tietoturvakorkeakoulujen koulutus- ja metodologisen liiton perustamista. (Borogan & Soldatov, 2022) Liittoon kuului edustajia yliopistoista, instituutioista sekä yrityksistä (ParkHous, 2022). IKSI:n perustaminen sopi FAPSI:n tarkoitusperiin, sillä näin pystyttiin vahvistamaan Venäjän sotateollistakompleksia, sekä sitomaan siviilioppilaitokset entistä tiukemmin osaksi valtiollista järjestelmää.

FAPSI ajettiin alas vuonna 2003 ja sen toiminnot siirrettiin osaksi turvallisuuspalvelu FSB:tä. Samalla myös yhteistyö siviilioppilaitosten kanssa, sekä niihin kohdistettu henkilöstörekrytointi siirtyi FSB:lle. Samoin KGB:n aikana perustettu ja sittemmin FAPSI:ssa toiminut kryptografian, tietoliikenteen ja tietojenkäsittelytieteiden instituutti IKSI siirrettiin osaksi FSB:tä, jolloin siitä tuli osa FSB:n akatemiaa. Tieto- ja kyberturvallisuuden opetusta lisättiin siviilioppilaitoksissa, kun opetus käynnistettiin 2000-luvun puolivälissä kaikkiaan 73 yliopistossa. IKSI vastasi opetuksen valvonnasta sekä opetustavoitteiden ja vaatimusten määrittelystä. (Borogan & Soldatov, 2022) Kyberkoulutuksessa noudatettiin tiukasti Neuvostoliiton mallia, jossa tekninen osaaminen ja tehokkuus menivät eettisyyden edelle. Venäjällä otettiin vuonna 2009 käyttöön uusi koulutusstandardi, jonka avulla kyberturvallisuudesta luotiin Venäjän korkeakoulutuksen kansallinen painopiste. Neuvostoliitolla oli yksi maailman suurimmista insinööriyhteisöistä, joka oli pitkälti sotateollisen yhteistyön ansiota. Erilaiset tutkimuslaitokset, korkeakoulut ja teollisuuden yritykset työskentelivät tuolloin yksinomaan asevoimille ja KGB:lle. Tätä valtiota ja sen tiedustelupalveluita palvelevaa järjestelmää ei Neuvostoliiton hajottua koskaan muutettu – päinvastoin. Vladimir Putinin ensimmäisen presidenttikauden alusta lähtien kyseistä lähestymistapaa vahvistettiin entisestään. (NATO, 2020, ss. 38–44)

Venäjän turvallisuus- ja tiedusteluviranomaiset eivät 2000-luvun loppupuolella rajoittaneet henkilöstörekrytointia ainoastaan oppilaitoksiin ja yksityisiin yrityksiin, vaan rekrytointeja alettiin kohdistamaan myös rikoksista tuomittuihin hakkereihin. Turvallisuuspalvelu FSB:n 18.keskus on vastuussa kyberrikollisia vastaan nostettavista syytteistä. (NATO, 2020, s. 38) FSB vastaa myös kyberyhteistyöstä ulkomaisten kyberviranomaisten kanssa, johon sisältyy muun muassa kyberrikollisten tunnistamista ja paikantamista. Muun muassa tätä yhteistyökanavaa on käytetty hyväksi potentiaalisten ja kyvykkäiden kyberrikollisten löytämiseksi sekä rekrytoimiseksi. Tämä yhteiskunnallinen asema on tarjonnut FSB:lle mahdollisuuden neuvotella rikoksesta tuomittavien kanssa, ja tarjota heille mahdollisuus joko liittyä FSB:hen tai siirtyä suorittamaan vankeusrangaistustaan. (Borogan & Soldatov, 2022).

Venäjän asevoimien vuonna 2013 perustettujen kyberjoukkojen ensirekrytointi kohdistettiin FSB:n tapaan niin ikään teknillisiin yliopistoihin. Puolustusministeri Sergei Shoigu tiukensi

myös asepalveluksen rajoja, jonka myötä yliopistosta valmistumisen jälkeen oli välttämätöntä suorittaa asepalvelus. (Brooks & Lysenko, 2018) Teknillisten korkeakoulujen opiskelijoille tarjottiin kaksi mahdollisuutta: lähteä suorittamaan asepalvelus Siperiassa sijaitsevaan yksikköön huonoilla lomamahdollisuuksilla, tai liittyä osaksi kyberjoukkoa ja päästä lomille jokainen viikonloppu. Vuoteen 2014 mennessä tietoturvallisuutta opettavien siviilikorkeakoulujen määrä oli kasvanut 73:sta 170:een. Asevoimat plagioivat myös muita FSB:n käyttämiä ja kehittämiä rekrytointikeinoja, kuten erilaisia siviilioppilaitoksissa järjestettäviä kyberhyökkäys ja -puolustuskilpailuja. (Borogan & Soldatov, 2022) Harjoitukset toimivat Venäjän tiedustelupalveluille erinomaisena rekrytointimenetelmänä.

Venäjän asevoimat on onnistunut rakentamaan omasta kybertoiminnastaan sekä rekrytointitapahtumistaan kiehtovan kokonaisuuden, jonka myötä asevoimista on opiskelijoiden keskuudessa tullut FSB:tä suositumpi kyberammattilaisuuden vaihtoehto. Edellä kuvattu koulutus- ja rekrytointimekanismi on pysynyt ennallaan vielä tähän päivään saakka. Perinteinen rekrytointipolku käynnistyy sillä, että yliopistossa teknillisiä aineita opiskelleelle miehelle tarjotaan mahdollisuus suorittaa pakollinen asepalvelus kaukana kotoa ilman lomia, tai vaihtoehtoisesti liittyä kyberjoukkoihin. Asepalveluksen jälkeen yksi tai useampi turvallisuusviranomaisista lähestyy häntä ja tarjoaa töitä, jolloin houkuttelevaksi verhoiltu työtarjous hyväksytään.

4.3 Venäläiset kyberuhkatoimijat (APT-ryhmät)

Venäjän valtiollista kybertoimintaa käytännön tasolla toteuttavat sen eri turvallisuus- ja tiedustelupalveluihin integroidut valtiolliset kyberuhkatoimijat, eli APT-ryhmät. Kuten tämän tutkimuksen luvussa 4.2. esiteltiin, niin kaikilla Venäjän turvallisuus- ja tiedustelupalveluilla on omat kybertoimintonsa, joiden lisäksi virastoilla on myös kybertutkimukseen ja -kehittämiseen keskittyneitä laitoksia, jotka muun muassa suunnittelevat ja valmistavat kyberaseita kyberuhkatoimijoiden käyttöön. Tässä alaluvussa käsitellään kaikki keskeisimmät Venäjän valtiolliset APT-ryhmät sekä niiden ominaispiirteet. Tämän alaluvun käsittelystä on rajattu pois tutkimus- ja kehittämistoimintaan keskittyneet laitokset. APT-ryhmistä käytetään lähteistä riippuen lukuisia eri nimityksiä, ja tässä alaluvussa käytettävät nimet ovat MITRE:n määritelmien mukaisia.

4.3.1 Gamaredon (FSB)

FSB:n alainen APT-ryhmä Gamaredon on perustettu vuonna 2013, juuri ennen Venäjän suorittamaa Krimin niemimaan miehitystä. Gamaredonin tehtävänä on erityisesti Ukrainaa vastaan kybertoimintaympäristössä suoritettavat tiedustelu-, datan keräys ja sabotaasitehtävät. Ryhmä suorittaa myös tiedustelu- ja sabotaasioperaatioita länsimaiden valtionhallintoa ja sotilasorganisaatioita vastaan. (Ukrainan turvallisuuspalvelu SBU, 2021a) Gamaredon koostuu venäläisten FSB-agenttien ohella myös entisistä Ukrainan turvallisuuspalvelu SBU:n *(ukr. Служба безпеки України)* loikkareista, joiden asemapaikka oli SBU:ssa ollessaan Krimin niemimaalla. Kyseiset henkilöt loikkasivat FSB:n palvelukseen niin ikään Krimin miehityksen myötä. (Ukrainan turvallisuuspalvelu SBU, 2021b) Ukrainan turvallisuuspalvelu SBU julkaisi marraskuussa 2021 Gamaredonia käsittelevän teknisen raportin. Raportissa osoitettiin, että Gamaredon kuuluu osaksi Venäjän turvallisuuspalvelu FSB:tä ja toimii fyysisesti Sevastopolissa, osana Krimin niemimaalle sen miehityksen myötä perustettua FSB:n vastatiedustelutoimintoa. (Ukrainan turvallisuuspalvelu SBU, 2021a)

Ryhmän operatiivista toimintaa ohjataan Moskovassa sijaitsevasta FSB:n 18. keskuksesta, joka tunnetaan myös tietoturvallisuuskeskuksena. Keskus on erikoistunut kybertoimintaympäristössä suoritettavaan vastatiedusteluun ja sabotaasitehtäviin (Dossier, n.d.). Se vastaa FSB:ssä muun muassa Venäjän kansalaisten internetin käytöstä, ja tekee päätökset verkosta poistettavasta materiaalista sekä siitä, millaiseen materiaaliin venäläisten IP-osoitteiden pääsyä rajoitetaan (Agentura, n.d.-b).

Venäjän suorittaman Krimin niemimaan laittoman miehityksen jälkeen Gamaredon on jatkanut säännöllistä vaikuttamista Ukrainan hallintoa, viranomaisia sekä kriittistä infrastruktuuria kohtaan. Ryhmä käyttää verrattain yksinkertaisia sekä koruttomia, itse rakennettuja menetelmiä ja se ei varsinaisesti pyri peiteltyyn toimintaan, eikä sitä haittaa, vaikka se paljastuisi. (Ukrainan turvallisuuspalvelu SBU, 2021a) Tämä ilmenee toisinaan erittäin röyhkeinä ja rohkeina tunkeutumisyrityksinä sekä jo paljastuneiden domainien kierrättämisenä (Paloalto, 2022).

Gamaredon on hyökkäyksissään erikoistunut erityisesti Windows-järjestelmiin, jonka lisäksi se on tiettävästi yrittänyt tunkeutua myös Android-laitteisiin. Hyökkäyksillä pyritään sijoittamaan haittaohjelma kohdeorganisaation sisälle, jossa käyttäjät huomaamattaan levittävät sitä itse eteenpäin. Näin saadaan tuhottua suuri joukko käyttäjiä samasta kohdeorganisaatiosta. (Ukrainan turvallisuuspalvelu SBU, 2021a) Ryhmän näkyvä toiminta käynnistyy tyypillisesti sähköpostiviestillä, jossa esiinnytään jonain ajankohtaiseen teemaan sopivana toimijana, kuten viranomaisena. Sähköpostissa on liitetiedosto, joka on nimetty vastaanottaja ja oma kuvitteellinen identiteetti huomioiden. (Ukrainan turvallisuuspalvelu SBU, 2021a)

Gamaredon käyttää kohteiden tiedustelussa ja tarvittavan ennakkotiedon hankkimisessa todennäköisesti hyväkseen Venäjän turvallisuuspalvelu FSB:n vastatiedustelun toteuttamia perinteisiä menetelmiä, kuten henkilötiedustelua. Lisäksi olisi luonnollista, että ryhmä hyödyntää kaikin mahdollisin keinoin ryhmän jäseninä toimivien entisten Ukrainan turvallisuuspalvelu SBU:n upseereiden kohdetuntemusta. Näillä keinoilla Gamaredon saa todennäköisesti tiedusteltua hyökkäyksille suotuisimmat kohteet ja henkilöt, sekä heillä käytössä olevat järjestelmät. Tällä on puolestaan suora vaikutus kyberaseiden valintaan. On kuitenkin huomioitava, että Ukrainan turvallisuuspalvelu ja valtionhallinto ovat todennäköisesti pyrkineet uudistamaan järjestelmäänsä mahdollisimman paljon Krimin niemimaan miehityksen jälkeen, jonka voi olettaa ainakin osittain vaikeuttaneen FSB:n vastatiedustelun ja Gamaredonin tiedonhankintaa. Ryhmä on toiminut Ukrainaa vastaan lähes vuosikymmenen ajan. Koska Ukrainan sodassa ei ole nähtävissä tosiasiallisia päättymisen merkkejä, on erittäin todennäköistä, että ryhmä jatkaa Venäjän etujen ajamista ja sotaan aktiivista osallistumista.

4.3.2 Turla (FSB)

Turla on yksi pitkäaikaisimmista venäläisistä kyberuhkatoimijoista, jonka johto- ja ohjaussuhteista ei ole toistaiseksi täyttä varmuutta. Yhdysvaltain kansallisen turvallisuuspalvelu NSA:n johtaman kyberkoalition julkaisemassa raportissa (2022) todetaan, että Turla on globaalissa kyberyhteisössä yhdistetty Venäjän hallinnon alaiseksi kyberuhkatoimijaksi, mutta koalitio ei toistaiseksi vastaavaa linkitystä ole tehnyt. Muun

muassa Viron ulkomaantiedustelupalvelu on yhdistänyt Turlan osaksi FSB:tä (Viron ulkomaantiedustelupalvelu, 2018, s. 53). Huolimatta Turlan johto- ja ohjaussuhteista, se on ollut MITRE:n (2022c) mukaan aktiivinen tiettävästi jo vuodesta 2004 lähtien. Tästä tekee mielenkiintoisen se, että kuten tämänkin tutkimuksen alaluvussa 4.1. todetaan Venäjän kybertoiminnan historiasta, turvallisuuspalvelu FSB:ssä koettiin kybertoiminnan reformi vuonna 2004. Tuolloin FSB:n ensimmäinen varsinainen kyberyksikkö, vuonna 1998 perustettu tietokone- ja tietoturvallisuuden päähallinto UKIB muutettiin nykyiseksi tietoturvakeskukseksi, eli 18. keskukseksi. Keskus sai tuolloin tehtäväkseen muun muassa ulkomaisiin tietoverkkoihin kohdistuvan tiedustelutoiminnan. Tämän reformin jälkeen myös Turla aktivoitui ja on ollut aktiivinen siitä lähtien. Ottaen huomioon, että FSB:n 16. keskus suorittaa kyberhyökkäyksiä Dragonfly APT-ryhmänä, olisi loogista, että myös 18. keskus suorittaisi tietoverkkoihin kohdistettavaa tiedustelutoimintaa omalla APT-aliaksellaan. Näin ollen voidaankin pitää mahdollisena, että Turla on tosiasiallisesti FSB:n 18. keskus.

Turlan hyökkäykset ovat tyypillisesti kohdistuneet Naton jäsenmaiden hallintoihin, diplomaatteihin, korkean tason poliitikkoihin, aseteknologian yrityksiin sekä muihin tahoihin, joilla Venäjä katsoo olevan tiedustelullista lisäarvoa (CISA, 2022). Turla hankkii pääsyn kohdejärjestelmään tyypillisesti toimitusketjuhyökkäyksen tai sähköpostikalastelun avulla. Sähköpostikalastelussa se käyttää erityisesti hyväkseen ohjelmistojen ominaisuuksia, joiden kautta se pystyy tunkeutumaan kohdejärjestelmään. Tällaisia ovat esimerkiksi Microsoft Office-palveluissa olevat makrot sekä Word-sovelluksen asiakirjamallit. (Cyberint, 2019)

Sisäänpääsyn jälkeen Turla, kuten useat muutkin APT-ryhmät, asentaa kohdejärjestelmään uusia haittaohjelmia ja työkaluja, joilla se kykenee liikkumaan järjestelmissä ja tietoverkoissa yhä syvemmälle. Turla käyttää hyväkseen modulaarisia haittaohjelmia, joiden avulla se pystyy mukauttamaan kunkin hyökkäyksen aina tarpeen mukaiseksi. Kohdejärjestelmässä toimiessaan Turla on erikoistunut erityisesti tiedustelullisiin ja tiedonhankintaan keskittyneisiin operaatioihin. Turlalle on tyypillistä myös se, että se käyttää kaapattuja satelliittiyhteyksiä omien kyberhyökkäystensä komentopalvelimina *(eng. command & control server, C2).* Tällä se kykenee vaikeuttamaan komentopalvelimen paikantamista ja hyökkäyksen yhdistettävyyttä juuri siihen itseensä. Tällä samalla tarkoitusperällä Turla

sijoittaa komentopalvelimia myös muiden, ei-venäläisten APT-ryhmien infrastruktuuriin. (David, 2021)

4.3.3 Dragonfly (FSB)

Dragonfly on Venäjän turvallisuuspalvelu FSB:n alainen kyberuhkatoimija, joka tunnetaan virallisesti 16. keskuksena. Se on ollut toiminnassa ainakin vuodesta 2010 lähtien. Dragonfly kohdistaa toimintansa tarkoin valittuihin kohteisiin, erityisesti länsimaiden puolustusteollisuuteen, valtionhallintoihin, energiasektoreihin sekä teollisuuden tarpeisiin elektroniikkaa valmistaviin yrityksiin. (MITRE, 2022e)

Dragonfly suorittaa kohteen tiedustelua muiden APT-ryhmien tapaan ensisijaisesti julkisten lähteiden perusteella. Tällä se pyrkii hankkimaan tietoa muun muassa kohdeorganisaatiossa käytössä olevista järjestelmistä sekä henkilöstöstä. Hankittua tietoa pystytään hyödyntämään edelleen kalasteluviestien yhteydessä. (CISA, 2018a)

Yhtenä keskeisimpänä tietojenkalastelumenetelmänä Dragonfly on käyttänyt sähköpostin liitetiedostoissa hyödynnettävää Microsoft Officen SMB-*protokollaa (eng. Server Message Block)*, joka on tarkoitettu työaseman ja etäpalvelimen väliseen asiakirjaliikenteeseen. Käytännössä tämä tarkoittaa sitä, että Microsoft Word suorittaa prosessin, jossa keskeisenä tekijänä on varmentaa, että käyttäjällä on tosiasiallinen oikeus käsitellä etäpalvelimella olevia asiakirjoja. Tämä tapahtuu siten, että Microsoft Wordin prosessi lähettää käyttäjän kirjautumistietojen tiivisteen *(eng. hash)* etäpalvelimelle ennen pyydetyn tiedoston hakemista. Tiiviste on kirjautumistiedoista generoitu numero- ja kirjainyhdistelmä, jolla selkokielinen teksti saadaan salattua. Dragonfly asettaa kalastelun yhteyteen oman etäpalvelimensa, jolloin se saa käyttöönsä myös käyttäjän kirjautumistietojen tiivisteen. Tämän jälkeen Dragonfly pystyy käyttämään erilaisia salasanan murtotekniikoita saadakseen selvitettyä selkokielisen salasanan. Murrettujen kirjautumistietojen avulla Dragonfly pystyy toimimaan sellaisissa ympäristöissä, joissa käytetään yksivaiheista todennusta. Kalasteluviestien ohella Dragonfly pyrkii murtautumaan kohdeorganisaatioihin myös toimitusketjuhyökkäysten, sekä luotetuille verkkosivuille asetetun haitallisen sisällön avulla. (CISA, 2018a) Sille on tähän saakka ollut tyypillistä erityisesti tiedustelu- ja

tiedonhankintatehtävät. Sen hyökkäykset kohdistuvat toisinaan myös kriittisen infrastruktuurin toiminnanohjausjärjestelmiin, jolloin lamauttaviin sekä tuhoaviin vaikutuksiin pyrkivien hyökkäysten uhka on ilmeinen. (Congressional Research Service, 2022)

4.3.4 APT29 (SVR)

APT29 on Venäjän ulkomaan siviilitiedustelupalvelu SVR:n alainen kyberuhkatoimija, joka on ollut aktiivinen ainakin vuodesta 2008 lähtien. Myös Cozy Bear-nimellä tunnetun APT-ryhmän toiminta kohdistuu erityisesti Euroopan Unionin ja Naton jäsenten valtionhallintoihin, poliittisiin puolueisiin, tutkimuslaitoksiin sekä ajatushautomoihin. (MITRE, 2022b) Sen ensisijaisena tehtävänä on Venäjän intressejä hyödyttävä tiedustelu ja tiedonhankinta. Toisinaan se toteuttaa myös tietoverkkojen ja -järjestelmien lamauttavia iskuja. APT29 pyrkii toimimaan erityisen huomaamattomasti ja tunkeutumaan järjestelmiin paljon ennen toteutettavaa iskua, joka tekee sen toimien havaitsemista erityisen hankalaa. Odotusaikana se keskittyy vain huomaamattomaan tiedonkeruuseen ja uusien haittaohjelmien asentamiseen. Tämän kyberuhkatoimijan käyttämät kyberaseet ovat tyypillisesti erilaisia haittaohjelmia, jotka ovat joko ryhmän itsensä tai Venäläisen sotateollisen kompleksin valmistamia, ja ne ovat rakennettu jotain tiettyä ohjelmistossa tai käyttöjärjestelmässä olevaa haavoittuvuutta varten. (TeamPassword, 2021)

APT29:n toiminta käynnistyy muiden toimijoiden tapaan kohdeorganisaation tiedustelulla ja sen sisältä löytyvien potentiaalisten haavoittuvuuksien kartoittamisella. Tämän jälkeen APT29 lähestyy kohdeorganisaation työntekijöitä tietojenkalastelusähköpostilla. (Kaspersky Lab, 2015) Sähköposti sisältää tyypillisesti joko linkin, joka ohjaa käyttäjän haittaohjelman sisältävälle verkkosivulle, tai vaihtoehtoisesti varsinaisen haittaohjelman sisältävän liitetiedoston. (Kaspersky Lab, n.d.)

Verkkosivu, jossa haittaohjelma sijaitsee, on usein nimetty jotain virallista verkkosivua muistuttavaksi. Käyttäjää houkutellaan lataamaan verkkosivulla oleva tiedosto. Tiedosto pitää sisällänsä automaattisesti käynnistyvän haittaohjelman, joka leviää kohdejärjestelmään, kun verkkosivuilta ladattu tiedosto avataan. (Kaspersky Lab, n.d.) Sähköpostin liitetiedostona oleva haittaohjelma toimii vastaavalla periaatteella, ja niitä on

havaittu muun muassa kuva-, ääni-, video- ja HTML-tiedostoina. (Baumgartner & Raiu, 2015) Sähköpostin liitetiedostona olevien haittaohjelmien leviäminen perustuu siihen, että tiedostot ovat houkuttelevasti nimettyjä ja niistä avautuu haittaohjelman lisäksi jokin video, ääni tai kuva, jota sähköpostin vastaanottaja lähtee jakamaan eteenpäin.

Tämän kyberuhkatoimija pyrkii massamaisen kirjautumistietojen hankinnan lisäksi luomaan järjestelmiin niin sanottuja takaovia, joita voidaan käyttää hyväksi tiedustelu- ja tiedonhankintatarkoituksessa. (Matisoft, n.d.) Näitä takaovia hyödyntäen APT29 on toteuttanut myös niin sanottuja toimitusketjuhyökkäyksiä. Toimitusketjuhyökkäyksessä hyökkäys tapahtuu kolmannen osapuolen, esimerkiksi laitevalmistajan, palveluntarjoajan tai operaattorin tarjoamien palveluiden tai tuotteiden kautta. Hyökkääjä suorittaa tiedustelua kohdeorganisaation yhteistyökumppaneihin ja pyrkii kartoittamaan niiden järjestelmissä olevia haavoittuvuuksia, joiden avulla hyökkääjä saisi pääsyn järjestelmään. Tavoitteena on jalansijan saaminen, jonka avulla voidaan suorittaa erilaisia jatkohyökkäyksiä. (Kyberturvallisuuskeskus, 2022) Eräs historian tunnetuimmista toimitusketjuhyökkäyksistä on APT29:n vuonna 2020 toteuttama, yhdysvaltalaista ohjelmistokehitysyhtiö SolarWindsiä hyväksikäyttäen tehty hyökkäys. Tässä tapauksessa APT29 hankki pääsyn SolarWindsin järjestelmiin muun muassa sähköpostikalastelujen avulla. Järjestelmässä ollessaan se kykeni sisällyttämään oman haittaohjelmansa erään SolarWindsin ohjelmistopäivityksen yhteyteen. SolarWindsin yli 18 000 asiakasta, mukaan lukien Microsoft, Intel, Cisco ja Deloitte, latasivat ohjelmistopäivityksen, jolloin myös APT29:n haittaohjelma asentui heidän järjestelmiinsä. (Kyberturvallisuuskeskus, 2020)

4.3.5 APT28 (GRU)

APT28 on Venäjän sotilastiedustelusta vastaavan tiedustelupäähallinto GRU:n alainen kyberuhkatoimija, joka tunnetaan virallisesti 85. Erikoispalvelukeskuksena (NSA, 2020). APT28 on ollut aktiivinen ainakin vuodesta 2007 lähtien ja se on kohdistanut toimintansa erityisesti länsimaiden valtionhallintoja, asevoimia ja turvallisuusviranomaisia kohtaan. Sen päätehtävänä on kohdeympäristössä toteutettava tiedustelu ja tiedonhankinta. Se pyrkii hankkimaan sellaisia tietoja ja asiakirjoja, joilla pystytään tukemaan Venäjän valtionjohdon päätöksentekoa sekä narratiivia. (FireEye, 2017) APT28 on toiminnassaan huomattavasti

SVR:n alaista APT29:ää suoraviivaisempi. Siinä missä APT29 saattaa piilotella tietoverkoissa kuukausia ja vuosia, APT28 on tyypillisesti toiminut lähes välittömästi kohdejärjestelmän sisään päästyään. (TeamPassword, 2021) Myös Fancy Bear nimellä tunnettu APT28 käyttää hyökkäyksissään tyypillisesti erilaisia, sen itsensä tai Venäjän sotateollisen kompleksin valmistamia haittaohjelmia, jotka on kehitetty jotain ohjelmistossa tai käyttöjärjestelmässä olevaa haavoittuvuutta varten. APT28 on myös erityisen kehittynyt hyödyntämään nollapäivähaavoittuvuuksia, eli sellaisia sovelluksissa tai järjestelmissä olevia haavoittuvuuksia, joita ei ole aiemmin tiedostettu olevan. (FireEye, 2017)

Myös APT28:n, kuten useiden muidenkin toiminta käynnistyy kohdeorganisaation tiedustelululla (FireEye, 2017). Tällä pyritään selvittämään kohdeorganisaatiossa käytössä olevia sovelluksia, käyttöjärjestelmiä, palveluntarjoajia sekä tietysti organisaation henkilöstö. Näiden tietojen avulla pystytään valitsemaan käytettävät kyberaseet sekä henkilöt, keihin suoritetaan ensivaiheen tietojenkalasteluoperaatio. Tämä voidaan suorittaa käytännössä minkä tahansa viestivälineen tai sosiaalisen median kautta, mutta suosituin keino on sähköpostitse lähetettävä kalasteluviesti.

APT28:lla on neljä sille ominaista keinoa tunkeutua kohdejärjestelmään. Se käyttää tyypillisesti kahden tyyppisiä kalasteluviestejä. Ensimmäisessä mallissa sähköpostin liitteenä on haittaohjelman sisältävä liitetiedosto, joka avattaessa laukaisee varsinaisen haittakuorman ja luo pääsyn kohdejärjestelmään. Toisessa mallissa sähköpostin yhteydessä on linkki, jonka uskotellaan olevan sähköpostin selainversio, niin sanottu webmail. Käyttäjän klikatessa linkkiä, avautuu täysin aidon näköinen webmailin kirjautumisikkuna, johon käyttäjä syöttää käyttäjätunnuksensa sekä salasanansa. Tosiasiallisesti tämä sivu on kuitenkin APT28:n ylläpitämä, jonka myötä se onnistuu kaappaamaan käyttäjän kirjautumistiedot ja hyödyntämään niitä sähköpostien lukemiseen ja niiden varastamiseen. (Mwiki ym., 2019, ss. 221–223)

Sähköpostitse tehtävien lähestymisien lisäksi APT28:lle on ominaista sijoittaa haittaohjelma jollekin aidolle verkkosivustolle. Tässä mallissa APT28 asettaa sivustolle haittaohjelman, joka uudelleenohjaa käyttäjän halutulle sivustolle, jonka yhteydessä käyttäjät myös profiloidaan. Tietyn kohdeprofiilin käyttäjät ohjataan edelleen haittaohjelman sisältävään ympäristöön,

jonka kautta se saadaan asennettua kohteen työasemalle ja tietojärjestelmään. Tätä menettelyä käytettiin muun muassa 2014 Puolan valtionhallinnon verkkosivuilla tehdyssä hyökkäyksessä ja profiloinnissa. Neljäs tiedossa oleva toimintamalli on käyttää hyväkseen kohdeorganisaation verkkoon yhteydessä olevia palvelimia, sekä palvelimilla olevien ohjelmistojen haavoittuvuuksia. Tässä on keskiössä itse toimintaa edeltävä, tietoverkoissa tapahtuva tiedustelu, jolla pyritään selvittämään kohdeorganisaation käyttämät ohjelmistot sekä niiden versiot. Näitä tietoja hyödyntäen APT28 pystyy valitsemaan sopivan lähestymistavan sekä kyberaseen, jolla se kykenee murtautumaan kohdejärjestelmään. Järjestelmään sisään pääsyn jälkeen se kartoittaa uusia haavoittuvuuksia ja keinoja päästäkseen yhä syvemmälle kohdeorganisaation tietoverkoissa. (FireEye, 2017, ss. 10–12)

4.3.6 Sandworm (GRU)

APT28:n ohella Venäjän tiedustelupäähallinto GRU:n alaisuudessa on ainakin vuodesta 2007 toiminut toinen merkittävä kyberuhkatoimija: Sandworm. Kyseessä on GRU:n alainen erikoistekniikan keskus (GTsST). Siinä missä APT28 on pääosin keskittynyt huomaamattomiin, valtionhallintoon, asevoimiin ja poliittiseen järjestelmään kohdistuviin tiedustelu- ja datavarkausoperaatioihin, Sandworm on erikoistunut aggressiivisiin kyberhyökkäyksiin, joiden on tarkoitus tuottaa lamauttavia sekä tuhoavia vaikutuksia erityisesti valtionhallintoon sekä energia-, kuljetus- ja taloussektoreiden kriittiseen infrastruktuuriin. (MITRE, 2022d)

Sandwormin toimet ovat keskittyneet erityisesti Ukrainaan ja Georgiaan, sekä niiden kriittiseen infrastruktuuriin. Ennen Venäjän vuonna 2008 aloittamaa Georgian sotaa Sandworm suoritti palvelunestohyökkäyksiä lukuisiin kohteisiin niin valtionhallinnossa, pankkisektorilla kuin myös mediataloissa. Palvelunestohyökkäykset sekä datan tuhoamiseen pyrkineet operaatiot *(eng. wiper)* jatkuivat Ukrainan kriittisessä infrastruktuurissa Krimin niemimaan miehityksen yhteydessä vuodesta 2014 lähtien. Sandwormin pääasiallinen tarkoitus on tunkeutua kohteen tietojärjestelmiin sekä teollisuuden ohjausjärjestelmiin (esim. vesi-, sähkö- ja ydinvoimaloissa), joissa se kykenee sen jälkeen esimerkiksi hävittämään datan tai sulkemaan energian tuotannon. (HHS, 2022) Erilaisia kriittisen infrastruktuurin ohjausjärjestelmiin sekä valtionhallinnon tietojärjestelmiin kohdistuneita

hyökkäyksiä on havaittu myös Ukrainan laajamittaisessa sodassa keväästä 2022 lähtien. Muun muassa erilaisten laajamittaisten datan hävitykseen keskittyneiden ”Wiper”-hyökkäysten on uskottu olevan Sandwormin toteuttamia.

4.3.7 Ember Bear

Toistaiseksi tuntemattomassa ohjaus- ja johtosuhteessa toimiva venäläinen kyberuhkatoimija Ember Bear on ollut aktiivinen ainakin maaliskuusta 2021 lähtien, ollen yksi tuoreimmista merkittävistä APT-ryhmistä. Se on kohdistanut toimintansa ensisijaisesti Ukrainaan ja Georgiaan, mutta on toiminut myös länsimaisia valtionhallintoja sekä lääke- ja taloussektoreita vastaan. (MITRE, 2022a) Ember Bear on sen lyhyen historian aikana keskittynyt tuhoavaan, datan hävittämiseen sekä sen varastamiseen tähtääviin operaatioihin. (Crowdstrike, 2022)

Se käyttää varastamaansa dataa Venäjän intressejä tukevien informaatio-operaatioiden tukemiseen. Yhtenä esimerkkinä informaatio-operaatioiden tukemisesta toimii vuonna 2022 Ukrainan sodan yhteydessä havaittu ”Free civilian leaks”, jossa Ukrainan kansalaisten henkilötietoja kerrottiin julkaistavan Tor-verkossa. Ember Bearin uskotaan olevan myös vastuussa tammikuussa 2022, ennen laajamittaisen sodan käynnistämistä, Ukrainassa suoritettuun WhisperGate-hyökkäykseen. (Crowdstrike, 2022)

4.4 Kybervaikuttaminen venäläisissä virallisasiakirjoissa

Tässä alaluvussa lukijalle esitellään kyber- ja informaatioympäristöä käsittelevät Venäjän valtion virallisasiakirjat: *Venäjän federaation ulkopolitiikan konsepti (2016), Venäjän federaation kansallinen turvallisuusstrategia (2021), Venäjän federaation tietoturvallisuuden doktriini (2016), Venäjän federaation kansainvälistä tietoturvallisuutta koskevat valtionpolitiikan perusperiaatteet (2021), Venäjän federaation sotilasdoktriini (2014)* sekä *Luonnos Venäjän federaation kyberturvallisuuden strategisesta konseptista (2014).* Nämä kuusi asiakirjaa ovat julkisia, strategisen tason dokumentteja, jotka edustavat ennen kaikkea Venäjän valtionjohdon virallisia näkökulmia ja mielipiteitä. Niiden strategisen tason luonteen

vuoksi niissä ei käsitellä kybertoimintaa kovinkaan seikkaperäisesti, vaan asiakirjoissa määritellään strategisen tason tavoitteet sekä tehtävät näiden tavoitteiden saavuttamiseksi.

Virallisasiakirjoja on käsitelty kybertoimintaympäristön, mutta myös Venäjän yleisestä ulko- ja turvallisuuspoliittisesta näkökulmasta. Tämän tutkimuksen viitekehyksessä on tarpeellista käsitellä kybertoiminnan lisäksi muun muassa Venäjän näkemyksiä kansainvälisistä kumppanuussuhteista sekä Venäjän naapurivaltioihinsa ja länsimaihin kohdistamaa narratiivia. Tällä lähestymistavalla lukijaa pyritään aktivoimaan avoimeen pohdintaan siitä, mikä venäläisessä ajattelussa on johtanut vuonna 2014 käynnistyneeseen Ukrainan sotaan ja sen laajenemiseen helmikuussa 2022.

4.4.1 Venäjän federaation ulkopolitiikan konsepti (2016)

Venäjän federaation ulkopolitiikan konseptissa käsitellään hyvin laajasti globaalia maailmanjärjestyksen tilaa venäläisestä näkökulmasta tarkasteltuna. Konseptissa käsitellään muun muassa Venäjän kumppanuuksia eri kansainvälisten järjestöjen ja valtioiden kanssa sekä hyvin laaja-alaisesti sotilaspoliittisia ja taloudellisia aihealueita. Ulkopolitiikan konseptin yhtenä pääviesteistä voidaan todeta olevan se, että Venäjä haluaa kaikin keinoin säilyttää sekä edelleen kehittää omavaraisuuttaan talouden ja osaamisen eri osa-alueilla, sillä konseptin mukaan länsimaisen yhteiskunnan koetaan pyrkivän pakottamaan Venäjä turvautumaan ulkomaiseen osaamiseen ja tekniikkaan. Konsepti on poliittisstrateginen asiakirja, joka käsittelee Venäjän federaation ulkopolitiikkaa kokonaisuudessaan. Tästä johtuen siinä sivutaan, mutta ei käsitellä merkittävän syvällisesti tietoturvaan ja kybertoimintaympäristöön liittyviä kokonaisuuksia.

Venäjä korostaa Yhdistyneiden kansakuntien (YK) turvallisuusneuvoston roolia ja tärkeyttä eräänä globaalin turvallisuuden ja maailmanjärjestyksen ajurina, ja kuinka se nojaa kaikissa turvallisuuspoliittisissa ratkaisuissaan YK:n säännöstöön ja peruskirjaan (Kreml, 2016a). YK:n turvallisuusneuvoston pysyväisjäsenenä oleminen on myös Venäjän näkökulmasta ilmeisen tärkeää, sillä turvallisuusneuvosto vaatii täyden yksimielisyyden päätöksiä tehdessään. Näin ollen Venäjä pystyy myötävaikuttamaan sille epäedullisten päätösten tekemättä jättämiseen. Ulkopolitiikan konseptissaan Venäjä muun muassa asettaa ehdottomaksi

tavoitteekseen sen, että YK:n turvallisuusneuvoston yleisten jäsenten mahdollisten lisäpaikkojen perustaminen tulee vaatia kaikkien jäsenmaiden suostumus, jonka lisäksi viiden pysyvän jäsenen asema on säilytettävä sellaisenaan (Kreml, 2016a, s. 8).

Turvallisuuspoliittisesta näkökulmasta tarkasteltuna konseptin yksi keskeinen päämäärä on ulkomailla asuvien venäläisten sekä ”maanmiesten” oikeuksien ja etujen turvaaminen (Kreml, 2016a, s. 8). Termin ”maanmies” erottelu ulkomailla asuvasta venäläisestä viittaa mahdollisesti entisiin Neuvostoliiton maihin ja niissä asuviin, yhä venäläismielisiin kansalaisiin. Asiakirjan mukaan Venäjä tulee estämään sotilaalliset interventiot sekä muut kolmansien osapuolten toimet YK:n suojeluvastuun periaatteen täytäntöönpanon varjolla (Kreml, 2016a, s. 8). Suojeluvastuun periaatteessa on kyse kansainvälisestä velvoitteesta puolustaa yksilöitä sellaisillakin alueilla, jossa aluetta laillisesti hallitseva valtio ei niiden turvallisuutta kykene takaamaan (Ulkoministeriö, 2020, s. 4). Venäjä on nojannut YK:n suojeluvastuun periaatteeseen muun muassa vuonna 2022, oikeuttaakseen itselleen Ukrainaan kohdistettuja hyökkäystoimiaan (Ashby, 2022). Ulkopolitiikan konseptin mukaan Venäjä aikoo myös tehostaa Venäjän federaation valtionrajojen kansainvälistä rekisteröintiprosessia erityisesti niillä alueilla, joissa Venäjä käyttää suvereeneja oikeuksia ja lainkäyttövaltaa (Kreml, 2016a, ss. 8–9). Tällaisia alueita on Ukrainassa muun muassa Krimin niemimaa sekä Itä- ja Kaakkois-Ukrainassa olevat, separatistien hallussa olleet ja vuonna 2022 Venäjän laittomasti itseensä liittäneet alueet.

Venäjä tunnistaa myös nykymaailmalle ominaisen, rajat ylittävän uhan olemassa olemisen ja kasvun. Näiden joukossa huomioidaan myös tietoverkoissa tapahtuva rikollisuus ja valtiollinen toiminta (Kreml, 2016a, ss. 16–17). Venäjä ilmaisee ryhtyvänsä kaikkiin tarvittaviin toimenpiteisiin varmistaakseen kansallisen ja kansainvälisen tietoturvan, sekä torjuakseen informaatioympäristössä esiintyviä valtiollisia ja sotilaspoliittisia uhkia (Kreml, 2016a, s. 9)

Konseptissa todetaan avoimesti myös se, että Venäjä tulee kehittämään omia informaatiovaikuttamiskeinojaan, joilla se pyrkii vaikuttamaan ulkomailla yleiseen mielipiteeseen ja vahvistamaan venäläismedian asemaa globaalissa informaatioympäristössä. Tieto- ja viestintäteknologian kehittämistä tullaan jatkamaan, ja

sitä tullaan käyttämään kyberuhkien torjumiseen sekä informaatiovaikuttamiseen. (Kreml, 2016a, s. 27)

4.4.2 Venäjän federaation kansallinen turvallisuusstrategia (2021)

Venäjän kansallinen turvallisuusstrategia päivitettiin vuonna 2021, jolla korvattiin vuonna 2015 julkaistu versio. Kyseessä on strategisen suunnittelun perusasiakirja, jolla määritellään Venäjän pitkän aikavälin kansalliset edut ja strategiset painopisteet, päämäärät sekä tavoitteet kansallisen turvallisuuden ja kestävän kehityksen takaamiseksi (Kreml, 2021a, ss. 1–2). Asiakirjan yleisessä narratiivissa korostuu uhmakkuus sekä sotilaallisen uhan ja sodan eskaloitumisen kasvanut riski. Kybertoimintaympäristön perspektiivistä tarkasteltuna merkittävin muutos aikaisempaan versioon on ensimmäistä kertaa omana lukunaan huomioitava tietoturvallisuus.

Geopoliittisen epävakauden ja konfliktien kasvu, valtioiden välisten ristiriitojen voimistuminen sekä niihin liittyvän sotilaallisen voimankäytön mahdollisuuden lisääntyminen koetaan kasvavana uhkana. Koetaan myös, että länsimaat rikkovat yhä toistuvasti asevalvontaa koskevia sopimuksia toimittaessaan sotateollisuuteen yhdistettäviä järjestelmiä Venäjän naapurimaihin. (Kreml, 2021a, s. 5) Asiakirjan kokonaisnarratiivi huomioiden asevalvontaa koskevien sopimusten rikkomisessa viitataan todennäköisesti Yhdysvaltoihin ja sen liittolaisten Ukrainalle toimittamaan materiaali- ja koulutustukeen, sekä Ukrainan sotaan jo vuodesta 2014 lähtien osallistuneisiin ulkomaalaisiin vapaaehtoistaistelijoihin. Geopoliittiseen epävakauteen liittyen asiakirjassa todetaan, että useat valtiot kutsuvat Venäjää uhaksi sekä sotilaalliseksi vastustajaksi, jonka myötä kerrotaan olevan olemassa kasvava uhka sille, että aseelliset konfliktit kärjistyvät paikallisiksi sekä alueellisiksi sodiksi (Kreml, 2021a, s. 5). Länsimaita arvostellaan myös liberaalisen elämänkatsomuksen laajentamisesta sekä tarkoituksellisesta venäläisten arvojen ja sen historian vääristämisestä, jolla länsimaiden puolestaan kerrotaan pyrkivän palauttamaan fasismia sekä synnyttämään etnisiä ja uskonnollisia konflikteja. Länsimaiden kuvataan rajoittavan Venäjän kielen käyttöä sekä venäläisten tiedotusvälineiden toimintaa. Lisäksi kansallisen turvallisuusstrategian mukaan Venäjää syytetään perusteettomasti kansainvälisten sopimusten rikkomisesta, kyberhyökkäyksistä sekä vieraan valtion sisäisiin

asioihin puuttumisesta. Ulkomailla asuvien Venäjän kansalaisten ja ”maanmiesten” koetaan joutuvan syrjinnän ja avoimen vainon kohteeksi. (Kreml, 2021a, s. 6)

Uudessa turvallisuusstrategiassa tunnistetaan avaruus ja kybertoimintaympäristö uusina sotilaallisina toimintaympäristöinä, joiden aktiivista tutkimista tulee jatkaa (Kreml, 2021a, s. 5). Asiakirjassa nostetaan yhdeksi kansalliseksi painopistealueeksi turvallisen informaatioympäristön kehittäminen. Tämä tavoite pyritään saavuttamaan keskittämällä koko yhteiskunnan voimavarat muun muassa maanpuolustukseen, yleiseen turvallisuuteen sekä tietoturvaan. Nämä edellä mainitut ovat samalla kolme, kaikkiaan yhdeksästä kansallisesta strategisesta prioriteetista. (Kreml, 2021a, ss. 8–9)

Venäjällä koetaan yhä tärkeämmäksi länsimaihin kohdistuvan teknologisen riippuvuussuhteen poistaminen, ja se pyrkii saavuttamaan globaaleilla markkinoilla johtavan aseman muun muassa tieto- ja viestintätekniikan alalla. Venäjä pyrkii myös nykyaikaistamaan jo Neuvostoliiton ajoilta toimineen sotateollisen kompleksin tuotantopohjan, sekä kasvattamaan niiden valmistamien korkean teknologian tuotteiden määrää. (Kreml, 2021a, ss. 24–25) Sotateollisella kompleksilla tarkoitetaan Venäjän asevoimien ja teollisuuden välistä yhteistyötä, jossa asevoimille kehitetään monipuolisesti materiaalia sotilaallisiin tarkoituksiin.

Turvallisuusstrategiassa on asetettu tavoitteeksi myös Venäjän tieteellinen ja teknologinen kehitys. Venäjällä on tulevaisuudessa pyrkimys panostaa nano- ja kvanttiteknologiaan, robotiikkaan, ”big datan” käsittelyyn sekä tekoälyteknologiaan. Tutkimuslaitosten ja teollisuuden toimijoiden tulee vahvistaa keskinäistä yhteistyötä, jotta maanpuolustusta ja valtion turvallisuutta kyettäisiin palvelemaan entistä paremmin. Asiakirjassa ohjataan myös teknologiaosaamisen ja -välineiden jakamisesta puolustus- ja siviilisektoreiden välillä. (Kreml, 2021a, ss. 29–30) Tämän ohjauksen tosiasiallinen tarkoitus on todennäköisesti mahdollistaa entistä laajempi teknologia-alan yritysten hyödyntäminen asevoimien teknologiatuotannossa ja -kehityksessä.

Venäjä on strategian mukaan sitoutunut käyttämään rauhanturvaamisen mekanismeja rajojensa sisä- ja ulkopuolella tapahtuvien konfliktien ratkaisemisessa. Asiakirjassa todetaan

lailliseksi toteuttaa vaadittavia symmetrisiä ja asymmetrisiä toimenpiteitä vihamielisten toimien lopettamiseksi sekä niiden toistumisen estämiseksi. Vihamielisiksi toimenpiteiksi luetaan muun muassa sellaiset suvereniteettia uhkaavat toimet, jotka liittyvät poliittisten tai taloudellisten pakotteiden soveltamiseen tai kyber- ja informaatiovaikuttamiseen. (Kreml, 2021a, ss. 39–40) Tällä lausumalla Venäjä oikeuttaa itse itselleen sekä kineettisen että kyber- ja informaatioympäristöissä tapahtuvan vaikuttamisen toista valtiota kohtaan. Jo pelkästään kyber- ja informaatiovaikuttamista on hyvin vaikea näyttää toteen, joka yhdessä lavean määrittelyn kanssa luo Venäjälle mahdollisuuden osoittaa perusteet esimerkiksi sotilaalliselle voimankäytölle toista valtiota kohtaan.

Turvallisuusstrategia kulminoituu Venäjän ulkopoliittisten tavoitteiden saavuttamiseen tarvittavien tekijöiden luokitteluun. Kaikkiaan 32 kohdan listasta on tämän tutkimuksen kannalta keskeistä nostaa esille kahdeksan tavoitetta, joilla pyritään lisäämään lukijan ymmärrystä tapahtuneista syy-seuraussuhteista: 1) avustaminen konfliktien syntymisen poistamisessa ja niiden estämisessä Venäjän federaation naapurivaltioiden alueilla, 2) Venäjän federaation liittolaisten ja kumppaneiden tukeminen maanpuolustuksen ja turvallisuuden varmistamiseen liittyvien asioiden ratkaisemisessa sekä neutralisoimalla kolmansien osapuolien yritykset puuttua heidän sisäisiin asioihinsa, 3) Venäjän federaation kansalaisten ja venäläisten yritysten oikeuksien ja etujen suojaaminen ulkomailla, 4) varmistaa ulkomailla asuvien maanmiesten oikeuksien toteutuminen sekä venäläisen kulttuuri-identiteetin säilyminen, 5) veljessuhteiden vahvistaminen Venäjän, Valko-Venäjän ja Ukrainan kansojen välillä, 6) Suorittaa vaadittavat toimenpiteet historian väärentämisyrityksiä kohtaan, suojella historiallista totuutta ja säilyttää historiatietämys, 7) Venäjän viestinnän aseman vahvistaminen globaalissa informaatioympäristössä ja 8) sotilaspoliittisen ja sotilasteknisen yhteistyön kehittäminen ulkomaiden kanssa. (Kreml, 2021a, ss. 39–42) Venäjän valtionjohto on toistanut lähes kaikkia näitä tekijöitä omassa narratiivissaan niin helmikuun 2014 kuin myös helmikuun 2022 Ukrainaan kohdistuneiden hyökkäysten jälkeen.

Asiakirja osoittaa Venäjän tunnistavan, että tieto- ja viestintäteknologian käyttö valtioiden turvallisuutta kohtaan sekä suvereniteetin loukkaamiseen tulee lisääntymään. Siihen kohdistuvien kyberhyökkäysten määrän todetaan kasvavan, ja turvallisuusstrategiassa

tuodaankin korostetusti esille, että näistä hyökkäyksistä suurin osa toteutetaan ulkomaisten valtioiden toimesta. Venäjä nähdään kansainvälisenä tietoturvan edistämisen promoottorina, jonka hyväntahtoisuutta kuitenkin vastustetaan niissä länsimaissa, jotka pyrkivät hallitsemaan globaalia informaatioympäristöä. (Kreml, 2021a, ss. 19–20) Tällä kiertoilmaisulla tarkoitetaan todennäköisesti ensisijaisesti Yhdysvaltoja. Venäjä on asettanut yhdeksi päätavoitteekseen tietoturvallisuuden varmentamisen ja sen toimintojen kehittämisen. Eräänä keskeisenä tekijänä tämän tavoitteen saavuttamisessa nähdään asevoimien, viranomaisten sekä eri laitevalmistajien tietoturvan kehittäminen (Kreml, 2021a, s. 21). Toisin sanoen, Venäjällä tunnistetaan erityiset riskit ulkopuolelta puolustusteollisuuteen ja tiedustelupalveluihin kohdistuvaan kybertiedusteluun. Turvallisuusstrategian mukaan Venäjä mieltää ylläpitävänsä suvereniteettiasemaa informaatio- ja kyberympäristöissä. (Kreml, 2021a, s. 20) Viimeisimpien yhdysvaltalaistutkimusten mukaan kyberturvallisuuden kärkimaat ovat kuitenkin Yhdysvallat, Iso-Britannia ja Suomi. Yhdysvallat, Iso-Britannia ja Kiina ovat puolestaan kybertoimintaympäristön kärkimaita, eikä Venäjä tosiasiallisesti sijoitu globaalien kärkimaiden joukkoon. (Broadband Search, n.d.)

4.4.3 Venäjän federaation tietoturvallisuuden doktriini (2016)

Joulukuun 5. päivänä 2016 Venäjän federaation presidentti Vladimir Putin hyväksyi allekirjoituksellaan käyttöönotettavaksi uuden *Venäjän federaation tietoturvallisuuden doktriinin*, joka korvaa sen aiemman, vuonna 2010 käyttöönotetun version (Kreml, 2016b). Doktriini on yksi lukuisista Venäjän federaation strategisen suunnittelun asiakirjoista, ja se perustuu vuonna 2015 käyttöönotettuun Venäjän federaation turvallisuusstrategiaan (Kreml, 2016b, s. 3). Siitä on tulkittavissa Venäjän federaation virallinen julkinen näkemys informaatioympäristössä toteutettavasta kansallisen turvallisuuden ja edun hallinnasta. Doktriinissa määritellään Venäjän federaation tietoturvallisuuden strategiset tavoitteet ja keskeiset osa-alueet, jotka on muodostettu tietoturvallisuuden uhka-analyysin sekä valtion sen hetkisen tietoturvallisuuden tilan pohjalta. Tietoturvallisuus koetaan olevan keskeisessä roolissa Venäjän federaation kansallisten, strategisen tason prioriteettien toteuttamisessa. (Kreml, 2016b, ss. 3–4).

Venäjän federaation virallisasiakirjoissa käytetään kyber-termiä hyvin harvoin. Kybertoimintaympäristöä käsittelevät asiakokonaisuudet sisällytetään sen yläkäsitteen, informaatioympäristön alle. Tietoturvallisuuden doktriinissa informaatioympäristö määritellään *”tiedon, tietojärjestelmien, tietoliikenneverkkojen, viestintäverkkojen, tietoteknologioiden, tiedon generointiin ja prosessointiin sekä aiemmin mainittujen teknologioiden kehittämiseen ja käyttöön osallistuvien toimijoiden, tietoturvan varmistamisen sekä alaan liittyvän julkisuuskuvan sääntelyyn luotujen mekanismien kokonaisuudeksi”* (Kreml, 2016b, s. 1). Kuten määrittelystä huomataan, informaatioympäristö sisältää niin digitaaliset tietojärjestelmät ja tietoverkot, kuin myös toimintaympäristön toimijat – aivan kuten tämän tutkimuksen luvussa 3.1. kybertoimintaympäristökin on määritelty. Näin ollen tietoturvallisuuden doktriinia voidaan pitää keskeisenä Venäjän federaation kybertoimintaa ohjaavana virallisasiakirjana.

Doktriinin peruskäsitteistössä yhteiskunnan osia sidotaan merkittävissä määrin osaksi tietoturvallisuuden tarjoamista. Valtion tiedustelu- ja turvallisuusviranomaisten toimintojen ohella doktriini velvoittaa myös oikeus- ja tutkimuslaitoksia, teknologia- ja talousalan toimijoita sekä ”muita” toimijoita osallistumaan tietoturvallisuuden tarjoamiseen. (Kreml, 2016b, s. 2) Näin ollen valtio voi niin halutessaan velvoittaa esimerkiksi yksityisiä teknologia-alan yrityksiä muun muassa luovuttamaan tietoa heidän kansainvälisistä asiakkaistaan tai käyttämään heidän välisiään suhteita tiedustelu- tai vahingoittamistarkoitukseen. ”Muita”-termin käyttö mahdollistaa käytännössä sen, että mikä tahansa yhteiskunnan osa pystytään tarvittaessa sitomaan osaksi tietoturvallisuuden tarjoamista, toisin sanoen kybertoimintaa. Virallisiksi tietoturvajoukoiksi doktriinissa nimetään Venäjän federaation valtion elimet sekä niiden alaiset yksiköt ja viranomaiset, paikallisviranomaiset sekä tietoturvallisuuden asiakokonaisuuksien käsittelyyn käsketyt organisaatiot (Kreml, 2016b, s. 2).

Merkille pantavaa on se, miten doktriinissa määritellään Venäjän federaation informaatioinfrastruktuuri. Sen on määritelty olevan tietojärjestelmien, verkkosivustojen sekä tietoverkkojen yhdistelmä, jotka sijaitsevat paitsi Venäjän maaperällä, mutta myös Venäjän federaation lainkäyttövaltaan kuuluvilla alueilla sekä alueilla, joita käytetään Venäjän federaation allekirjoittamien kansainvälisten sopimusten nojalla (Kreml, 2016b, s. 2). Toisin sanoen, tämä doktriinin merkintä luo venäläisestä perspektiivistä juridisen

mahdollisuuden sijoittaa sen omaa informaatioinfrastruktuuria muun muassa Ukrainan maaperälle Krimin niemimaan, Donetskin, H'ersonin, Luhanskin ja Zaporižžjan alueille – jotka se on laittomasti liittänyt itseensä, ja jotka ovat sittemmin siirtyneet Venäjän federaation lainkäyttövallan alaisuuteen. Tästä yhtenä osoituksena voidaan todeta olevan muun muassa Ukrainasta käsin toimivat venäläiset ja venäläismieliset disinformaatiota levittävät toimijat, niin sanotut trollitehtaat.

Doktriinissa näyttäytyy myös jo vuosia jatkunut narratiivi, jossa länsimaiden kuvataan olevan aikeissa horjuttaa Venäjän sisäpoliittista tilannetta ja valmistelevan erilaisia hyökkäyksiä Venäjän maaperälle. Doktriini sisältääkin propagandistista ja venäläisyleisölle suunnattua sanomaa. Yhtenä keskeisimpänä Venäjän federaation tietoturvallisuusuhkana pidetään sitä, että useat vieraat valtiot rakentavat omia tietoteknisiä toimintojaan pyrkiäkseen vaikuttamaan Venäjän federaation informaatioinfrastruktuuriin sotilaallisin tarkoituksin. ”Tiettyjen” valtioiden tiedustelupalveluiden koetaan käyttävän kasvavissa määrin teknillispsykologisia välineitä horjuttaakseen maiden sisäpoliittisia tilanteita ympäri maailmaa. Lisäksi ulkomaisten tiedotusvälineiden kerrotaan julkaisevan kasvavissa määrin sellaista sisältöä, joka esittää puolueellisia arvioita Venäjän federaation politiikasta samalla, kun venäläiset tiedotusvälineet kohtaavat räikeää syrjintää ja venäläisiä toimittajia estetään suorittamasta tehtäviään. Ulkovaltojen koetaan harjoittavan omien medioidensa kautta informaatiovaikuttamista venäläisväestöön, jolla pyritään murentamaan venäläisiä perinteisiä henkisiä ja moraalisia arvoja. (Kreml, 2016b, ss. 5–6)

Maanpuolustuksen osalta koetaan ominaiseksi se, että tietyt valtiot ja järjestöt käyttävät tietotekniikkaa yhä kasvavissa määrin sekä sotilaallisiin että poliittisiin tarkoituksiin, osittain kansainvälisen lain vastaisesti. Doktriinin mukaan näillä pyritään heikentämään kohdevaltion suvereniteettia, poliittista ja sosiaalista vakautta sekä Venäjän ja sen liittolaisten alueellista koskemattomuutta. (Kreml, 2016b, s. 6) Myös ulkovaltojen tiedustelupalveluiden toteuttama kybervakoilu koetaan toistuvasti merkittävänä uhkana. Maanpuolustuksen tietoturvallisuuden varmistamiseksi doktriinissa on esitetty viisi keskeisintä osa-aluetta: strategisen pelotteen varmistaminen, tietoturvajärjestelmien parantaminen, tietoturvauhkien ennakointi ja tunnistaminen sekä vastatoimet informaatiopsykologisessa ympäristössä. (Kreml, 2016b, s. 8)

4.4.4 Venäjän federaation kansainvälisen tietoturvallisuuden kenttää koskevat valtionpolitiikan perusperiaatteet (2021)

Venäjän presidentti Vladimir Putin otti 12. huhtikuuta 2021 käyttöön Venäjän federaation kansainvälisen tietoturvallisuuden kenttää koskevat valtionpolitiikan perusperiaatteet sisältävän asiakirjan. Tällä strategisen tason suunnitteluasiakirjalla määritellään keskeisimmät kansainvälisen tietoturvallisuuden uhat sekä kansainväliseen tietoturvallisuuteen liittyvät Venäjän federaation valtionpolitiikan tavoitteet. Tässä virallisasiakirjassa valtionpolitiikalla tarkoitetaan joukkoa koordinoituja toimenpiteitä, joiden tarkoituksena on luoda kansallinen järjestelmä kansainvälisen tietoturvan varmistamiseksi. Asiakirja nojautuu keskeisiltä osin Venäjän federaation kansalliseen turvallisuusstrategiaan, tietoturvallisuuden doktriiniin sekä ulkopolitiikan konseptiin. (Kreml, 2021b, ss. 1–2)

Perusteissa on kuvattu kaikkiaan kuusi yksittäistä tekijää suurimpina uhkina kansainväliselle tietoturvalle, joista viisi muodostuu tieto- ja viestintätekniikan käytöstä eri ympäristöissä: sotilaspoliittisesti, terroristisessa tarkoituksessa, rikollisessa tarkoituksessa, suvereenin valtion sisäisiin asioihin puuttumiseen sekä hyökkäysten kohdistuminen valtion tietokantoihin ja kriittiseen infrastruktuuriin. Näiden lisäksi kuudentena merkittävänä uhkatekijänä koetaan yksittäisten valtioiden käyttämä teknologinen dominanssi, jolla kyetään monopolisoimaan tieto- ja viestintätekniikan markkinat ja lisäämään muiden riippuvuutta näistä valtioista. (Kreml, 2021b, ss. 2–3)

Asiakirjassa säädellään myös tietoturvallisuuden alalla toteutettavaa kansainvälistä yhteistyötä. Yleisellä tasolla sekä kyberrikollisuuden torjuntaan liittyvissä aihealueissa yhteistyötä kuvataan tehtävän Itsenäisten valtioiden yhteisön (IVY), BRICS-maiden, Kollektiivisen turvallisuusjärjestön (KTSJ), Shanghain yhteistyöjärjestön (SCO), Kaakkois-Aasian maiden yhteistyöjärjestön (ASEAN), G20-maiden sekä muiden valtioiden ja kansainvälisten järjestöjen kanssa. Sen sijaan ASEAN ja G20-maat, ja näin ollen kaikki länsivaltiot, jätetään kyberhyökkäysten torjunnan ja tiedonvaihdon osalta tehtävän yhteistyön ulkopuolelle. (Kreml, 2021b, ss. 4–9) Eri järjestöt ja niihin kuuluvat valtiot on esitelty alla olevassa kuvassa 7.

Kuva 7. Kansainväliset järjestöt sekä niiden jäsenvaltiot

4.4.5 Venäjän federaation sotilasdoktriini (2014)

Venäjän sotilasdoktriini on valtion virallisasiakirja, jolla ohjataan Venäjän aseellista puolustamista ja jossa esitellään valtioon kohdistuvat sotilaalliset uhat (Kreml, 2014, ss. 1–2). Viimeisin sotilasdoktriini julkaistiin joulukuussa 2014, 10 kuukautta Krimin miehityksen jälkeen. Asiakirjasta on löydettävissä sellaisia erityispiirteitä, jotka ovat todennäköisesti seurausta Krimin miehityksestä. Doktriinissa kuvataan muun muassa sitä, kuinka alueellisia konflikteja on edelleen ratkaisematta, ja niiden ratkaiseminen tulee jatkumaan myös Venäjän rajoilla (Kreml, 2014, s. 4).

Tämän tutkimuksen viitekehyksessä keskeisimpiä doktriinin mukaisia ulkoisia sotilaallisia uhkia ovat 1) Naton voimapotentiaalin laajentaminen ja tuominen lähemmäksi Venäjän rajoja, 2) Vieraiden valtioiden sotilasosastojen ja kaluston sijoittaminen Venäjän sekä sen naapurivaltioiden alueille, 3) alueelliset vaatimukset Venäjän federaatiota ja sen liittolaisia

vastaan sekä puuttuminen niiden sisäisiin asioihin, 4) sotilaallisen voiman käyttö Venäjän federaation sekä sen naapurivaltioiden alueilla, 5) aseellisten selkkausten kärjistyminen Venäjän federaation ja sen naapurivaltioiden alueilla, 6) ulkomaisten yksityisten sotilasyritysten toiminta Venäjän rajojen läheisyydessä sekä ristiriitojen ja separatismin kasvu tietyillä maailman alueilla, 7) tieto- ja viestintätekniikan käyttö sotilaspoliittisiin tarkoituksiin, joilla pyritään horjuttamaan valtioiden suvereniteettia sekä poliittista riippumattomuutta ja jotka muodostavat uhan kansainväliselle turvallisuudelle sekä 8) Venäjän politiikan vastaisten hallintojen perustaminen Venäjän naapurivaltioihin (Kreml, 2014, ss. 5–6). Listatuista uhista heijastuu Krimin niemimaan miehitys sekä uhkarealismi länsimaiden puuttumisesta Krimin ja Itä-Ukrainan konflikteihin. Venäjä tiedostaa myös kybertoimintaympäristössä piilevät sotilaspoliittiset uhat sen kansalliselle sekä kansainväliselle turvallisuudelle. Ulkoisten uhkien lisäksi doktriinissa on listattu myös sisäiset sotilaalliset vaarat, jotka painottuvat terrorismiin, ääriliikkeisiin ja kansalaisiin kohdistuvaan informaatiovaikuttamiseen (Kreml, 2014, ss. 6–7). Yhdeksi nykyaikaiseksi sotilaallisen konfliktin tunnusomaiseksi piirteeksi luetaan epäsuorien ja epäsymmetristen sodankäynnin menetelmien käyttö, jollaiseksi myös kybersodankäynti voidaan tulkita (Kreml, 2014, s. 8).

Doktriinissa on myös määritelty lista päätehtävistä, joilla pyritään ehkäisemään sotilaallisia konflikteja. Yhtenä tehtävänä on luoda sellaiset olosuhteet, joilla kyetään vähentämään kyberhyökkäysten muodostamaa riskiä sotilaspoliittisiin kohteisiin. Myös sotilasdoktriinissa tuodaan esille se, että Venäjä pitää laillisena käyttää asevoimiaan sekä muita viranomaisiaan, sen liittolaisia tai ulkomailla asuvia kansalaisiaan kohtaan kohdistuvan hyökkäyksen torjuntaan. Asevoimista voidaan muodostaa operatiivisen toiminnan yksiköitä Venäjän ulkopuolelle, suojatakseen kansalaisiaan ja ylläpitääkseen turvallisuutta. Asevoimien sekä muiden joukkojen käytöstä vastaa Venäjän presidentti. (Kreml, 2014, ss. 11–13) Sotilasdoktriinissa korostuu myös venäläinen systeemiajattelu, jossa yksityinen sektori on kiinteästi osana valtiollista järjestelmää. Venäjän asevoimien ja muiden elinten kehittämisen yhtenä päätehtävänä nähdään sekä yksityisten että valtiollisten yliopistojen rakenteiden parantaminen ja teknisen koulutuksen lisääminen. (Kreml, 2014, ss. 18–19)

4.4.6 Luonnos Venäjän federaation kyberturvallisuuden strategisesta konseptista (2014)

Venäjän liittoneuvosto, eli parlamentin ylähuone järjesti marraskuussa 2013 parlamentaarisen kuulemisen koskien *luonnosta Venäjän federaation kyberturvallisuusstrategian konseptista.* Kyseessä on ensimmäinen Venäjän federaation virallisasiakirja tai sellaisen luonnos, jossa kybertoimintaympäristöä käsitellään omana kokonaisuutenaan. Tämä virallisasiakirjan luonnos julkaistiin julkisesti kommentoitavaksi tammikuussa 2014. Konseptin täytäntöönpanon jälkeen Venäjälle oli tarkoitus perustaa kyberturvallisuusstrategian kehittämistyöryhmä, johon osallistuisivat edustajia turvallisuusneuvostosta, turvallisuus- ja tiedustelupalveluista sekä muista valvontaelimistä, valtiollisista sekä merkittävistä yksityisomisteisista yrityksistä, tutkimus- ja opetuslaitoksista sekä kyberturvallisuuden parissa toimivista, voittoa tavoittelemattomista järjestöistä (Venäjän liittoneuvosto, 2014b, ss. 9–10).

Kyberturvallisuusstrategian konseptin valmistelusta vastannut, silloinen perustuslakivaliokunnan varapuheenjohtaja, senaattori Ruslan Gattarov totesi antamassaan videoidussa tiedotustilaisuudessa tammikuussa 2014, että strategia on suunniteltu täydentämään kyberturvallisuuden alalla olevat legitiimiset aukot, koska nykyiset alaa käsittelevät virallisasiakirjat käsittelevät pääasiassa valtion rakenteita (Venäjän liittoneuvosto, 2014a). Gattarov kuitenkin Venäjän liittoneuvoston tiedotteen (2014) mukaan jätti tehtävänsä kuukautta myöhemmin, joka saattaa olla syynä siihen, että tämän luonnoksen mukaista strategista konseptia ei ole vielä kevääseen 2023 mennessä hyväksytty käyttöön otettavaksi.

Konseptin luonnoksessa määritellään kyberturvallisuusstrategian kehittämisen merkitys, kyberturvallisuuden paikka osana tietoturvallisuuden kokonaisuutta sekä kybertoimintaympäristön peruskäsitteistö. Kyseessä on ensimmäinen kerta, kun venäläisissä strategisen tason asiakirjoissa määritellään kybertoimintaympäristö *(eng. cyber space, ven. киберпространство)* ja kyberturvallisuus *(ven. кибербезопасность).* Kybertoimintaympäristö määritellään informaatioympäristön alaksi, joka muodostuu internetin sekä muiden tietoliikenneverkkojen viestintäkanavien, niiden toiminnan takaavan teknologisen infrastruktuurin ja kaikenlaisten ihmisten toiminnan muotojen yhdistelmästä

(yksilö, organisaatio, valtio), ja joka tapahtuu edellä mainittujen teknologioiden avulla. Konseptin luonnoksessa kyberturvallisuus puolestaan määritellään joukoksi olosuhteita, joissa kaikki kybertoimintaympäristön komponentit on suojattu mahdollisimman suurelta määrältä uhkia. (Venäjän liittoneuvosto, 2014b, ss. 1–2) Näin ollen määritelmien voidaan ymmärrettävästi todeta olevan linjassaan länsimaisten määritelmien kanssa.

Kyberturvallisuuden strategialla on luonnoksessa esitetty olevan neljä keskeistä tarkoitusta: 1) poistaa olemassa olevat puutteet Venäjän federaation kyberturvallisuuden varmistamista koskevassa sääntelyssä ja asiakirjoissa, 2) luoda perusteet sisällyttää Venäjän federaation kyberturvallisuuden varmistamisprosessiin yhteiskunnan rakenteet tasa-arvoisina toimijoina valtion elinten kanssa, 3) yhtenäistää ja koordinoida kaikkien asianomaisten osapuolten toimet Venäjän federaation kyberturvallisuuden tason nostamiseksi ja 4) luoda Venäjän federaation kyberturvallisuuden uhkamalli sekä ohjeet ja toimenpiteet niiden torjumiseksi (Venäjän liittoneuvosto, 2014b, ss. 1–5). Konseptiluonnoksessa korostettiin myös kansainvälisen tietoturva- ja kyberyhteistyön kehittämistä, väestön tietoturva- ja kybertietoisuuden parantamista sekä Venäjän kansallisten kyberturvallisuuden laitteistojen kehittämistä (Venäjän liittoneuvosto, 2014b, s. 8). Näitä kyseisiä piirteitä on tuotu toistuvasti esille myös myöhemmin julkaistuissa virallisasiakirjoissa, kuten vuoden 2016 tietoturvallisuuden doktriinissa sekä 2021 julkaistussa Venäjän federaation kansainvälisen tietoturvallisuuden kenttää koskevissa valtionpolitiikan perusperiaatteissa.

Venäjän valtiollisissa virallisasiakirjoissa korostuu tietotekniikan ja tietoteknisten menetelmien implementointi osaksi valtion hallintoa, turvallisuus- ja tiedustelupalveluja sekä asevoimia näiden eri tasoilla. Venäjä kokee länsimaat selkeänä uhkana tietotekniikan ja kyberturvallisuuden asiakokonaisuuksissa sekä niiden kehittämisessä. Asiakirjojen perusteella Venäjä pyrkii ylläpitämään pintapuolista informaatioympäristön yhteistyötä länsimaiden kanssa, jota korostetaan muun muassa Venäjän pyrkimyksillä luoda vakautta ja turvallisuutta takaavia prosesseja. Sen sijaan yhteistyö Kiinan, sekä muiden venäjämielisten valtioiden ja järjestöjen kanssa kuvataan erityisen arvokkaaksi ja syvälliseksi. Venäjän keskeisenä sotilaallisena uhkana koetaan olevan erityisesti Yhdysvallat ja NATO. Näiden ohella Venäjä kokee myös sen naapurivaltioihin sijoitetut länsimaiden asejärjestelmät uhakseen, jonka myötä se pyrkii myös perustelemaan ja oikeuttamaan omat aktiiviset

toimensa näiden uhkien eliminoimiseksi. Asiakirjoista korostuu ennen kaikkea Venäjän itse itselleen valtuuttama mahdollisuus suojata ulkomailla asuvia venäläisiä sekä venäläismielisiä henkilöitä, mikäli heitä kohtaan toimitaan väärin tai kohdistetaan uhkaa. Tämä valtuutus sisältää käytännössä rajattoman keinovalikoiman, johon sisältyy myös muun muassa valtiollisia kohteita ja kriittistä infrastruktuuria vastaan tehdyt kyberhyökkäykset.

5 Venäjän kybervaikuttamisoperaatiot Ukrainan sodassa 2014–2021

Venäjän hyökkäys Ukrainaan voidaan katsoa alkaneen keväällä 2014, kun venäläisjoukot miehittivät Krimin niemimaan sekä Ukrainan itäosat, jotka se myöhemmin liitti laittomasti itseensä. Tämä tapahtui Ukrainan vallankumouksen jälkeen, jonka yhteydessä Ukrainan venäläismielinen presidentti Viktor Janukovitš erotettiin. Venäjä on siitä lähtien jatkanut Ukrainaan kohdistettuja kyberhyökkäyksiään. (Euroopan Parlamentti, 2022)

Venäjän kybervaikuttamisoperaatioita Ukrainan sodassa vuosina 2014–2021 tutkittaessa keskityttiin tämän tutkimuksen rajauksen mukaisesti niihin venäläisiin kyberuhkatoimijoihin, joilla on globaalisti tunnustettu yhteys Venäjän turvallisuus- ja tiedustelupalveluihin. Näin ollen tutkimuksesta ja sen tuloksista on jätetty pois yksityisten, venäläismielisten ryhmittymien kyberhyökkäykset.

Seuraavissa alaluvuissa käsitellään tutkimustuloksia siitä, millaisia kybervaikuttamisen menetelmiä Venäjän valtiolliset kyberuhkatoimijat hyödynsivät Ukrainan sodassa vuosina 2014–2014 sekä millaisiin kohteisiin näitä menetelmiä kohdistettiin. Lisäksi esitellään tutkimustulokset siitä, mitkä kyberuhkatoimijat olivat aktiivisesti osana näitä kybervaikuttamisoperaatiota. Tässä luvussa esiteltävä tutkimusaineisto on kerätty Euroopan parlamentin (2022) sekä yhdysvaltalaisten Council of Foreign Relations (2023) ja Center for Strategic and International Studies (2023) ajatushautomoiden aineistoista. Council of Foreign Relations on keskittynyt Yhdysvaltojen ulkopolitiikkaan sekä kansainvälisiin suhteisiin ja Center for Strategic and International Studies puolestaan kansainväliseen politiikkaan, talouteen ja turvallisuuteen.

5.1 Kyberuhkatoimijoiden käyttämät kybervaikuttamisen menetelmät

Venäläisten kyberuhkatoimijoiden eri kybervaikuttamisen menetelmät on tämän tutkimuksen tuloksissa jaettu viiteen ryhmään: 1) tietojenkalastelu, 2) palvelunestohyökkäykset, 3) datan varastaminen, 4) datan tuhoaminen sekä 5) muut. Näiden kaikkien menetelmien osuus Ukrainan sodassa vuosina 2014–2021 suoritetusta kybervaikuttamisesta on esitetty tämän alaluvun lopussa olevassa kuvassa 8.

Kybervaikuttamisen menetelmiä tutkittaessa tuli huomioida se, että yleisesti ottaen etenkin laajamittaisissa kyberhyökkäyksissä saatetaan tavoitteen saavuttamiseksi hyödyntää useaa eri menetelmää. Esimerkiksi toiminta saattaa käynnistyä tietojenkalastelulla, jolla pyritään hankkimaan pääsy esimerkiksi kohdeorganisaation ennalta tiedustellun työntekijän työasemalle. Työasemalta saatetaan varastaa siellä olevaa dataa, jota puolestaan pystytään hyödyntämään operaation muissa vaiheissa. Tämän jälkeen operaatio jatkuu kohdeverkossa edeten, kunnes on saavutettu ajallinen ja toiminnallinen valmius esimerkiksi laajamittaiseen datan tuhoamiseen tai palvelunestohyökkäykseen tähtäävään kyberhyökkäykseen.

Kaikista tutkimuksen yhteydessä käsitellyistä ja analysoiduista tapauksista 43,2 % oli eri keinoin toteutettua tietojenkalastelua. Tietojenkalastelua toteutetaan tyypillisesti sähköpostitse, tekstiviestitse sekä sosiaalisen median kanavien välityksellä. Prosenttiosuuden suuruus selittyy osittain jo sillä, että tietojenkalastelu on lähes poikkeuksetta osana muita kyberoperaatioita. Kaikista tietojenkalastelua sisältäneistä tapauksista 50 % johti jollain toisella menetelmällä toteutettuun kyberhyökkäykseen. Tällaisina menetelminä havaittiin datan varastaminen, datan tuhoaminen sekä palvelunestohyökkäykset. Näistä datan varastamisen ja tuhoamisen osuus oli 87,5 %, ja palvelunestohyökkäysten 12,5 %. Ne tapaukset, joissa tietojenkalastelu ei johtanut kyberhyökkäykseen jättävät jäljelle kaksi vaihtoehtoa: hyökkäys joko havaittiin ja kyettiin torjumaan tai vaihtoehtoisesti kyseistä hyökkäystä ei ole vielä toteutettu.

Eri valtiollisiin tai kriittisen infrastruktuurin kohteisiin suoritetut palvelunestohyökkäykset olivat tietojenkalastelun jälkeen merkittävin kybervaikuttamisen menetelmä 18,9 % osuudellaan. Mikäli operaation valmisteluvaiheeseen linkittyvä tietojenkalastelu jätettäisiin

huomioimatta, niin palvelunestohyökkäykset muodostaisivat 33,3 % osuuden Ukrainan sodassa vuosina 2014–2021 suoritetuista kybervaikuttamisen operaatioista. Tutkimustulos on linjassaan tämän tutkimuksen luvussa 4.3 esiteltyjen venäläisten kyberuhkatoimijoiden toimintaperiaatteiden kanssa, joiden perusteella niiden toiminta on suoraviivaista ja selkeään vaikutukseen pyrkivää.

Datan varastamisella pyritään hankkimaan sellaista tietoa ja materiaalia, jota pystytään hyödyntämään joko käynnissä olevan operaation myöhemmässä vaiheessa tai vaihtoehtoisesti jossain toisessa kontekstissa. Tätä kybervaikuttamisen menetelmää voidaan käyttää esimerkiksi ihmisten mielipiteiden vaikuttamiseen vaalien alla, jolloin ehdokkaaseen liittyvää arkaluontoista tietoa tuodaan julkisuuteen – kuten vuoden 2016 Yhdysvaltain presidentin vaaleissa ehdokas Clintonille tehtiin. Toinen käyttötarkoitus voi muun muassa olla käyttäjätunnustietojen hyödyntäminen johonkin toiseen järjestelmään tai palveluun kirjautumisessa. Ukrainan sodassa vuosina 2014–2021 suoritetuista kybervaikuttamisenoperaatioista datan varastamisen osuus oli 16,2 %. Mikäli tietojenkalastelun osuus jätettäisiin huomioimatta, oli Ukrainan sodassa vuosina 2014–2021 datan varastamiseen tähtäävien operaatioiden osuus kaikista kybervaikuttamisoperaatioista 28,6 %.

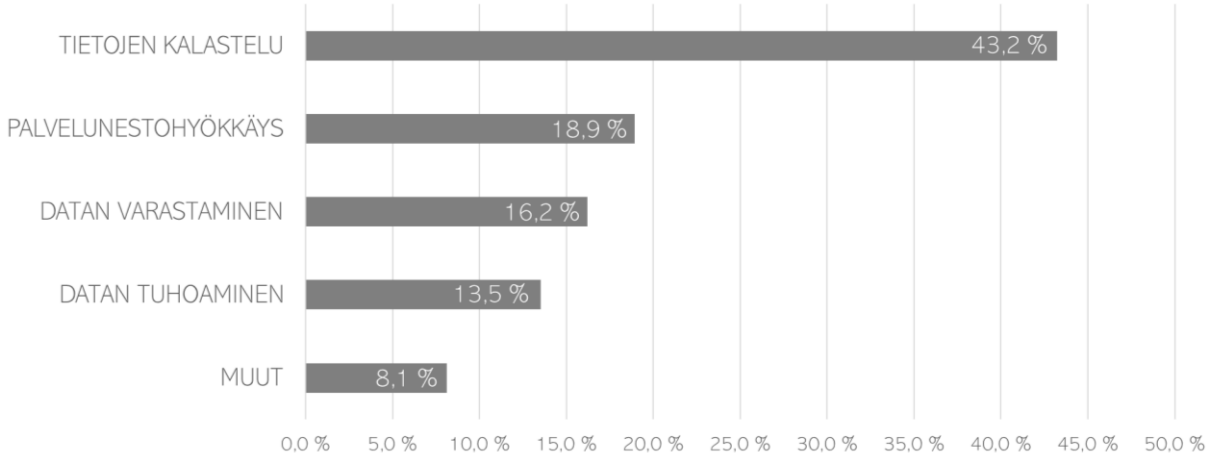
Datan tuhoamisella pyritään samansuuntaiseen lopputulokseen palvelunestohyökkäysten kanssa, ja ne saattavatkin toisinaan sekoittua keskenään. Datan tuhoamisen tarkoituksena on lopullisesti estää tietyn tiedon tai tietomassan käyttö. Tällaisia esimerkkejä ovat muun muassa vaalituloksiin vaikuttaminen sekä kriittisen infrastruktuurin kohteisiin suoritetut hyökkäykset. Yhtenä historian tunnetuimmista datan tuhoamiseen tähdänneistä haittaohjelmista ja operaatioista on venäläisten kyberuhkatoimijoiden alun perin Ukrainaan kohdistama ”NotPetya”, joka sittemmin levisi maailmanlaajuisesti. Datan tuhoamiseen pyrkivien kyberoperaatioiden osuus oli kaikki kybervaikuttamisen menetelmät huomioiden 13,5 %. Mikäli myös datan tuhoamisen osuutta tarkastellaan huomioimatta tietojenkalastelua, oli sen osuus kaikista kyberhyökkäyksistä lähes neljännes, 23,8 %.

Viidentenä kategoriana tarkasteltiin sellaisia muita tutkimuksen yhteydessä esiin tulleita kybervaikuttamisen menetelmiä, jotka esiintyivät vain yksittäisiä kertoja tai eivät muutoin

muodostaneet merkittävää kokonaisosuutta. Tällaisia menetelmiksi koettiin datan manipulointi, tiedustelu, sekä toimitusketjuhyökkäykset *(eng. Supply Chain Attack)*. Näiden osuus kaikista vaikuttamismenetelmistä oli 8,1 %.

Datan manipuloinnista on yksittäinen esimerkki kesältä 2021, kun Ukrainan merivoimien verkkosivuille hyökättiin ja sivustolle upotettiin kansainvälistä Sea Breeze-merisotaharjoitusta koskevia, disinformaatiota sisältäneitä asiakirjoja (Zinets, 2021). Vuosien 2014 ja 2016 välillä Ukrainan asevoimien tykistöjoukoissa käytettiin laajasti Android-alustoille luotua sovellusta, jonka tarkoituksena oli yksinkertaistaa tykistön maalitiedon käsittelyä sekä nopeuttaa tulenkäyttöä. Sovellus oli alun perin Ukrainan asevoimien upseerin luoma, mutta sittemmin Venäjän sotilastiedustelusta vastaavan GRU:n kyberuhkatoimija APT28 julkaisi siitä manipuloidun päivityksen, jota mainostettiin ukrainalaisten sotilaitten suosimilla vKontakte-kanavilla. Manipuloitu sovellus lähetti käyttäjän paikkatiedot Venäjän asevoimien käyttöön, jonka avulla venäläisjoukot onnistuivat tuhoamaan noin 20 % Ukrainan kenttätykistöstä. (Crowdstrike, 2017) Huhtikuussa 2018 toinen GRU:n alainen kyberuhkatoimija Sandworm suoritti toimitusketjuhyökkäyksen Ciscon kytkin- ja reititinlaitteiden kautta, joilla pyrittiin luomaan GRU:n intressejä palvelevia takaportteja. Hyökkäyksellä pyrittiin tiettävästi saavuttamaan pääsy Ukrainan valtionhallinnon ja kriittisen infrastruktuurin lisäksi myös ainakin Yhdysvaltojen merkittäviin kohteisiin. (CISA, 2018b)

Kuva 8. Kybervaikuttamisen menetelmät Ukrainan sodassa 2014–2021



5.2 Kybervaikuttamisen kohteet

Tässä tutkimuksessa analysoitiin tutkimuksen rajauksen mukaisesti sellaisia Venäjän kybervaikuttamisen kohteeksi joutuneita ukrainalaisia kohteita, joilla on erityinen yhteiskunnallinen tai maanpuolustuksellinen merkitys. Tutkimusaineiston pohjalta nousi esiin kolme selkeää pääryhmää: 1) valtionhallinto, 2) kriittinen infrastruktuuri sekä 3) asevoimat ja turvallisuuspalvelut. Näiden kolmen ryhmän keskinäiset osuudet kybervaikuttamisen kohteiksi joutumisesta on esitetty tämän alaluvun lopussa olevassa kuvassa 9.

Selkeä enemmistö Venäjän kybervaikuttamisesta kohdistui vuosina 2014–2021 Ukrainan valtionhallintoon, osuuden ollessa 46,2 %. Valtionhallintoon kohdistuneesta kybervaikuttamisesta merkittävin osa oli tietojenkalastelua, kaikkiaan 59,1 %. Tietojenkalastelun suuri selittyy todennäköisesti ainakin osittain sillä, että valtionhallinnossa työskentelevillä virkamiehillä on pääsy vastustajan kannalta tavoiteltavaan tietoon. Lisäksi valtion virkamiesten määrä on huomattavan suuri, ja valmiudet kybervaikuttamiselta suojautumiseen ovat todennäköisesti hyvin vaihtelevat. Tämä yhtälö tekee heistä vastustajan näkökulmasta todennäköisesti erityisen suotuisia kohteita tietojenkalastelulle.

Ukrainan valtionhallintoon kohdistui merkittävästi myös datavarkauksia. Datavarkaudet muodostivat lähes viidenneksen koko valtionhallintoon kohdistuneesta kybervaikuttamisesta (18,2 %). Mikäli tietojenkalastelu rajataan pois, niin datavarkauksien osuus on yli puolet (55,6 %) valtionhallintoon kohdistuneesta kybervaikuttamisesta. Tietojenkalastelun ja datavarkauksien ohella Ukrainan valtionhallintoon kohdistui helmikuussa 2021 yksittäinen palvelunestohyökkäys, huhtikuussa 2018 Ciscon verkkolaitteiden kautta suoritettu toimitusketjuhyökkäys sekä yksittäisiä datan tuhoamisoperaatioita, kuten esimerkiksi vuonna 2017 esiintynyt ”NotPetya”.

Kriittiseen infrastruktuuriin luetaan yhteiskunnan toimivuuden kannalta keskeiset laitokset ja yhteiskunnan rakenteet. Tällaisia ovat esimerkiksi energian tuotanto-, siirto- ja jakelulaitokset, liikennepalvelut, vesi- ja jätehuolto sekä tieto- ja viestintäjärjestelmät. (Sanastokeskus, ei pvm.) Kriittiseen infrastruktuuriin kohdistuneet hyökkäykset muodostavat

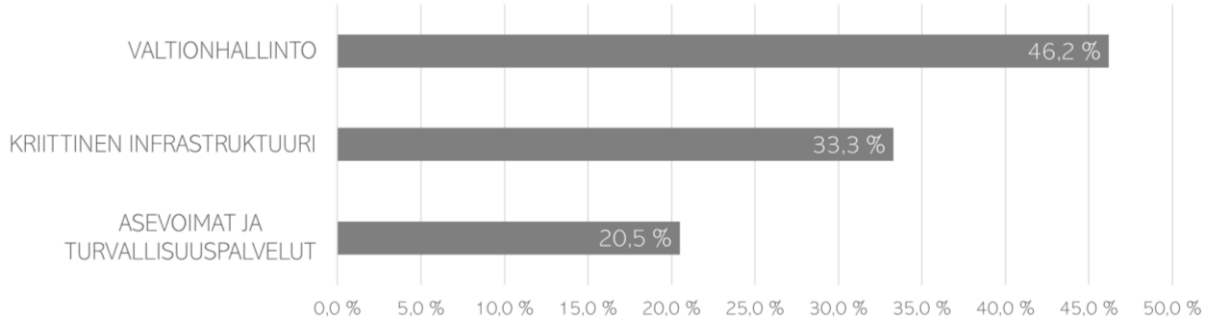
kolmanneksen (33,3 %) kaikista Ukrainan merkittäviin kohteisiin suoritetuista hyökkäyksistä. Yhtenä keskeisimpänä kriittiseen infrastruktuuriin kohdistuneena hyökkäyksenä voidaan pitää joulukuussa 2015 tehtyä datan tuhoamishyökkäystä, joka kohdistui kolmeen ukrainalaiseen energiayhtiöön. Tämän seurauksena yli 230 000 käyttäjää jäi kuudeksi tunniksi ilman sähköä. Kyseessä oli maailman ensimmäinen energiasektoriin kohdistunut kyberhyökkäys, joka lamautti koko energiantuotantojärjestelmän. (CISA, 2021)

Ukrainan kriittiseen infrastruktuuriin kohdistetuista kyberhyökkäyksistä selkeän enemmistön muodostivat palvelunestohyökkäykset sekä datan tuhoamiseen tähdänneet hyökkäykset. Molemmat näistä menetelmistä muodostivat 31,3 % osuuden, eli yhteensä 62,6 % osuuden kaikista kriittiseen infrastruktuuriin kohdistuneista hyökkäyksistä. Muutoin tässä tutkimuksessa aktiivisesti esiintynyt tietojenkalastelu nousi esille vain 18,8 % kriittiseen infrastruktuuriin tehdyissä hyökkäyksissä. On merkillepantavaa, että palvelunestohyökkäykset sekä datan tuhoamiseen tähtäävät operaatiot pyrkivät molemmat häiritsemään tai lamauttamaan kohdejärjestelmän toiminnan. Näin ollen on perusteltavaa, että erilaisista teknisistä toiminnanohjausjärjestelmistä muodostuviin kriittisen infrastruktuurin kohteisiin kohdistuu merkittävissä määrin toiminnan lamauttamiseen tähtääviä hyökkäyksiä.

Kaikista Ukrainan merkittäviin kohteisiin kohdistetuista kybervaikuttamisoperaatioista viidennes (20,5 %) kohdistui Ukrainan asevoimiin ja turvallisuuspalveluihin. Näistä kybervaikuttamisen menetelmistä 41,7 % oli sähköpostitse, tekstiviestitse tai sosiaalisen median kautta tehtyjä tietojenkalasteluja sekä niiden yrityksiä. Näissä yhteyksissä esiintyi usein yhteydenoton liitteenä ollut haittaohjelma tai linkki haittaohjelman sisältävälle verkkosivulle. Tietojenkalastelun ohella toinen merkittävä Ukrainan asevoimiin ja turvallisuuspalveluihin kohdistunut kybervaikuttamisen menetelmä oli datavarkaudet. Kaikesta asevoimiin ja turvallisuuspalveluihin kohdistetusta kybervaikuttamisesta neljännes (25 %) oli datavarkauksia. Datavarkauksilla pyrittiin muun muassa hankkimaan Venäjän sotilasoperaatioita tukevia tietoja, joista yhtenä esimerkkinä marraskuussa 2018 suoritettu Ukrainan merivoimien alusten kaappaus. Tutkimusaineiston analyysin yhteydessä kävi ilmi, että jokaista datavarkaustapausta edelsi tietojenkalastelu. Näin ollen voidaan todeta, että

yksittäinen henkilö on merkittävässä roolissa osana koko organisaation kyber- ja tietoturvallisuutta.

Kuva 9. Kybervaikuttamisen kohteet Ukrainan sodassa 2014–2021



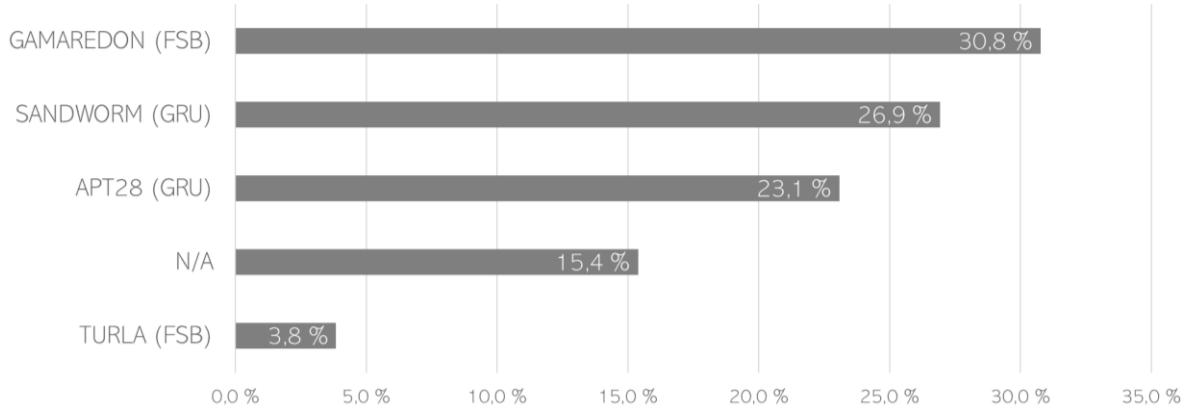
5.3 Venäläiset kyberuhkatoimijat Ukrainan sodassa 2014–2021

Tutkimusaineistoon valitut venäläiset kyberuhkatoimijat valikoituivat tutkimuksen rajauksen mukaisesti sellaisiksi, jotka ovat selkeästi valtion ohjauksen alaisia sekä osana jotain Venäjän turvallisuus- ja tiedustelupalveluista. Kuten kuvassa 10 esiteltävissä tutkimustuloksissa käy ilmi, Venäjän Ukrainassa vuosina 2014–2021 suorittamista kyberhyökkäyksistä valtaosa toteutettiin Venäjän turvallisuuspalvelu FSB:n (34,6 %) sekä Venäjän sotilastiedustelusta vastaavan tiedustelupäähallinto GRU:n (50 %) alaisten kyberuhkatoimijoiden toimesta.

Kyberhyökkäyksille on ominaista se, että hyökkäyksen suorittajia on yleisesti haastavaa, ellei miltei mahdotonta faktuaalisesti identifioida. Myös osa tämän tutkimuksen aineistoksi kerätyistä kybervaikuttamisen tapahtumista oli tuntemattomien kyberuhkatoimijoiden toteuttamia, mutta niiden kohdistuttua merkittäviin kohteisiin, ne päätettiin kuitenkin sisällyttää osaksi tutkimusaineistoa ja -tuloksia. Tuntemattomiksi jääneiden kyberuhkatoimijoiden osuudet on esitetty alla olevassa kuvassa 10 termillä ”N/A” *(suom. ei saatavilla, eng. not available).* Tuntemattomiksi jääneiden toimijoiden kybervaikuttamisoperaatioissa oli yhteistä se, että ne olivat lähes poikkeuksetta toteutettu erityisen hienostuneesti sekä monimutkaisia haittaohjelmia ja menetelmiä hyväksikäyttäen. Hyökkäykset kohdistuivat kriittiseen infrastruktuuriin ja valtionhallintoon, pitäen sisällään hajautettuja palvelunestohyökkäyksiä sekä datan varastamisoperaatioita. Tutkimustuloksissa

on merkillepantavaa, että Venäjän ulkomaan siviilitiedustelupalvelu SVR:n alaisia kyberuhkatoimijoita ei ole havaittu osallisena yhdessäkään Ukrainaan vuosina 2014–2021 suoritetussa kybervaikuttamistapahtumassa. Kyberhyökkäysten hienostuneisuus ja diskreettiys on kuitenkin ominaista SVR:n alaiselle kyberuhkatoimija APT29:lle. Näin ollen on mahdollista, että ainakin osa näistä tuntemattomiksi jääneistä kybervaikuttamistapahtumista olisi APT29:n toteuttamia.

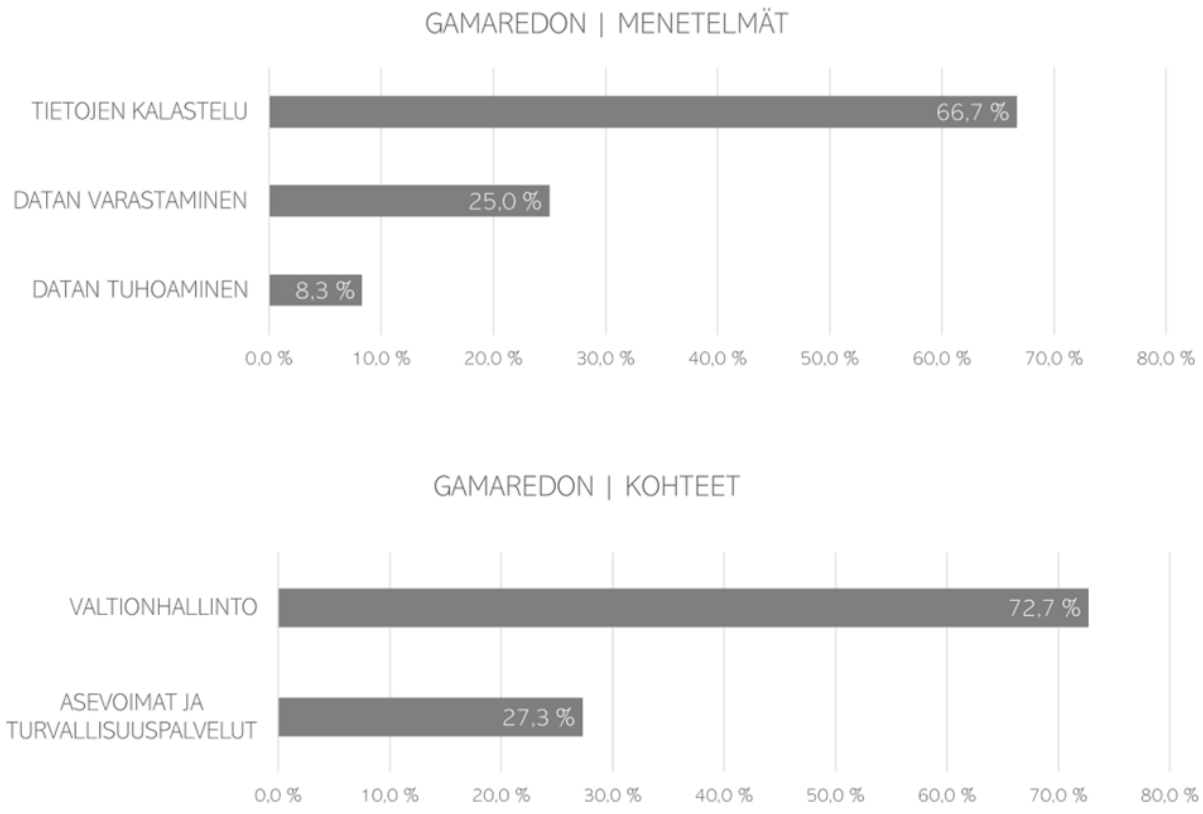
Kuva 10. Venäläiset kyberuhkatoimijat Ukrainan sodassa vuosina 2014–2021



Venäjän turvallisuuspalvelu FSB:n alainen kyberuhkatoimija Gamaredon on perustettu vuonna 2014 alkaneen Ukrainan sodan kynnyksellä, toimimaan erityisesti Ukrainan valtionhallintoa ja yhteiskuntaa vastaan. Gamaredonin toiminta merkittäviin ukrainalaisiin kohteisiin, kuten valtionhallintoon, asevoimiin ja kriittiseen infrastruktuuriin on ajoittunut tämän tutkimuksen tarkastelujakson loppujaksolle, vuosien 2018 ja 2021 välille. Tämän kyberuhkatoimijan toiminta on kiihtynyt erityisesti helmikuusta 2021 lähtien, joka mahdollisesti osittain viittaa Venäjän helmikuussa 2022 aloittaman suurhyökkäyksen valmisteluihin. Gamaredon on tämän tutkimuksen tulosten perusteella kaikista aktiivisin Ukrainassa vuosina 2014–2021 toiminut Venäjän valtiollinen kyberuhkatoimija 30,8 % kokonaisosuudella. Tämä selittyy ainakin osittain Gamaredonin toiminnalle tyypillisillä, Ukrainan valtionhallintoon kohdistuvilla tietojenkalasteluoperaatioilla. Tietojenkalastelun osuus muista Gamaredonin kybervaikuttamismenetelmien käytöstä oli 66,7 %, jonka jälkeen toiseksi eniten käytetty menetelmä oli 25 % osuudellaan datan varastamiseen tähdänneet operaatiot, kuten kuvassa 11 on esitetty.

Gamaredonin tapauksessa datan varastamisoperaatiot muodostivat tietojenkalastelun kanssa usein eräänlaisen toisiaan tukevan operaatioprosessin. Datavarkauksilla saatiin haltuun esimerkiksi viranomaisten virallisia asiakirjoja, joita käytettiin hyväksi myöhempien kyberoperaatioiden tietojenkalasteluvaiheessa, kun kohdetta lähestyttiin sähköpostitse ja esittäydyttiin jonain viranomaisena. Varastettuja asiakirjoja käytettiin kalastelusähköpostien liitetiedostoina. Asiakirjoja oli manipuloitu, ja niihin oli sisällytetty skripti tai varsinainen haittakuorma, joiden avulla pystyttiin tunkeutumaan käyttäjän työasemalle. Gamaredonin kybervaikuttaminen kohdistui Ukrainan valtionhallintoon (72,7 %) sekä Ukrainan asevoimiin ja turvallisuuspalveluihin (27,3 %).

Kuva 11. Kyberuhkatoimija Gamaredonin kybervaikuttamisen menetelmät ja kohteet

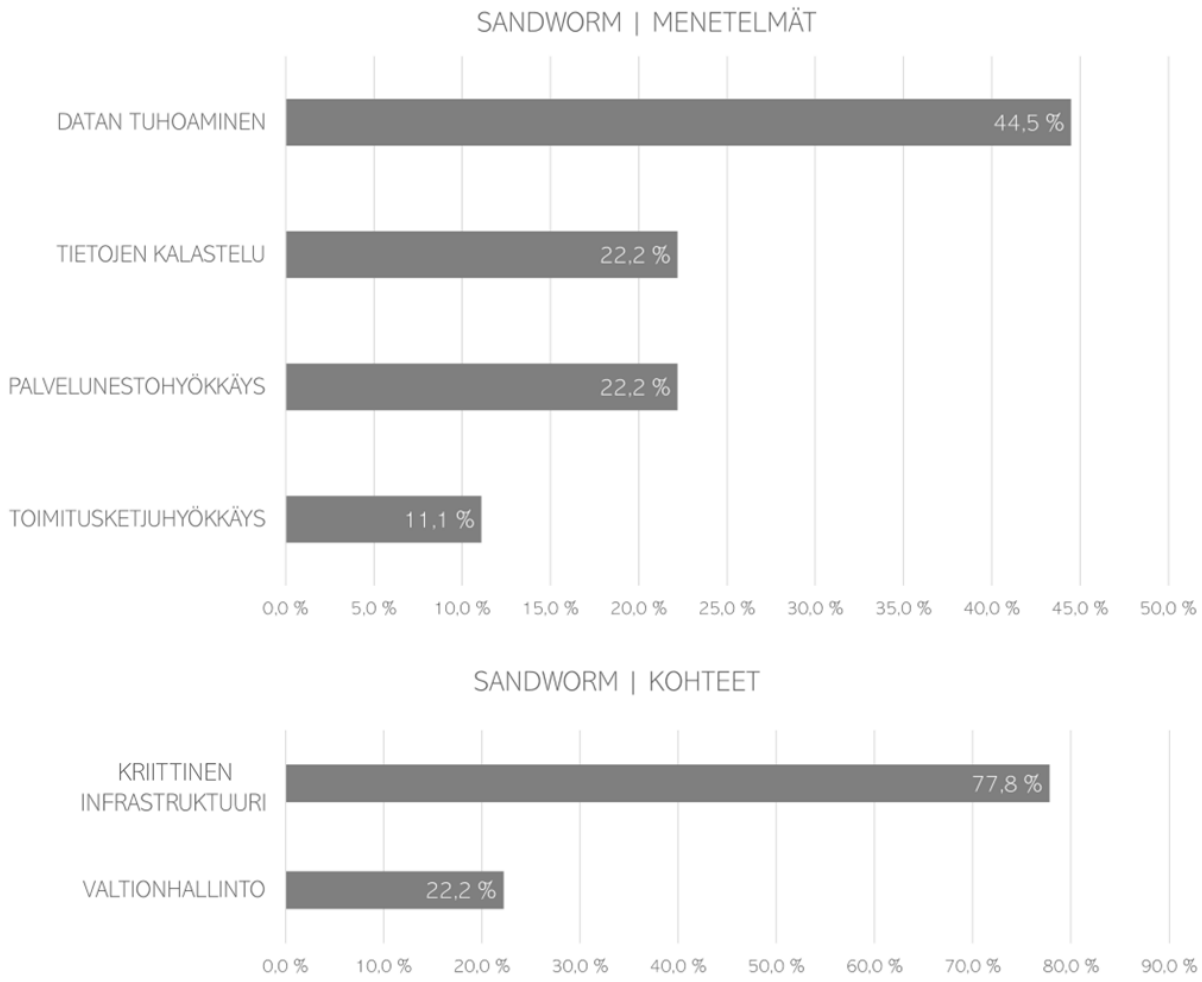


Venäjän sotilastiedustelusta vastaavan tiedustelupäähallinto GRU:n alainen kyberuhkatoimija Sandworm on erikoistunut lamauttaviin sekä tuhoavia vaikutuksia tavoitteleviin kyberhyökkäyksiin. Sandwormin kybervaikuttamisoperaatiot Ukrainassa vuosina 2014–2021 ajoittuvat joulukuun 2015 sekä kesäkuun 2018 välille. Näiden osuus kaikista venäläisten kyberuhkatoimijoiden suorittamista operaatioista Ukrainan sodassa

vuosina 2014–2021 oli yli neljännes (26,9 %). Tämän tutkimuksen näkökulmasta voidaan todeta, että Sandwormin toimet Ukrainan sodassa ovat linjassaan sen kanssa, miten Sandwormin koetaan yleisesti operoivan.

Kaikista Sandwormin toteuttamista kybervaikuttamisoperaatioista lähes puolet (44,5 %) tavoitteli kohdejärjestelmän tai kohdeorganisaation tietomassojen tuhoamista, kuten kuvassa 12 on esitetty. Muun muassa joulukuussa 2015 energiasektoriin kohdistunut ja koko energiantuotantojärjestelmän lamauttanut kyberhyökkäys oli Sandwormin toteuttama. Datan tuhoamiseen keskittyneiden operaatioiden lisäksi Sandworm on suorittanut palvelunesto- ja toimitusketjuhyökkäyksiä sekä tietojenkalasteluoperaatioita. Sandwormin hyökkäykset ovat kohdistuneet kriittiseen infrastruktuuriin sekä Ukrainan valtionhallintoon, joista kriittinen infrastruktuuri on ollut selkeästi keskeisin kohde 77,8 % kokonaisosuudellaan. Sandwormin voidaankin todeta keskittyneen erityisesti kriittiseen infrastruktuuriin kohdistuvien ja tuhoaviin vaikutuksiin pyrkiviin kybervaikuttamisoperaatioihin.

Kuva 12.Kyberuhkatoimija Sandwormin kybervaikuttamisen menetelmät ja kohteet



Ukrainan sodassa vuosina 2014–2021 oli myös toinen GRU:n alainen aktiivinen kyberuhkatoimija, APT28 nimellä paremmin tunnettu GRU:n 85.Erikoispalvelukeskus. Sille on ominaista kohdeympäristössä toteutettava tiedustelu ja tiedonhankinta, jolla se pyrkii hankkimaan sellaisia tietoja ja asiakirjoja, joita ei muilla sotilastiedustelun keinoin kyettäisi saamaan.

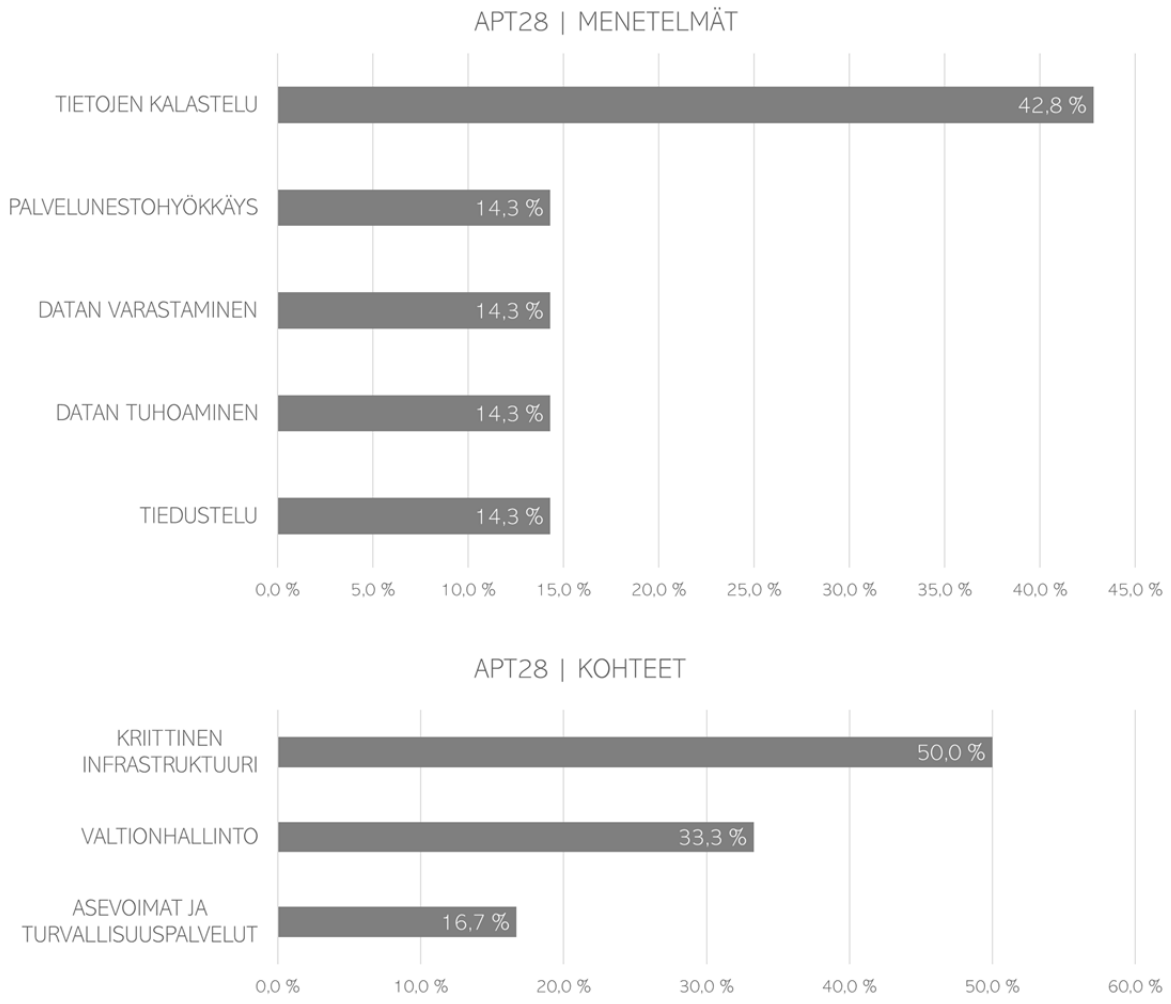
APT28:n toteuttamat kybervaikuttamisoperaatiot Ukrainassa käynnistyivät joulukuussa 2016, ja niiden osuus kaikista Ukrainassa vuosina 2014–2021 tehdyistä kybervaikuttamisoperaatioista oli 23,1 %. Myös tämän tutkimuksen tutkimustulokset puoltavat APT28:n yleisesti ymmärrettyä päätehtävää, sillä tietojenkalastelu ja sen avulla

suoritettu tiedonhankinta oli lähes puolet (42,8 %) kaikista APT28:n suorittamista operaatioista.

Tietojenkalastelun lisäksi kyberuhkatoimija suoritti palvelunestohyökkäyksiä, datan varastamiseen ja tuhoamiseen tähdänneitä operaatioita sekä Ukrainan asevoimien taisteleviin joukkoihin kohdistuneita tiedusteluoperaatioita, kuten tykistöjoukkojen käytössä olleen Android-sovelluksen manipulointi. APT28 murtautui tammikuussa 2020 Ukrainan suurimpiin yksityisiin kaasuyhtiöihin lukeutuvan Burisman tietojärjestelmiin, ja varasti yrityksen sensitiivisiä sähköposteja. Yhdysvaltain silloisen varapresidentin Joe Bidenin poika, Hunter Biden oli tuolloin Burisman hallituksen jäsen ja Joe Biden oli asettumassa ehdolle marraskuussa 2020 järjestettyihin presidentin vaaleihin republikaanien ehdokasta Donald Trumpia vastaan.

APT28:n kybervaikuttamisoperaatioiden keskeisimpinä kohteina olivat kriittinen infrastruktuuri (50 %) sekä valtionhallinto (33,3 %). Tämän kyberuhkatoimijan käyttämät menetelmät ja hyökkäysten kohteet on esitetty alla olevassa kuvassa 13.

Kuva 13. Kyberuhkatoimija APT28:n kybervaikuttamisen menetelmät ja kohteet



Venäjän turvallisuuspalvelu FSB:n alainen kyberuhkatoimija Turla on toteuttanut tiettävästi yhden merkittävään ukrainalaiseen kohteeseen kohdistetun kybervaikuttamisoperaation vuosien 2014–2021 välillä. Kyseessä on maaliskuussa 2014 toteutetusta, kahdeksan minuuttia kestäneestä ja 32 kertaa Georgian sodassa havaittua suuremmasta hajautetusta palvelunestohyökkäyksestä *(DDoS, eng. Distributed Denial of Service)*. Hyökkäys tapahtui kolme päivää ennen Krimin niemimaasta järjestettyä kansanäänestystä. Hyökkäyksellä pyrittiin lamauttamaan Ukrainan tietoliikenneverkot sekä kääntämään ihmisten huomio pois Krimillä toimivista venäläismielisistä joukoista. (Euroopan Parlamentti, 2022)

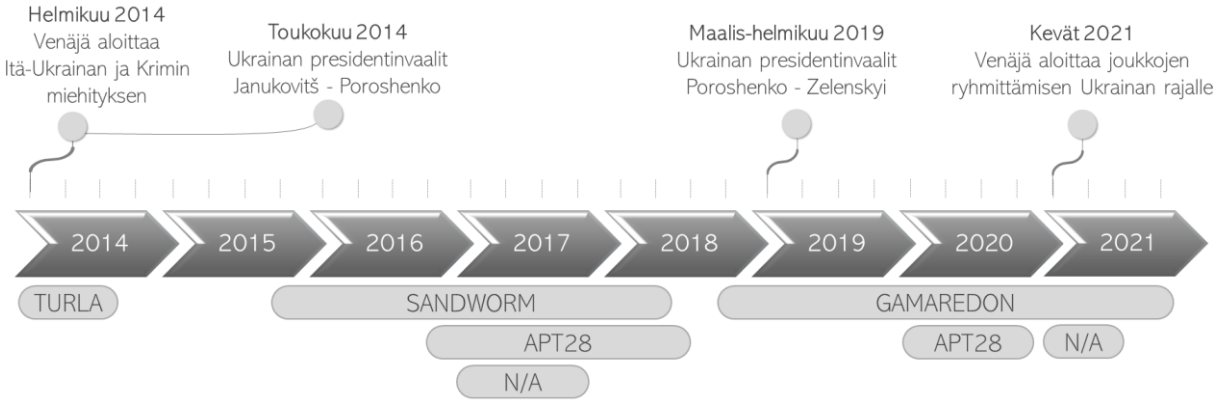
5.4 Yhteenveto

Tutkimustulosten perusteella voidaan todeta, että Venäjän sotilastiedustelu GRU:n kybervaikuttamisen kohteena on Ukrainan sodassa vuosina 2014–2021 ollut ensisijaisesti kriittinen infrastruktuuri, kuten sähkön- ja vedentuotanto, tietoliikenneyhteydet sekä ydinvoimalat. Pystyäkseen vaikuttamaan näissä kohteissa, GRU:n alaiset kyberuhkatoimijat pyrkivät sosiaalisen hakkeroinnin menetelmin onnistuneeseen tietojenkalasteluun. Näin onnistuttiin saavuttamaan pääsy kriittisen infrastruktuurin kohteiden tietojärjestelmiin. Tämä puolestaan mahdollisti kineettisten sotilasoperaatioiden kannalta sopivana ajanhetkenä suoritettavat, lamauttamiseen tai tuhoamiseen pyrkivät kybervaikuttamisoperaatiot. Tällä Venäjän asevoimat pyrki todennäköisesti edesauttamaan sen kineettisen sodankäynnin menestymistä Ukrainan suunnalla.

Venäjän turvallisuuspalvelu FSB keskittyi omissa kybervaikuttamisoperaatioissaan sen sijaan enemmän Ukrainan poliittisen järjestelmän horjuttamiseen ja yhteiskunnallisen epävakauden luomiseen. Kyberuhkatoimija Gamaredon profiloitui tutkimusaineiston perusteella erityisesti datavarkauksiin, jotka pitivät sisällään Ukrainan valtiollisia dokumentteja, joita FSB pystyi hyödyntämään myöhemmissä kybervaikuttamisoperaatioissaan. Turla oli puolestaan FSB:n aggressiivisempi kyberuhkatoimija, joka suoritti lamauttavat ja tuhoavat kyberhyökkäykset.

Tutkimusta ja sen tuloksia tarkasteltaessa on syytä ottaa huomioon, että helmikuussa 2022 käynnistynyt Venäjän laajamittainen hyökkäyssota on aktivoinut myös venäläisiä kyberuhkatoimijoita. Muun muassa GRU:n alainen Sandworm on aktivoitunut jälleen vuoden 2018 jälkeen, jonka ohella myös Venäjän ulkomaan siviilitiedustelupalvelu SVR:n alainen APT29 on yhdistetty viimeisimpiin kybervaikuttamisoperaatioihin. Tämän tutkimuksen tarkastelujaksoon vuosien 2014–2021 välille sijoittuvat merkittävimmät sotilaspoliittiset tapahtumat sekä kyberuhkatoimijoiden aktiivisuusjaksot on kuvattu alla olevassa kuvassa 14.

Kuva 14. Merkittävimmät sotilaspoliittiset tapahtumat ja kyberuhkatoimijoiden aktiivisuusjaksot Ukrainan sodassa vuosina 2014–2021.



6 Johtopäätökset

Tämän tutkimuksen tavoitteena oli selvittää laadullisen tutkimuksen menetelmin, *millaista kybervaikuttamista Ukrainan sodassa havaittiin vuosina 2014–2021 ja mitkä kyberuhkatoimijat vastasivat kybervaikuttamisoperaatioista.* Tähän tutkimuksen pääkysymykseen haettiin vastausta kolmella alatutkimuskysymyksellä. Ensimmäinen alatutkimuskysymys oli, *mitä on kybervaikuttaminen?*

Tässä tutkimuksessa *kybervaikuttaminen* määriteltiin luvussa 3.4. siten, että:

> *Kybervaikuttaminen on kybertoimintaympäristössä toteutettavaa, vastustajan tietojärjestelmiin ja -verkkoihin kohdistettavaa sellaista toimintaa, jolla pyritään häiritsemään tai rajoittamaan niiden, sekä niissä olevan tiedon käyttöä.*

Kybervaikuttamisoperaatioita kyetään suorittamaan suhteellisen alhaisilla kustannuksilla verrattuna kineettiseen vaikuttamiseen. Kybervaikuttamisen kohteita tulisi tarkastella osana vaikuttamisen kokonaisuutta, jolloin mahdollistettaisiin sekä suora että epäsuora vaikutus. Kybervaikuttamisen sekä kineettisen sodankäynnin tulee toimia yhdessä, osana keskitetysti johdettua yhteisoperaatiotoimintaa, jotta kybervaikuttamisen vaikutukset pystyttäisiin maksimoimaan kybersodankäynnin viitekehyksessä. Hyökkääjän eduksi on huomioitava, että sen faktuaalinen identifiointi on haastavaa ja paikoin jopa mahdotonta.

Toinen alatutkimuskysymys oli, *millainen on Venäjän valtiollinen kyky kyberoperaatioiden suorittamiseen?* Tähän kysymykseen vastataan tutkimuksen neljännessä luvussa. Venäjän valtiollista kybertoimintaa toteuttaa pääasiassa kolme keskeistä tiedustelu- ja turvallisuuspalvelua: sotilastiedustelusta vastaava tiedustelupäähallinto GRU, ulkomaan siviilitiedustelupalvelu SVR sekä turvallisuuspalvelu FSB. Viranomaisten kybertoimintoja tuetaan laajasti Venäjän sotateollisen kompleksin toimesta, esimerkiksi haittaohjelmia valmistamalla sekä tietoteknisten laitteiden kehitys- ja valmistusprosesseilla. Turvallisuus- ja tiedusteluviranomaisilla on keskinäistä valtataistelua muiden toimintaympäristöjen tavoin myös kybertoimintaympäristössä, joka näyttäytyy keskinäisenä kilpailuna ja valtataisteluna. Venäjällä ei ole olemassa prosesseja kansalliselle, keskitetylle kybertoiminnan johtamiselle. Tästä johtuen viranomaiset toimeenpanevat kyberoperaatioita toisistaan tietämättä, ja kohdistavat hyökkäykset näin ollen myös samoihin kohteisiin. Tämä puolestaan saattaa johtaa jopa toisen viranomaisen operaation tahattomaan paljastumiseen.

Venäjällä on ollut kryptografiaan, tietotekniikkaan ja tietoturvallisuuteen keskittyvää koulutusta aina Neuvostoliiton ajoilta lähtien. Koulutus on toteutettu niin viranomaisten omien koulutuskeskusten kuin myös Venäjän valtiollisten yliopistojen toimesta. Valtiolliset yliopistot ovatkin pääosin osana Venäjän valtiollista järjestelmää, ja toimivat valtionjohdon tiukassa ohjauksessa. Tämä on mahdollistanut myös kybertoiminnan laajamittaisen kouluttamisen sekä kyberosaajien rekrytoinnin. Valtion yliopistot sekä erityisesti niissä toimivat matematiikan ja fysiikan laitokset toimivat keskeisinä valtiollisten kyberuhkatoimijoiden rekrytointikanavina. Venäjän asevoimat on viimeisen vuosikymmenen aikana onnistunut rakentamaan omasta kybertoiminnastaan kiehtovan kokonaisuuden, jonka myötä siitä on tullut opiskelijoiden keskuudessa FSB:tä suositumpi kyberammattilaisuuden vaihtoehto. Venäläinen kyberosaamisen koulutusjärjestelmä kykenee optimaalisissa olosuhteissa luomaan uusia osaajia sen operatiivisiin tarpeisiinsa.

Venäjän valtionhallinnon virallisasiakirjoissa käsitellään kybertoimintaa varsin rajallisesti. Ainoastaan vuonna 2014 julkaistussa kyberturvallisuuden strategisen konseptin luonnoksessa käsitellään terminologisesti kyberturvallisuutta. Muissa virallisasiakirjoissa aihealuetta käsitellään tietoturvallisuuden käsitteen kautta. Virallisasiakirjoissa korostuu tietotekniikan ja tietoteknisten menetelmien implementointi osaksi valtionhallintoa. Venäjä

pyrkii ylläpitämään näennäistä kyberturvallisuuden yhteistyötä länsimaiden kanssa. Samalla se korostaa yhteistyön laajuutta ja edelleen syventämistä esimerkiksi Kiinan kanssa. Venäjä tuo virallisasiakirjoissaan ilmi myös tarpeen ylläpitää ”teknologiasuurvallan asemaansa”, vastatakseen Yhdysvaltojen ja Naton kohdistamaan kyberuhkaan. Asiakirjoissa luodaan edellytykset Venäjän kyberteknologian kehittämiselle sekä teknologian hankinnalle sen kansainvälisiltä kumppaneilta, jotka mahdollistavat osaltaan Venäjän valtiollisen kybersuorituskyvyn kasvattamisen.

Venäjän valtiollista kybervaikuttamiskykyä arvioitaessa voitaisiin todeta, että Venäjän kybertoiminnan laajamittainen koulutusjärjestelmä mahdollistaa uusien ammattilaisten kouluttamisen. Venäjän valtionhallinnon virallisasiakirjoissa luodaan lisäksi toimintaedellytykset rajat ylittäville hyökkäyksellisille toimille, sekä kansainväliselle yhteistyölle erityisesti Kiinan kanssa. Valtion viranomaisten keskinäinen valtataistelu, sekä toimintojen hyvin vajavainen koordinointi ja johtaminen vaikuttavat kuitenkin merkittävästi kyberoperaatioiden menestyksekkääseen suorittamiseen.

Kolmanteen alatutkimuskysymykseen, *millaisia kybervaikuttamisen menetelmiä käytettiin ja millaisiin kohteisiin Venäjän valtiolliset kyberuhkatoimijat vaikuttivat Ukrainan sodassa vuosina 2014–2021,* vastattiin tutkimuksen viidennessä luvussa. Venäjän kyberuhkatoimijoiden hyökkäysten kohteet sekä käytetyt menetelmät poikkeavat hieman kunkin toimijan ja viraston kohdalla. Venäjän sotilastiedustelun kybervaikuttamisen kohteina oli ensisijaisesti kriittiseen infrastruktuuriin lukeutuvat sähkö-, vesi- ja ydinvoimalat sekä tietoliikenneyhteydet. GRU:n kybervaikuttamisen roolit vaikuttivat olleen jaettu sen alaisten toimijoiden välillä. APT28 eteni kohteisiin sosiaalisen hakkeroinnin menetelmillä, kun puolestaan Sandworm suoritti kohteissa pääosin järjestelmät lamauttavia tai tietojen tuhoamiseen pyrkiviä kybervaikuttamisoperaatioita. Tällä pyrittiin todennäköisesti edesauttamaan Venäjän asevoimien kineettisen hyökkäyksen menestymistä.

Turvallisuuspalvelu FSB kohdisti omat kybervaikuttamisoperaationsa Ukrainan poliittisen järjestelmän horjuttamiseen sekä yhteiskunnallisen epävakauden luomiseen. Myös FSB:ssä kybervaikuttamisen roolit olivat jakautuneet selkeästi kyberuhkatoimijoiden kesken. Toinen kyberuhkatoimijoista, Gamaredon, oli keskittynyt selkeästi sosiaaliseen hakkerointiin ja

datavarkauksiin. Turla suoritti sille ominaiseen tapaansa lamauttavan ja tuhoavan kyberhyökkäyksen. Ulkomaan siviilitiedustelupalvelu SVR:n alaisia kyberuhkatoimijoita ei tutkimusaineiston perusteella toiminut Ukrainan sodassa vuosina 2014–2021 ainakaan siten, että niiden toiminta olisi kyetty identifioimaan. On kuitenkin mahdollista, että osa tuntemattomiksi jääneistä kyberuhkatoimijoista olisi toiminut SVR:n alaisuudessa.

Tutkimustulokset osoittavat, että kyberhyökkäyksiltä suojautumisen keskiössä ovat laitteiden, palveluiden sekä tietojärjestelmien käyttäjät. Valtaosa kybervaikuttamisoperaatioista käynnistyy käyttäjään kohdistuvalla tietojenkalastelulla. Tästä johtuen käyttäjien tulisi kasvattaa tietoisuuttaan siitä, miten tietojenkalastelun tunnistaa ja miten näissä tapauksissa tulisi toimia. Erityisen tärkeää on ylläpitää ajantasaiset päivitykset käytössä olevissa laitteissa ja sovelluksissa. Tämän lisäksi tulisi ottaa mahdollisimman laajasti käyttöön monivaiheinen tunnistautuminen, jossa salasanan lisäksi käyttäjää pyydetään vahvistamaan kirjautuminen jollain toisella, ulkoisella mekanismilla. Etenkin suomalaisissa organisaatioissa tekninen tietoturvallisuus on toteutettu pääosin hyvin, mutta käyttäjien huolimattomuutta tai tietämättömyyttä hyväksikäyttäen suoritettu tunkeutuminen tekee erinomaisestikin toteutetusta tietoturvallisuudesta lähes merkityksetöntä.

Voidaan todeta, että alatutkimuskysymyksien avulla kyettiin vastaamaan tutkimuksen päätutkimuskysymykseen. Alatutkimuskysymyksillä haettiin aluksi määritelmä kybervaikuttamiselle, jota hyödynnettiin loppututkimuksen ajan. Lisäksi alatutkimuskysymyksillä hahmotettiin Venäjän valtiollinen kyky kyberoperaatioiden suorittamiseen virallisasiakirjojen, eri kybertoimintaa suorittavien organisaatioiden sekä koulutus- ja rekrytointijärjestelmien kautta. Näiden jälkeen perehdyttiin Ukraina sodan kybertapahtumiin vuosien 2014 ja 2021 välillä. Tutkimuksen myötä voidaankin todeta, että Venäjä todennäköisesti pyrkii synkronoimaan kybervaikuttamisoperaatiot siten, että ne tukisivat sen poliittisia ja sotilaallisia tavoitteita. Venäjällä valtiollista kybertoimintaa toteutetaan useiden toistensa kanssa kilpailevien virastojen alaisuudessa, eikä tällä kybertoiminnan kokonaisuudella ole keskitettyä valtiollista koordinointia eikä johtamisrakennetta. Todennäköisesti ainakin osittain näistä syistä myös kineettisten sotilasoperaatioiden tukeminen yhdenaikaisella kybervaikuttamisella on osoittautunut haasteelliseksi. Vaikka kybervaikuttamisella ei olla merkittävästi kyetty tukemaan kineettisiä

sotilasoperaatioita, on sillä kuitenkin muiden ei-kineettisten vaikuttamisen muotojen ohella kyetty epävakauttamaan Ukrainan yhteiskuntaa.

Jatkotutkimuksen kannalta olisi tarpeen tutkia Venäjän kybervaikuttamista Ukrainan sodassa vuodesta 2022 lähtien sekä Georgian sodassa vuonna 2008. Näin kyettäisiin muodostamaan käsitys Venäjän kybervaikuttamisen kehittymisestä kineettisen sodankäynnin rinnalla. Kyseistä jatkotutkimusaihetta ja tutkimusongelmaa käsitellään tämän tutkimussarjan toisessa, erillisenä tutkimuksena julkaistavassa osassa.

Olisi myös mielenkiintoista tutkia länsimaihin ja erityisesti Naton jäsenmaihin kohdistettua kybervaikuttamista, sillä siitä ei ole saatavilla aiempaa kotimaista tutkimustietoa. Toisaalta niin Ukrainan kuin myös Venäjän kyberpuolustuskyky olisi myös mielenkiintoinen tutkimusaihe, sillä niitä on käsitelty hyvin vähän myös kansainvälisten tutkimusten yhteydessä.

Venäjän jo vuonna 2014 käynnistämä sota Ukrainassa, sekä helmikuusta 2022 lähtien todistetut sotarikokset ovat muuttaneet pysyvästi länsimaista, eurooppalaista sekä ennen kaikkea suomalaista turvallisuuskulttuuria. Venäjällä oli Ukrainaan hyökkäämisellään Naton suhteen yksi keskeinen tarkoitus: estää Naton laajentuminen ja Naton Venäjän vastaisen rajan kasvattaminen. Hyökkäyssodallaan Venäjä kuitenkin pakotti länsimaat adaptoitumaan muuttuneeseen turvallisuustilanteeseen. Tämä puolestaan johti siihen, että huhtikuun 4. päivänä vuonna 2023 Naton jäsenmaiden lukumäärä kasvoi yhdellä, jolloin samalla Naton ja Venäjän vastainen raja kaksinkertaistui 1215 kilometristä 2555 kilometriin. Tämä tutkimusraportti on ajankohtaan nähden sopivaa päättää jalkaväenkenraali ja Mannerheim-ristin ritari Adolf Ehrnroothin lausumiin talvisodan oppeihin: ”E*i enää koskaan yksin!”.*

”Suomesta on tänään tullut puolustusliitto Naton jäsen. Sotilaallisen liittoutumattomuuden aikakausi historiassamme päättyy.
Uusi aikakausi alkaa.”

Suomen tasavallan presidentti Sauli Niinistö, Brysselissä 4.4.2023

Lähteet

Agentura. (n.d.-a). *16 Центр ФСБ. [FSB:n 16. keskus]*. Haettu 25.1.2023 osoitteesta https://agentura.ru/profile/federalnaja-sluzhba-bezopasnosti-rossii-fsb/16-centr/

Agentura. (n.d.-b). *Центр информационной безопасности ФСБ. [FSB:n tietoturvakeskus].* Haettu 20.12.2022 osoitteesta https://agentura.ru/profile/federalnaja-sluzhba-bezopasnosti-rossii-fsb/centr-informacionnoj-bezopasnosti-fsb/

Ashby, H. (7.4.2022). *How the Kremlin Distorts the 'Responsibility to Protect' Principle*. United States Institute of Peace. https://www.usip.org/publications/2022/04/how-kremlin-distorts-responsibility-protect-principle

Bastian, N. (2019). *Information Warfare and Its 18th and 19th Century Roots.* US Government. https://cyberdefensereview.army.mil/portals/6/documents/cdr%20journal%20articles/fall%202019/cdr%20v4n2-fall%202019_bastian.pdf?ver=2019-11-15-104103-203

Baumgartner, K., & Raiu, C. (21.4.2015). *The CozyDuke APT*. Kaspersky Lab. Haettu 22.2.2023 osoitteesta https://securelist.com/the-cozyduke-apt/69731/

BBC News Russia. (24.2.2022). *Путин о начале «специальной военной операции» в Донбассе. [Putin sotilaallisen erikoisoperaation alkamisesta Donbassissa] [video].* Youtube. BBC News. https://www.youtube.com/watch?v=iPvB_TcItgQ

Bing, C. (31.3.2022). *U.S. warned firms about Russia's Kaspersky software day after invasion - sources.* Reuters. https://www.reuters.com/technology/exclusive-us-warned-firms-about-russias-kaspersky-software-day-after-invasion-2022-03-31/

Borogan, A., & Soldatov, I. (2022). *Russian Cyberwarfare: Unpacking the Kremlin's Capabilities*. CEPA. https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/

British Council. (2019). *Social media influencers*. LearnEnglish. Haettu 4.1.2023 osoitteesta https://learnenglish.britishcouncil.org/skills/reading/b1-reading/social-media-influencers

Broadband Search. (n.d.). *Know the Risk: The Best and Worst Countries for Cybersecurity*. Haeuttu 20.2.2023 osoitteesta https://www.broadbandsearch.net/blog/best-worst-countries-cybersecurity

Brooks, C., & Lysenko, V. (2018). *Russian information troops, disinformation, and democracy.* First Monday. https://doi.org/10.5210/fm.v22i5.8176

Cambridge University. (n.d.). *Cambridge dictionary: influence*. Haettu 4.1.2023 osoitteesta https://dictionary.cambridge.org/dictionary/english/influence

Candolin, C. (13.4.2022). *Kriittinen infrastruktuuri ja kybervaikuttaminen*. Uusi Suomi Puheenvuoro. https://puheenvuoro.uusisuomi.fi/catharinacandolin/kriittinen-infrastruktuuri-ja-kybervaikuttaminen/

Center for Strategic and International Studies. (2023). *Significant Cyber Incidents Since 2006*. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-02/230207_significant_cyber_incidents.pdf?versionid=f3tcddnq0yczpy72d_adhyuyy21ifk_h

CISA. (2018a). *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.* Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical

CISA. (2018b). *Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices.* Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/alerts/2018/04/16/russian-state-sponsored-cyber-actors-targeting-network-infrastructure

CISA. (20.7.2021). *Cyber-Attack Against Ukrainian Critical Infrastructure.* Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

CISA. (20.4.2022). *Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.* Cybersecurity and Infrastructure Security Agency CISA. https://media.defense.gov/2022/apr/20/2002980529/-1/-1/1/joint_csa_russian_state-sponsored_and_criminal_cyber_threats_to_critical_infrastructure_20220420.pdf

Congressional Research Service. (2022). *Russian Cyber Units*. https://crsreports.congress.gov/product/pdf/IF/IF11718

Council on Foreign Relations. (2023). *Tracking State-Sponsored Cyberattacks Around the World*. Council on Foreign Relations. https://www.cfr.org/cyber-operations

Crowdstrike. (2017). *Use of Fancy Bear android malware in tracking of Ukrainian field artillery units*. https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf

Crowdstrike. (30.3.2022). *EMBER BEAR: Threat Actor Profile*. Haettu 26.2.2023 osoitteesta https://www.crowdstrike.com/blog/who-is-ember-bear/

Cyberint. (2019). *Russian Backed Turla Resourfaces with a Sophisticated RAT*. https://e.cyberint.com/hubfs/CyberInt_Russian%20Backed%20Turla%20Resourfaces%20with%20a%20Sophisticated%20RAT_Report.pdf

David. (4.2.2021). *Turla—High sophistication Russian-nexus threat group*. Cyberint. Haettu 25.2.2023 osoitteesta https://cyberint.com/blog/research/turla-high-sophistication-russian-nexus-threat-group/

Distant Writing. (n.d.). *Telegraph at War 1854-68*. Haettu 5.1.2023 osoitteesta https://distantwriting.co.uk/telegraphwar.html

Dossier. (n.d.). *FSB Counter Intelligence Department and Information Security Center*. Haettu 26.2.2023 osoitteesta https://fsb.dossier.center/1s/

Ertan, A., Floyd, K., Pernik, P., Stevens, T. (2020). *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

Euroopan neuvosto. (2001). *The Budapest Convention (ETS No. 185) and its Protocols.* Council of Europe. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Euroopan Parlamentti. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf

Euroopan Unionin neuvosto. (2014). *EU Cyber Defence Policy Framework*. The Council of the European Union. https://ccdcoe.org/uploads/2018/11/EU-141118-EUCyberDefencePolicyFrame-2.pdf

FBI. (2017). *Assessing Russian Activities and Intentions in Recent Elections*. Federal Bureau of Investigation. https://www.fbi.gov/news/testimony/assessing-russian-activities-and-intentions-in-recent-elections

FCC. (25.3.2022) *FCC Expands List of Equipment and Services That Pose Security Threat*. Federal Communications Commission. https://www.fcc.gov/document/fcc-expands-list-equipment-and-services-pose-security-threat

FIIA. (2021). *Russia's quest for digital competitiveness - the role of private businesses in securing state interests*. FIIA. https://doi.org/10.32040/PolicyBrief.2021.SciTechDev

FireEye. (2017). *APT28: At the center of the storm—Russia strategically evolves its cyber operations*. FireEye. https://www.mandiant.com/sites/default/files/2021-09/APT28-Center-of-Storm-2017.pdf

Flyktman, J. (2017). *Informaatiosodankäynnin merkitys: Käsitetutkimus, doktriinitutkimus sekä tapaustutkimus Krimin ja Syyrian operaatioista*. [Diplomityö, Maanpuolustuskorkeakoulu]. https://www.doria.fi/handle/10024/144308

Flyktman, J., Laari, T., Härmä, K., Timonen, J., & Tuovinen, J. (2019). *#kyberpuolustus: Kyberkäsikirja Puolustusvoimien henkilöstölle*. Maanpuolustuskorkeakoulu. https://www.doria.fi/handle/10024/173254

F-Secure. (n.d.). *Mitä on kyberturvallisuus?* Haettu 7.1.2023 osoitteesta https://www.f-secure.com/fi/home/articles/what-is-cyber-security

Global Defence Technology. (n.d.). *The evolution of electronic warfare.* Global Defence Technology. Haettu 5.1.2023 osoitteesta https://defence.nridigital.com/global_defence_technology_special/the_evolution_of_electronic_warfare

Global Security. (n.d.). *Eighth Directorate of the General Staff / State Secret Protection Service of the Armed Forces*. Haettu 27.1.2023 osoitteesta https://www.globalsecurity.org/intell/world/russia/8gumo.htm

Heickerö, R. (2020). *Emerging Cyberthreats and Russian Views on Information Warfare and Information Operations.* Swedish Defense Research Agency FOI. https://www.foi.se/rest-api/report/FOI-R--2970--SE

HHS. (2022). *Major Cyber Organizations of the Russian Intelligence Services*. Health Sector Cybersecurity Coordination Center. https://www.hhs.gov/sites/default/files/major-cyber-orgs-of-russian-intelligence-services.pdf

i-SCOOP. (2021). *The CIA triad of confidentiality, integrity and availability.* https://www.i-scoop.eu/cybersecurity/cia-confidentiality-integrity-availability-security/

Iso-Britannian hallinto. (2022a). *UK National Cyber Strategy*. HM Government. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf

Iso-Britannian hallinto. (2022b). *Russia's FSB malign activity*. HM Government. https://www.gov.uk/government/publications/russias-fsb-malign-cyber-activity-factsheet/russias-fsb-malign-activity-factsheet

ISO/IEC 27001:2005. (2022). *Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.*

Kari, M. (2019). *Russian Strategic Culture in Cyberspace: Theory of Strategic Culture – a tool to Explain Russia´s Cyber Threat Perception and Response to Cyber Threats*. [Väitöskirja, Jyväskylän yliopisto]. http://urn.fi/URN:ISBN:978-951-39-7837-2

Kaspersky Lab. (n.d.). *What's behind APT29?* Kaspersky Lab. Haettu 22.2.2023 osoitteesta https://www.kaspersky.com/enterprise-security/mitre/apt29

Kotimaisten kielten keskus. (n.d.). *Kielitoimiston sanakirja: vaikuttaa*. Haettu 3.1.2023 osoitteesta https://www.kielitoimistonsanakirja.fi/#/Vaikuttaa?searchMode=all

Kreml. (2000). *Доктрина информационной безопасности Российской Федерации 2000. [Venäjän federaation tietoturvadoktriini 2000].* Haettu 3.1.2023 osoitteesta http://base.garant.ru/182535/

Kreml. (24.4.2014). *Media Forum of Independent Local and Regional Media.* http://en.kremlin.ru/events/president/news/20858

Kreml. (2014). *Военная доктрина Российской Федерации 2014. [Venäjän federaation sotilasdoktriini 2014]*. Haettu 20.2.2023 osoitteesta http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf

Kreml. (2016a). *Концепция внешней политики Российской Федерации 2016. [Venäjän federaation ulkopolitiikan konsepti 2016]*. Haettu 17.2.2023 osoitteesta http://static.kremlin.ru/media/events/files/41d447a0ce9f5a96bdc3.pdf

Kreml. (2016b). *Доктрина информационной безопасности Российской Федерации 2016. [Venäjän federaation tietoturvadoktriini 2016]*. Haettu 13.2.2023 osoitteesta http://static.kremlin.ru/media/acts/files/0001201612060002.pdf

Kreml. (2021a). *О Стратегии национальной безопасности Российской Федерации 2021. [Venäjän federaation kansallinen turvallisuusstrategia 2021]*. Haettu 17.2.2023 osoitteesta

http://static.kremlin.ru/media/events/files/ru/QZw6hSk5z9gWq0plD1ZzmR5cER0g5tZC.pdf

Kreml. (2021b). *Основы государственной политики Российской Федерации в области международной информационной безопасности 2021. [Venäjän federaation kansainvälisen tietoturvallisuuden kenttää koskevat valtionpolitiikan perusperiaatteet 2021]*. Haettu 13.2.2023 osoitteesta http://static.kremlin.ru/media/events/files/ru/RR5NtCWkkZPTuc5TrdHURpA4vpN5UTwM.pdf

Kuusisto, T. (2014). *Kybertaistelu 2020*. Maanpuolustuskorkeakoulu. https://urn.fi/URN:ISBN:978-951-25-2618-5

Kyberturvallisuuskeskus. (18.12.2020). *SolarWinds Orion Platformin takaovi mahdollisti vakoilun ja tietomurtoja*. Haettu 22.3.2023 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/solarwinds-orion-platformin-takaovi-mahdollisti-vakoilun-ja-tietomurtoja

Kyberturvallisuuskeskus. (2022). *Toimitusketjuhyökkäyksen toimintaohje*. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Toimitusketjuhy%C3%B6kk%C3%A4ysToimintaohje.pdf

Lehto, M. (2021). *Digitaalisen kybermaailman ilmiöitä ja määrittelyjä*. Jyväskylän yliopisto. https://www.jyu.fi/it/fi/hae-opiskelemaan/hakukohteet/kybma/kybermaailma_v15-0.pdf

Lehto, M., & Henselmann, G. (2020). *Non-Kinetic Warfare: The New Game Changer in the Battle Space*. Jyväskylän yliopisto. https://jyx.jyu.fi/bitstream/handle/123456789/68860/Non-Kinetic_Warfare_The_New_G.pdf?sequence=1&isAllowed=y

Lehto, M., & Limnéll, J. (2017). Kybersodankäynnin kehityksestä ja tulevaisuudesta. *Tiede ja ase, 75.* Haettu 4.1.2023 osoitteesta https://journal.fi/ta/article/view/67730

Lilly, B. (2022). *Russian information warfare: Assault on democracies in the cyber wild west*. Naval Institute Press.

Limnéll, J., Majewski, K., & Salminen, M. (2014). *Kyberturvallisuus*. Docendo.

Maïche, K. (2015) *Mitäs me länsimaalaiset! Suomi ja lännen käsite.* Info Kustannus.

Matisoft. (n.d.). *Matisoft Case Studies Page: Into the mind of The Dukes hacking group AKA Cozy Bear and Apt29*. Haettu 22.2.2023 osoitteesta https://www.matisoftlabs.com/case-studies/apt29

Meduza. (6.11.2018). *What is the GRU? Who gets recruited to be a spy? Why are they exposed so often?* Meduza. Haettu 27.1.2023 osoitteesta https://meduza.io/en/feature/2018/11/06/what-is-the-gru-who-gets-recruited-to-be-a-spy-why-are-they-exposed-so-often

MITRE. (2019). *TEMP.Veles | MITRE ATT&CK®*. https://attack.mitre.org/versions/v10/groups/G0088/

MITRE. (2022a). *Ember Bear | MITRE ATT&CK®*. Haettu 26.1.2023 osoitteesta https://attack.mitre.org/groups/G1003/

MITRE. (2022b). *APT29 | MITRE ATT&CK*. Haettu 26.2.2023 osoitteesta https://attack.mitre.org/groups/G0016/

MITRE. (2022c). *Turla | MITRE ATT&CK®*. Haettu 22.2.2023 osoitteesta https://attack.mitre.org/groups/G0010/

MITRE. (2022d). *Sandworm | MITRE ATT&CK®*. Haettu 25.2.2023 osoitteesta https://attack.mitre.org/groups/G0034/

MITRE. (2022e). *Dragonfly | MITRE ATT&CK®*. Haettu 25.2.2023 osoitteesta https://attack.mitre.org/groups/G0035/

Mwiki, H., Dargahi, T., Dehghantanha, A., & Choo, K. (2019). Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin. Teoksessa D. Gritzalis, M. Theocharidou & G. Stergiopoulos (toim.), *Advanced Sciences and Technologies for Security Applications. Critical Infrastructure Security and Resilience: Theories, Methods, Tools and Technologies.* (ss. 221–244). Springer.

NATO. (28.2.2023). *Statement by NATO Secretary General Jens Stoltenberg with the Prime Minister of Finland, Sanna Marin* [Tiedote]. Haettu 28.3.2023 osoitteesta https://www.nato.int/cps/en/natohq/opinions_212274.htm

NATO. (2016). *Warsaw Summit Guide 8-9 July 2016*. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160715_1607-Warsaw-Summit-Guide_2016_ENG.pdf

NATO. (2017). *Cyber Definitions.* NATO Cooperative Cyber Defence Centre of Excellence. Haettu 8.1.2023 osoitteesta https://ccdcoe.org/cyber-definitions.html

NSA. (2020). *Cybersecurity Advisory: Russian GRU 85th GTsSS Deploys Previously Undisclosed Drovorub Malware*. National Security Agency https://media.defense.gov/2020/Aug/13/2002476465/-1/-1/0/CSA_DROVORUB_RUSSIAN_GRU_MALWARE_AUG_2020.PDF

Paloalto. (3.2.2022). *Russia's Gamaredon aka Primitive Bear APT Group Actively Targeting Ukraine.* Haettu 26.2.2023 osoitteesta https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021

ParkHous. (7.9.2022). *Specialization in cryptography. Cryptography—What is it? Fundamentals of cryptography*. Haettu 21.1.2023 osoitteesta https://park-hous.ru/en/specialnost-kriptografiya-kriptografiya---chto-eto-takoe-osnovy/

Puusa, A. (2008). Käsiteanalyysi tutkimusmenetelmänä. *Premissi,* (4) (ss. 35–42).

Zinets, N. (9.7.2021). *Ukraine says Russian hackers hit its Navy website*. Haettu 20.3.2023 osoitteesta https://www.reuters.com/world/europe/ukraine-says-russian-hackers-hit-its-navy-website-2021-07-09/

Sanastokeskus. (n.d.). Kriittinen infrastruktuuri. Teoksessa *TEPA-Termipankki*. Haettu 20.3.2023 osoitteesta https://termipankki.fi/tepa/fi/haku/kriittinen%20infrastruktuuri

Sanastokeskus. (2018). *Kyberturvallisuuden sanasto*. https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf?file=pdf/Kyberturvallisuuden_sanasto.pdf

Sarajärvi, A., & Tuomi, J. (2011). *Laadullinen tutkimus ja sisällönanalyysi*. Tammi

Saressalo, T. (2012). *Psykologinen vaikuttaminen CAST LEAD -operaatiossa* [Esiupseerikurssin tutkielma, Maanpuolustuskorkeakoulu]. https://urn.fi/URN:NBN:fi-fe201206186041

Sherman, J. (12.1.2023). *Russia's largest hacking conference reflects isolated cyber ecosystem.* Brookings. https://www.brookings.edu/techstream/russias-largest-hacking-conference-reflects-isolated-cyber-ecosystem/

Suomen perustuslaki 731/1999 § 14. https://www.finlex.fi/fi/laki/ajantasa/1999/19990731

TeamPassword. (24.8.2021). *Who is Cozy Bear and how can you protect yourself?* Haettu 22.2.2023 osoitteesta https://teampassword.com/blog/who-is-cozy-bear-and-how-can-you-protect-yourself

Toikko, T., & Rantanen, T. (2009). *Tutkimuksellinen kehittämistoiminta: Näkökulmia kehittämisprosessiin, osallistamiseen ja tiedontuotantoon*. Tampere University Press.

Turvallisuuskomitea. (2013). *Suomen kyberturvallisuusstrategia*. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_SUOMI_WEB_300919.pdf

Vilkka, H. (2021) *Tutki ja kehitä*. PS-kustannus.

Ukrainan turvallisuuspalvelu SBU. (2021a). *Gamaredon Group Technical Report*. https://ssu.gov.ua/uploads/f les/DKIB/Technical%20report%20Armagedon.pdf1

Ukrainan turvallisuuspalvelu SBU. (2021b). *СБУ встановила ха-керів ФСБ, які здійснили понад 5 тис. Кібератак на державні органи України [The Security Service of Ukraine identified FSB hackers who carried out more than 5,000 cyberattacks on state bodies of Ukraine]*. Haettu 26.2.2023 osoitteesta https://ssu.gov.ua/novyny/sbu-vstanovyla-khakeriv-fsb-yaki-zdiisnyly-ponad-5-tys-kiberatak-na-derzhavni-orhany-ukrainy

Ulkoministeriö. (n.d.). *Kyberturvallisuus ja kybertoimintaympäristö*. Haettu 4.1.2023 osoitteesta https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto

Ulkoministeriö. (2020). *Suomi ja suojeluvastuu—Viisitoista vuotta suojeluvastuuperiaatteen hyväksymisestä*. https://um.fi/documents/35732/0/Suomi+ja+suojeluvastuu_NET+%285%29.pdf/d484dbd6-ebce-2e41-11a5-babdc025e029?t=1611729760507

U.S. Marine Corps Forces & Cyberspace Command. (2018). *Final MARFORCYBER Trifold*. USCYBERCOM. https://www.marforcyber.marines.mil/Portals/215/Site%20Images/FINAL%20MARFORCYBER%20Trifold.pdf

Valtioneuvosto. (25.2.2022). *Tasavallan presidentin ja pääministerin tiedotustilaisuus 24.2.2022 [video]*. Youtube. Valtioneuvosto. https://www.youtube.com/watch?v=G_km3l4ri5k

Venäjän kansainvälisen tietoturvallisuuden järjestö. (5.1.2019). *Руководство Ассоциации. [Yrityksen johto]*. https://namib.online/rukovodstvo-associacii/

Venäjän liittoneuvosto. (2014a). *Проект стратегии кибербезопасности России вынесен на общественное обсуждение—Р. Гаттаров [Luonnos Venäjän kyberturvallisuusstrategiasta julkiseen keskusteluun – R. Gattarov] [video]*. http://council.gov.ru/events/multimedia/video/26170/

Venäjän liittoneuvosto. (2014b). *Концепция стратегии кибербезопасности Российской Федерации—Проект 2013 [Luonnos Venäjän federaation kyberturvallisuuden strategisesta konseptista 2013]*. Haettu 15.2.2023 osoitteesta http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf

Venäjän puolustusministeriö. (n.d.). *Федеральное агентство связи и информации ФАПСИ [Liittovaltion viestintä- ja tiedonantovirasto FAPSI]*. Haettu 25.1.2023 osoitteesta https://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=11261@morfDictionary

Venäjän turvallisuusneuvosto. (n.d.). *Члены Совета Безопасности Российской Федерации с момента его создания [Venäjän federaation turvallisuusneuvoston jäseniä sen perustamisesta lähtien]*. Haettu 25.1.2023 osoitteesta http://www.scrf.gov.ru/about/all_time/

Venäjän turvallisuuspalvelu FSB. (n.d.-a). *История создания: Федеральная Служба Безопасности [Venäjän turvallisuuspalvelun historia]*. Haettu 25.1.2023 osoitteesta http://www.fsb.ru/fsb/history.htm

Venäjän turvallisuuspalvelu FSB. (n.d.-b). *Академия Федеральной службы безопасности Российской Федерации*. *[Venäjän federaation turvallisuuspalvelun akatemia].* Haettu 27.1.2023 osoitteesta http://academy.fsb.ru/i_hist_8.html

Venäjän turvallisuuspalvelu FSB. (26.4.2001). *ФСБ хакеров на работу не приглашает. [FSB ei etsi työntekijöikseen hakkereita].* Haettu 25.1.2023 osoitteesta http://www.fsb.ru/fsb/smi/interview/single.htm%21id%3D10342758%40fsbSmi.html

Viron ulkomaantiedustelupalvelu. (2018). *International Security and Estonia 2018*. Välisluureamet. https://www.valisluureamet.ee/doc/raport/2018-en.pdf

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, (ss. 97–102). https://doi.org/10.1016/j.cose.2013.04.004

Yhdysvaltain asevoimat. (2018). *Cyberspace Operations*. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf

Yhdysvaltain liittovaltion hallinto. (2017). *Cyber Warfare in the 21st Century: Threats, Challenges, and Opportunities*. U. S. Government Publishing Office. https://www.govinfo.gov/content/pkg/CHRG-115hhrg24680/pdf/CHRG-115hhrg24680.pdf

Yhdysvaltain liittovaltion hallinto. (2018). *Grand Jury Indicts 12 Russian Intelligence Officers for Hacking Offenses Related to the 2016 Election*. U.S. Department of the Justice. https://www.justice.gov/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election

Yhdysvaltain liittovaltion hallinto. (2019). *Future Warfare: Army Is Preparing for Cyber and Electronic Warfare Threats, but Needs to Fully Assess the Staffing, Equipping, and Training of New Organizations*. U. S. Government Accountability Office. https://www.gao.gov/products/gao-19-570

Yhdysvaltain liittovaltion hallinto. (2022). *Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide*. U.S. Department of the Justice. https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical