Markus Takamaa

KYBEROPERAATIOT POLIITTISEN JA SOTILAALLISEN VAIKUTTAMISEN KEINOINA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Takamaa, Markus
Kyberoperaatiot poliittisen ja sotilaallisen vaikuttamisen keinoina
Jyväskylä: Jyväskylän yliopisto, 2024, 59 s.
Kyberturvallisuus, Pro gradu -tutkielma
Ohjaajat: Kari, Martti & Lehto, Martti

Tietoverkoissa toteutettavat kyberoperaatiot ovat uusimpia keinoja valtioille kohdistaa voimaansa toisia valtioita kohtaan. Näiden käyttömahdollisuudet ovat tulleet ensimmäisen kerran laajemman yleisön tietouteen Stuxnet-tapauksen myötä 2010-luvun vaihteen paikkeilla. Koska kyberoperaatiot ovat olleet laajassa tiedossa vasta hieman yli vuosikymmenen ajan, on niiden käytössä monia kysymyksiä, joita ei vielä ole toistaiseksi tiedossa. Erityisesti kokonaiskattavaa poikkitieteellistä ymmärrystä ei ole toistaiseksi ollut saatavissa.

Tämä tutkielma tavoittelee kokonaisvaltaisen ymmärryksen muodostamista kyberoperaatioista. Tutkimus pyrkii luomaan ymmärryksen analysoimalla ja kokoamalla yhteen poikkitieteellisistä hajanaisista yksityiskohdista muodostuvaa tietoa ilmiöstä. Tutkimuksen tarkoituksena on tarjota akateemiselle tutkimukselle parempaa ymmärrystä toistaiseksi melko tuntemattomasta ilmiöstä. Lisäksi pyritään selventämään nykytietämyksen laajuutta mahdollisia jatkotutkimuksia varten.

Tutkimus toteutettiin soveltamalla Anselm Strauss:in ja Juliet Corbin:in luomaa versiota Grounded Theory -tutkimusmetodologiasta. Metodologiaa sovellettiin pääasiassa akateemisissa julkaisuissa löydettävään tiedon murusiin, joissa käsitellään kyberoperaatioiden käyttöä eri näkökulmista. Erityisesti tutkimuksessa tarkasteltiin valtioiden kyberoperaatioiden käyttöä vuoden 2010 jälkeisellä ajanjaksolla, joiden tarkoituksena on ollut toisen valtion toimintaan vaikuttaminen. Yhteensä tieteellisiä julkaisuja tutkittiin tutkimuksen aikana 37 kappaletta, ja julkaisuja tukemaan käytettiin myös muutamaa valtioiden ja organisaatioiden julkaisemaa dokumenttia.

Tuloksissa havainnoitiin kyberoperaatioiden käyttömenetelmiä valtioiden välisessä toiminnassa. Tuloksissa havaitaan kyberoperaatioihin liittyviä aspekteja niin hyökkäyksellisen, puolustuksellisen, sotilaallisen, kuin myös eri toimijoiden näkökulmasta. Lisäksi tuloksissa selitetään osa-alueiden välisiä riippuvuussuhteita. Tulosten havainnoitiin olevan kokonaiskattavia ja onnistuneen tutkimuksen tavoitteissa. Tutkimustulosten katsottiin olevan verifioitavissa ja toistettavissa, sekä tarjoavan kokonaisakattavaa ymmärrystä akateemisen tutkimuksen piiriin ilmiöstä, jonka avulla voidaan myös suorittaa jatkotutkimuksia aiheesta.

Asiasanat: Kyberoperaatio, Valtio, Hyökkäys, Puolustus, Politiikka, Kybersodankäynti, Verkkotoiminta

ABSTRACT

Takamaa, Markus
Cyberoperations as a means for political and militaristic impact
Jyväskylä: University of Jyväskylä, 2024, 59 pp.
Cyber Security, Master's Thesis
Supervisors: Kari, Martti & Lehto, Martti

Cyber operations through information networks are among the newest means for nations to project their power onto other nation-states. The possibilities of their use were first brought to general awareness through the Stuxnet case around the turn of the 2010s. Since the public has been aware of the phenomenon for more than ten years, there are still unknown aspects of cyber operations. This is especially true for the comprehensive interdisciplinary understanding of the subject.

This thesis aims to form a holistic understanding of cyber operations. The study aims to create this understanding by analysing and gathering the current information made of interdisciplinary, fragmented details. The goal is to provide scholars with a complete picture of the current understanding of the use of cyber operations between states. The thesis also aims to clarify the extent of current knowledge of the subject matter for the basis of potential future studies.

The study was conducted using the version of the Grounded theory - methodology by Anselm Strauss and Juliet Corbin. The methodology was used to form a complete picture provided by scientific publications, each providing small amounts of information about the studied phenomenon from different perspectives. The study especially used the publications to study the usage of cyber operations from 2010 and beyond in cases where the goal has been to disrupt the target nations' actions or regular operations. In total, the thesis studied 37 publications from academic journals, as well as a few papers published by governments and organisations, to support the gathered information.

The results show methods of using cyber operations in interstate activities. We observed various aspects relating to cyber operations in offensive, defensive, and militaristic aspects while also providing the viewpoints of different actors. We also present dependencies between these sub-areas and concepts. The results provided a holistic understanding of the studied phenomenon, and therefore, the study was deemed successful in its goals. The results were also verifiable and repeatable while providing scholars with a new understanding on which to base their further studies.

Keywords: Cyberoperation, State, Defence, Politics, Cyberwarfare, Online Activities.

KUVIOT

SISÄLLYS

1 JOHDANTO

Kyberoperaatiot kuuluvat uusimpiin poliittisen vaikuttamisen keinoihin, joita valtiot voivat käyttää keskinäisessä vuorovaikutuksessaan. Uuden keinon on mahdollistanut tietojärjestelmien ja -teknologioiden nopea kehittyminen, joka on johtanut teknologian laajaan käyttöönottoon yhteiskunnissa (Lehto, 2019, s. 8-10). Koska valtiot ovat yhä kytketympiä ja riippuvaisempia tietojärjestelmien toiminnasta, on valtioilla mahdollisuus kohdistaa voimaansa toisia valtioita kohtaan tietoverkkojen kautta.

Kyberoperaatioiden mahdollisuuksiin on havahduttu tutkijoiden keskuudessa 2010-vuosikymmenen vaihteessa, kun esimerkkejä näiden käytöstä levisi ensimmäisen kerran yleiseen tietouteen (Lehto, 2019, s. 27). Ajanjaksosta eteenpäin on valtioiden kyberoperaatioista ilmennyt lukuisia tapauksia, jotka ovat julkisessa tiedossa saatavilla. Esimerkiksi Natanzin ydinrikastamoon kohdistunut tapaus Iranissa nousi erityisesti laajemman yleisön tietouteen (Buzatu, 2022, s. 238; Lehto, 2019, s. 32).

Kaikki yksityiskohdat ja menetelmät kyberoperaatioiden käytöstä eivät ole vielä saatavilla julkisessa tiedossa, johtuen kyberoperaatioiden salaisesta luonteesta. Toistaiseksi ilmiöstä on saatavissa julkisesti hajanaista yksityiskohdista muodostuvia tietoja, minkä pohjalta on havainnoitavissa merkittävää tiedon puutetta kyberoperaatioiden käytöstä. Täten kokonaisvaltaista ymmärrystä kyberoperaatioiden luonteesta ja toimintamalleista on vielä toistaiseksi saavuttamatta akateemisen tutkimuksen piirissä.

Tämä pro gradu- tutkielman tavoitteena on koota hajanaisista lähteistä ja yksityiskohdista muodostuvia tietoja ilmiöstä ja muodostaa tiedon avulla laajempaa ymmärrystä kyberoperaatioiden luonteesta. Tutkielman tarkoituksena on luoda akateemisen tutkimusalan kaipaamaa kokonaisvaltaista ymmärrystä ilmiöstä. Lisäksi tarkoituksena on havainnoida kyberoperaatioiden soveltamismenetelmiä, joiden pohjalta pyritään tuottamaan realistinen kuva kyberoperaatioiden yleisestä käytöstä. Tutkielman tavoitteena on kokonaisvaltaisen ymmärryksen tuottaminen ilmiöstä, jonka toiminnasta on usein aikaisemmin keskusteltu spekulatiivisesti. Tutkimus pyrkii tuottamaan ymmärrystä kybe-

roperaatioista ja tarjota parhaat mahdolliset puitteet tulevien keskustelujen ja tutkimuksen pohjaksi.

Tutkielman toteutus muodostuu seuraavanlaisista kokonaisuuksista ja rakenteista. Tutkielman ensimmäisessä luvussa esitellään tutkimuksen toteutukseen ja taustatekijöihin kuulua aspekteja. Näihin kuuluvat aikaisemmin tuotetun tutkimuksen esittäminen ilmiöstä ja alasta, sekä tutkimuksen aikana käytettävän termistön kuvaaminen. Toisessa luvussa käsitellään taustakirjallisuuden tarjoamia tietoja kyberoperaatioista. Lisäksi esitellään kyberoperaatioihin liittyvistä aspekteja, joilla selvitetään tarkemmin tutkimusaiheen ymmärryksen kokonaistilannetta. Toteutettu tutkimus ja tutkimusmetodin soveltaminen kuvataan sisällön kolmannessa luvussa. Tämän jälkeen kuvataan vielä tutkimuksessa havaittuja havaintoja, sekä näihin liittyviä analyyseja ja pohdintaa. Lisäksi tutkielman lopussa esitellään mahdollisia jatkotutkimuksen aiheita, joita tutkimuksen toteutuksessa havainnoitiin.

1.1 Motivaatio

Ollessaan laajemmassa tiedossa noin 15 vuoden ajan, ovat kyberoperaatiot varsin uusi aihe tieteellisen tutkimuksen alalla. Suomessa kyberoperaatioita on tarkemmin tarkasteltu vasta viime vuosien aikana (Laari, 2019, s. 50). Myös tutkimusmaailmassa ovat valtioiden väliset kyberoperaatiot olleet tutkimuskohteena vasta viime vuosien aikana. Tilanteen takia monitieteellistä ja monitieteistä tutkimusta aiheeseen liittyen ei olla vielä suuressa määrin tuotettu. Toistaiseksi alan tutkimukset ovat pääasiassa tarkastelleet hajanaisesti tarkempien tutkimusalojen erityiskysymyksiä. Lisäksi Danny Steed kommentoi vuoden 2015 kirjoituksessaan, että tutkimusalaan vaikutti yhä merkittävästi spekulatiivinen keskustelu, joka johtui aikaisemmin mainittujen empiiristen tutkimuksien vähyydestä (s. 73-74).

Tutkimusalan uutuudesta, sekä ilmiön tuntemattomuuden takia voidaan havaita olevan tarvetta uuden ymmärryksen tuottamiselle akateemisen tutkimuksen alalle. Tämä tutkimus tavoittelee tämän tavoitteen täyttämistä luomalla uutta poikkitieteellistä tietoa kyberoperaatioista ja tavoittelee laajemman ymmärryksen tuottamista uudesta tutkittavasta ilmiöstä.

1.2 Käytettävän termistön kuvaus

Tässä kappaleessa pyritään tarjoamaan lukijalle ymmärrystä käytettävän erityistermistön sisällöstä ja käyttötavoista tutkimuksen sisällössä, johtuen käytettävän erityistermistön laajuudesta. Tämän tutkimukseen valitun termistön tulkinta perustuu tutkimuksen näkökulman kannalta oleellisimpiin, sekä lukijan kannalta selkeimpiin yleisesti käytettyihin käyttötapoihin. Lisäksi termistö tullaan esittämään järjestyksessä, jonka ajatellaan kokonaisuudessaan tuottavan

parhaimman ymmärryksen termistöjen sisällöstä lukijalle. Erityistermistöä tarkastellessa on suositeltavaa huomioida, että joidenkin käytettävien termien merkitys on yhä epävakiintunutta uudella tutkimusalalla. Ilmiön johdosta käytettävän termistön soveltamistavat voivat poiketa joistain ilmiötä tutkivista muista tutkimuksista. Tämä osaltaan riippuu myös muiden tutkimuksen soveltamista käyttötavoista, jotka pohjautuvat muiden tutkimusnäkökulmien kannalta oleellisimpiin.

Lisäksi tutkimuksen aikana tullaan esittämään suomenkielisten termien lisäksi termien englanninkielisiä vastineita ja lyhenteitä, mikäli kyseiset termit esiintyvät myös englannin kielellä tuotetussa aineistossa. Valintaa perustellaan englannin kielen olemisesta valtakieli, jota aihetta tutkivat tutkijat käyttävät aineistossaan. Alan termit ovat myös enemmän vakiintuneita englannin kielessä suhteessa suomalaiseen termistöön. Usein myös suomen kielessä käytettävä termistö perustuu alan englanninkielisiin termistöön. Toisaalta kaikille englanninkielisille alan termistöille ei vielä ole toistaiseksi vakiintuneita käännöksiä suomeksi. Englanninkieliset vastineet termistölle kuvataan tutkimuksen sisäisessä tekstissä sulkeiden sisällä suomenkilisten termien ohessa.

Seuraavaksi listataan tutkimuksessa käytettäviä termistöjä, ja kuvataan näiden käyttötapoja tutkimuksen sisällä.

Kyber-sanaa käytetään suomenkielisten sanojen määriteosana, jolla tarkennetaan sanojen merkitys kohdistumaan digitaaliseen tiedon käsittelyyn tai tämän kontekstissa tapahtuviin ilmiöihin. Tieteellisessä aineistossa määriteosaa ei käytetä melkein koskaan itsenäisenä sanana. (Laari, 2019, s. 9). Myös tämä tutkimus noudattaa vastaavaa menettelytapaa. Suomen sotilasorganisaation sisäisessä puhekielessä voidaan kuitenkin joskus havainnoida käytettävän kyber-termiä itsenäisenä sanana, jolloin tämän käytöllä viitataan yleensä sotilastoimintaan tietoverkoissa tai tähän rinnastettavissa olevaan vastaavaan toimintaan.

Kybertoimintaympäristö (engl. cyber environment) kuvaa yhdestä tai useammassa digitaalisessa tietojärjestelmästä muodostuvaa toimintaympäristöä. (Lehto, 2019, s. 7).

Kyberkonfliktilla (engl. cyber conflict) viitataan yksittäisiin tarkoituksellisesti toteutettujen tapahtumien ja toiminnan sarjaan valtiollisten toimijoiden välillä. Lisäksi toiminta toteutetaan tietoverkoissa ja on luonteeltaan vihamielistä tai vihamieliseen rinnastettavissa olevaa toimintaa. Yksittäiseen kyberkonfliktiin voi esimerkiksi sisältyä kyberhyökkäyksiä tai vakoilua tietoverkoissa (Applegate, 2015, s. 24). Joskus muissa aiheissa kijoitetussa materiaalissa voidaan havaita kybersodankäynti-termiä käytettävän vastaavalla merkityksellä. Tässä tutkimuksessa Kyberkonfliktilla viitataan kuitenkin ensisijaisesti sotatilanteiden ulkopuolella tapahtuvaan toimintaan, joka täyttää aikaisemmin kuvatun määrityksen.

Kybersodankäynnillä (engl. cyber warfare) viitataan tutkimuksen sisällä sotatoimien toteuttamiseen tietoverkoissa. Termiä käytetään kuvaamaan tapahtuvia toimia valtioiden välillisissä sotatilanteissa tai sotatilanteeseen rinnastettavissa tapahtumissa.

Kyberavaruus (engl. cyber space) kuvaa maailmanlaajuisia kybertoimintaympäristöjä kokonaisuudessaan, johon kuuluvat esimerkiksi internetin käyttäjät, laitteistot, ohjelmistot, ja tietoliikenneverkot.

Kybermaailma. (engl. cyber world) kts. Kyberavaruus.

Kyberoperaatio (engl. cyber operation) on kybertoimintaympäristössä tai sen avulla tehtäviä toiminnan kokonaisuus. Lisäksi se on tarkoituksella toteutettu, ja operaatiolla pyritään vaikuttamaan kohteena olevan tahon toimintaan (Laari, 2019, s. 49; Sanastokeskus, 2018, s. 27; Lemieux, 2015, s. 1).

Haittaohjelma on tiedosto tai ohjelma, joka vaikuttaa ei-toivotulla tavalla tietokoneiden tai tietoverkkojen toimintaan negatiivisesti (Sanastokeskus, 2018, s. 31). Haittaohjelmat voivat esimerkiksi tuhota tietoverkkojen sisällä olevaa tietoa tai vuotaa salassa pidettäviä tietoja tietojärjestelmien sisältä.

Kriittinen infrastruktuuri (engl. critical infrastructure, CI) on yhteiskunnan normaalin toiminnan kannalta elintärkeitä järjestelmiä, organisaatioita, ja toimintoja. Kriittisellä infrastruktuurilla tarkoitetaan perusrakenteita, palveluja ja niihin liittyviä toimintoja, jotka ovat elintärkeitä yhteiskunnan normaalin toiminnan ylläpidossa (Valtioneuvosto, 2018; Sanastokeskus, 2018, s. 14). Kriittiseen infrastruktuuriin sisältyy fyysisiä laitoksia ja rakenteita, kuin myös elektronisia toimintoja ja palveluja (Valtioneuvosto, 2018). Kriittiseksi infrastruktuuriksi voidaan määritellä kuuluvan esimerkiksi sähköntuotanto, sairaanhoito, sekä veden jakelu (Sanastokeskus, 2018, s. 14).

Valtiollisella toimijalla viitataan yksityishenkilöihin, ryhmiin tai organisaatioihin, jotka toimivat suoraan yksittäisen valtion osana tai alaisuudessa. Ne toimivat valtion viranomaisten ohjeistusta noudattaen. Toimijat voivat tehtävissään olla avoimesti valtioon kuuluvia tahoja tai voivat pyrkiä pitämään kytköksensä valtioon salassa. Esimerkkeinä valtiollisesta toimijasta voivat olla valtion alaiset organisaatiot, armeija, ja tiedustelua toteuttava henkilöstö (Applegate, 2015, s. 30-31).

Sotilaallisella kontekstilla viitataan ensisijaisesti armeijan ja sotilaallisten joukkojen suorittamaan toimintaan. Termiä voidaan käyttää myös kuvaamaan sotatoimia yleisesti tai tapahtumien yhteyttä sotatoimiin.

Politiikalla tarkoitetaan usein toimintaa, jolla pyritään vaikuttamaan valtiollisiin, valtioiden välisiin, tai yhteiskunnallisiin asioihin. Lisäksi politiikaksi voi-

daan luokitella toimintaa, jolla hoidetaan aikaisemmin mainittuja asioita (Kielitoimiston sanakirja, 2022)

Kansainvälinen sopimus (engl. international treaty) on valtioiden välistä yhteisymmärrystä, tahtotilaa, oikeuksia, tai velvollisuuksia kuvaava kirjallinen oikeudellisesti velvoittava asiakirja, jonka on ratifioinut, eli hyväksynyt, kaksi tai useampaa valtiota (Takamaa, 2023).

Attribuutio-ongelmalla (engl. attribution) viitataan tilanteisiin, joissa tekijään viittaavia todistusaineistoja on hyvin haastavaa löytää ja kerätä, jotta kyberhyökkäyksen suorittanutta tekijää voidaan todeta vedenpitävästi tai riittävällä varmuudella. (Solis, 2022, s. 543; Delerue, 2020, s. 51; ks. m. Woltag, 2015, s. 319).

Valtioidenvälinen aseellinen selkkaus (engl. militarised interstate dispute, MID), on valtioiden välinen konflikti tai ristiriita, jossa osapuolivaltiot uhkaavat, esittelevät, tai käyttävät armeijoidensa kapasiteettia. Kapasiteetin käyttäminen voi sisältää myös muita toimia kuin suoria sotatoimia konfliktin aikana (Maness ja Valeriano, 2016a, s. 51-52).

Vaikuttamisella tarkoitetaan tutkimuksen sisällä valtioiden suorittamaa toimintaa, joiden avulla pyritään muokkaamaan toisen valtion ajatusmalleja tai toimintaa.

1.3 Kyberturvallisuuden tutkimus

Kyberturvallisuudella tarkoitetaan toimenpiteitä, joiden avulla suojaudutaan haitallisen toiminnan tai tapahtumien vaikutuksilta kybermaailmassa. (Lehto, 2019, s. 76, Rahman, Sairi, Zizi & khalid, 2020, s. 379). Kyberturvallisuus muodostuu esimerkiksi prosesseista, teknologiasta ja kontrollointimenetelmistä, joilla suojataan It-järjestelmiä, tietoverkkoja ja näissä olevaa tietoa (Kari, 2019, s. 21). Lisäksi kyberturvallisuudella voidaan myös viitata haitallisilta tapahtumilta suojattuun olotilaan (Rahman, ym., 2020, s. 379). Suomessa kyberturvallisuuden tutkimusta suoritetaan Jyväskylän Yliopistossa, jossa tämä pro Gradu-tutkielma on toteutettu osana kyberturvallisuuden tutkintoa.

Kyberturvallisuuden tutkimus on osa informaatiojärjestelmätieteen tutkimusalaa. Informaatiojärjestelmätieteellinen tutkimus on kiinnostunut informaatioteknologian hyödyntämisestä yksilöiden ja organisaatioiden jokapäiväisessä käytössä. Aihetta lähestytään alalla monista näkökulmista, kuten esimerkiksi teknologian, käyttäjien, ja tietojärjestelmien kautta. Informaatiojärjestelmätieteen tutkimus koostuu useasta tutkimusalueesta ja -kokonaisuudesta, ja se voi olla luonteeltaan niin sosiaalinen, yhteiskunnallinen kuin myös tekninen aiheeltaan (Kari, 2019, s. 21).

1.4 Aikaisempi tutkimus

Seuraavaksi tarkastellaan aikaisemmin tuotettua valikoitua aineistoa, joka liittyy tutkimuksen aihealueeseen. Kappaleessa avataan lukijalle aikaisemmin tuotettujen tutkimuksien sisältöä, jotka ovat luoneet uutta tietoa kyberoperaatioiden aihealueeseen liittyvistä teemoista. Tarkoituksena on jakaa ymmärrystä tutkimusalan tilanteesta ja aikaisemmin luodusta tiedosta.

Tutkija Danny Steed Exeter:in Yliopistosta totesi toteuttamassaan artikkelissaan *The Stradegic inplications of Cyber Warfare* vuodelta 2015, että tutkijoiden keskuudessa on oltu yksimielisiä kybersodankäynnin merkityksestä ja sen tarjoamista mahdollisuuksista. Hänen mukaansa ala kärsi ajankohtana erityisesti strategisen ja poliittisen ymmärryksen puutteesta, joka on puolestaan johtunut empiirisen todisteiden puutoksesta. Tämän seurauksena Steed sanoo alan kirjallisuuden olleen koostuneen spekulatiivisista kirjoituksista, joka on jakautunut kybersodankäynnin mahdollisuuksia ylilioittelevaan koulukuntaan, sekä siihen skeptisesti ajatteleviin tutkijoihin. (s. 73-77).

Tilannetta Steed pyrkii korjaamaan artikkelinsa sisällössä, jossa hän tarkastelee tarkemmin kolmea kyberkonfliktia, joista kirjallisuus oli ajankohtana kirjoittanut eniten. Nämä olivat Viron pronssisoturikiista 2007, Georgian sota 2008, sekä Iranilaisessa ydinrikastuslaitokseen kohdistunut Stuxnet-virus vuodelta 2010. Päätelmissään Steed sanoo, että poliittinen ymmärrys tapausten seurauksista on jäänyt ajankohtana vielä epäselviksi. Ymmärryksen puuttumisen seurauksena myös lainsäädännölliseen tulkinta on tapauksia kohtaan yhä hajanaista. Steed kuitenkin kommentoi, että kyberoperaatioilla vaikuttaisi olevan eniten potentiaalia, kun ne yhdistetään osaksi sotilaallista voimankäyttöä. Kirjoitusajankohtana operaatioita on kuitenkin käytetty enimmäkseen rauhanaikaisen toiminnan aikana. Steedin mielestä kyberiskujen tutkiminen tulee vaatimaan vielä enemmän empiiristen todisteiden kokoamista, jotta tarkempi ymmärrys näiden käytöstä selviää paremmin tutkijoille tulevaisuudessa (2015, s. 73-93).

Tohtori Martti J. Kari tutki vuonna 2019 julkaistussa väitöksessään Venäjän kokemaa kyberuhkakuvaa. Väitöksessään Kari tutki aiheitta tarkastelemalla 140:tä Venäjän valtion virallisesta asiakirjaa ja loi kokonaiskuvan asiakirjojen tarjoamasta tiedosta. Asiakirjojen analysoimisessa Kari sovelsi Grounded Theory -tutkimusmetodia kokonaiskuvan luomiseksi. Tarkastelun tuloksena Kari tulee johtopäätökseen, että Venäjän kyberuhkakuvaan vaikuttaa tämän kertoma historiallinen narratiivi. Narratiivissa Neuvostoliitto koettiin olevan jatkuvasti Euroopassa valtiota ympäröivien vihollisten hyökkäysuhan alla. Suojellakseen itseään on Venäjä valmistelemassa omien verkojensa eristämistä internetistä. Lisäksi valtio on pyrkimässä korvaamaan verkoissaan käytettävää länsimaista teknologiaa kotimaisella tuotannolla, ja valtio on lisännyt verkkonsa valvontaa (Kari, 2019).

Kansainvälisen sopimusten (engl. International Law) asiantuntijat ovat tuottaneet paljon aineistoa, jolla asiantuntijat ovat pyrkineet selvittämään kybe-

roperaatioiden merkitystä sopimusten näkökulmasta. Kattavin tuotetuista aineistoista on ollut Tallinnan manuaalina tunnettu selvitys, joka tarkastelee aihetta erityisesti valtiollisesta näkökulmasta. Selvityksen tarkoituksena oli selvittää sotilaallista voimankäyttöä (engl. use of force) koskevien kansainvälisten oikeussääntöjen, sekä aseellisia selkkauksia (engl. armed conflict) käsittelevien sopimuksien merkitystä kyberoperaatioiden käyttöön nähden. Selvityksessään noin 20:stä asiantuntijasta muodostunut ryhmä päätyi johtopäätökseen, jonka mukaan kansainvälisiä sopimuksia voidaan soveltaa valtioiden suorittamiin kyberoperaatioihin. Lisäksi sopimusten periaatteita tulee noudattaa kyberoperaatioiden käytössä. Selvitys sisältää joukon ehdotettuja sääntöjä, joilla kuvataan kansainvälisen sopimuksien soveltamista kybersodankäynnin toteuttamisessa. Vuonna 2017 Tallinnan manuaalista julkaistiin päivitetty 2.0 versio, joka sisältää kattavammin kansainvälisen sopimusten tulkintaa aiheeseen liittyen (Schimtt, 2017, s. 1-3, 11-50). Tallinnan manuaali on myös muodostunut kattavimmaksi asiantuntijoiden ohjeistukseksi toistaiseksi, mikä perehtyy kansainvälisten sopimuksien soveltamiseen kybermaailmaa kohtaan.

Usein myös pohdittu aihe asiantuntijoiden keskuudessa on ollut, voivatko kyberhyökkäykset johtaa sotatoimien aloitukseen valtioiden välillä. Tohtorit Ryan C. Maness ja Brandon Valeriano tutkivat aihetta artikkelissaan, joka julkaistiin osana Conflict in Cyber Space -kirjaa vuonna 2016 (Friis K & Ringmose J (toim.)). Artikkelissaan tohtorit tarkastelivat 111:sta kyberkonfliktia vuosien 2001 ja 2011 välillä. Tarkastelullaan tutkijat selvittivät, onko valtioiden kybertoimintaa seurannut militarisoitu kiista valtioiden välillä (engl. militarised interstate dispute, MID) kuukauden sisällä tapahtumien aloituksesta (s. 45-65).

Tutkimuksen tuloksena tutkijat totesivat, että vain yhdessä heidän tutkimissaan tapauksesta on seurannut militarisoitu kiista valtioiden välillä. Tapaus koskee vuonna 2008 käytyä sotaa Venäjän ja Georgian välillä, jonka kohdalla Venäjän sanotaan toteuttaneen palvelunestohyökkäyksen ennen sotilaallisen kiistan alkua. Tapauksen lisäksi tutkijat havaitsivat kolme muuta tapausta, joissa kyberoperaatioiden toteuttamista on edeltänyt sotilaallinen kiista valtioiden välillä. Nämä tapaukset eivät kuitenkaan johtaneet kiistojen eskaloitumiseen seuraavan kuukauden aikana. Johtopäätöksissään tutkijat sanovat tutkimuksen tulosten tuottavan jonkin verran viitteitä, että kyberturvallisuuden tutkijoiden keskusteluissa on liioiteltu huomattavasti kybertoiminnan mahdollisuutta johtaa perinteiseen sodankäyntiin alkamiseen (2016, s. 45-65).

2 KYBEROPERAATIOT

2.1 Kansainvälisen kybermaailman konteksti ja kyberoperaatiot

Kyberoperaatiolla (engl. cyber operation) tarkoitetaan kybertoimintaympäristössä tai sen avulla tehtäviä toiminnan kokonaisuuksia, joilla pyritään vaikuttamaan operaation kohteena olevan tahon toimintaan (Laari, 2019, s.49; Sanastokeskus, 2018, s. 27; Lemieux, 2015, s.1). Kyberoperaatioihin voivat kuulua esimerkiksi tietoverkkohyökkäykset, näiltä suojautumiseen liittyvä toiminta, sekä muut mahdolliset menetelmät tietoverkkojen hyväksikäytölle. Yleisemmin termillä kuvataan valtioiden välillä tapahtuvaa toimintaa tietoverkoissa sotilaallisesta näkökulmasta (Lemieux, 2015, s. 1). Kyberoperaatioiden määrityksen ulkopuolelle jäävät puolestaan fyysiset hyökkäykset tietoverkkojärjestelmiä kohtaan, mitkä voivat aiheuttaa vastaavanlaisia vaikutuksia tietojärjestelmien toimintaan kuin kyberoperaatiot. Esimerkiksi tietokoneen fyysinen hajottaminen voi tuhota tietokoneen kovalevyllä olevan tiedon samalla lailla kuin jotkin haittaohjelmista (Delerue, 2020, s. 35).

Kyberoperaatioiden muotoja jaotellaan usein kahteen alaluokkaan: hyökkäyksellisiin ja puolustuksellisiin kyberoperaatioihin. Hyökkäyksellisillä kyberoperaatioilla, eli kyberhyökkäyksillä, tarkoitetaan yleisellä tasolla toimia, joilla pyritään vaikuttamaan voimankäytöllä kohteen kybertoimintaympäristöön epäsuotuisasti (Josefsson, Anderson, Norlander & Marcusson 2019, s. 7; Chapple & Seidl, 2015, s. 14-16). Epäsuotuisaa vaikuttamista voidaan tehdä esimerkiksi heikentämällä, tuhoamalla tai manipuloimalla kohteena olevan tahon tietojärjestelmiä. Lisäksi hyökkäyksissä voidaan pyrkiä vaikuttamaan tietojärjestelmissä olevan tiedon saatavuuteen tai sisältöön (Delerue, 2020, s. 35-36; Chapple & Seidl, 2015, s. 14-16). Puolustuksellisiksi kyberoperaatioiksi kutsutaan puolestaan toimia, joilla pyritään suojelemaan ja turvaamaan tietojärjestelmiä. Toimilla voidaan esimerkiksi ehkäistä ja estää auktorisoimatonta ja vihamielistä toimintaa, ylläpitää järjestelmien toimivuutta, sekä toteuttaa vastatoimia hyökkäyksiä kohtaan (Josefsson ym., 2019, s. 7; Chapple & Seidl, 2015, s. 14-16; Lemieux, 2015, s. 2). Tämän tutkimuksen aikana kyberoperaatioita jaotel-

laan ensisijaisesti tämän kahtia jaottelun avulla. Toisaalta on suositeltavaa huomioida, että muissa tutkimuksissa voidaan käyttää vaihtoehtoisia tapoja ja jaotteluita kyberoperaatioiden määrittämisessä.

Hyökkäyksellisten kyberoperaatioiden edistyneempää muotoa kutsutaan APT:ksi (Advanced Persistent Threat). APT:t ovat huomattavasti enemmän edistyneempiä, monimutkaisempia, ja pidempikestoisempia kuin tavallisemmat kyberhyökkäykset. Ne voivat esimerkiksi olla muodoltaan monivaiheisia ja sisältää lukuisia erilaisia haittaohjelmien tyyppejä. APT:teiksi kutsutut kyberhyökkäykset voivat myös kestää hyvin pitkän ajanjakson ajan, kuten esimerkiksi useiden kuukausien ja vuosien ajan. Tällöin operaatioissa voidaan pyrkiä pikkuhiljaa tunkeutumaan operaation kohteena olevaan tietojärjestelmään huomaamatta, kunnes kohde mahdollisesti huomaa tapahtuvan hyökkäyksen tietojärjestelmissä. (Hejase, Fayyad-kazan & Moukadem, 2020, s. 1; Laari, 2019, s. 38).

Hyökkäyksellisten kyberoperaatioiden tunneituimpiin tapauksiin kuuluu vuonna 2010 julkiseen tietoon tullut kyberhyökkäys, joka kohdistui Natanzin ydinrikastamoon Iranissa. Tapauksen aikana ydinrikastamon ohjausjärjestelmissä levisi Stuxnet:iksi jälkeenpäin nimetty haittaohjelma. Haittaohjelma sai rikastettavien ydinsentrifugien värähtelytaajuuden vaihtumaan näiden normaalista toimintatasoista poikkeaviksi. Muutos aiheutti sentrifugien muuttumisen käyttökelvottomiksi ydinrikastamon käyttötarkoituksissa (Broeders, Busser, Cristiano & Tropina, 2022, s. 100; Buzatu, 2022, s. 238; Josefsson ym., 2019, s. 11-12; Lehto, 2019, s. 32). Vaikka operaation toteuttanutta valtioita ei ole voitu vedenpitävästi varmistaa, on iskujen mahdollisiksi suorittajaksi epäilty Yhdysvaltojen ja Israelin valtioita aihetodisteiden perusteella (Borederes ym., 2022, s. 100-101; Buzatu, 2022, s. 238; Josefsson ym., 2019, s. 11-12). Tapausta pidetään erityisen merkittävänä, koska tapaus on ensimmäisiä julkiseen tietoon tulleita kyberoperaatiota, jotka ovat olleet hyvin tarkasti kohdennettuja, sekä tekniseltä toiminnaltaan poikkeuksellisen monimutkaisia. Tämän johdosta ydinrikastamoon kohdistunutta kyberoperaatiota luokitellaan myös yhdeksi esimerkiksi APT:eistä (Järvinen, 2018; S. 41-41; Buzatu, 2022, s. 238; Josefsson ym., 2019, s. 11-12).

2.2 Kyberoperaatioiden hyökkäysmenetelmiä

Kyberoperaatioissa käytettävät aseet vaihtelevat huomattavasti enemmän toimintatavoiltaan kuin perinteisen sodankäynnin aseistukset (Rowe, 2015, s. 61). Vaihtelevuuden mahdollistaa tietokonejärjestelmiin luontaisesti kuuluva monimutkaisuus, joka luo monia potentiaalisia tapoja vaikuttaa koneiden ja verkkojen toimintaan (Rowe, 2015, s. 61; Gaycken, 2019, s. 48; Goldsmith, 2013 s. 130). Vaikuttamisessa käytetään hyödyksi esimerkiksi monimutkaisten järjestelmien sisältämiä heikkouksia, joiden olemassaolon mahdollistaa tietojärjestelmien ohjelmistokoodin suuri määrä (Gaycken, 2019, s. 48). Professori Jack Goldsmith Harwardin Yliopiston lakitieteiden

koulutuslaitoksesta tiivistää tämän it-teknologiaan kohdistuvan heikkouden pääpiirteittäin jo vuonna 2013 julkaistussa kirjoituksessaan:

> Operaatiojärjestelmän ohjelmisto, joka hallinnoi tietokoneen suorittamia tehtäviä sekä tietokoneen suhdetta tämän käyttäjää kohtaan, sisältää tyypillisesti kymmeniä miljoonia, joskus yli 100 miljoonaa riviä toimintaohjeita, eli koodia. On käytännössä mahdotonta tunnistaa ja analysoida kaikkia erilaisia tapoja, joilla nämä koodirivistöt voivat toimia keskenään, tai muuten epäonnistua toimimaan odotella tavalla. Kun operaatiojärjestelmän ohjelmisto yhdistyy ja toimii yhdessä tietokoneprosessoreiden, lukuisten ohjelmistosovellusten, selainten, sekä loputtomien ja loputtoman monimutkaisten laitteisto- ja ohjelmisto-osien kanssa, jotka muodostavat tietokoneen ja telekommunikaatioverkostojen luoman internetin, nousee potentiaali ennalta näkemättömille virheille, sekä toiminnan epäonnistumiselle läpitunkemattoman suureksi (Goldsmith, 2013, s. 130).

On todennäköistä, että tietojärjestelmiin jää yhä tietoturvallisuusaukkoja, vaikka järjestelmien kehittämiseen sijoitettaan suuria summia. (Gaycken, 2019, s. 48-49; Laari 2019, s. 29). Tietojärjestelmien suojaamista voidaankin katsoa usein olevan luonteeltaan riskinhallintaa, mihin sijoittamisella vähennetään riskien ilmenemisen todennäköisyyttä (Laari 2019, s. 29). Tällöin on kuitenkin mahdollista, että tietojärjestelmien havaitsemattomia haavoittuvuuksia voidaan yhä hyväksikäyttää mahdollisissa tulevissa hyökkäyksissä, kuten kyberoperaatioissa (Laari 2019, s. 29; Gaycken, 2019, s. 48-49). Näitä valmistajille, kehittäjille sekä yleisesti muille tuntemattomista haavoittuvuuksista käytetään nimitystä nollapäivähaavoittuvuus (engl. zero-day vulnerability) (Laari 2019, s. 29, Järvinen, 2018, s. 42).

Yhtenä kyberhyökkäyksissä käytettäviä menetelmiä voidaan pitää palvelunestohyökkäystä (engl. Denial of Service, DoS). Palvelunestohyökkäykseksi kutsutaan hyökkäystä, joka kohdistaa verkoissa olevaa palvelua kohtaan hyvin suuren määrän verkkoliikennettä. Tällöin palvelu ei enää kykene ylikuormittuessaan palvelemaan normaaliin tapaan tämän käyttäjiä (Järvinen, 2018, s. 338; Sari, 2019, s. 130; Kettani & Wainwright, 2019, s.177). Tilanteessa palvelut voivat esimerkiksi hidastua, pysähtyä kokonaan tai kaatua palvelunestohyökkäyksen seurauksena (Leitzel & Hillebrand, 2022, s. 19). Palvelunestohyökkäykset pyrkivätkin estämään palveluiden käyttöä rajaamalla palvelun saatavuutta käyttäjille (Sari, 2019, s. 130; Laari 2019, s. 34 & 37).

Kun palvelunestohyökkäys toteutetaan usean hyökkäyslähteen avulla, kutsutaan hyökkäystä hajautetuksi palvelunestohyökkäykseksi (engl. distributed denial of service, DDoS) (Kettani & Wainwright, 2019 s.177; Järvinen 2018, s. 338; Leitzel & Hillebrand 2022, s. 19). Hajautettu palvelunestohyökkäys voidaan toteuttaa esimerkiksi kaappaamalla lukuisia tietokoneita tai muita verkkoon kytkettäviä laitteita haitallisella koodilla. Tällöin laitteiden muodostamaa bottiverkkoa voidaan käyttää hyökkäyksen toteuttamiseen (Leitzel & Hillebrand 2022, s. 19; Laari 2019, s. 34 & 37; Järvinen 2018, s. 338). Hajautettua palvelunestohyökkäystä on käytetty esimerkiksi Georgian sodan alkaessa vuonna 2008. Tapauksen kyberoperaatio kohdistettiin valtiossa toimivaa teleoperaattoria sekä valtion omia verkkosivuja kohtaan. DDoS-hyökkäyksen seurauksena kohteiden

tarjoamat palvelut eivät olleet käytettävissä normaaliin tapaan (Maness & Valeriano, 2016a, s. 52).

Palvelunestohyökkäysten ohella on myös monia muita keinoja toteuttaa kyberhyökkäyksiä, ja esimerkiksi tietojärjestelmän käyttäjiä voidaan käyttää hyödyksi hyökkäyksissä. Käyttäjä voidaan manipuloinnilla saada toimimaan hyökkääjän hyötymällä tavalla. Käyttäjien manipuloinnilla voidaan esimerkiksi päästä järjestelmien sisälle tai kerätä tietoja järjestelmistä. (Laari, 2019, s. 35; Hodges & Creese, 2015, s. 38; Leitzel & Hillebrand 2022, s. 21). Käytännössä nämä voidaan toteuttaa esimerkiksi houkuttelemalla käyttäjä lataamaan sähköpostin liitteenä löytyvä tiedosto tietokoneeseen, minkä mukana haittaohjelma saadaan tartutettua tietokoneeseen. Myös yhtenä vaihtoehtona on houkutella käyttäjä kytkemään haittaohjelman sisältävän Usb-tikun kohdejärjestelmän koneeseen, jolloin haittaohjelma saadaan levitettyä tietojärjestelmään (Hodges & Creese, 2015, s. 38). Lisäksi käyttäjää voidaan houkutella itse jakamaan vapaaehtoisesti hyökkääjän himoitsemaa tietoa erilaisien manipulointitekniikkojen avulla. (Leitzel & Hillebrand 2022, s. 21; Laari, 2019, s. 35).

Käyttäjien manipuloinnilla on todennäköisesti onnistuttu saastuttamaan muun muassa Iranin ydinrikastamislaitoksen sentrifugien ohjausjärjestelmä vuonna 2010. Tapauksessa ydinrikastamislaitoksen työntekijä saatiin houkuteltua kytkemään Usb-tikku järjestelmään kuuluvaan laitteiseen, minkä kautta kyberoperaatiossa käytetty Stuxnet -haittaohjelman arvellaan päässeen tietojärjestelmien sisälle (Josefsson ym., 2019, s. 7; Järvinen, 2018, S. 41).

Samalla Natanzin ydinrikastuslaitokseen kohdistunut kyberoperaatio osoittaa, miten haittaohjelmia voidaan käyttää kyberhyökkäyksen käytännön toteutukseen. Haittaohjelmien käyttöä pidetään yhtenä yleisenä kyberhyökkäysten toteutusmenetelmänä. Haittaohjelmia jaotellaan tarkemmin näiden teknisen toiminnan perusteella moniin alaluokkiin, kuten viruksiin, matoihin ja troijalaisiin (Kettani & Wainwright, 2019 s.176; Laari, 2019 s. 36-37; Leitzel & Hillebrand 2022, s. 20). Esimerkiksi Stuxnet -haittaohjelma kuuluu näistä tietokonematoihin (Josefsson ym., 2019, s. 11-12; Laari, 2019 s. 36-37), jotka leviävät itsenäisesti tartutetusta tietokoneesta toiseen. Tällöin tietokonemato ei tarvitse kohdejärjestelmän käyttäjien toimenpiteitä, kun ohjelma on ensin saatu tartutettua yhteen tietojärjestelmän koneeseen (Laari, 2019 s. 36-37; Leitzel & Hillebrand 2022, s. 20).

2.3 Poliittinen vaikuttaminen

Politiikka -termin määritykset vaihtelevat alan tutkijoiden välillä, ja tutkijoiden keskuudessa ei ole yhtä hyväksyttyä tulkintaa termistä. Termin laajimmassa tulkinnassa politiikalla viitataan toimintaan, jonka avulla luodaan, ylläpidetään ja muokataan yleisiä sääntöjä, joiden alaisuudessa väestöt elävät. Muiden tulkintojen mukaan politiikaksi voidaan kutsua muun muassa vallan käyttöä, yhteisten päätösten tekemistä ja rajattujen resurssien jakamista. (Heywood 2019, s. 2).

Kotimaisten kielten keskus määrittää julkaisemassaan sanakirjassa politiikan olevan toimintaa, jolla pyritään vaikuttamaan valtiollisiin, valtioiden välisiin ja yhteiskunnallisiin asioihin (Kielitoimiston sanakirja, 2022). Tämän tutkimuksen sisällössä politiikan määrityksessä käytetään Kotimaisten kielten keskuksen määritelmää, ja sillä tullaan viittaamaan ensisijaisesti valtioiden johdon tekemään toimintaan. Lisäksi termillä voidaan viitata tutkimuksessa vallankäyttöön, joka pyrkii vaikuttamaan valtiollisiin, valtioiden välisiin tai yhteiskunnallisiin asioihin.

Valtioiden välistä kansainvälistä politiikkaa kuvataan usein termillä maailmanpolitiikka (Harle 2010, s. 35-37). Termillä kuvataan poliittista toimintaa maailmanlaajuisessa kontekstissa yleisellä tasolla. Termin yleinen käyttö johtuu valtioiden rinnalle tulleista toimijoista, jotka osaltaan vaikuttavat kansainväliseen politiikkaan (Harle 2010, s. 35-37; Hocking & Smith, 1990, s. 70-81). Näihin toimijoihin voivat kuulua esimerkiksi kansainväliset organisaatiot, kuten Yhdistyneet Kansakunnat ja Euroopan Unioni. Lisäksi toimijoihin voidaan lukea myös nykyaikaiset yksittäiset vaikuttajahenkilöt, jotka saavat laajaa kansainvälistä tukea poliittiseen toimintaansa (Harle 2010, s. 35-37).

Maailmanpolitiikassa on aikaisemmin havaittu kasvavaa poliittista halua ja toimia, joilla pyritään lisäämään valtioidenvälistä yhteistyötä kyberhyökkäyksiltä suojautumisessa (Lemieux, 2015, s. 9). Kyberavaruutta pidetään jatkuvana valtioiden kilpailun kohteena, johon sovelletaan yleisiä valtiollisen toiminnan ja sodankäynnin periaatteita (Havu & Häyhtiö, 2023, s. 101). Länsimaiden yhteistoiminnan kasvattamista ovat aikaisemmin rajoittaneet kuitenkin valtioiden vaihtelevat poliittiset ja juridiset rakenteet. Suurin osa näiden valtioiden kyberturvallisuuden toimintamalleista on pohjautunut valtioiden sisäisten lainsäädäntöjen muodostamiin periaatteisiin, jotka ovat olleet aluksi yhteensopimattomia muiden valtioiden vastaavien periaatteiden kanssa. Tilanne on aikaisemmin rajoittanut vastatoimien yhteistä toimeenpanoa sekä kansainvälisten tutkimusten toteuttamista kyberhyökkäysten tapahtuessa (Lemieux, 2015, s. 9).

Viime aikoina useat valtiot ovat alkaneet antaa kannanottojaan kyberoperaatioista ja niihin liittyvistä kansainvälisen oikeuden kysymyksistä. Näihin valtioihin ovat kuuluneet esimerkiksi Saksa, Suomi ja Italia (The Federal Goverment of Germany, 2021; Ulkoasiainministeriö, 2020; Ministry of Foreign Affairs in Italy, 2021). Myös EU on ottanut kantaa asiaan julkaisemalla oman kyberturvallisuuden strategiansa (European Commission, 2013). Kannanotot ovat helpottaneet mahdollisuutta valtioiden välisen yhteisymmärryksen muodostumiselle ja sen ympärille rakentuvalle kyberturvallisuuden yhteistyölle (Takamaa, 2023). Esimerkiksi Suomi on todennut kannanotossaan kansainvälisen oikeuden olevan keskeinen ohjauskeino valtioiden vastuullisille käyttäytymiselle kyberavaruudessa (Ulkoministeriö, 2020).

2.4 Sotilaallinen vaikuttaminen ja kybersodankäynti sen osana

Tunnetuimpiin sotateoreetikoihin kuuluva Carl von Clausewitz määritteli sodankäynnin olevan politiikan jatkamista muilla keinoilla. Hänen mukaansa sotia voidaan aina pitää poliittisina tekoina, joiden tarkoituksena on taivuttaa vastustaja väkivallan avulla noudattamaan valtion tahtoa. Tämän takia Clausewitzin mukaan sotia ei ole suositeltavaa tarkastella tyhjiössä itsenäisinä ilmiöinä, vaan sotia on aina tarkasteltava poliittisten keinojen välineenä. Vain tämä näkökulma mahdollistaa kokonaisymmärrykseen perustuvan sotien tarkastelun (1998, s. 15, 27, 28). Kirjoituksen perusteella Clausewitzin voidaan nähdä ajatelleen, että sodankäynti on yksi toimintamenetelmä toteuttaa poliittista tahtoa.

Kybersodankäyntiä pidetään viimeisimpänä sotilaallisena teknologisena vallankumouksena, mikä luo uuden ulottuvuuden sodankäyntiin (Gartzke, 2013, s. 41; Kari, 2019, s. 15). Kybermaailman sotilaallinen hyödyntäminen nousee erityisesti esille Ukrainassa tapahtuneissa sotilaallisissa toimissa (Havu & Häyhtiö, 2023, s. 101), ja kybersodankäynnin katsotaan tuovan merkittävän lisän sotilaalliseen toimintaan (Lehto, 2019, s. 52). Lisäksi useiden valtioiden sanotaan kehittävän kyberkapasiteettiansa (Mačák, 2021, s. 411).

Kybersodankäynti-käsitteelle ei toisaalta toistaiseksi ole yleisesti hyväksyttyä määritelmää, joka selittäisi termin merkitystä tarkasti. Sen sijaan käsitettä on käytetty hyvin laajasti kuvaamaan erilaisia toimia ja tapahtumia kybermaailmassa (Lehto, 2019, s. 52). Usein julkisessa keskustelussa on havaittu kybersodankäynniksi kutsuttavan kaikkea haitallista toimintaa tietoverkoissa, kuten vakoilua, yksittäisiä kyberhyökkäyksiä sekä rikollisuuteen liittyviä toimia (Applegate, 2015, s. 26). Tällöin on kuitenkin hyvä huomioida, että kybersodankäynti-termiä käytetään vastaavassa kontekstissa enemmän sanan metaforisessa merkityksessään kuin tieteellisten määritysten kautta. Kybersodankäynnin varsinainen toteuttaminen edellyttää aina valtioiden välistä yleistä sotatilaa, jotta toimia voidaan kutsua sanan todellisessa merkityksessä kybersodankäynniksi. Sotatilanteen aikana suoritettavien kyberoperaatioiden voidaan katsoa olevan osa yleistä valtioiden välistä sodankäyntiä (Lehto, 2019, s. 18).

Esimerkiksi kansainvälisen oikeuden tutkija James Green on määritellyt kybersodankäynnin olevan valtiollisen toimijan poliittisten menettelytapojen jatketta kyberavaruudessa (2011, s. 2). Scott Applegate Yhdysvaltain armeijasta kuvaa puolestaan kybersodankäynnin olevan aseellisten hyökkäysten suorittamista kyberavaruuden kautta tai sen sisällä, mitkä toimivat valtion politiikan jatkeena ja joiden pyrkimyksenä on langettaa valtion poliittista tahtoa toista valtiota kohtaan (2015, s. 26).

Edellä mainituilla kuvauksilla voidaan havainnoida esimerkkejä asiantuntijoiden vaihtelevista kybersodankäynnin määrityksistä. Kirjoitusten perusteella Reading vaikuttaisi tarkastelevan kybersodankäyntiä enemmän politiikan kautta, kun taas Applegate painottaa määritelmässään enemmän sotatoimien merkitystä. Molempien tutkijoiden kybersodankäynnin määrityksissä voidaan havaita, että molemmat heijastelevat Carl von Clausewitzin sodankäynnin määritel-

mää. Tässä tutkimuksessa termin määritykseen käytetään Applegaten määritelmää, ja termillä viitataan vain valtioiden väliseen toimintaan sotatilanteiden aikana.

Kybersodankäynnin käytössä on jotain rajoituksia. Esimerkiksi maa-alueiden valtaamista pidetään pelkästään kyberhyökkäysten avulla mahdottomana. Tämän toteuttamiseksi tarvitaan muiden sodankäynnin tekniikoiden käyttöä kyberhyökkäysten ohella, kuten esimerkiksi maajoukkoja. Ilmiön takia kyberteknologiaa pidetään sodankäynnissä usein yhtenä vaikuttamisen keinoina muiden sotatoimien ohella (Gratzke, 2013 s. 43).

2.5 Kansainvälinen oikeus

Valtioidenväliset sopimukset ovat toistaiseksi jättäneet erityisesti käsittelemättä kybermaailmassa tapahtuvia konflikteja (Applegate, 2015, s. 34; Mačák, 2021, s. 413). Tilanteen johdosta aikaisempiin kyberkonflikteihin ja -hyökkäysiin on sovellettu yleistä kansainvälistä normistoa sekä maiden sisäistä oikeussäädäntöä (Havu & Häyhtiö, 2023, s. 101; Applegate, 2015, s. 34; Mačák, 2021, s. 413-414). Kansainvälisen oikeuden pohjalta on lisäksi aikaisemmin luotu yleisellä tasolla toimivia ohjeennuoria tapausten tulkintaan (Palojärvi 2009, s. 68-69). Lisäksi valtiot ovat pyrkineet viime vuosina luomaan kybermaailmassa hyväksyttyjen toimintamuotojen vapaaehtoisesti noudatettavia normeja, jotka ovat olleet luonteeltaan epäsitovia valtioille (Mačák, 2021, s. 413).

Tarkempien valtioidenvälisien sopimuksien puuttuessa on ensimmäisten kyberkonfliktien ilmaannuttua pyritty selvittämään, miten voimassa olevat kansainväliset oikeuden säännöt soveltuvat kybermaailmassa tapahtuvan toiminnan tulkintaan. Koska oikeussäännöt luotiin alun perin ensisijaisesti muiden reaalimaailman tilanteiden pohjalta, ei ensimmäisten kyberkonfliktien ilmaantuessa ollut tietoa, miten kansainväliset valtiosopimukset soveltuvat uuden ilmiön tarkastelemiseen (Delerue, 2020, s. 1; Takamaa 2023).

Kybermaailman kansainvälisen oikeuden kysymyksiä on pyritty selvittämään 2000-luvun alusta alkaen (Takamaa, 2023). Vuonna 2009 asian selvittämiseksi koottiin Naton toimesta yhteen kansainvälisen oikeuden asiantuntijoita pohtimaan vastauksia kyberoperaatioista esille nousseisiin kysymyksiin. Tallinnan tapaamisessa käytyjen keskustelujen perusteella asiantuntijat päätyivät johtopäätökseen, että valtioiden välisiä sopimuksia tulee noudattaa kyberkonflikteissa ja -sodissa. Käytyjen keskustelujen pohjalta luotiin Tallinnan manuaalina tunnettu käsikirja. Käsikirja sisältää alan asiantuntijoiden neuvoa-antavan arvion, kuinka kansainvälisiä valtiosopimuksia ja muita oikeussääntöjä on sovellettava kybermaailman kontekstiin. Lisäksi annettuja arvioita päivitettiin vuonna 2017. Tällöin käsikirjan uudempaan versioon lisättiin ohjeellinen arvio valtiosopimuksien soveltuvuudesta rauhanaikaisiin kyberoperaatioihin (Schmitt, 2017, s. 1-3, 11-50).

Tallinnan manuaalissa sanotaan esimerkiksi valtion suvereenisuuden (eng. sovereignty) eli itsemääräämisoikeuden koskevan kaikkia kyberavaruuden osia,

jotka sijaitsevat valtion alueilla ja täten sen lainsäädännön alaisuudessa. Itsemääräämisoikeuden johdosta valtioilla ei ole oikeutta hallinnoida toisen valtion sisäisen toimivallan alaisuuteen kuuluvaa kybertoimintaympäristöä (Schmitt, 2017, s. 11-50). Lisäksi asianmukaisen huolellisuuden periaatetta (engl. due diligence) noudattaen on valtioiden pidettävä huolta, että valtion maa-alueella ei toteuteta toisen valtion vastaisia toimia kyberavaruuden kautta. Ollessaan tietoinen tämänkaltaisesta toiminnasta, on valtiolla velvollisuus tehdä kaikki kohtuullisissa rajoissa pidettävät toimet, jotta toiminta saataisiin lopetettua (Schmitt, 2017, s. 11-50; Shaw, 2021, s. 736; Delerue, 2020, s. 353-360).

Monet valtiot ovat myöhemmin todenneet kansainvälisen oikeuden soveltuvan keskeisiltä sopimuksiltaan kyberoperaatioiden käytön tulkintaan sodankäynnissä. Tällöin keskeisiksi kansainvälisen oikeuden kysymyksiksi nousevat esimerkiksi siviili- ja sotilaskohteiden erottaminen toisistaan, sekä sotilaallisten kyberoperaatioiden vaikutusten varotoimivelvoitteet. Varotoimivelvoitteella viitataan esimerkiksi velvoitteeseen rajoittaa sotatoimet vain sotilaskohteisiin. Valtioiden välillä on kuitenkin ollut epäselvyyksiä tulkita sotatilanteiden alempien kontekstien kyberoperaatioiden käyttöä, kuten aseellisen voimankäytön tapauksia (engl. use of force) (Takamaa 2023). Seuraavaksi käydään läpi joitain esimerkkejä aiheesta käydyistä keskustelunaiheista kansainvälisessä oikeudessa.

Isoimpina keskeisimpinä kysymyksinä sotatilanteita alemmissa konteksteissa on toistaiseksi ollut tutkijoiden keskuudessa, minkälainen kybermaailman toiminta voidaan luokitella olevan rinnastettavissa aikaisemmin mainittuun aseelliseen voimankäyttöön ja mitkä toimet voivat aiheuttaa aseellisia selkkauksia (engl. armed conflict) (Solis, 2022, s. 538-539; Mačák, 2021, s. 418). Kansainvälisissä sopimuksissa on toistaiseksi tarkasti määrittelemättä, mitkä toimet voivat aiheuttaa aseellisia selkkauksia. Tutkijoille on ollut tilanteessa haastavaa yksityiskohtaisesti määritellä, minkälaisia kyberoperaatioita voidaan luokitella rauhanaikaiseksi toiminnaksi ja sodankäyntiä alemman voimankäytön toteuttamiseksi (Palojärvi 2009, s. 68-69; Solis, 2022, s. 538-540). Määrittelyn haastavuuteen on myös vaikuttanut valtioiden tekemä harmaan alueen toiminta, joka tapahtuu rauhan ja sodan välisessä välimaastossa (Mačák, 2021, s. 417).

Toista valtiota kohtaan kohdistettu valtion voimankäyttö voidaan luokitella sotilaalliseksi hyökkäykseksi (engl. armed attack), mikäli hyökänneen valtion toiminta on ollut luonteeltaan erityisen vakavaa (Hendriksen 2016, s. 154, Solis, 2022, s. 541). Tällöin YK:n peruskirjan 51 artiklan mukaan hyökkäyksen kohteena olevalla valtiolla oikeus aseelliseen itsepuolustukseen (United Nations, 1945). YK:n pääasiallisena oikeuselimenä toimiva Kansainvälinen tuomioistuin luokittelee kuitenkin vain kaikkein törkeimpien tapauksen olevan sotilaallisia hyökkäyksiä. Voimankäytön määritystä matalampien tapauksien käsittelyssä on tuomioistuimessa sovellettu muita kansainvälisen oikeuden oikeussääntöjä (International Court of Justice, 1986, kpl. 195; Hendriksen 2016, s. 154).

Kyseisten tapausten tulkintaan vaikuttaa hyvin paljon, kuinka paljon tapausten voimankäyttö rikkoo voimankäytön kieltoa. Mitä suurempi rike on, sitä vahvemmin voimankäytön kohteeksi joutuneen valtion sallitaan kansainvälisen oikeuden puitteissa reagoida tapahtuvaan toimintaan (Hendriksen 2016, s.

154). Tilanteessa toteutettavia vastatoimia on toteutettava suhteessa tapauksen vakavuuteen, jotta kohteeksi joutunut valtio tulee toteuttamaan vain tarvittavan, joka on välttämätöntä vihamielisen toiminnan lopettamiseksi (International Law Commission, 2001, art. 51; Shaw, 2021, s. 692; Banks, 2021, s. 1064).

Jotta aseellisia selkkauksia koskevia kansainvälisiä oikeussääntöjä (engl. law of armed conflict) voidaan soveltaa suoritettujen kyberiskujen tulkitsemiseen, on iskun totuttama taho voitava selvittää ja kytkeä konkreettisen todistusaineiston avulla tapahtumien tekijäksi. Lisäksi todistusaineistojen on kyettävä osoittamaan kyseisen toimijan toimineen yksittäisen valtion alaisuudessa kyberiskuja suorittaessaan (Palojärvi, 2009, s. 72; Delerue, 2020, s. 53).

Kybermaailman luonne on kuitenkin luonut attribuutio-ongelmaksi kutsutun ilmiön (engl. attribution). Attribuutio-ongelmalla viitataan tilanteisiin, joissa hyökkäyksen tekijään viittaavia todistusaineistoja on hyvin haastavaa löytää ja kerätä, jotta kyberiskun tekijä voidaan vedenpitävästi tai riittävällä varmuudella todeta. (Solis, 2022, s. 543; Delerue, 2020, s. 51; ks. m. Woltag, 2015, s. 319). Tilanne on toisin kuin esimerkiksi perinteisessä sodankäynnissä, jossa hyökkäävien joukkojen käyttämä varustus, uniformut ja puhekieli antavat viitteitä hyökkäävän tahon identiteetistä (Takamaa, 2023).

Kyberaseet ja muut tekniset menetelmät eivät usein sisällä tekijän varmuudella tunnistamista tukevia tietoa. Tämä attribuutio-ongelman luoma tilanne aiheutuu esimerkiksi internetin tarjoamasta anonymiteetista ja identiteetin väärentämismahdollisuudesta (Tsagourias & Farrell, 2020, s. 944; Rove, 2015. s. 61-62; Solis 2022, s. 543). Kokenut hyökkääjä kykenee esimerkiksi piilottamaan kyberhyökkäyksensä jäljet reitittämällä hyökkäyksen tietoliikennedatan kulkemaan useiden tietokoneiden tai palvelimien kautta kohteeseensa. Tällöin kyberhyökkäys voidaan saada vaikuttamaan tulevan melkein mistä tahansa päin maailmaa tahansa, ja alkuperäisen lähettäjän IP-osoite voidaan salata ja piilottaa (Goldsmith, 2013, s. 131-132; Rove, 2015. s. 61-63; Borghard & Lonergan, 2019, s. 135). Lisäksi käytettäviä kyberaseita voidaan aktivoida kohteen järjestelmissä jopa vuosien viiveellä haittaohjelmien asentamisesta, mikä myös lisää haastavuutta todisteiden keräämiselle ja tapahtumien selvittämiselle. Johtuen aikaisemmin mainituista toiminnan mahdollisuuksista tietoverkoissa, jää kyberhyökkäysten lähettäjä usein epävarmaksi (Goldsmith, 2013, s. 131-132; Rove, 2015. s. 61-63).

Tämän takia suurinta osaa kyberaseista saatavissa olevissa todistusaineistoista pidetään aihetodisteina, jotka eivät suoraan osoita mahdollisen hyökkääjän ja tapahtuman välistä yhteyttä (Rove 2015, s. 62). Vaikka havaitut aihetodisteet osoittavat mahdollisen todennäköisen tekijän suuntaan, eivät ne suoraan todista juridisesti yksittäistä tekijää hyökkäyksen toteuttajaksi. Tämän takia hyvin monien kyberiskujen tekijänä esitetty taho esittää todellisuudessa kaikkein todennäköisintä tekijää iskujen suorittajaksi (Shaw, 2021, s. 736). Tämä näkyy esimerkiksi julkisuudessa esille tuoduista tapauksista, jossa esitetyt todisteet hyökkääjästä ovat usein olleet vaihtelevia, epäloogisia, ja ne on joskus jätetty kokonaan kertomatta (Tsagourias & Farrell, 2020, s. 944). Näissä tilanteissa

täydellisiä varmuutta iskujen todellisen suorittajan henkilöllisyydestä ei voida kuitenkaan taata (Shaw, 2021, s. 736).

Valtio on kyettävä toteamaan hyökkäyksellisen kyberoperaation toteuttajaksi, jotta valtion voidaan todeta olevan vastuussa toiminnastaan (Schmitt 2017, s. 84-87). Tämä vaatii todistusaineistoa suorasta linkistä, joka todistaa valtion olevan tapahtumien toimeenpanija. Vaikka hyökkäys havainnoitaisiin mahdollisesti lähteneen valtion alueelta, ei tämä vielä todista suoraan, että kyseisen valtio olisi ollut iskujen toteuttamisen takana. Valtion ulkopuolisten yksilöiden, ryhmien tai organisaatioiden toiminnan poissulkemiseksi on vielä löydettävä suoria linkkejä hyökkäyksen toteuttaneen tahon ja valtion väliltä, jotka osoittavat tahon toimineen valtion alaisuudessa (Rowe, 2015, s. 67).

3 TUTKIMUS JA SEN TOTEUTUS

3.1 Tutkimusongelma

Kyberoperaatioista saatavissa olevaa tietoa tarkastellessa voidaan havaita, että ilmiön ymmärryksessä on puutoskohtia. Akateemisella alan ymmärrys ilmiöstä on enimmäkseen koostunut yksittäisistä kyberoperaatioiden käyttötapauksista sekä keskusteluista kansainvälisen oikeuden kysymyksistä. Lisäksi alalla on toteutettu yksittäistä tieteellisiä tutkimuksista, jotka ovat tarkastelleet ilmiötä ja sitä ympäröiviä asioita hyvin tarkasti rajattujen pienempien teemojen rajoissa. Kokonaistilannetta tarkastellessa voidaan havaita saatavilla olevan tiedon oleminen hajanaista.

Tilanteessa voidaan havainnoida kyberoperaatioiden ymmärryksessä olevan merkittäviä tiedonpuutteita akateemisella alalla, mikä osaltaan selittänee myös aihetta käytävien keskustelujen spekulatiivista luonnetta. Lisäksi ymmärryksen puuteen voidaan osittain katsoa selittävän myös ilmiöstä käytettävän terminologian vakiintumattomuutta. Kokonaistilannetta tarkastellessa on lisätutkimuksen tuottamiselle selvästi havaittavissa olevan tarvetta, jotta kyberoperaatioista voidaan tuottaa kattavampaa ymmärrystä.

Tilanteen korjaamiseksi toteutetaan seuraava tutkimus, joka pyrkii tarjoamaan ratkaisuja kyberoperaatioiden tutkimuksessa havaittuihin tiedonpuutteisiin. Tutkimus ratkaisee ongelmaa luomalla saatavissa olevan tietojen ja todisteiden pohjalta uutta kokonaisvaltaista tietoa akateemisen tutkimuksen piiriin. Tarkoituksena tiedon luomisella on luoda ymmärrystä, jonka avulla täytetään olemassa olevia tiedonpuutoksia. Lisäksi kokonaisvaltaisen ymmärryksen luomisella pyritään luomaan pohjaa tulevaisuuden jatkotutkimuksia varten. Seuraavaksi käydään läpi tutkimukseen valittuja metodeja, joiden toivotaan tarjoavan parhaimmat työkalut- ja menetelmät tutkimuksen tavoitteiden toteuttamiseksi.

3.2 Tutkimuskysymys

Tämä tutkimus tavoittelee vastausten löytämistä seuraavaan kysymykseen:

Millaisia ovat valtioidenväliset kyberoperaatiot?

Tutkimuskysymyksen tueksi tullaan tutkimuksen suorittamisessa tavoittelemaan myös seuraaviin kysymyksiin vastaamista:

-Miten kyberoperaatioita on toteutettu?
-Miten kyberoperaatiot ovat vaikuttaneet operaation kohteena olleeseen valtioon?
-Miten valtiot kokevat kyberoperaatioiden käytön?

3.3 Tutkimusmetodi

Tutkimuksen toteuttamisessa tullaan käyttämään Anselm Strauss:in ja Juliet Corbin:in luomaa versiota Grounded Theory -tutkimusmetodista vuodelta 1990. Grounded theory on luonteeltaan aineistopohjainen laadullisen tutkimuksen muoto, (Metsämuronen, 2008, s. 16, 24), jonka tarkoituksena on luoda uutta teoriaa tutkitun datan pohjalta. Tarkoituksen takia tutkimusmetodia toteutetaan ilman ennalta luotuja teoreettisia ideoita tai hypoteeseja (Birks & Mills, 2015, s. 2) Tutkimusmetodi katsotaan soveltuvan erinomaisesti tutkimuksen suorittamiseen, jossa laadullisen materiaalin tutkinnalla tavoitellaan uuden tiedon luomista. Metodin soveltamisella pyritään tarjoamaan ymmärrystä tutkittavan kohteen käyttäytymisestä, sekä rakentamaan mallin tai järjestelmän, joka muodostuu toisiinsa loogisesti liittyvien konseptien joukoista (Kari, 2019, s. 30).

Tutkimusmetodi valittiin tutkimuksen suorittamiseen johtuen kyberoperaatioista saatavissa olevan kokonaistiedon tilanteesta. Kyberoperaatioista ei toistaiseksi ole saatavilla laajaa aikaisempaa teoria-aineistoa tai rakenteellista ymmärrystä, mikä selittäisi kokonaiskattavasti valtioiden käyttäytymismalleja kyberoperaatioita käyttäessään. Koska kyberoperaatioiden ymmärrys akateemisessa keskustelussa on toistaiseksi muodostunut hajanaisista tiedoista, katsotaan metodin olevan erinomaisesti soveltuva nykytutkimuksen tilanteeseen, tutkimuskysymykseen vastaamiseen, sekä kokonaisymmärryksen tuottamiseen kyberoperaatioiden luonteesta.

Seuraavaksi kuvataan Grounded theory -tutkimusmetodin toteuttamisessa yleisesti käytettävien vaiheiden etenemistä, niin kuin tämä on kuvattu tutkimusmetodin luojien Strauss:in ja Corbin:in mukaan.

Grounded Theory -metodologiassa tutkimusprosessin aloittavaa ensimmäistä vaihetta kutsutaan avoimeksi koodaamiseksi. Vaiheen aikana tutkija kokoaa tutkimuksessa käytettävää tutkimusaineistoa, sekä analysoi aineistojen sisällössä löytyvää tietoa. Avoimen koodaamisen aikana aineiston analysoiminen toteutetaan havainnoimalla aineiston sisällä löytyviä konsepteja, jotka ku-

vaavat tekstissä kuvatun ilmiön luonnetta kokonaisvaltaisesti (Strauss & Corbin, 1990, s. 6-8 12; Kari, 2019, s, 34). Esimerkiksi aineistosta löytyvä lause: "Joka aamun aikana jaksotan toimintaani lepäämällä parranajon ja kylpemisen välissä" voidaan kuvata käyttämällä lausetta kuvaavana konseptina sanaa "Ajoittaminen" (Strauss:in & Corbin, 1990, s. 7).

Aineistossa havaittuja konsepteja verrataan lisäksi keskenään, jotta näiden eroavaisuuksia ja yhdistäviä tekijöitä voidaan arvioida toisiinsa nähden (Strauss & Corbin, 1990, s. 12). Mikäli aineistossa havaitaan sisällöltään identtisiä konsepteja, jotka tutkija on nimennyt käyttämällä erilaisia termejä, ne yhdistetään yhdeksi konseptiksi aineiston analysoinnin aikana (Kari, 2019, s. 34).

Kun konsepteja on alettu aineiston sisällä havaitsemaan, tullaan samankaltaisia konsepteja ryhmittelemään erilaisiin kategorioihin ja alakategorioihin, jotka kuvaavat havaittuja konsepteja yhdistäviä tekijöitä. (Strauss & Corbin, 1990, s. 12). Ryhmittelyn aikana voidaan esimerkiksi konseptit "lintu", "lentokone" ja "leija" määritellä yhteiseen kategoriaan "lentäminen" (Kari, 2019, s. 34). Havainnoidut kategoriat tulevat tutkimusprosessin edetessä luomaan perustan seuraaville analysoinnin vaiheille, joita toteutetaan tutkimusmetodin soveltamisen aikana.

Grounded theory:n toista vaihetta kutsutaan aksiaaliseksi koodaukseksi (axial coding). Vaiheen aikana havainnoituja konsepteja tuodaan yhteen visuaalisen mallin avulla. Aksiaalisena koodauksen tarkoituksena on visuaalista mallia käyttämällä havaita kategorioiden välisiä suhteita, merkata ylös kategorioiden välillä havaittuja yhteyksiä, sekä testata yhteyksiä tutkimuksen aineiston avulla. Samalla myös kategorioiden sisältöä jatkokehitetään, jotta mahdollisia merkkejä kyetään havainnoimaan uusista kategorioista aineiston sisällä (Strauss & Corbin, 1990, s. 13). Aksiaalisten koodauksen aikana uuden datan keräämistä jatketaan kategorioiden välisiä linkkien havainnoinnin ja testauksen aikana (Kari, 2019, s. 36-37).

Grounded Theory:n kolmatta ja viimeistä vaihetta kutsutaan valikoivaksi koodaukseksi (selective coding), jossa havainnoidut kategoriat ryhmitellään ja liitetään näitä parhaiten yhdistävien ydinkategorioiden ympärille. Ydinkategoriat esittävät täten tutkimuksen keskeisintä ydinteemaa, jonka avulla voidaan parhaiten selittää tutkittavan ilmiön luonnetta. Lisäksi kategorioita tullaan täydentämään aineistosta löydettävien tietojen avulla, mikäli nämä tarvitsevat vielä lisää selittäviä tietoja (Strauss & Corbin, 1990, s. 13). Valikoivassa koodauksessa uuden tiedon hakeminen on kohdennettua, ja sen tarkoituksena on vahvistaa havaittujen kategorioiden välisiä suhteita, sekä havainnoitujen kategorioiden sisältöä (Kari, 2019, S. 36-37; Strauss & Corbin, 1990, s. 13).

Valikoivaa koodausta pidetään samalla Grounded Theory -tutkimusmetodin ydinprosessina. Se muuntaa kerätyn ja analysoidun datan uudeksi malliksi, jonka sisällöt ovat loogisesti yhteydessä toisiinsa. Valikoivassa koodauksessa on tärkeää tunnistaa toistuvia teemoja ja malleja, jotka ilmenevät tutkimuksen aineiston analysoinnin aikana (Kari, 2019, s. 36-37). Teemojen ja mallien havainnointi mahdollistaa ilmiön käyttäytymismallien kokonaisvaltaisen ymmärryksen luomisen.

Lisäksi merkittävässä osassa tutkimusmetodin toteutuksessa on muistiinpanojen kirjoittaminen koko tutkimusprosessin ajan. Muistiinpanojen kirjoittamisen tarkoituksena tutkimusprosessissa on ylläpitää tutkijan näkemyksiä analysoidun tiedon kokonaiskuvasta. Muistiinpanot sisältävät tietoa havaituista kategorioista, konseptien ominaisuuksista, sekä nousseista hypoteeseista. Lisäksi muistiinpanoihin kuvataan tietoa uusista kysymyksistä, joita ilmenee tutkimusprosessin aineiston analysoinnin aikana. (Strauss & Corbin, 1990, s. 10). Toisin sanoen muistiinpanoja käytetään tutkimusprosessissa ylläpitämään tietoja ja havaintoja analysoidun tiedon yksityiskohdista ja yleisestä kokonaiskuvasta.

Tutkimusmetodia käyttäessään on tutkijan suositeltavaa kyseenalaistaa jatkuvasti tutkimaansa aihealuetta, käsitellyn datan sisältöä, kuin myös käytettyjä metodeja. Tutkijan muodostamaa tietoa ei ole suositeltavaa pitää faktoina tutkimusprosessin aikana, minkä lisäksi tutkijan on hyvä etäännyttää itseään datan käsittelystä aika ajoin. Näiden tekniikoiden soveltamisella tutkija voi verrata objektiivisemmin datasta nousevan kokonaiskuvan suhdetta tämän todelliseen sisältöön nähden (Kari, 2019, s. 41). Näiden metodien soveltamisella tutkimustyöhön pyritään ehkäisemään tutkijan omien maailman näkemyksen ja ajattelun virheiden vaikutusta tutkimuksen tuloksiin tutkimustyön toteutuksen aikana.

3.4 Näkökulma ja rajaus

Tutkimuksen toteutuksessa tarkastellaan kyberoperaatioita, jotka ovat toteutettu ensisijaisesti valtioiden välisessä toiminnassa. Tutkimuskohteen painopisteen takia tutkimus ei tule ottamaan huomioon valtion ulkopuolisten toimijoiden, kuten henkilöiden, organisaatioiden, rikollisten ryhmien tai terroristien toteuttamaa toimintaa, mikäli nämä eivät ole toimineet valtioiden suorassa alaisuudessa toteuttaessaan toimia muita valtioita kohtaan. Rajauksen avulla pyritään rajaamaan tutkimus kohdistumaan ensisijaisesti valtioiden välillä tapahtuvaa toimintaa kohtaan ja rajata tutkimuksesta esimerkiksi ensisijaisesti rikolliseen toimintaan luokiteltavia tapahtumia. Rajauksen reunaehtona on, että aikaisemmin mainitut toimijat, eivät ole työskennelleet valtion organisaation alaisuudessa, ohjaamana, tai rahoittamana tekoja toteuttaessaan. Mikäli tahon toiminta havaitaan kytkettävän valtion organisaatioon tai tämän väliseen yhteistyöhön tutkittavassa aineistossa, voidaan nämä ottaa huomioon tutkimusanalyysin sisällössä.

Toisena rajauksena tutkimuksen sisällössä ei tulla ensisijaisesti tarkastelemaan valtioiden toteuttamaa tiedustelua kyberavaruudessa. Tutkimuksen pääpainopisteenä tullaan pitämään aineistosisältöä, joka ensisijaisesti käsittelee valtioiden toimintaan konkreettisesti vaikuttaneita kyberoperaatioita. Rajauksella pyritään kohdentamaan tutkimus ensisijaisesti viimeksi mainittuun. Lisäksi rajauksen avulla pyritään ensisijaisesti tarkastelemaan operaatioita, joiden käytön voidaan katsoa olevan poliittiseen ja sotilaalliseen vaikuttamisen keino

tiedon keräämisen sijasta. Rajauksen takia tiedustelutoimintaa käsittelevää aineistoa tullaan vain esittämään tutkimustuloksissa, mikäli näiden tutkiminen koetaan välttämättömäksi tutkimuskysymysteen vastaamiseksi. Lisäksi tiedustelua voidaan tuoda esille, mikäli esille tuomista edellytetään tutkimuksessa havaittujen konseptien kokonaisvaltaiseksi ymmärtämiseksi.

Kolmantena rajauksessa tutkimuksessa ei oteta huomioon kyberoperaatioihin liittyviä tapahtumia, ilmiöitä, julkaisuja, tai muita aspekteja, jotka ovat tapahtuneet sekä tulleet julkiseen tietoon ennen vuoden 2010 alkua. Rajauksen avulla pyritään takaamaan kerätyn tiedon ajankohtaisuus tutkimusaiheelle, joka on toistaiseksi kehittynyt poikkeuksellisen nopealla tahdilla suhteessa muihin akateemisiin tutkimusaloihin. Lisäksi tutkimuksen aineistoa rajataan julkaisuihin, joita on julkaistu vuoteen 2022 asti. Tällä varmistetaan materiaalin saatavuus tutkimustyön aikana, sekä materiaalin koon kohtuullisuus suhteessa tutkimustyöhön käytettävissä oleviin resursseihin.

Lisäksi tutkimuksen sisällössä ei oteta kantaa, onko aineistossa esitetty hyökkäyksellisen kyberoperaation toteuttaja kyseisen operaation todellinen tekijä. Rajaus perustellaan attribuutio-ongelmasta johtuvista epävarmuustekijöistä, joiden takia operaation toteuttajaa ei voida todeta akateemisen tutkimuksen vaatimalla varmuudella. Tilanteen takia kyberoperaatioiden toteuttajaan liittyviä aineistoja tullaan pitämään epävarmoina tietoina aineistossa.

3.5 Tutkimuksen aineisto ja kokoaminen

Tutkimuksen pääasiallisena lähdeaineistona tullaan käyttämään akateemisissa aikakausilehdissä tai konferenssien yhteydessä levitykseen annettuja englanninkielisiä julkaisuja, jotka käsittelevät sisällössään tutkimuskohteen aihealuetta. Aineiston valinnalla pyritään takaamaan tutkimukselle materiaalin mahdollisimman luotettavaa sisältö, jota julkisista lähteistä on toistaiseksi saatavissa ilmiöstä. Akateemisten julkaisujen lisäksi tutkimuksen aineistomateriaalina täydennetään tarvittaessa valtioiden julkaisemilla dokumenteilla, kuin myös tutkijoiden tuottamalla kirjallisuudella. Täydentävien lähteiden käytöllä pyritään kattamaan mahdollisia puutoksia, joita tutkimuksen aikana mahdollisesti havaitaan tieteellisissä artikkeleissa. Lisäksi tiedon ajankohtaisuuden varmistamiseksi pyritään tutkimuksessa painottamaan aineistoja, jotka on julkaistu vuosien 2017-2022 välisenä aikana.

Aineiston kokoaminen aloitetaan käyttämällä Jyväskylän Yliopiston kirjaston tarjoamaa JykDok -aineistonhakujärjestelmää. Aineistohakujärjestelmän tiedonhakua kohdistetaan aineistoon, jonka sisältö vastaa tutkimuksen kohdetta ja näkökulmaa. Lisäksi artikkeleiden hakua tullaan laajentamaan tutkimusprosessin alun jälkeen, jotta koottavaa materiaalia voidaan laajentaa. Tällöin hakua laajennetaan etsimällä artikkeleja suoraan tieteellisten aikakausilehtien ja -konferenssien sivustoilta, sekä muista saatavista olevista lähteistä. Aineiston keruuta ja lisätiedon hakua tullaan jatkamaan koko tutkimusprosessin suorittamisen ajan, kunnes tutkimusprosessi katsotaan olevan suoritettu. Erityisesti

tutkimuksen loppupuolella tullaan uuden lähdeaineiston etsintää kohdistamaan vielä havaittavissa olevien puuttuvien tietojen täydentämiseen. Lopullinen tutkimusmateriaalin määrä tullaan kuvaamaan tutkimusprosessin toteuttamista kuvaavassa kappaleessa, minkä lisäksi tarkempi luettelo käytetyistä aineistosta on löydettävissä tämän tutkimuksen liitteenä.

3.6 Materiaalin lähdekritiikki

Tutkimusmateriaali valittiin tutkimukseen kohteeksi, koska materiaalin sisällön katsottiin edustavan tarkinta saatavissa olevaa tietoa tutkimuksen kohteesta. Asiaa perusteltiin materiaalin kirjoittajien tietämyksellä, kuin myös materiaalin käytännön sisällöllä. Lisäksi valinnassa otettiin huomioon materiaalin maine luotettavana tietolähteenä. Tämän perusteella materiaalin katsottiin olevan myös laadukkainta, mitä julkisesta tiedossa on saatavilla toistaiseksi aiheesta. Toisaalta akateemisissa aikakausilehdissä ja konferensseissa julkaistun materiaalin soveltamiseen tutkimuksessa liittyy omia rajoitteitaan, jotka vaikuttavat tutkimuksen analysoimisen ja suorittamiseen.

Aineiston tarjoaman sisällön voidaan havaita olevan kokonaisuudessaan melko hajanaisia ja erinäisistä näkökulmista kirjoitettua, minkä takia yksittäisien artikkelien sisältö ei usein suoraan vastaa tutkimuksen näkökulmia ja rajauksia. Materiaalissa voidaan myös havaita vaihtelevia termien määrityksiä ja käyttötapoja, kuin myös kyberoperaatioiksi määriteltävän tapauksia. Asian voidaan katsoa lisäävään aineiston analysoinnin vaikeutta, sekä edellyttävän aineiston tutkijan kapasiteettia tunnistaa käytettävien termien näkökulmaeroja suhteessa tutkimuksen ottamaan näkökulmaan.

Lisäksi osa artikkelien sisällöistä voidaan havaita olevan spekulatiivisia luonteeltaan, ja esitettyjä väitteitä ei olla perusteltu todisteiden avulla. Ilmiön voidaan katsoa johtuvan julkisissa lähteiden osittaisesta tiedon puutoksesta, joka kohdistuu tutkimuksen kohteeseen. Spekulatiivisuuden olemassaolo edellyttää tutkijalta sisällön luonteen havainnointia, jotta kyseisen sisällön luonne otetaan tutkimuksen analyysissa huomioon. Tällöin sisältö tullaan jättämään tutkimusanalyysin ulkopuolelle, jotta tutkimustuloksien luotettavuus kyetään takaamaan.

Lisäksi rajoitteena tutkimuksen materiaalin käytöllä voidaan havaita olevan kohdistuvan tieteellisten artikkelien kirjoittajiin. Materiaalin kirjoittajien ovat tyypillisesti olleet tutkijoita, jotka eivät itse ole olleet osallisena kyberoperaatioiden suunnittelemisessa tai toteutuksessa. Tilanne johtuu kyberoperaatioiden liittyvään vaitiolovelvollisuuteen, mikä rajoittaa merkittävästi kyberoperaatioihin osallisena olleen henkilöiden mahdollisuuksia jakaa tietojaan julkisuuteen. Vaitiolovelvollisuuden takia enemmistö tutkijoiden kokoamista tiedoista tieteellisiin artikkeleihin, pohjautuu tyypillisesti kyberoperaatioiden tapausten konkreettiseen ilmenemisen havainnoimiseen, sekä näihin liittyviin todisteiden analysoimiseen julkisista lähteistä. Näihin lähteisiin voivat liittyä

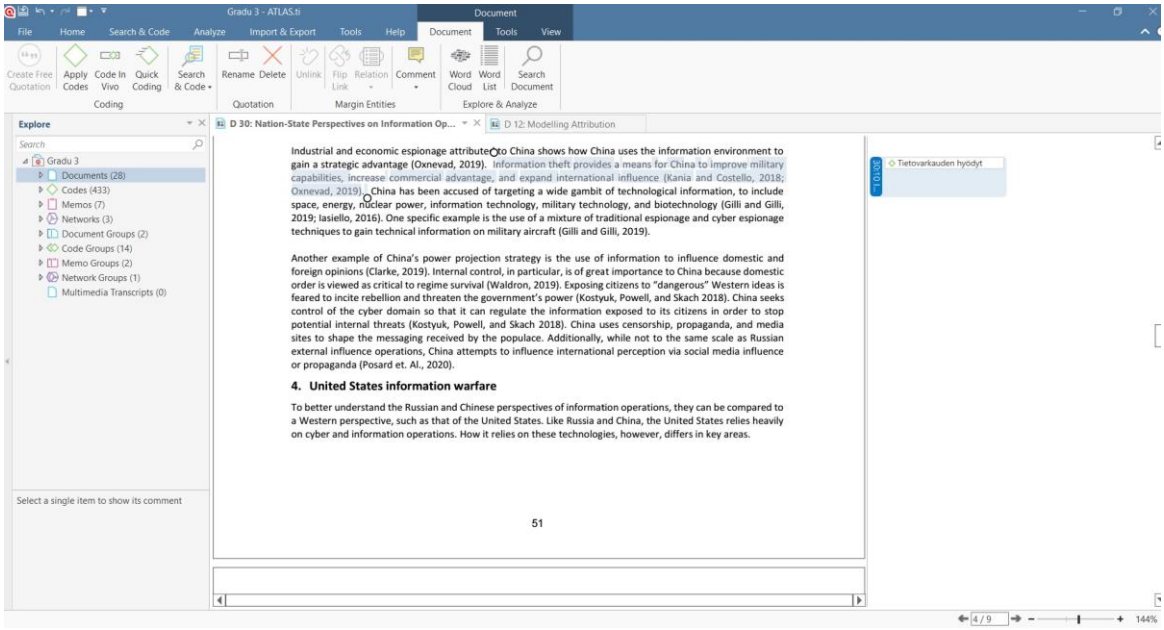
esimerkiksi havaittavissa olevat seuraukset tapahtumista, kuin myös valtioiden viranomaisten toteuttamaa keskustelua aiheeseen liittyen.

Tutkimusmateriaalin rajoituksia otetaan huomioon tutkimustuloksien arvioinnissa. Rajoituksistaan huolimatta materiaalin katsotaan tarjoavan parhaan julkisesta lähteistä saatavissa olevan tiedon ja olevan sovellettavissa tutkimuksen toteutukseen.

Seuraavaksi käsitellään, kuinka aineiston sisältöä analysoidaan käyttämällä Grounded Theory -metodia tutkimuksen suorittamisessa, jotta kattavin mahdollinen ymmärrys voidaan saavuttaa kyberoperaatioiden luonteesta.

3.7 Tutkimusprosessi

Tutkimuksen aineiston analysoinnissa käytettiin Atlas.Ti[9] -ohjelmistoa analysoinnin suorittamiseksi (Kuvio 1). Ohjelmiston valinta perusteltiin ohjelmiston soveltumisesta Grounded Theory -tutkimusmetodin toteuttamiseen sekä aineistojen kokonaisvaltaiseen hallintaan. Lisäksi sovelluksen käytön soveltuvuutta vahvistettiin tutkijoiden suosituksilla, jotka ovat aikaisemmissa tutkimuksissaan soveltaneet ohjelmiston käyttöä samaan tutkimusmetodin soveltamisessa.



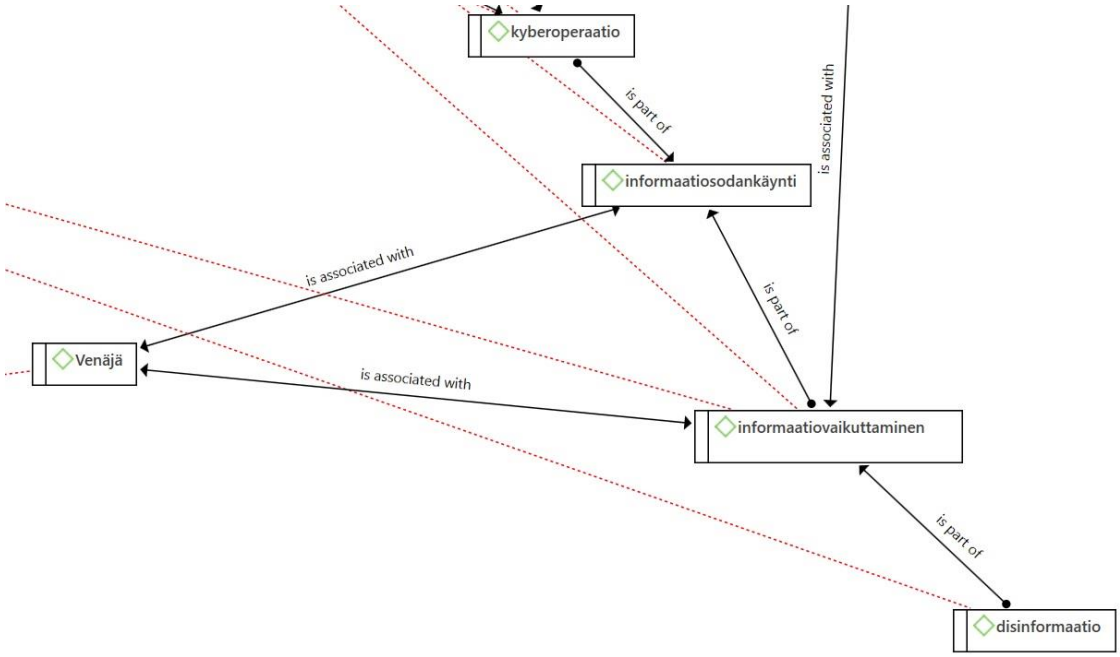
KUVIO 1 Atlas.Ti[9] -ohjelmiston käyttöliittymä havainnoidessa aineiston sisältämiä konsepteja

Tutkimuksen avoin koodaus aloitettiin etsimällä ja kokoamalla yhteen tutkimuksen alussa käytettävää aineistomateriaalia, ja sen sisältö analysointiin lause kerrallaan Atlas.Ti[9] -ohjelmistoa käyttäen. Analysoinnin pohjalta tekstin sisällössä havaittuja tietoja merkittiin sisältöjä kuvaavilla konsepteilla, perustuen

tekstin sisällön tarjoamaan tietoon. Esimerkiksi ensimmäisiin havaittuihin konsepteihin kuuluivat termit ”Puolustuksen kehittäminen”, ”turvallisuuspoliittinen strategia” sekä ”hyökkäysmetodi”. Avoimen koodauksen aikana aineiston sisällöissä otettiin huomioon tutkimuksen rajauksen ja näkökulman sisälle kuuluneita tietoja, ja tämän ulkopuolille jääneitä tietoja ei otettu huomioon konseptien nimeämisen yhteydessä. Rajauksen toteuttamisen varmistamista suoritettiin myös tutkimusprosessin muiden vaiheiden aikana, jotta konseptien sisällöt vastaavat tutkimukselle asetettuja tavoitteita.

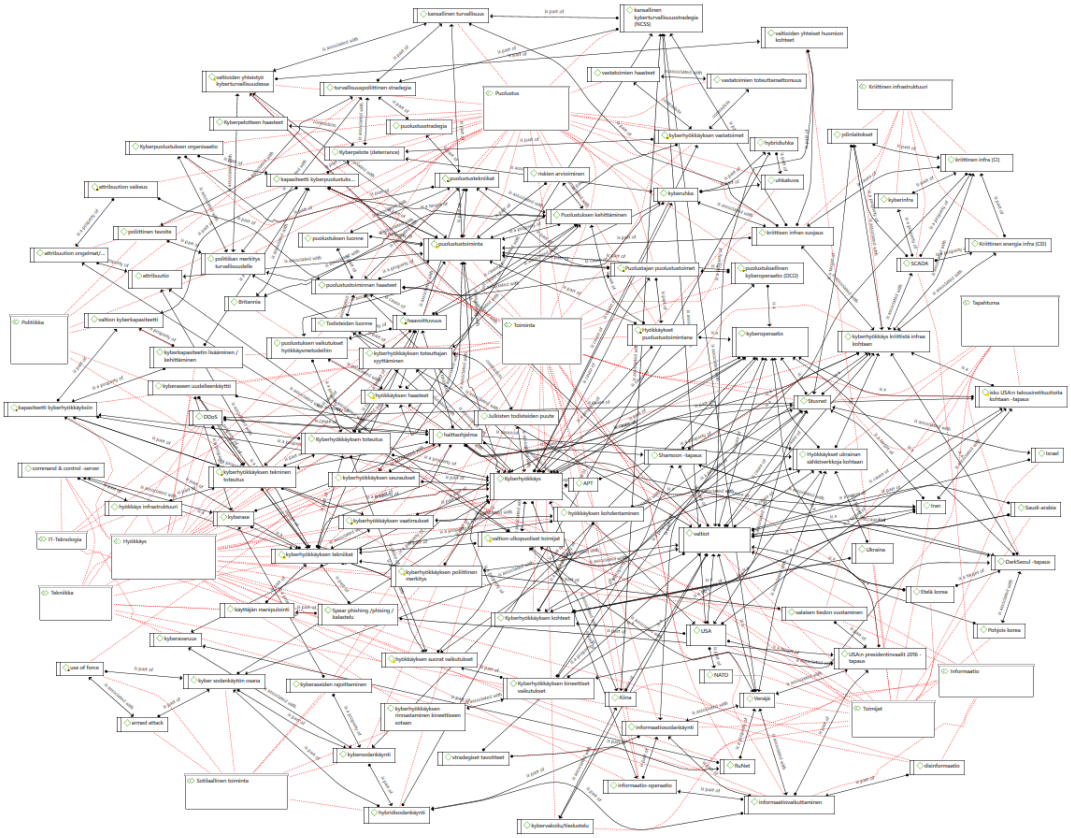
Havainnoitujen konseptien sisältöä vertailtiin tutkimuksessa jatkuvasti keskenään, jotta mahdollisia samankaltaisia konsepteja sekä toisistaan ristiriitaisia tietoja voitaisiin havaita. Kun konseptien sisällössä havainnoitiin yhdistäviä tai samankaltaisia tekijöitä, ne ryhmiteltiin yhteisen kategorian alaisuuteen kuuluviksi. Esimerkiksi havainnoidut konseptit ”Puolustuksen kehittäminen”, ”kyberhyökkäyksen vastatoimet ” ja ”valtioiden yhteistyö kyberpuolustuksessa” ryhmiteltiin tutkimuksessa ”Puolustus” -kategoriaan kuuluvaksi. Mikäli kahden eri konseptien sisällöt havainnoitiin puolestaan olevan luonteeltaan identtisiä tutkimusprosessin aikana, ne yhdistettiin yhdeksi konseptiksi. Periaatetta noudattaen esimerkiksi konseptit ”Puolustuksen kehittäminen” ja ”puolustuksen parantaminen” yhdistettiin yhdeksi konseptiksi tutkimuksen suorittamisen aikana.

Kun havainnoituja konsepteja ja kategorioita alkoi olemaan merkittävä määrä, siirryttiin vähitellen tutkimusprosessin toteutuksessa aksiaalisen koodaukseen. Vaiheen alkaessa Atlas.Ti[9] -ohjelmistossa luotiin konseptien yhteyksiä kuvaava visuaalinen kartta, johon kuvattiin aineiston sisällössä havaittujen konseptien välisiä yhteyssuhteita (Kts. Kuvio 2). Havaittujen yhteyksien paikkansapitävyyttä testattiin, validointiin, ja analysointiin tutkimalla aineiston sisällössä havaittuja yksityiskohtia, tietoja, sekä mahdollisia ristiriitaisuuksia. Lisäksi lisätietoa havaittujen kategorioiden ja konseptien sisällöstä etsittiin uusien artikkelien sisällöstä, jotta näiden sisältöjä kyettäisiin kehittämään ja monipuolistamaan tutkimuksessa.



KUVIO 2 Esimerkki havaittujen konseptien välisistä yhteyksistä aksiaalisen koodauksen aikana. Informaatiosodankäynti on enimmäkseen Venäjälaisissa ajattelussa käytetty konsepti, jonka alaisuuteen voidaan länsimaisen kyberoperaatio-termin havainnoida kuuluvan (Kts. asiaa laajemmin tutkimustuloksissa).

Viimeisenä tutkimuksessa toteutettiin valikoivan koodauksen vaihe, johon siirryttiin havainnoitujen kategorioiden yhteyksien ollessa selkeitä. Yhteyksien avulla tutkimuksessa löydetyt kategoriat ja konseptit aseteltiin havaitun ydinkategorian ympärille, joka selittää parhaiten tutkittavan ilmiön luonnetta. Tämä asettelu toteutettiin visuaalisen mallin avulla, joka luotiin Atlas.Ti[9] -ohjelmistossa (Kuvio 3). Lisäksi kategorioita ja konseptien välisiä riippuvuussuhteita täydennettiin kohdentamalla uuden tiedon hakua tarkemmin näihin sisältöihin, kun sisältöjen koettiin tarvitsevan täydentävää tietoa ydinkategorian kokonaisvaltaiseksi ymmärtämiseksi. Tutkimus katsottiin valmistuneeksi, kun uuden tutkitun aineiston analysoinnissa ei enää havainnoitu merkittäviä tietojen muutoksia, täydennyksiä, tai nousevia uuden materiaalin sisällä. Havaitun ydinkategorian ja havaittujen konseptien riippuvuussuhteiden sisältöä kuvataan tarkemmin tutkimustuloksien esittelyn kohdalla.



KUVIO 3 Atlas.Ti[9] -ohjelmistossa luotu visuaalinen malli, joka kuvaa kategorioiden ja keskeisten konseptien välisiä suhteita valikoivan koodauksen loppuvaiheessa. Ydinkategoriaksi havaittu termi voidaan havaita kaavion keskialueella.

Tutkimuksen toteuttaminen kokonaisuudessaan perustui huolelliseen aineiston analyysiin ja jatkuvaan vertailuun lähdeaineistojen välillä. Tällä tavoiteltiin mahdollisien yhdistävien tekijöiden ja ristiriitaisuuksien havaitsemista tutkitun aineiston sisältämässä tiedossa ja datassa. Lisäksi tutkimuksen lopputuloksissa pyrittiin luomaan mahdollisimman kattava ja kokonaisvaltainen kuva tutkitun aineiston tarjoamasta tiedosta, minkä takia tutkimuksen suorittamisessa käytettäviä tutkimuskysymyksiä tulkittiin laajasti ja joustavasti tutkimuksen aikana.

Havaittujen konseptien ja kategorioiden sisältöä, näiden välisiä yhteyksiä, ja muita tutkimuksen aikana havainnoituja tietoja merkattiin ylös Atlas.Ti[9] -ohjelmiston muistiinpano-ominaisuuksien avulla. Muistiinpanojen avulla tutkimuksessa ylläpidetiin ja säilytettiin konseptien ja kategorioiden sisältöön liittyviä tietoja. Lisäksi muistiinpanoja käytettiin myös seuraamaan koko tutkimusprosessin eri vaiheiden yleistä etenemistä tutkimusprosessin aikana, kuin myös kirjaamaan tutkijan omia ajatuksia tutkimuksen prosessista ja sisällöstä. Tekniikalla pyrittiin havainnoimaan tutkijan omia ajatuksia suhteessa datan todelliseen sisältöön nähden, jotta mahdollisia ristiriitaisuuksia kyettäisiin havainnoimaan näiden välillä. Samalla pyrittiin poistamaan tutkijan oman ajattelutavan ja näkemyksien mahdollisia vaikutuksia tutkimuksen lopputuloksiin. Lisäksi tutkijan ajatuksia pyrittiin etäännyttämään aineiston sisällöstä pitämällä tutkimusprosessin suorittamisessa taukoja, tutkijan edistäessä muiden projek-

tien etenemistä. Samalla tutkimus pyrittiin toteuttamaan mahdollisimman pitkällä ajanjaksolla, jotta tutkimusprosessin toteutukselle kyettäisiin takaamaan mahdollisimman parhaat edellytykset.

Tutkimuksen prosessi katsottiin valmistuneeksi, kun uuden aineiston analysoinnin avulla ei enää kyetty havaitsemaan merkittäviä lisätietoa konseptien ja kategorioiden sisällöstä, tai näiden välisistä suhteista. Yhteensä tieteellisiä artikkeleita analysoitiin tutkimuksen suorituksessa 32 kappaletta, minkä lisäksi käytettiin kahta organisaatioiden julkaisemaa dokumenttia, kahta valtioiden julkista asiakirjaa, sekä yhtä akateemisen tutkijan tuottamaa kirjallisuuslähdettä (Liite 1). Viimeksi mainittuja aineistoja käytettiin erityisesti valikoivan koodauksen aikana täydentämään artikkeleissa tiedoissa havaittuja avoimia kysymyksiä ja tiedon puutoksia. Lisäksi yhdestä mainitusta organisaatioiden julkaisemassa dokumentista käytettiin tutkimuksen suorittamiseen kolme itsenäistä asiantuntijoiden kirjoittamaa artikkelia, jotka ovat liitteessä 1 mainittuna erikseen.

Seuraavaksi kuvataan tutkimuksen aikana hainoituja kategorioita, konsepteja, sekä näiden välisiä yhteyssuhteita tutkimuksen tuloksissa.

4 TUTKIMUSTULOKSET

Tutkimuksen aikana keskeisimmäksi kyberoperaatioita kuvaavaksi yläkategoriaksi muodostui Toiminta. Yläkategorian ilmeneminen havaittiin aksiaalisen koodauksen alkumetrien aikana, ja pian havaitsemisensa jälkeen tämä alkoi muodostumaan ilmiötä parhaiten selittäväksi ydinkategoriaksi. Toiminnan lisäksi tutkimuksen aikana havainnoitiin neljä muuta yläkategoriaa, jotka nousivat keskeisiksi teemoiksi tärkeimmän ydinkategorian yhteydessä. Nämä yläkategoriat ovat Hyökkäys, Puolustus, Politiikka, ja Sotilaallinen toiminta, joista Hyökkäys keräsi eniten koodimerkintöjä neljästä muista yläkategoriasta. Yläkategorioiden lisäksi merkittävinä kategorioina havaittiin tutkittavan ilmiön selittämisessä olevan Tekniikka, Toimija ja Tapahtuma. Yhteensä tutkimusprosessin loppuvaiheessa havaittuja konsepteja havaittiin tekstin sisällöstä olleen hieman yli 500 kappaletta.

Havaittujen yläkategorioiden sisällössä havaittiin jonkin verran päällekkäisyyttä keskenään konsepteja sisäisissä yksityiskohdissa. Näiden ei kuitenkaan havaittu vaikuttavan merkittävällä tavalla kategorioiden määrittelemiseen omiksi itsenäisiksi sisältökokonaisuuksiksi. Täten havaittujen päällekkäisyyksien ei havaittu olevan tarpeeksi merkittäviä, jotta nämä olisivat johtaneet kategorioiden yhdistämiseen tai uudelleen muokkaamiseen.

Seuraavaksi käsitellään kategorioita, konsepteja, sekä ilmiötä selittäviä tekijöitä, joita tutkimustuloksissa havainnoitiin aineiston analyysin pohjalta. Esiteltävässä tiedoissa painotetaan kyberoperaatiota selittäviä tekijöitä toimintana, jotta havaitun yläkategorian sisältöä voidaan selittää kokonaisuudessaan. Lisäksi kyberoperaatioita tarkastellaan muiden havaittujen yläkategorioiden näkökulmassa osana kyberoperaatioiden toimintaa. Johtuen kuitenkin tutkimuksessa havaittujen tietojen laajuudesta, ei kaikkia yksityiskohtia tutkimuksen tuloksista tulla esittämään seuraavien kappaleiden kohdalla, jotta tutkimuksen tulokset pysyisivät selkeinä keskeisimpien havaintojen kohdalla.

4.1 Hyökkäykselliset kyberoperaatiot

4.1.1 Hyökkäyksen toteuttaminen

Valtion toimintaan vaikuttaneiden kyberhyökkäysten kohdalla havaittiin kaksi yleisintä metodia, joita aikaisemmissa tapauksissa on käytetty ensisijaisina hyökkäysmetodeinaan. Havaitut yleisimmät metodit olivat haittaohjelmat ja DDoS-palvelunestohyökkäykset. Nämä kaksi hyökkäysmetodia saivat kohdalleen myös eniten mainintoja hyökkäysmetodeista, ja ne nousivat merkittävään asemaan materiaalissa käydyssä keskustelussa hyökkäyksellisistä operaatioista.

Haittaohjelmia voidaan havaita olleen käytetyn esimerkiksi Shamoon-tapauksessa elokuussa 2012, joka kohdistui Saudi-Arabian valtion omistuksessa olevan Aramco -öljy-yhtiön käyttämiä järjestelmiä kohtaan. Tapauksessa Shamoon -nimistä haittaohjelmamatoa käytettiin tuhoamaan kohteina olleiden tietokoneiden kovalevyjen sisältämä tieto. Kovalevyjen tyhjennyksen seurauksena koneita ei enää kyetty käynnistämään, tähän tarvittavan tiedon ollessa tuhottua tietokoneen muistissa. Tapahtuman katsotaan aiheuttaneen yhtiön tuotannossa häiriöitä noin parin päivän ajan, ennen kuin öljy-yhtiön normaali toiminta onnistuttiin palauttamaan (esim. Lemay, Knight, Fernandez & Leblanc, 2016, s. 193-194, Henning, 2020, s. 8-9; Izycki & Vianna, 2021, s. 459). Öljyntuotanto on Saudi-Arabian valtion ensisijainen tulon lähde, ja iskujen voidaan katsoa vaikuttavan merkittävästi tilanteessa valtion toimintaan (Lemay ym., 2016, S. 193).

DDoS-hyökkäyksiä voidaan puolestaan havaita käytetyn hyökkäysmetodina esimerkiksi USA:n talousinstituutioita kohtaan vuonna 2012. Hyökkäyksessä pankkien käyttämiin palvelimiin kohdistettiin massiivisen luokan palvelunestohyökkäys, mikä hidastutti pankkijärjestelmien normaalia toimintaa noin kahden viikon ajan. Tyypilliseen aikakauden DDoS-palvelunestohyökkäykseen nähden USA:n pankkijärjestelmiin kohdistuneen toiminnan kokoluokkaa on arvioitu olleen noin 10-20 kertaa suurempaa, kuin tuon aikakauden tyypillisessä DDoS-palvelunestohyökkäyksessä. Tilanteessa hyökkäyksen kokoa voidaan pitää poikkeuksellisen suurena ajankohtanaan (Boyte, 2017, s. 57-58; Watney, 2014, s. 4; Nye, 2017, s. 49).

Molemmissa esitellyissä tapauksissa voidaan havaita kyberoperaatioiden kohteena olleen valtion talous. Lisäksi molempia esimerkkitapauksia yhdistää näiden todennäköisin tekijä, jonka on arveltu olleen tutkitussa materiaalissa Iranin valtio (esim. Watney, 2014, s. 4; Henning, 2020, s. 8-9).

Näiden kahden mainitun hyökkäysmetodin lisäksi havaittiin sosiaalisella manipulaatiolla olleen joissain tapauksissa merkittävä vaikutus hyökkäyksen onnistumiseen. Sosiaalisen manipulaation avulla ollaan yksittäinen tai useampi henkilö saatu toimimaan hyökkäyksen onnistumisen kannalta edullisella tavalla, jotka kuuluvat hyökkääjän ulkopuoliseen organisaatioon tai toimintaan.

Esimerkiksi USA:n vuoden 2016 presidentinvaaleihin liittyneessä tapauksessa voidaan sosiaalisen manipulaatiolla katsoa olleen merkittävä vaikutus hyökkäyksen onnistumiseen. Tuolloin demokraattipuolueen jäseniä saatiin

avaamaan sähköpostiviestien liitteenä löytyneen tiedoston, joka asensi tiedonkeruuseen tarkoitetun haittaohjelman puolueen jäsenten käyttämiin järjestelmiin (tarkempaa hyökkäystekniikkaa kutsutaan myös kohdennetuksi tietojenkalasteluksi (engl. spear phishing). Menetelmän avulla kerättyä tietoa käytettiin häiritsemään Demokraattipuolueen presidenttikampanjan toimintaa, julkaisemalla säännöllisesti puolueen sähköpostiviestien sisältöjä, aiheuttaen samalla merkittäviä kohuja puoluetta kohtaan (Darraj, Sample & Cowley, 2017, s. 92; Mueller, 2019, s. 37-38; Nye, 2017, s. 48-49, 64).

Näiden kolmen yleisempien mainittujen hyökkäysmetodien lisäksi kyberoperaatioiden toteuttamisessa havaittiin käytettävän yksittäisien tietojärjestelmien loogiseen toimintaan liittyviä heikkouksia hyödyksi, joita hyödyntämällä ensisijaisia hyökkäysmetodeja onnistutaan soveltamaan. Havaintojen pohjalta nämä heikkoudet ovat luonteeltaan tapauskohtaisia, ja vaihtelevat merkittävästi tapauksen mukaan. Lisäksi näiden hyödyntämiseen käytettäviä tarkempia tekniikoita havaittiin olevan lukuisia.

Hyökkäysprosessissa käytettävät laitteistot mainitaan usein tutkitussa materiaalissa keskusteltaessa hyökkäyksen toteuttamisen keinoista. Yleisimpiin mainituista laitteistoista kuuluivat hyökkäyksessä käytettävät komentopalvelimet (Command & control -server), joiden tehtävänä on välittää hyökkääjän antamia komentoja ja tietoa tietoverkkojen lävitse muille hyökkäyksessä käytettäville työkaluille (esim. Huskaj, Iftimie, & Wilson, 2020, s. 476-478; Burita, 2020 s. 56). Komentopalvelimet voivat esimerkiksi välittää komentoja hyökkäyskohteeseen asennetulle haittaohjelmistolle tai esimerkiksi kaapatuille laitteille, joiden avulla hyökkäyksen kohteeseen kohdennetaan DDoS -hyökkäys (Gisel & Ojenik, 2018 s. 57; Pihelgas, 2013, 55-56).

Lisäksi hyökkäysdataa uudelleenohjaavat palvelimet saivat mainintoja materiaalissa. (Redirectors/proxy servers). Näiden toissijaisten palvelimien tehtävänä on ohjata liikennettä komentopalvelimen ja hyökkäysten kohteen välillä. Uudelleenohjaavien palvelimien käytöllä pyritään naamioimaan ja suojaamaan aikaisemmin mainittuja komentopalvelimia sekä hyökkäyksen alkuperäislähdettä. Välipalvelimet näyttäytyvät puolustajalle hyökkäyksen suorana lähettäjänä, näiden näyttäytyessä saapuvan hyökkäysdatan suorana lähteenä puolustajan näkökulmasta. Käyttämällä hyökkäyksessä useita uudelleenohjaavia palvelimia hyökkäysdatan lähettämiseksi, voidaan hyökkäyksessä käytettäviä komentopalvelimien ja hyökkäyslähteiden identiteettiä ja alkuperää piilottaa puolustajan näköpiiristä. Välipalvelimia voidaan myös käyttää tarkoituksessa ilman palvelimessa olevaa tietoa tämän toimimisesta välipalvelimena, mikä lisää puolustajan haastavaa havaita hyökkäyksen alkuperäistä lähdettä (Huskaj, Iftimie, & Wilson, 2020, s. 476-478; Gisel & Ojenik, 2018, s. 57; Philegas, 2013, s. 40-43).

4.1.2 Hyökkäykset kohteet ja seuraukset

Ilmenneiden hyökkäyksellisten operaatioiden kohteina havaittiin olleen pääsääntöisesti poliittisia ja valtiollisia organisaatioita, sekä kriittisen infrastruktuurin luokiteltavia järjestelmiä ja organisaatioita. Poliittisten ja valtiollisten organisaatioiden kohdalla kohdistuneiden iskujen vaikutukset ovat vaikuttaneet tahojen hallinnoimien sivustojen toimivuuden estämiseen, minkä lisäksi joihinkin tapauksiin liittyy tietojärjestelmälaitteiden tuhoamista, sekä poliittiseen prosessiin vaikuttamista. Kriittisen infrastruktuurin kohdalla hyökkäyksellisten operaatioiden vaikutukset vaihtelevat näiden toiminnan häiritsemisestä, keskeyttämisestä, sekä käyttävien järjestelmien tuhoamisesta. Kriittisen infrastruktuurin kohdistuneiden iskujen kohteena ovat olleet muun muassa sähkönjakelu, talousinstituutiot, sekä öljyn tuotanto. Havaintojen perusteella kriittiseen infrastruktuuriin kohdistuneiden kyberoperaatioiden voidaan katsoa olleen yleisellä tasolla vaikutuksiltaan vakavampia suhteessa poliittisten ja valtiollisten tietojärjestelmiin kohdistuneisiin.

Lisäksi hyökkäyksellisten kyberoperaatioiden vaikutukset kohteisiinsa ovat olleet riippuvaisia käytettävästä hyökkäysmetodeista. Haittaohjelmia käyttävät hyökkäykset aiheuttavat tyypillisesti vahinkoja kohteena olleen organisaation järjestelmiä kohtaan. Tilanne on havaittavissa esimerkiksi Etelä-Koreaan kohdistuneessa DarkSeoul -tapauksessa, jossa haittaohjelmaa käytettiin estämään talousinstituutioiden ja mediatalojen käyttämien tietojärjestelmien laitteiden käynnistäminen, tyhjentämällä näiden kovalevyillä oleva tieto (Kyoung, Sung & Joshua, 2017, s. 317; Lee, Kwon, Lee, & Shin, 2015, s. 71-72, 74-75). Käytetty tekniikka vastaa myös Shamoon-tapauksessa sovellettua hyökkäysmenetelmää. Arvioiden mukaan noin 48 000 tietokonetta lakkasi toiminasta DarkSeoul-tapauksen seurauksena, joiden korvaamisesta seuranneiden kustannusten arvioitiin olleen n. 900 miljardia Wonia (noin 665 miljoonaa euroa) (Kyoung, Sung & Joshua, 2017, s. 317).

DDoS-hyökkäyksien kohdalla vaikutukset ovat puolestaan olleet järjestelmien toimintaa häiritseviä ja ovat pääasiassa vaikuttaneet kohteena olevaa tahoa kohtaan hidastamalla tai pysäyttämällä tämän käyttämien palveluiden ja järjestelmien toimintaa väliaikaisesti, aiheuttamatta kuitenkaan fyysisiä vahinkoja järjestelmille. Vaikutukset ovat pääsääntöisesti loppuneet kyberoperaation suorittamisen päätyttyä, kun palveluita hidastavaa tietoliikennettä ei ole enää lähetetty operaation kohteeseen. Vastaavalla tavalla vaikutettiin myös Etelä-Korean valtion organisaatiota kohtaan vuonna 2011, aikaisemmin mainitun USA:n talousinstituutioita kohtaan kohdistetun hyökkäyksen lisäksi (Boyte, 2017, s. 57-58; Watney, 2014, s. 4; Lee, Ym. 2015, s. 73-74).

Myös haittaohjelmien kohdalla voidaan katsoa tapauksien seuraamuksien jääneen omalta osaltaan pääsääntöisesti väliaikaisiksi. Vaikka haittaohjelmat ovat aiheuttaneet fyysisiä tuhoja kohteisiinsa, on enemmistössä tekniikkaa käyttäneiden tapausten kohdalla kohteena olleen organisaation toiminta kyetty palauttamaan normaaliksi viimeistään kahden viikon sisällä operaation jälkeen.

Havaittujen tietojen perusteella ovat kyberoperaatiot pääsääntöisesti aiheuttaneet lyhytaikaisia vaikutuksia.

4.1.3 Hyökkäysprosessit

Tutkitun materiaalin sisällössä esiteltiin monia vaihtoehtoisia menetelmiä toteuttaa hyökkäysprosesseja. Eniten mainintoja saanut näistä oli malli, josta käytetään englanninkielistä nimitystä Cyber Kill Chain (CKC) (esim. Maybaum, 2013, s. 106; Karlzén, 2020, s. 170; Gunneriusson & Oittis, 2013). Alun perin malli luotiin hyökkäyksien ehkäisyä varten (Karlzén, 2020, s. 170) CKC-Malli muodostuu seitsemästä hyökkäyksen askeleesta, jotka ovat seuraavanlaiset yleisessä etenemisjärjestyksessään: kohteen kartoittaminen, hyökkäyksen valmistelu/aseistaminen, kyberaseen toimittaminen järjestelmään, haavoittuvuuden hyväksikäyttö järjestelmässä, kyberaseen asentaminen, komentoketjun muodostaminen, ja tavoiteltujen toimenpiteiden toteuttaminen (Maybaum, 2013, s. 106-129; Gisel & Olejnik, 2018 s. 11).

Tilannekontekstin mukaan hyökkäysprosessissa voidaan myös palata aikaisempiin kuvattuihin askeleisiin tai vaihtoehtoisesti toteuttaa askeleita myös vaihtoehtoisessa järjestyksessä. Esimerkiksi hyökkääjä voi toteuttaa tämän parantaakseen tilannekuvaansa hyökkäyskohteesta, tai havaitessaan tarpeita muokata käytettäviä työkaluja hyökkäyksen onnistumiseksi. Myös esimerkiksi hyökkäystavoitteiden muuttuessa voidaan hyökkäyksessä palata hyökkäyksen aikaisempiin askeleisiin (Maybaum, 2013, s. 129-130; Gisel & Olejnik, 2018, s. 57).

Lisäksi tutkitussa materiaalissa huomioitiin, että hyökkäyksessä tavoiteltuja vaikutuksia on haastavaa arvioida puolustajan tai ulkopuolisten tahojen toimesta, ennen kuin hyökkäysprosessi on onnistuneesti saatettu päätökseen. Tilanne johtuu, koska käytettävät hyökkäysmetodit eivät pääsääntöisesti paljasta tavoiteltuja vaikutuksia ennen viimeisien hyökkäyksen vaiheiden toteutusta. Vasta tällöin mahdollisesti selvenee puolustajalle, pyritäänkö hyökkäyksellä aiheuttaa häiriöitä järjestelmien toimivuudessa, vai onko hyökkäyksen tavoitteena esimerkiksi tiedustelun toteuttaminen. Lisäksi hyökkäyksen tavoitteen vaihtuessa voi hyökkäysprosessin luonne muuttua nopeasti. (Gunneriusson & Oittis, 2013, s. 99; Gisel & Olejnik, 2018 s. 7 & 12; Lindsay, 2015, s. 33).

4.2 Puolustuksellinen toiminta

4.2.1 Yleinen puolustuksellinen toiminta

Tutkimuksen kohteena olleessa materiaalissa korostui näkemys, jossa koettiin tarvetta parantaa puolustuskapasiteettia hyökkäyksellisiä kyberoperaatioita kohtaan. Usein nähtyä tarvetta perustellaan yhteiskunnan järjestelmien riippuvuudella internetin tietoliikenteestä. Yhteiskuntien toiminnan ollessa yhä entistä enemmän kytketympiä internettiin, sekä riippuvaisempia tämän toimivuu-

desta, nostavat riippuvaisuudet uhkakuvia mahdollisen hyökkäyksellisten kyberoperaatioiden vaikutuksista internettiin kytkettyjä järjestelmiä kohtaan (Yong-joon, Hyuk-jin, Jaeil, & Dong-kyoo, 2015, s. 72-73).

Kyberhyökkäyksiltä puolustautumiseksi käytettäviä metodeja kuvattiin tutkitussa aineistossa lukuisia, ja ne olivat luonteeltaan moninaisia. Mainittuihin metodeihin kuuluvat esimerkiksi havaittujen haavoittuvuuksien korjaaminen järjestelmissä, järjestelmien fyysinen erottaminen laajemman internetin kytköksistään, sekä käytettävien järjestelmien vahvistaminen eli ”koventaminen” tapahtuvia hyökkäyksiä kohtaan. Myös tietoliikennedatan vahvan salauksen käyttämistä autentikoinnin aikana mainittiin aineistossa useamman kerran (esim. Mattila & Parkinson, 2017, s. 615; Kiviharju, Huttunen ja Kantola, 2020, s. 191-192; Gisel & Olejnik, 2018, s. 23; 27-28). Lisäksi tietoliikenteen estäminen, joka poikkeaa tietoturvasäännösten sallimasta tietoliikenteestä, voidaan katsoa kuuluvan vastaavanlaiseen toimintaan, jonka toteuttaminen tapahtuu ensisijaisesti tapahtuvien hyökkäyksien ulkopuolella (Kiviharju, Huttunen ja Kantola, 2020, s. 191-192).

Tutkitussa materiaalissa mainitaan myös useasti puolustajan mahdollisuus toteuttaa puolustustoimintaansa myös tapahtumassa olevan kyberhyökkäyksen aikana. Tämän aktiivisen puolustustoiminnan tarkoituksena on tapahtuvan hyökkäyksen pysäyttäminen, sekä hyökkäyksen vaikutusten minimoiminen omia järjestelmiä kohtaan. Lisäksi toiminnan aikana puolustaja voi pyrkiä eliminoimaan hyökkääjän kapasiteettia toteuttaa tapahtuvaa hyökkäystä, esimerkiksi toteuttamalla vastahyökkäyksiä (esim. Kiviharju ym., 2020, s. 191-192; Kello, 2013, s. 32-33; Mattila & Parkinson, 2017, s. 615). Vastahyökkäysten lisäksi puolustaja voi puolustaja hyökkäyksien aikana muokata omistamiensa tietoverkkojen ympäristöä ja konfiguraatiota, tehdäkseen hyökkäyksen toteuttamisesta ja edistämisestä huomattavasti haastavampaa hyökkääjälle muuttuvassa ympäristössä (Kiviharju ym., 2020, s. 191-192).

Artikkelien sisällössä kuvattiin usein myös yhtenä puolustuksellisena keinona pelotteen (engl. deterrance) luomista ja ylläpitoa kybermaailmassa, joskin mielipiteet pelotteen soveltumisesta kybermaailman kontekstiin olivat vaihtelevia ja ristiriitaisia tutkitussa materiaalissa. Pelotteen käytöllä viitataan toiminnan ehkäisemiseen saamalla toiminnan mahdollinen toteuttaja ajattelemaan, että toiminnan kustannukset tulevat olemaan suurempia, kuin tästä saatavat hyödyt ovat (Nye, 2017, s. 45). Pelote-teoriaa tukevat kirjoittajat katsovat pelotteen luomisen avulla voitavan ehkäistä hyökkäyksellisten operaatioiden toteuttamista saamalla kyberoperaation toteuttaminen vaikuttamaan potentiaaliselle hyökkääjälle epäkannattavalta. Ajatuksissaan kannattajat kokevat pelotetta voitavan luoda esimerkiksi mahdollisen rangaistuksien uhalla, toimijoiden välisten riippuvuussuhteiden aiheuttamasta hyökkäyksen vastavaikutuksista hyökkääjälle, tehokkaiden puolustuskeinojen avulla, sekä normien ja tabujen ylläpidolla kansainvälisessä toiminnassa (Nye, 2017, s. 45, 54-62). Toisaalta pelote ei todennäköisesti toimi puolustuskeinona, mikäli attribuution epävarmuus hyökkäyksessä vähentää vastatoimien todennäköisyyttä hyökkääjää kohtaan (Guitton, 2013, s. 96).

Tutkitussa materiaalissa havaittiin myös lukuisia keinoja, joilla valtion johtotasolla on pyritty parantamaan kyberpuolustusta. Näihin ovat kuuluneet muun muassa koulutuksen ja puolustusharjoituksien kehittäminen, laki-, sopimus- ja organisaatiouudistukset, sekä rahalliset sijoitukset kyberpuolustuksen kehittämiseen (esim. Dupuy, Iftimie, Nussbaum & Pickl, 2020, s. 103; Greiman, 2017, s. 149-150). Rahallista sijoittamista voidaan nähdä esimerkiksi Isossa-Britanniassa, jossa valtio sijoitti 1,9 miljardia puntaa (noin 2,2 miljardia euroa) kyberpuolustuksensa kehittämiseen vuonna 2016. Lisäksi USA on asettanut voimaan lakiuudistuksia koskien kansallisen kyberturvallisuusinformaation jakoa, minkä avulla valtio pyrkii parantamaan tiedonjakoa tämän ja USA:ssa toimivien organisaatioiden kanssa (Greiman, 2017, s. 149-150).

Puolustustoiminnan merkittävimpinä haasteina kerrotaan tutkimusmateriaalissa olevan verkkoon kytköksissä olevien järjestelmien kokonaisvaltainen laajuus ja monimutkaisuus. Järjestelmien ollessa laajoja ja monimutkaisia, eivät kaikki järjestelmissä löytyvät heikkoudet ole puolustavan tahon tietoisuudessa ja huomion kohteena. Tietämättömyys kaikista käytettävien järjestelmien heikkouksista tekee samalla hyökkäysten etenemistapojen ennakoimisesta huomattavasti haastavampaa puolustajalle. Lisäksi tietoverkkoihin luontaisesti kuuluva anonymiteetti katsotaan lisäävän puolustajalle vaikeuksia tunnistaa toteutuneen hyökkäyksen tuottaneen tahon (Boyte, 2017, s. 61; Kello, 2013, s. 27-29). Erityisenä haasteena puolustustoiminnalle pidetään APT:ksi luokiteltavia hyökkäyksellisiä operaatiota, joista jotkin ovat onnistuneet hyvästä puolustuksen toteuttamisesta huolimatta vaikuttavaan kohteeseen halutulla tavalla. Hyvän puolustuksen avulla katsotaan kuitenkin pystyvän ehkäisemään enemmistön näitä yksinkertaisemmista hyökkäyksistä (Nye, 2017, 2016, s. 58).

4.2.2 Puolustuksen kohteet

Tutkimuksen kohteena olleessa materiaalissa korostui erittäin vahvasti puolustustoiminnan kohteena kriittinen infrastruktuuri ja sen alaisuuteen luokiteltavat järjestelmät. Kriittiseen infrastruktuuriin voidaan luokitella kuuluvaksi palveluja, toimintoja ja järjestelmiä, joita pidetään elintärkeinä yhteiskuntien normaalille toiminnalle (Valtioneuvosto, 2013, s. 12). Esimerkiksi energian- ja ruuantuotanto on luokiteltu kuuluvan näihin järjestelmiin tutkitussa materiaalissa. Kriittisen infrastruktuurin ollessa elintärkeää valtioiden normaalille toiminnalle, pidetään näihin kohdistuvia hyökkäyksellisiä operaatiota merkittävänä uhkana valtioiden kansalliselle turvallisuudelle. Uhkakuva tekee myös kriittisen infrastruktuurin suojelemisen myös merkittäväksi strategiseksi tavoitteeksi valtioille (Boyte, 2017, s. 54-55; Guitton, 2013, s. 93; Izycki & Colli, 2019, s. 222).

Uhkakuvaa kriittisen infrastruktuurin kohdistuvista kyberhyökkäyksistä perustellaan viittaamalla pääsääntöisesti aikaisempiin tapahtuneisiin kyberoperaatioihin, jotka ovat toiminnallaan vaikuttaneet kriittiseen infrastruktuurin toimivuuteen. Erityisesti Stuxnet -tapaukseen viitataan usein perustellessa uhkakuvien syitä ja tarpeita kriittisen infrastruktuurin suojaamiselle (Esim. Dupuy, ym., 2020, s. 100; Gunneriusson & Ottis, 2013, s. 102). Aikaisempien tapauksen

voidaan katsoa myös lisäävän uhkakuvaa omiin järjestelmiin kohdistuvista kyberhyökkäyksistä.

Kriittiseen infrastruktuuriin kohdistettujen uhkien toteutuminen on toistaiseksi ollut kuitenkin suhteellisen vähälukuista tapahtuneiden kyberhyökkäyksien kohdalla. Tutkitussa materiaalissa vähälukuisuutta sanotaan johtuvan vaadittavasta erityistuntemuksesta ja taidosta, joka hyökkäyksien toteuttaminen edellyttää kriittiseen infrastruktuuriin. Erityisesti erityistuntemus kohdistuu kyberoperaation kohteena olevan laitoksen käyttämien ratkaisujen tuntemista kohtaan. Kriittisen infrastruktuurin kuuluvat laitokset käyttävät pääsääntöisesti tämän erityistarpeisiin kustomoituja ohjausjärjestelmiä ja kokonaisratkaisuja, jotka pohjautuvat yksittäisen laitoksen toimintaan vaadittavista erityistarpeista. Tilanteessa kyberhyökkäyksen onnistuminen edellyttää hyökkääjältä kyberhyökkäyksen tarkkaa kohdentamista laitoksen käyttämiä uniikkeja ratkaisuja kohtaan, sekä hyökkäysvälineiden tarkkaa kustomointia (Zycki & Vianna, 2021, s. 457-458, 460-462; Maybaum, 2013, s. 128). Ilmiön johdosta vain valtiollisilla toimijoilla katsotaan olevan käytännössä kapasiteettiä toteuttaa onnistuneita kyberoperaatioita kriittistä infrastruktuuria kohtaan (Zycki & Vianna, 2021, s. 460-462).

4.3 Kyberoperaatiot sotilaallisessa kontekstissa

4.3.1 Sotilaallinen toiminta

Tutkitussa materiaalissa kyberavaruudessa tapahtuvaa toimintaa luokitellaan usein viidenneksi sodankäynnin tantereeksi Maa-, Meri-, Ilma- ja Avaruussodankäynnin ohella (esim. Nye, 2017, s. 46; Gunneriusson & Ottis, 2013, s. 99; Boyte, 2017, s. 55; Akbariavaz, Tehrani & Sabaruddin, 2020, s. 452). Kyberavaruuden ottamisen osaksi sotilastoimia katsotaan olleen mahdollista johtuen monien valtioiden toiminnan riippuvuudesta tietojärjestelmien toimivuudesta, sekä tietoteknisten laitteiden kehittymisestä. Tilanteen katsotaan tekevän kyberavaruudesta otollisen sotilastoimintaan mukaanottoon (Akbariavaz, Tehrani & Sabaruddin, 2020, s. 452). Ainakin 30 valtiota on jo ottanut kybersodankäynnin huomioon näiden sotilasorganisaatioiden suunnittelussa (Czosseck, 2013, s. 15-16).

Sotilaallisen kontekstin sisällä kyberoperaatioita katsotaan usein käytettävän osana hybridisodankäyntiä. Hybridisodankäynti on nykyään useasti esiintyvä termi, jolla viitataan epäsymmetrisien taktiikoiden käyttöön sodankäynnissä (Darraj, Sample & Cowley, 2017, s. 92; Boyte, 2017, s. 54, 58; Cole & Noel, 2021, s. 49). Näitä epäsymmetrisiä taktiikoita jaotellaan kineettisten, eli perinteisen aktiivisen sodankäynnin, sekä ei-kineettisen taistelumuotojen käyttämiseen. Ei-kineettisen taistelun muotoihin voidaan luokitella esimerkiksi kyberoperaatioiden käyttäminen, informaatiovaikuttaminen, sekä energiasaarrot sotatilanteen aikana (Boyte, 2017, s. 55). Toisin sanottuna hybridisodankäynnissä perin-

teisiin sodankäynnin muotojen lisäksi sodankäynnissä käytetään myös joitain rauhan aikana käytettäviä vaikuttamisen muotoja sotilastavoitteiden saavuttamiseksi. Taistelukentästä voidaan tällöin katsoa olevan multidimensionaalinen, jossa käytetään myös perinteisen sodankäynnin ulkopuolella olevia keinoja (Darraj, Sample & Cowley. 2017, s. 93).

Sotilasoperaatioiden tavoitteet voidaan sotatilanteesta ja -tavoitteista riippuen toteuttaa lukuisia vaihtoehtoisia tapoja käyttäen, joista kyberoperaatioiden käyttäminen katsotaan olevan yksi vaihtoehto. Kontekstista ja tilanteesta riippuen sotilaallisia tavoitteita voidaan mahdollisesti saavuttaa käyttämällä kyberoperaatioita muiden sodankäynnin muotojen kanssa, kuten esimerkiksi perinteisten sotilasvoimien rinnalla. Sotilaallisia tavoitteita voidaan myös tapauskohtaisesti saavuttaa kyberoperaatioiden itsenäisellä käytöllä, joskin kyberoperaatioiden rajoitukset ja tekninen toteuttaminen ovat omanlaisiaan muiden sodankäynnin tantereiden lailla. (Granåsen & Jaitner, 2019, s. 197; Akbariavaz, Tehrani & Sabaruddin, 2020, s. 452; Kiviharju, Huttunen & Kantola, 2020, s. 192-193).

Kyberoperaatioista ei kuitenkaan tutkimusmateriaalin perusteella ole toistaiseksi havaittavissa monia esimerkkejä aktiivisten sotatilanteiden aikaisesta käytössä ennen vuotta 2022. Vuoden 2010 jälkeisenä ajankohtana tutkimuksessa havaittiin kyberoperaatioita olleen käytetyn sotatilanteen aikana vain Ukrainan konfliktiin liittyvien tapahtumien kohdalla. Tällöin tapahtuneet kyberoperaatiot ovat kohdistuneet esimerkiksi Ukrainan sähkönjakelua sekä kommunikaatiovälineitä kohtaan (Nye, 2017, s. 69; Boyte, 2017, s. 61). Johtuen kyberoperaatioiden käytön vähyydestä sodankäynnin aikana tutkitussa ajanjaksossa, voidaan kyberoperaatioita luokitella olleen käytetyn pääsääntöisesti rauhanaikaisessa tilanteessa tutkittuna ajanjaksona.

4.3.2 Sotilaallinen toiminta kansainvälisessä oikeudessa

Tutkimusmateriaalissa keskusteltiin huomattavan paljon sotilaallisen voimankäytön (engl. use of force) tulkinnasta kyberoperaatioiden käytössä. Sotilaallinen voimankäyttö ja tämän käytöllä uhkaaminen nähdään kiellettynä toista valtiota kohtaan kansainvälisissä oikeudessa. Erityisesti YK:n peruskirjan artikla 2(4) kieltää vastaavanlaisen toiminnan valtioiden välisessä toiminnassa (Kyoung, Sung & Joshua, 2017, s. 318-319; Watney, 2014, s. 3). Poikkeuksena voimankäytön kieltoon katsotaan olevan valtion joutuminen sotilaallisen hyökkäyksen (engl. armed attack) kohteeksi, jolloin valtiolla katsotaan olevan oikeus käyttää sotilaallista voimankäyttöä itsepuolustukselliseen tarkoitukseen ja lopettaakseen tähän kohdistuvan hyökkäyksen (Kyoung, Sung & Joshua, 2017, s. 318-319). Aikaisemmissa tulkinnoissa on sotilaallinen voimankäyttö assosioitu vahvasti perinteisen fyysisten sotilasvoimien ja -toimien käyttämiseen.

Vahva enemmistö aihetta käsitelleistä tutkimusmateriaalin kirjoittajista toteaa sotilaallisen voimankäytön ja hyökkäyksen olevan sovellettavissa kyberoperaatioiden toteuttamiseen kansainvälisessä oikeudessa. Tällöin he pyrkivät painottamaan tapahtumien tulkinnassaan ja arvioimisessaan käytettyjen hyök-

käysvälineiden sijasta tapahtuneen toiminnan vaikutuksia sekä kohteen merkitystä. Jotta kyberoperaatioita voidaan luokitella aseelliseksi hyökkäykseksi, on operaation seurauksien oltava rinnastettava vastaavanlaisiin vaikutuksiin, joita perinteisen sodankäytön välineillä voidaan tuottaa kyberoperaation kohteeseen. Tällöin merkittävänä tarkasteltavana indikaattorina vaikutuksien arvioimisessa, on yleensä ollut hyökkäyksellisen kyberoperaation aiheuttaman fyysisten vahinkojen määrä, sekä mahdolliset tapauksesta aiheutuneet ihmisuhrit. (esim. Gisel & Ojenik, 2018 s. 8, Akbariavaz, Tehrani & Sabaruddin, 2020, s. 456-457, Watney, 2014, s. 3-4;). Artikkelien sisällössä kuvatuissa kyberoperaatioissa ei ole kuitenkaan havaittu tapauksia, joissa kyberoperaation kohteena ollut valtio olisi vedonnut aseellisen hyökkäyksen kohteeksi joutumistaan ja aloittanut tämän perusteella sotilaallisen itsepuolustuksen tapahtumien johdosta. Tilanteessa kansainvälisen oikeuden tulkintaa ei ole kyetty tarkennettaman yksityiskohtaisemmin asiantuntijoiden keskuudessa, koska käytännön esimerkit ovat toistaiseksi puuttuneet tulkinnan tueksi. Nykyisessä tilanteessa kyberoperaatioiden tulkintaa tultaneen tekemään tapauskohtaisesti kansainvälisessä oikeudessa (Watney, 2014, s. 4; Kyoung, Sung & Joshua, 2017, s. 319).

4.4 Poliittinen toiminta

Hyökkäyksellisistä kyberoperaatioista on muodostunut valtioiden uusimmaksi tavaksi projisoida voimaansa toisia valtioita kohtaan, näiden edistäessään kansallisen turvallisuuden ja ulkopolitiikan tavoitteita (Granåsen & Jaitner, 2019, s. 194; Martins, 2018, s. 32-33). Olleessaan uusimpia työkaluja valtiolle, voidaan valtioiden havaita olevan yhä selvittelemässä, missä kyberoperaatioiden käytölle sallittavat rajat tulevat olemaan (Granåsen & Jaitner, 2019, s. 194). Vaikka kaikista yksityiskohdista kyberoperaatioiden sallitussa käyttötavoista ei olla vielä tehty yhteisiä päätöksiä, voidaan valtioiden toiminnassa havaita yhteisiä toimintamalleja poliittisessa kontekstissa. Useimmin esiintynyt valtioiden reaktiotapa näihin kohdistuneisiin kyberhyökkäyksiin on ollut toisen valtion syyttäminen tapahtuneen kyberhyökkäyksen toteuttamisesta.

Useimmin aineistossa esiintynyt valtioiden reagointitapa näihin kohdistuneisiin kyberhyökkäyksiin on ollut toisen valtion syyttäminen tapahtuneen kyberhyökkäyksen toteuttamisesta. Näiden mainintojen esiintyessä kyberoperaatioiden kohteena olleet valtiot ovat melkein kaikkien mainintojen kohdalla sanoneet kyberoperaation toteuttajaksi olleen valtion, jonka välisessä vuorovaikutuksessa on aikaisemmin ollut havaittavissa merkittäviä poliittisia jännitteitä. Esimerkiksi Etelä-Korean kohdistuvien kyberhyökkäysten kohdalla valtion viranomaiset ovat tyypillisesti sanoneet Pohjois-Korealaisien toimijoiden olleen kyberhyökkäysten toteutuksen takana. Puolestaan Ukrainan kohdistuneista kyberoperaatioista ovat valtion edustajat tyypillisesti sanoneet Venäjän olleen tapahtumien toteuttajana (esim. Kyoung, Sung & Joshua, 2017, s. 315-318, 320; Lee, Ym. 2015, s. 73-84; Kostyuk & Zhukov, 2019, s. 317-318). Havaituista toi-

mintamalleista voidaan päätellä, että julkiseen tietoon tulleiden tapauksien taustalla vaikuttavat vahvasti poliittiset taustatekijät.

Enimmissä aineistossa mainittujen hyökkäyksellisten kyberoperaatioiden kohdalla ei havaittu muita tapauksissa esiintyneitä poliittisia reagointitapoja mahdollisen toteuttajan syyttämisen lisäksi. Yksittäisissä tapauksissa havainnoitiin kuitenkin myös voimakkaampien vastakeinojen käyttöä. Esimerkiksi esiintyneitä muita reagointitapoja yksittäistapauksissa ovat olleet sanktioiden asettaminen tapauksen tekijäksi sanottua valtiota kohtaan, valtion kyberkapasiteetin kehittäminen, kuin myös mahdollisesti uusien hyökkäyksellisten operaatioiden toteuttaminen syytettyä valtiota kohtaan (esim. Mueller, 2019, s. 37-38, Martins, 2018, s. 34; Nye, 2017, s. 48). Lisäksi aineistossa esitetään usein potentiaalisina valtioiden reagointitapoina tapauksen tuomista YK:n turvallisuusneuvoston tai kansainvälisien tuomioistuimien käsiteltäväksi, sekä sotilaallinen toiminnasta päättäminen. (esim. Schmitt, 2021, 762; Akbariavaz, Tehrani & Sabaruddin, 2020, s. 451)

Kyberoperaatioiden kohdalla valtioiden edustajat toteuttavat tyypillisesti julkisen attribuution tapahtumien tekijästä, kriminaalitapauksia käsittelevien tuomioistuimien sijasta. Tilanne on johtunut valtioiden ollessa ainoita tahoja, joilla on ollut sallittua auktoriteettia toteuttaa asiaa julkisesti. Tällöin myös tapausten tekijän julkiseen attribuutioon tulee liittymään oikeusteknisten todisteiden arvioimisen lisäksi poliittista arvioita. Kansallisen turvallisuuden kohdalla oikeusteknisten todisteiden kerääjät vaihtelevat paljon suhteessa kriminaalitapausten käsittelyyn, mutta parhaiten arvioidaan olevan tämän toiminnan toteuttamiseksi kapasiteettia tiedusteluorganisaatioilla (Guitton, 2013, s. 95).

Enemmissä kyberoperaatioiden kohdalla ovat valtiot reagoineet tyypillisesti tapahtuneisiin toimiin vain sanallisella tuomitsemisella, eikä muita reaktiotapoja ole näyttäytynyt julkisuuteen (Maness & Valeriano, 2016b, S.317-319). Ilmiön voi nähdä Esimerkiksi Ukrainaan ja Etelä-Koreaan kohdistuneiden kyberoperaatioiden kohdalla, joissa valtiot ovat päättäneet sanallisesti paheksua kyberoperaatioiden toteuttamista, toteuttamatta tuomitsemisen lisäksi muita toimia sanottua kyberoperaation tekijää kohtaan (Kyoung, Sung & Joshua, 2017, s. 310; Kostyuk, Powell & Skach, 2018, s. 123).

Poikkeuksena tähän ovat olleet kuitenkin DDoS-hyökkäyksiä metodinaan käyttävät operaatiot, kuin myös kyberhyökkäykset, joiden tavoitteena on ollut kohdevaltion pakottaminen poliittisen suunnanvaihdokseen. Molemmat näistä ovat tyypillisesti johtaneet kohdevaltion julkisuudessa näkyvään vahvaan negatiiviseen reaktioon. Poliittiseen suunnanvaihdokseen pyrkivät operaatiot ovat usein myös johtaneet kohdevaltion päinvastaiseen reaktioon tavoitelluista. (Maness & Valeriano, 2016b, s. 317-319).

Esimerkiksi vuoden 2016 presidentinvaalien jälkeen Obaman hallinto asetti sanktioita Venäjää kohtaan, sekä karkotti venäläisiä diplomaatteja, sanottuaan julkisuudessa Venäjän valtion olleen tapahtumaan liittyneen kyberoperaation takana. Kyberoperaatiossa Demokraattipuolueen palvelimelta kaapattiin tietoja, joita myöhemmin käytettiin pyrkimyksissä vaikuttaa vaalien tulokseen, vuota-

malla kohua aiheuttaneita sähköpostiviestejä julkisuuteen (Schmitt, 2021, s. 792; Nye, 2017, s. 65; Mueller, 2019, s. 37-38).

4.5 Poliittiset toimijat

Tutkimusmateriaalin sisällössä eniten keskustelua havaittiin käytävän valtioiden kohdalla USA:n, Kiinan ja Venäjän toiminnasta kyberavaruudessa. Näitä kolmea valtiota pidetään kyberavaruuden suurvaltoina ja -toimijoina, joilla katsotaan olevan kapasiteettia toteuttaa toimintaansa kyberavaruudessa (Martins, 2018, s. 33; Czosseck, 2013, s. 15–16). Yhteisiä havaittavina yksityiskohtia Kiinan ja Venäjän toiminnassa on valtioiden pyrkimys ylläpitää puolustussyistä valtioiden kontrollia tietoliikenteen sisällöstä ja yleisestä toiminnasta. USA:n pyrkimykset vaikuttavat taas olevan vastakkaisia. Näiden kolmen valtion lisäksi materiaalissa havaittiin paljon keskustelua valtioiden ulkopuolisista toimijoista, jotka toimivat valtioiden ohjaamina hyökkäyksellisiä kyberoperaatioita muita valtioita kohtaan. Seuraavaksi käydään tarkemmin aikaisemmin mainittujen toimijoiden tekemää toimintaa ja tilannetta, minkä lisäksi käsitellään valtioiden näkökulmia kyberavaruudessa tapahtuvaa toimintaa kohtaan.

4.5.1 USA

Tutkitussa materiaalissa korostuvat USA:n kohdalla yksityisen ja valtiollisen tahoihin liittyvät toimet, sekä tietoverkkojen merkitys valtiolle.

USA:n valtiojärjestelmässä valtio ja yksityisen kaupallisten tahot pyritään erottamaan toisistaan. Erottelupyrkimysten takia kaupalliset yritykset toimivat USA:ssa autonomisina toimijoina, ja ne päättävät itsenäisesti valtion organisaatioiden tavoitteiden ja toiminnan mahdollisen tukemisen omassa operoinnissaan (Cole & Noel, 2021, s. 52). Lisäksi USA:n valtio pyrkii tukemaan avointa ja ilmaista kyberavaruutta ylläpitääkseen valtion perustuslaissa perusoikeutena määriteltyä sananvapautta. Tämän takia valtio ei pyri kontrolloimaan tietoverkkojen sisällä liikkuvaa informaatiota, jota sen kansalaiset kohtaavat ja käyttävät tietoverkoissa (Cole & Noel, 2021, s. 52; Greiman, 2017, s. 147).

Noin 90–95 prosenttia USA:n sisäisestä tietoliikenteestä kulkee yksityisomistuksessa olevien tietoliikennekaapeleiden kautta, ja noin 85 prosenttia USA:n kriittisestä infrastruktuurista on yksityisomistuksessa (Payne & Mienie, 2019, s. 38). Johtuen valtion tavoitteista erottaa valtio ja yksityinen puoli toisistaan, ei USA:n valtiolla ole pyrkimystä suoraan vaikuttaa yksityisessä omistuksessa olevien infrastruktuurien ja organisaatioiden kyberturvallisuuden ylläpitoon. Tämän takia valtion asema näiden entiteettien puolustuksen kehittämissä pysyttelee ohjaavassa ja neuvoa antavassa asemassa (Cole & Noel, 2021, s. 52). Esimerkiksi USA:n kyberturvallisuusstrategiassa valtio kehottaa kansalaisiaan ja yrityksiään ehostamaan kyberturvallisuutta kansallisen turvallisuuden ylläpitämiseksi suorien käskyjen antamisen sijasta (Greiman, 2019, s. 28). Tilantees-

sa valtio pyrkii pysäyttämään tapahtuvia kyberhyökkäyksiä ennen kuin nämä saavuttavat USA:n sisäalueilla olevat kohteensa (Cole & Noel, 2021, s. 52).

Valtion ja sen alueilla toimivien yritysten voidaan katsoa olevan riippuvaista tietoliikenneyhteyksien toimivuudesta (Boyte, 2017, s. 57). Internetistä riippuvaisia järjestelmiä ovat USA:ssa armeijajärjestelmien komentoketju, kriittisen infrastruktuurin toiminnan tukemiseen käytettävät järjestelmät, sekä tuotteiden ja palveluiden toimittaminen asiakkaille (Nye, 2017, s. 44). Koska USA:n toiminta on riippuvainen kyberavaruudesta, nähdään valtion olevan alttiina potentiaalisten kyberoperaatioiden vaikutuksille (Boyte, 2017, s. 57). Näiden uhkakuvien katsotaan toteutuneen esimerkiksi massiivisen DDoS -hyökkäyksen kohdalla USA:n talousinstituutioita kohtaan vuonna 2012, mikä hidasti talousjärjestelmien toimintaa noin kahden viikon ajan. Tapahtuman takana on sanottu olleen todennäköisimmin Iranissa oleskelleet toimijat (Boyte, 2017, s. 57–58; Watney, 2021, s. 4; Martins, 2018, s. 31).

USA:n riippuvuussuhteiden tietoliikenteestä voidaan katsoa motivoivan hallinon pyrkimyksiä ehkäistä kyberoperaatioita, jotka kohdistuvat valtion alueilla toimiviin yksityisiin toimijoihin. Valtio on pyrkinyt toteuttamaan tätä toimintaansa säätämällä esimerkiksi lakeja, jotka helpottavat kansallisen kyberturvallisuusinformaation jakoa valtion ja tämän ulkopuolisten tahojen välillä (Greiman, 2017, s. 149-150). Lisäksi USA on ehdottanut kansainvälisessä keskustelussa kyberhyökkäyksien kieltämistä tiettyjä siviilikohteita kohtaan rauhan aikana, mikä koskee erityisesti kriittistä infrastruktuuria. Tämän toteuttamiseksi USA on ajanut kansainvälisissä keskusteluissa näkemystä, jonka mukaan kansainvälisiä sopimuksia koskien aseellisia selkkauksia (Law of Armed Conflict) voidaan katsoa olevan sovellettavissa kyberavaruudessa tapahtuvaa toimintaa kohtaan. Kyseiset sopimukset kieltävät tarkoituksella toteutettujen iskujen toteuttamisen siviilikohteita kohtaan (Nye, 2017, s. 61). Lisäksi USA säilyttää doktriinissaan oikeuden vastata kyberhyökkäyksiin kaikilla mahdollisilla keinoilla, joita pidettään suhteellisina ja välttämättömänä kyseisessä tapahtumassa. Näihin mahdollisiin keinoihin katsotaan kuuluvan esimerkiksi diplomaattiset, taloudelliset, informaatiolliset, kuin myös sotilaalliset toimet (Nye, 2017, s. 66-67; Maness & Valeriano, 2016b, s. 303).

USA:n hallinto vaikuttaa myös reagoivan joissain tapauksissa muita valtioita kohtaan, joita se pitää kyberoperaatioiden mahdollisina toteuttajina. Esimerkiksi vuoden 2016 presidentinvaalien jälkeen USA:n viranomaiset sanoivat Venäjän valtion olevan vuonna 2016 tapahtuneen kyberoperaation takana. Tapatuksessa Demokraattipuolueen palvelimelta kaapattiin tietoja, joita myöhemmin käytettiin pyrkimyksissä vaikuttaa vaaleihin. Tapauksen seurauksena Obaman hallinto asetti sanktioita Venäjää kohtaan ja karkotti venäläisiä diplomaatteja tapahtumien jälkeen. (Schmitt, 2021, s. 792; Nye, 2017, s. 65; Mueller, 2019, s. 37-38).

Yleisesti ottaen tutkitun materiaalin esittämä näkökulma kuvaa USA:n alttiina olevana valtioina kyberhyökkäyksille, mitä kohtaan kohdistuu kyberoperaatioiden käytön uhka. Valtiota kuvataan pääsääntöisesti hyvin puolustuksellisesta näkökulmasta, jota kohtaan muut valtiot suunnittelevat jatkuvasti uusia

kyberhyökkäyksiä. Esimerkiksi aikaisemmin kappaleissa mainitut Vuoden 2016 presidentinvaaleihin ja vuoden 2011 USA:n talousinstituutioihin kohdistuneita hyökkäyksellisiä mainitaan usein USA:ta toimintaa käsitellessä materiaalissa (esim. Schmitt, 2021, s. 792; Mueller, 2019, s. 37-38; Watney, 2014, s. 4).

Toisaalta tutkitussa materiaalissa on USA:n sanottu olevan myös todennäköisin toteuttaja joidenkin kyberoperaatioiden kohdalla. Erityisesti Stuxnet-tapauksen kohdalla USA:n sanotaan usein olevan toinen mahdollisista tekijöistä Israelin ohella (esim. Barbosa, 2020a, s. 36; Guitton, 2013, s. 95; Izycki & Vianna, 2021, s. 458). USA:n hallinto itse ei kuitenkaan ole kommentoinut asiaa virallisesti tapauksen kohdalla (Lemay ym. 2016, s. 195).

4.5.2 Venäjä

Venäläisessä uhkakuvissa muut valtiot ja vihollismieleiset toimijat tavoittelevat kyberavaruuden käytön avulla epästabiiliuden luomista Venäjän alueille. Läntisten valtioiden, kuten USA:n, katsotaan pyrkivän kaatamaan Venäjän hallitusta ja riisumaan valtion asekapasiteetistaan (Cole & Noel, 2021, s. 49; Ristolainen, 2017, s. 372). Tämä piiritetyn linnakkeen ajattelumalli on vaikuttanut venäläiseen ajattelutapaan jo hyvin pitkän aikaa Venäjän historiassa. Uhkakuvan seurauksena valtio kokee USA:n luoman ja USA:laisesta ohjelmistoista ja palveluista riippuvaisen internetin olevan uhkana Venäjän teknologian eheydelle sekä valtion autonomialle (Ristolainen, 2017, s. 372) Lisäksi läntisvaikutteista ajatuksia ja informaatiota pelätään käytettävän valtion kansalaisten vaikuttamiseen informaatio- ja disinformaatiokampanjoissa. Länsimaisten vaikutteiden leviäminen katsotaan aiheuttavan venäläisten perinteisten arvojen heikkenemistä, sekä luovan säröjä valtion sisäiseen harmoniaan (Kostyuk, Powell & Skach, 2018, s. 130; Ristolainen; 2017, s. 370).

Uhkakuvien katsotaan selittävän Venäjän pyrkimystä tiukentaa kontrolliaan ja valvontaansa internetistään, sekä valtion sisällä kulkevasta informaatiosta (Ristolainen, 2017, S. 372-374; Greiman, 2017, s. 149; Kostyuk, Powell & Skach, 2018, s. 130). Sen informaatioturvallisuusdoktriinissa kuvataan valtion tavoitteina järjestelmien riippuvuussuhteiden poistaminen Venäjän ulkopuolista teknologiasta, ohjelmistoista sekä tietoverkkoista. Tavoitetta perustellaan kykenevyydellä varmistaa valtion suvereeninen kontrolli tämän tietojärjestelmistä (Ristolainen, 2017, S. 372-374). Venäjän hallitus on tavoitteidensa johdosta pyrkinyt erottamaan venäläisen internetin maailmanlaajuisesta verkosta, jotta valtio kykenee rajoittamaan sen alueilla liikkuvan tietoliikenteen valtion sisäiseen (Kiviharju, Huttunen & Kantola, 2020, s. 193; Ristolainen, 2017, s. 373;). Lisäksi valtio on säätänyt lakeja edistääkseen tavoitettaan, kuten esimerkiksi Yarovaya -lain (Закон Яровой), jolla valtio on kasvattanut pääsyään internetissä olevaan sisältöön, sekä lisäännyt elektronista valvontaansa (Greiman, 2017, s. 149).

Venäjän katsotaan kehittävän lisäksi puolustuksellista ja hyökkäyksellistä kapasiteettiaan operoidakseen tehokkaammin kyberavaruudessa ja valmistautuakseen yhteenottoihin (Ristolainen, 2017, S. 376). Konflikti- ja sodankäytön strategiassaan valtio painottaa paljon kyberavaruudessa tapahtuvaa toimintaa

ja kuvaa kyberavaruudessa tehtäviä toimia uutena toimintaa muuttavana metodina (Cole & Noel, 2021, s. 49; Kostyuk & Zhukov, 2019, s. 320). Kybertoimintaympäristöä ajatellaan käytettävän laajasti perinteisten sodankäynnin rinnalla muiden epäsymmetristen tekniikoiden, kuten informaatiovaikuttamisen kanssa, jotta valtio saavuttaa informaatiollisen ylivoiman. (Cole & Noel, 2021, s. 49, Gunneriusson & Ottis, 2013, s. 100; Granåsen & Jaitner, 2019, s. 197).

Venäläiset näkemykset eroavat länsimaalaisen kyberoperaatioiden käsityksestä, ja valtiossa käytetään kyberoperaatio -termin sijasta informaatio-operaatio-termiä kuvaamaan verkossa tapahtuvaa toimintaa. Venäjän näkökulmasta informaatio-operaatioilla viitataan toimiin, joiden tarkoituksena on vaikuttaa vastustajan informaatioon ja informaatiojärjestelmiin, sekä suojella omia vastaavia järjestelmiä ja valtion infrastruktuuria. (Granåsen & Jaitner, 2019, s. 197). Venäjän valtion ajattelutavassa informaatio-operaatioita voidaan käyttää esimerkiksi informaatiovaikuttamiseen, strategiseen harhauttamiseen, hyökkäyksellisien toimien toteuttamiseen, sekä hybridisodankäyntiin (Cole & Noel, 2021, s. 49). Kansallisessa sotilasstrategiassa kuvataan operaatioiden tarkoituksena olevan informaatioylivoiman saavuttaminen. Informaatio-operaatioita käytetään venäläisessä ajattelutavassa informaatiosodankäynnin toteuttamiseen, jolla viitataan vahingon tuottamiseen informaatiojärjestelmissä, psykologiseen vaikuttamiseen kansaan, sekä valtioiden päätöksentekoprosesseihin vaikuttamiseen (Granåsen & Jaitner, 2019, S. 197).

Yleisesti Venäjän kohdalla keskustellessa aineistossa korostuu vahvasti informaation hallintaan liittyvä toiminta, sekä informaatioturvallisuus. Lisäksi Venäjää kuvataan usein aineistossa sotilaallisesta ja uhkaavasta näkökulmasta. Venäjän on tutkimusmateriaalissa sanottu mahdollisesti toteuttaneen informaatio-operaatioita muun muassa lamauttaakseen ukrainalaisia telekommunikaatiovälineitä DDoS-hyökkäyksellä vuonna 2013, sekä saman valtion sähköverkkoja vuonna 2015 BlackEnergy-haittaohjelmalla (Boyte, 2017, s. 59; Dupuy, ym., 2020, s. 98). Lisäksi valtion on sanottu mahdollisesti toteuttaneen informaatio-operaation vaikuttaakseen USA:n vuoden 2016 presidentinvaalien tuloksiin Martins, 2018, s. 32-33; Darraj, Sample & Cowley, 2017, s. 93). Mikäli sanottu tekijä voidaan vahventaa näiden tapausten kohdalla, sopisivat ne aikaisemman kuvatun informaatiosodankäynnin määrityksen alaisiin toimiin.

4.5.3 Kiina

Kiinaa kuvataan tutkitussa materiaalissa usein uhkana muille valtioille, joka voi mahdollisesti toteuttaa toimia muita valtioita kohtaan (esim. Dupuy, ym., 2020, s.102-103 & Cole & Noel, 2021, s. 48). Vaikka Kiina on tutkimusmateriaalissa usein keskustelun kohteena kyberhyökkäyksistä puhuttaessa, ei tutkimusmateriaalissa löydetty tapauksia Kiinan toteuttamista kyberhyökkäyksistä, jotka olisivat vaikuttaneet toisen valtion toimintaan tuhoavalla tai häiritsevällä tavalla. Sen sijaan Pohjois-Koreaan assosioidut kyberhyökkäykset ovat sanottu usein lähteneen Kiinan alueilta sijainneista lähteistä (Kong, Lim, & Kim, 2019, s. 15-

16). Itse Kiinasta käytävät keskustelut painottuvat vahvasti tiedon kontrolloimisen ja kokoamisen liittyviin osa-alueisiin. Saatavissa olevista tiedoista voidaan kuitenkin havaita kyberoperaatioiden liittyviä teemoja, joita käydään valtion kohdalla seuraavaksi läpi.

Kiinan valtion ympärillä käytävä keskustelu kyberavaruuden toiminnasta on pääasiassa keskittynyt tiedustelutoimintaan. Tutkitun materiaalin sisällössä havaittiin lukuisia mainintoja, joissa Kiinan on sanottu toteuttaneen kyberavaruudessa tiedustelutoimintaa kerätäkseen erityisesti immateriaalioikeuksien koskevaa tietoa kiinalaisyritysten käyttöön. (Akoto, 2021, s. 3-4; Payne & Mienie, 2019, s. 42; Nye, 2017, s. 65). Toiminnan tarkoituksena sanotaan olevan kilpailuedun saaminen muita valtioita kohtaan (Akoto, 2021, s. 4) ja Kiinan huomattavaa taloudellisen kasvun ylläpitäminen. Erityisesti viimeksi mainittua pidetään tärkeänä tekijänä valtion luotettavuuden ylläpidolle Kiinan kansan näkökulmasta (Nye, 2017, s. 58). Kiinan viranomaiset ovat kuitenkin kieltäneet toimivansa kyberavaruudessa tämänkaltaisen tiedustelutoiminnan avulla muita valtioita kohtaan (Payne & Mienie, 2019 s. 43).

Puolustuksellisesta näkökulmasta Kiinan katsotaan pyrkivän rajoittamaan sen rajojen lävitse kulkevaa tietoliikenteen sisältöä. Se on ulkomaisten vaikutteiden ja vaikutusoperaatioiden estämiseksi luonut Suureksi palomuuriksi kutsutun järjestelmän, jolla ulkomailta saapuvaa tietoliikennettä suodatetaan. Tietoliikenteen rajoittaminen katsotaan johtuvan uhkakuvasta, jossa ulkomaalaisten ja erityisesti länsimaalaisten vaikutteiden pelätään aiheuttavan levottomuutta ja kapinointia valtion kansalaisten keskuudessa. Sisäisen harmonian ylläpitämistä nähdään Kiinassa elintärkeänä toimena valtion jatkuvuudelle ja selviytymiselle, minkä seurauksena valtio pyrkii kontrolloimaan sen sisäisessä ympäristössä liikkuvaa informaatiota ja esitettyjä mielipiteitä. Kontrollointia toteutetaan myös hallinnoimalla valtion sisäisessä tietoliikenteessä kulkevaa informaatiota, jotta mahdollisia valtion sisäisiä uhkia kyetään ehkäisemään ja pysäyttämään (Cole & Noel, 2021, s. 51; Ristolainen, 2017, s. 376). Tavoitteidensa edistämiseksi Kiina on myös toteuttanut muun muassa lakiuudistuksia, jotka pyrkivät tiukentamaan ja keskittämään valtion kontrollia tietovirroista ja -laitteistoista (Greiman, 2021, s. 149).

Lisäksi valtion havaitaan kohoavasti painottavan valtion sotilaalliseen kapasiteettiin kehittämistä kyberavaruudessa. Kiinan vapautusarmeija kävi rakenneuudistuksen vuonna 2015, jonka aikana armeijaan luotiin uusi asevoimien haara. Strategiseksi tukijoukoksi kutsuttu sotilashaara sisältää muun muassa kyber-, sähköisen- ja psykologisen sodankäynnin yksiköiden toiminnan. Kiina katsookin informaatiollisen sodankäynnin olevan avainasemassa sotilaalliseen menestyksen varmistamiseksi. Tämä menestys saavutetaan lamauttavalla vastustaja informaatiojärjestelmiä hyödyntämällä, joista vastustaja on riippuvainen. Lisäksi menestystä saavutetaan dominoivan aseman luomisella informaatiokentällä (Cole & Noel, 2021, s. 48, 50-51).

4.5.4 Valtion ulkopuoliset toimijat

Tutkimuksen aikana havaittiin huomattavan paljon mainintoja valtion ulkopuolisten toimijoiden käytöstä kyberoperaatioiden toteuttamisessa. Näihin toimijoihin voidaan luokitella ryhmiä tai yksilöitä, jotka toteuttavat tai tukevat valtion kyberoperaatioita kuulumatta itse suoraan valtion organisaatioihin. Nämä voivat esimerkiksi toteuttaa hyökkäyksellisiä kyberoperaatioita valtion ohjaamana tai rahoittamana, sekä tukea valtiota muulla toiminnallaan (esim. Gisel & Ojenik, 2018, s. 7; Czosseck, 2013, s. 16-18; Martins, 2018, s. 35). Valtioiden ulkopuolisiin toimijoihin voivat kuulua erilaisissa konteksteissa esimerkiksi hakkeriryhmät, yksilöt, yksityiset organisaatiot tai rikollisryhmät (esim. Martins, 2018, s. 42; Dupuy, ym., 2020, s.102).

Valtiot käyttävät kyberoperaatioissa ulkopuolisia toimijoita monista syistä. Yleisempiä syiden mainintoja olivat attribuution vaikeuttaminen, sekä toiminnan toteuttamisen hinta. Mikäli ulkopuolinen toimija toteuttaa valtion tukemana kyberhyökkäyksen, on hyökkäyksen kohteella haastavampaa löytää attribuutiota valtioon. Lisäksi hyökkäyksen suunnitellulla valtiolla on parempi mahdollisuus kieltää osallisuuteensa tapaukseen. (esim. Martins, 2018, s. 35-36, Kello, 2013, s. 36; Czosseck, 2013, s. 2) Hyökkäyksen ulkoistaminen valtion ulkopuolisille toimijoille voi usein olla myös halvempaa toteuttaa suhteessa itse toteutettuun kyberhyökkäykseen (Gisel & Ojenik, 2018, s. 14; Martins 2018, s. 36). Lisäksi valtio voi myös kääntyä ulkopuolisien toimijoiden puoleen, mikäli valtiolla ei ole omaa kapasiteettia toteuttaa kyberoperaatiota omalta osaltaan. (Czosseck, 2013, s. 16).

Tutkimuksessa mainintoja ulkopuolisten toimijoiden mahdollisesta käytöstä havaittiin eniten kohdistuvan Venäjän valtioon (esim. Cole & Noel, 2021 s. 49-50; Burita, 2020, s. 59). Lisäksi Iranin ja Kiinan toimintaan liitettiin valtion ulkopuolisten toimijoiden mahdollista käyttöä kyberoperaatioissa (esim. Kello, 2013, s. 35-36; Martins 2018, s. 42).

5 TUTKIMUSTULOSTEN ANALYYSI

5.1 Johtopäätökset

Tutkimustulosten perusteella eniten keskustelua käytettävistä hyökkäysmetodeista kohdistuu haittaohjelmistojen ja palvelunestohyökkäyksien kohdalle. Metodin mukaan hyökkäykset voivat aiheuttaa vahinkoja tietojärjestelmille tai häiritä järjestelmien toimintaa. Eniten hyökkäyksiä vaikutettaisiin kohdistettavan kriittinen infrastruktuuria ja valtioiden organisaatiota kohtaan.

Puolustustoiminnassa puolestaan nousee yleiseksi huolenaiheeksi kriittisen infrastruktuurin turvallisuus, ja suojeltavia järjestelmiä pyritään turvaamaan monenlaisilla käytännön ja valtiollisen tason tekniikoilla. Tarkistellut valtiot kokevat kybermaailman mahdollisena hyökkäysalueena näitä kohtaan. Valtiot pyrkivät myös suojautumaan hyökkäyksiltä monenlaisilla tekniikoilla, kuten tietoliikenteen rajoittamisella ja kyberpuolustuksen kehittämisellä. Erityisesti USA:n kohdalla korostetaan alttiutta kyberhyökkäyksille, joka johtuu valtion riippuvuussuhteista tietoverkoista.

Aikaisemmin tapahtuneet kyberhyökkäykset ovat erityisesti lisänneet valtioiden huomiota puolustustoiminnan kehittämisen tarpeestaan. Kriittisen infrastruktuurin oleminen valtioiden erityisenä suojelukohteena selittyy näiden toiminnan merkityksellä koko yhteiskunnan toimivuuteen. Kriittiseen infrastruktuuriin kohdistettavien kyberoperaatioiden katsotaan vaativan kuitenkin tarkkaa erityistietoa kohteena olevien järjestelmien toimivuudesta, minkä nähdään selittävän kyberoperaatioiden vähälukuisuutta näitä kohtaan. Vain valtiolliseen alaisuuteen kuuluvilla toimijoilla katsotaan materiaalissa olevan kapasiteettia vaikuttaa laajasti kriittistä infrastruktuuria kohtaan.

Kyberoperaatioita katsotaan käytettävän yhtenä hybridisodankäynnin toteutustapana. Toisaalta kyberoperaatioista havaittiin hyvin vähän mainintoja sodankäynnin aikaisessa toiminnassa tutkittuna ajanjaksona. Tilanteessa käydään yhä keskustelua, jossa pyritään löytämään vastauksia sotilaalliseksi voimankäytöksi määriteltävästä toiminnasta kybermaailmassa. Vaikka tarkempia

määrityksiä ei toistaiseksi ole tehty, on tulkintavälineenä pyritty korostamaan kyberoperaatioiden vaikutuksia kohteeseensa ja operaation kohteen merkitystä.

Toistaiseksi kyberoperaatiot ovat olleet enimmäkseen rauhan aikana sovellettava toimintaväline valtioiden toiminnassa. Toisaalta monien valtioiden kohdalla voidaan havaita viitteitä, että nämä pyrkivät kehittämään, kasvattamaan ja uudelleenorganisoimaan sotilaallista kapasiteettiaan kyberoperaatioiden käyttämiseksi sodankäynnissä. Esimerkiksi Venäjän ja Kiinan mainitaan tutkimusmateriaalissa kehittäneen viimeisen kymmenen vuoden aikana tämänkaltaista kapasiteettia. Materiaalissa molempia valtioita kuvataan näkevän kyberoperaatioita ja informaation hallinnan merkittävänä osa-alueena sotilaallisen toiminnan toteuttamiseen, mikä osaltaan selittää kapasiteetin kehittämisen halukkuutta.

Venäjän ja Kiinan kerrotaan lisäksi pyrkivän ylläpitämään kyberpuolustustaan tiukemmalla valtion sisäisten tietoverkkojen kontrollilla, kun taas USA:n kerrotaan pyrkivän tukemaan avoimen internetin toimintaa. Tilanteessa USA:n valtion kuvataan rajoittaneen kapasiteettiaan kontrolloida yksityisomistuksessa olevia tietoliikennejärjestelmiä, joihin valtion toiminta pohjautuu. Tämän takia valtion kerrotaan pyrkivän ehkäisemään kyberhyökkäysten tapahtumista muilla tavoilla, kuten keskustelemalla kansainvälisien sopimuksien soveltamisesta kyberavaruudessa tehtävään toimintaan.

5.2 Pohdinta

Tutkimuksen tuloksia tarkastellessa voidaan tutkimuksen katsoa onnistuneen tavoitteissaan. Tutkimuksen tulokset muodostavat aikaisemman kirjallisuuden pohjalta uuden synteesin, joka selittää kokonaisvaltaisesti kyberoperaatioiden toimintamenetelmiä. Tulokset avaavat muun muassa yleisimpiä kyberoperaatioiden hyökkäysmetodeja ja vaikutuksia kohteeseensa, sekä valtioiden toteuttamia puolustuskeinoja. Lisäksi tutkimustuloksissa avataan valtioiden näkökulmia, jotka ovat eniten mainittuja materiaalissa. Tutkimustulosten kokonaisvaltaisen tarkastelun perusteella voidaan sanoa, että kaikkiin tutkimuskysymyksiin onnistuttiin vastaamaan tuloksissa.

Suoritettu tutkimus luo tulostensa pohjalta uuden ymmärryksen, jolla kyberoperaatioiden toimintaa voidaan ymmärtää kokonaiskattavasti. Tätä uutta ymmärrystä voidaan käyttää tulevaisuuden julkaisujen ja tutkimusten pohjana. Luodun ymmärryksen avulla voidaan paremmin ennakoida tulevia kyberoperaatioiden toimintatapoja, sekä hahmottaa ja yhdistää tapahtumia laajempaan kontekstiin. Lisäksi tulokset luovat pohjaa uuden teorian luomiseksi, jonka pohjana voidaan käyttää tutkimustuloksissa havaittuja havaintoja.

Tutkimustulosten sisällössä havaittiin hyvin mielenkiintoisena yksityiskohtia. Vaikka valtiot ovat kiinnittäneet erityistä huomiota kriittisen infrastruktuurin suojaamiseen, ei artikkeleiden sisällössä havaittu laajasti mainintoja tarpeesta suojata muita hyökkäysten pääasiallisten kohteita. Nämä kohteet olivat poliittisia ja valtiollisia organisaatioita. Asiaa voinee selittää, että kyberhyök-

käyksissä poliittiseen ja valtiollisiin organisaatioihin kohdistuneet vaikutukset ovat toistaiseksi jääneet pienemmiksi suhteessa kriittiseen infrastruktuuriin. Lisäksi ilmiötä selittänee kriittisen infrastruktuurin laajempi vaikutus yhteiskuntaan valtion organisaatioiden ohella. On myös mahdollista, että valtiollisiin organisaatioihin kohdistetaan kyberavaruudessa enemmän tiedustelutoimintaa suhteessa toimintaan vaikuttaviin kyberoperaatioihin nähden. Koska tutkimuksen painopistettä kohdistui tiedustelutoiminnan ulkopuolelle, vaatii tämä vielä jatkotutkimuksia asian tarkemmaksi selvittämiseksi.

Tutkimustuloksissa havaitaan kohteena olleen valtion sanovan usein kyberhyökkäyksen toteuttajana olleen toisen valtion, jonka kanssa tällä on ollut poliittisia jännitteitä kyberhyökkäyksen tapahtuessa. Ilmiö voi mahdollisti johtua esimerkiksi poliittisten jännitteiden tuomasta vaikutuksesta päätökseen toteuttaa kyberhyökkäyksiä. Toisena mahdollisena vaihtoehtona on, että poliittiset jännitteet suurentavat mahdollisuutta kohteena olleen valtion sanoa julkisesti jännitteiden vastapuoli kyberhyökkäyksen toteuttajaksi. Johtuen julkisen attribuution puutoksista johtuvista rajoitteista, ei tutkimustulosten pohjalta kyetä kuitenkaan arvioimaan mahdollisia tarkempia syitä ilmiölle. Ilmiötä voinee mahdollisesti tutkia, mikäli tulevaisuuden tutkimukselle saadaan tietoja suljettujen ovien takana tehtävästä päätöksenteosta. Tämä kuitenkin edellyttää mahdollisesti salassa pidettävien tietojen käsittelemistä, jotka ovat tämän tutkimuksen rajauksen ulkopuolella.

Lisäksi kyberoperaatioiden käytöstä sodankäynnissä havaittiin olevan hyvin vähän esimerkkejä artikkeleiden sisällössä. Ilmiö voi johtua valtionvälisten sotatilanteiden vähyydestä tutkittuna ajanjaksona. Tilanteessa ovat tapahtuneet kyberoperaatiot luontaisesti ilmenneet lähempänä rauhaa ja harmaata vyöhykettä vastaavaa tilannetta. Tilanteen johdosta voitaneen sanoa, että maailmanpolitiikan tilanne vaikuttaa osaltaan kyberoperaatioiden luonteen havaintoihin ajanjakson aikana.

Merkittävänä huomionkohteena havaittiin myös, että artikkelien kirjoittajien tuottaman sisällön painopiste käsitteli USA:n kohdalla enimmäkseen puolustuksellista näkökulmaa. Venäjän ja Kiinan käsittelyssä havaittiin puolestaan yhtä lailla myös hyökkäyksellistä näkökulmaa puolustuksen rinnalla. Usein myös viimeksi mainittuja valtioita havaittiin esitettävän uhkaavana toimijana tutkitussa materiaalissa. Kollektiivista ilmiötä saattaa selittää, että tutkitun materiaalin painopiste kohdistui erityisesti länsimaalaisista instituutioissa luotuun materiaaliin. Materiaali saattaa täten heijastella alueella olevia poliittisia näkemyksiä. Toisaalta arvion varmistaminen edellyttää ilmiön tarkastelua tarkemmin mahdollisessa tulevaisuuden tutkimuksessa, jotka etsivät mahdollisia vaikutuksia havaitulle ilmiölle.

Lisäksi on mielenkiintoista, että Kiina nousee tutkitussa materiaalissa keskusteluun, vaikka valtion sanotaan toteuttaneen tuhoisten kyberoperaatioiden sijasta vaan tiedustelutoimintaa. Syitä havainnolle voivat olla esimerkiksi valtioin yleinen poliittinen ja taloudellinen merkitys maailmanpolitiikassa. Myös poliittiset jännitteet suurien valtioiden välillä voivat mahdollisesti osaltaan lisätä tutkitussa materiaalissa esiintynyttä uhkakuvaa valtiosta. Mikäli Kiinan toi-

minnan luonne voidaan varmentaa tulevaisuudessa attribuution parantumisen myötä, voidaan Kiinan havaita noudattaneen toiminnassaan parhaiten kansainvälisen oikeuden periaatteita tuloksissa esitellyistä valtioista. Toisaalta tiedustelutoiminnan toteuttaminen vaikuttaa osaltaan aiheuttavan muissa valtioissa uhkakuvan nousua Kiinasta, mutta tämän esille nostaminen voi olla myös poliittisten jännitteiden aiheuttamaa vaikutusta muissa valtioissa.

Kyberoperaatioiden vaikutukset vaikuttavat myös olevan enimmäkseen lyhytaikaisia tutkittujen tapausten pohjalta. Suurimmassa osassa tutkittuja tapauksia on kohteen toiminta saatu palautettua normaaliksi kahden viikon sisällä kyberhyökkäyksestä. Tapausten pohjalta on viitteitä, että kyberhyökkäysten vaikutukset ovat rajattuja, ja että kohteiden palautumiskyky on ollut tehokasta. Tilanne voi johtua, koska kyberhyökkäysten rinnalla ei tapauksissa ole käytetty muita toimia tai kyberhyökkäyksiä operaatioiden tukemiseksi. Toisaalta voi olla, että kyberoperaatioiden vaikutuksia pyritään pääsääntöisesti rajaamaan, jotta vaikutukset pysyisivät sodankäynnin kynnyksen alapuolella. Tällöin tämä osaltaan viittaisi, että kansainvälisen oikeuden periaatteet vaikuttavat kyberoperaatioiden vaikutusten luonteeseen.

Tutkimustuloksissa havaittiin myös materiaalissa esiintyvän yleisimpinä hyökkäysmetodeina haittaohjelmat ja palvelunestohyökkäykset. Ihmisten manipulaation käyttäviä hyökkäyksiä havaittiin puolestaan muita metodeja vähemmän. On mahdollista, että ihmisten manipulaatioon pohjautuvia hyökkäysmuotoja käytetään enemmän tiedustelutoiminnan, informaatiovaikuttamisen tai siviilipuolen rikosten toteuttamiseen. Asiaan vastaaminen vaatii kuitenkin muiden tutkimuksien tuloksien tarkastelua ja yhdistelyä, jotta ihmisten manipulaation mahdollista merkitystä näissä konteksteissa voidaan tarkemmin selventää. Lisäksi lisätutkimuksilla tulevaisuudessa tuottaa näihin kysymyksiin vastaamiseksi.

5.3 Tutkimuksen luotettavuus

Tutkimuksen lopputulokset perustuvat tieteellistä artikkelien pohjalta luotuun ymmärryksen kyberoperaatioiden käytöstä valtioiden välisessä vuorovaikutuksessa. Materiaali valittiin, koska akateemisten julkaisujen koettiin tarjoavan parhaimman edellytyksen kokonaiskattavan ymmärryksen luomiselle ilmiöstä. Koska näiden tarjoama tiedon havaittiin hajanaiseksi tutkimuksen alussa, katsottiin Grounded theory -metodologian tarjoavan parhaimmat edellytykset uuden tiedon tuottamiseen materiaalin pohjalta. Tutkimuksen päättyessä havaittiin tutkimusmetodin olleen sovelletun samalla lailla, kuin miten sitä kuvaava lähdeaineisto on tutkimusmetodin soveltamisen esittänyt. Tämän perusteella tutkimuksen katsottiin olevan toteutettu oikeaoppisesti, mikä osaltaan katsotaan validoivan saatujen tutkimustulosten luotettavuutta. Lisäksi tutkimustulosten voidaan katsoa olevan tarvittaessa toistettavissa samaan aineistomateriaalin avulla. Lisäksi tutkimustulosten katsotaan tuoneen uutta ymmärrystä kyberoperaatioiden toimintamenetelmistä ja käytöstä ilmiönä. Näistä aikaisem-

mista syistä tutkimuksen katsotaan onnistuneen kokonaisuudessaan, ja tutkimustulosten edustavan parhainta ymmärrystä, jota salassa pidettävälle toiminnalle on toistaiseksi saatavissa julkisessa aineistossa.

Tutkimuksen tuloksia tarkastelleessa on otettava huomioon, että tutkimusaineisto pohjautuu julkiseen tietoon. Tilanteessa tutkimustuloksien ulkopuolelle voivat jäädä ymmärrettävästi salassa pidettävät aineistot, joissa mahdollisesti käsitellään kyberoperaatioiden toteuttamista. Kyseisessä aineistossa voidaan mahdollisesti käsitellä esimerkiksi kyberoperaatioiden suunnitteluun ja toteuttamispäätökseen liittyvää tietoa, jota ei tutkimuksen kohdemateriaalissa ilmennyt laajasti. Asian selvittäminen vaatinee lisätietojen tuomista julkisuuteen, jotta asia voidaan ottaa huomioon tulevaisuuden tutkimuksissa.

Lisäksi on mahdollista, etteivät kaikki aikaisemmista kyberoperaatioista ole saatettu julkiseen tietoon. Tällaisiin kyberoperaatioihin voivat mahdollisesti kuulua esimerkiksi hyökkäykselliset operaatiot, joiden vaikutukset eivät ole merkittävästi näkyneet julkisuudessa. Voi myös olla, että joitain aikaisemmista hyökkäyksistä ei olla havaittu olleen valtiollisen toimijan toteuttama. Mikäli vastaavanlaisia tapauksia nousee mahdollisesti esille monia tulevaisuudessa, voivat ne osaltaan nostaa tarvetta toteutetun tutkimuksen uudelleenarvioinnille. Toisaalta nykyisen saatavissa olevan tiedon valossa voidaan tutkimuksen tuloksia pitää tietoon nähden luotettavina.

On myös hyvä huomioida, että tutkimustuloksissa ei havaittu tarkkoja tietoja puolustuksellisien kyberoperaitioiden toteutuksista. Ilmiö voi johtua mahdollisesti tarkkojen puolustustoimien salassa pidettävyydestä. Mikäli sovellettavat tarkat puolustusmetodit tuodaan julkisuuteen, luo tiedon julkisuus ulkopuolisille mahdollisuuden havainnoida puolustuskeinoista mahdollisesti löytyviä heikkouksia. Tietoa voidaan käyttää tällöin hyödyksi kyberhyökkäysten suunnittelussa ja toteutuksessa. Ilmiö selittäisi osaltaan tiedon vähyyttä julkisuudessa, mikä osaltaan vaikuttaisi tutkimustuloksissa havaittujen tulosten sisältöön.

Lisäksi valtioilla itsellään voi olla laajempaa tietoa kyberoperaatioiden aikaisemmista tapauksista ja laajemmasta yleisestä käytöstä, kuin mitä julkisessa tiedossa on saatavilla. Erityisesti asia voi koskea hyökkäyksen attribuutiota käsittelevää tietoa ja metodeja, joita valtiot käyttävät mahdollisen hyökkääjän tunnistamisessa. Tutkimuksen pohjalta ei kyetä kuitenkaan arvioimaan valtioiden ymmärryksen mahdollista laajuutta. Laajuuden arvioiminen edellyttää valtioiden tietämyksen tuomista kokonaisuudessaan julkisuuteen, mitä saattaisi osaltaan tuoda haasteita valtion turvallisuuden ylläpidossa.

6 LOPPUSANAT JA MAHDOLLISET JATKOTUTKIMUKSET

6.1 Mahdollisia jatkotutkimuksien aiheita

Tämä tutkimus tarkastelee valtioiden välisessä vuorovaikutuksessa suoritettuja kyberoperaatiota vuodesta 2010 eteenpäin, jotka ovat vaikuttaneet valtioiden normaaliin toimintaan. Toteutetun tutkimuksen rajaus jättää tutkimuksen ulkopuolelle monia aihealueeseen liittyviä seikkoja, joiden tarkasteleminen voi tarjota tulevaisuuden tutkimuksessa mielenkiintoisia tuloksia. Lisäksi toteutetun tutkimuksen aikana havaittiin aineistossa uusia mielenkiintoisia yksityiskohtia, ilmiöitä ja näkökulmia, joita pidettiin mielenkiintoisina tulevaisuuden tutkimusten näkökulmasta. Seuraavaksi käsitellään muutamia vielä mainitsemattomia aiheita, jotka tutkimuksen suorittamisen aikana havaittiin mielenkiintoisiksi tutkimuskohteiksi.

Ensimmäiseksi tutkimusaineiston sisällössä havaittiin huomattava määrä keskustelua tiedustelutoiminnan toteuttamisesta kybermaailmassa. Tutkimuksen rajauksen mukaisesti, tiedustelua ei tarkasteltu laajasti tutkimuksen sisällössä. Koska materiaalissa havaittiin paljon mainintoja tiedustelusta, voidaan todeta saatavissa olevan tarpeeksi tietoa tutkimusten toteuttamiseksi aiheesta. Lisäksi tutkimuksen toteutuksen aikana ei havaittu laajoja aikaisempia tutkimuksia aiheesta. Tilanne mahdollistaa potentiaalisen uuden tutkimuskohteen tieteenalalle. Tiedustelun tutkinnalla voidaan laajentaa alan ymmärrystä valtioiden toiminnasta kyberavaruudesta. Lisäksi aihetta tutkimalla voidaan myös täydentää tässä tutkimuksessa havaittuja tuloksia, ja luoda kokonaisymmärrystä valtioiden toiminnasta tietoverkoissa.

Toisena mielenkiintoisena tutkimuksen kohteena havaittiin valtioiden toiminnan ulkopuoliset toimijat kybermaailmassa, joita myös osaltaan käsiteltiin tämän tutkimustulosten sisällössä. Aihetta voidaan tutkia tarkastelemalla esimerkiksi toimijoita, jotka toimivat täysin itsenäisesti valtioiden ohjauksen ulkopuolella. Tällöin voidaan tarkastella, milloin ja miten nämä toimijat päättävät itsenäisesti toimia yksittäistä valtiota kohtaan. Lisäksi tulevaisuuden tutki-

muksissa voidaan tarkastella toimijoiden välisiä dynamiikkoja, ja miten ne toimivat keskenään valtioiden välisessä vuorovaikutuksessa.

Tutkimuksessa havaittiin kyberoperaatioiden taustalla vaikuttavan poliittisia taustatekijöitä. Tulevaisuuden tutkimuksessa voidaan tarkastella yksityiskohtaisemmin poliittisten jännitteiden vaikutusta kyberoperaatioiden käyttöön. Esimerkiksi politiikan tiedekunnissa voidaan tulevaisuudessa luoda teorioita poliittisten jännitteiden vaikutuksista kyberhyökkäysien toteuttamiseen. Mahdolliset tulevaisuuden jatkotutkimukset voivat pyrkiä selittämään myös kyberoperaatioiden taustalla vaikuttavia poliittisia tekijöitä laajemmin, ja avaamaan historiallista kehitystä valtioiden it-teknologian käytöstä.

Lisäksi kyberoperaatiot ovat ilmiönä melko uusia, ja ovat joiltaan toimintatavoiltaan vielä toistaiseksi kehittymässä oleva. Tilanteessa voidaan nähdä olevan tarvetta tutkia ilmiön kehitystä myös tulevaisuudessa. Tällöin voidaan toteuttaa jatkotutkimus, joka uudelleenarvioi tämän tutkimuksen johtopäätöksiä uuden tiedon pohjalta. Esimerkiksi jatkotutkimus voidaan toteuttaa 2030-luvun jälkipuoliskolla, jolloin valtioiden toiminnasta on saatavissa vähintään kymmenen vuoden edestä lisää tietoja. Tällöin voidaan myös laajemmin arvioida, miten kyberoperaatiot ovat kehittyneet ilmiönä vuosien saatossa, ja miten valtiot ovat sopeutuneet kyberoperaatioiden käyttömahdollisuuteen.

6.2 Lopuksi

Kyberoperaatiot ovat toistaiseksi olleet uusin väline, jonka avulla valtiot ovat pyrkineet kohdistamaan voimaansa toisia valtioita kohtaan. Ollessaan uusimpia käyttömetodeja, on niiden toiminnan luonteesta keskusteltu paljon monien tahojen toimesta. Havaittujen todisteiden puitteissa on näiden käyttötavoista saatavilla tarpeeksi tietoa näiden yleisen toimintakaavan tutkimiselle myös tulevaisuudessa.

Todisteiden puitteissa kyberoperaatioiden käyttöön on alkamassa muodostumaan oma normistonsa; Hyökkäyksellisiä operaatioita toteutetaan ensisijaisesti kahdenlaisilla tekniikoilla, ja näiden käyttöä kohdistetaan yleisesti tiettyjä organisaatioita kohtaan. Lisäksi puolustuksen painopisteet ovat näkyvissä selvästi saatavissa olevassa aineistossa. Kyberoperaatiot ovat olleet tutkittuna ajanjaksona toistaiseksi pääasiassa rauhanaikana käytettäviä tekniikoita, vaikka toisaalta nämä vaikuttavat korreloivan valtioiden poliittiset jännitteiden kanssa.

Kyberoperaatioiden käyttö tulee hyvin todennäköisesti jatkumaan myös seuraavan vuosikymmenen aikana valtioiden välillä. Kyberoperaatiot ovat vaikuttamisen keinoja, joiden käyttö on riippumaton operaation kohteen ja toteuttajan fyysisitä sijainneista. Lisäksi kyberoperaatioiden käytön etuina ovat käytön kiistämisen mahdollisuus tämän toteuttaneelle valtiolle. Kyberoperaatiot vaikuttaisivat toistaiseksi pysyvän valtioiden vaikuttamisen keinoina, joita voidaan soveltaa heikkouksien löytämisen ja huolellisen valmistelun jälkeen.

Toistaiseksi ei ole nähtävissä kovin suuria merkkejä, että kyberoperaatioiden käyttö päättäisi valtioiden välillä olevan rauhan. Aikaisemmat tapaukset

ovat osoittaneet, että kyberoperaatioiden takia ei ole toistaiseksi haluttu eskaloida valtioiden välisiä suhteita. Täten voidaan sanoa, että kyberoperaatioiden vaikutukset ovat toistaiseksi pysyneet kohtuullisina valtioille. Rauhanaikainen tilanne vaikuttaa toistaiseksi pysyvän kyberoperaatioiden käytön aikana, ja muutos tilanteeseen vaikuttavan riippuvan enemmän valtioiden välisten suhteiden kokonaistilanteesta. Täten kyberoperaatiot vaikuttaisivat olevan enemmän käytettäviä vaikuttamisen työkaluja, jotka osaltaan heijastelevat valtioiden välisten suhteiden tilannetta.

LÄHTEET

Applegate, S. (2015). *Cyber Conflict: Disruption and Exploitation in the Digital age.* Teoksessa Lemieux, F (toim). *Current and emerging trends in cyber operations: Policy, Stradegy and Practice.* Basigstoke: Palgrave Macmillan. s. 19-36.

Banks, W. (2021). Cyber attribution and State Responsibility. *International Law Studies*, Vol. 97, 2021. s. 1039-1072.

Birks, M. & Mills, J. (2015). *Gorunded Theory: A Practical Guide.* (Toinen uud. painos). Lontoo: SAGE publications Ltd.

Borghard, E. & Lonergan, S. (2019). Cyber Operations as Imperfect Tools of Escalation. *Strategic Studies Quarterly, Vol. 13, Issue 3. (Fall 2019).* s. 122-145.

Broeders, D., Busser, E., Cristiano, F. & Tropina, T. (2022). Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand?. *Journal of Cyber Policy. Volume 7, Issue 1.* s. 97-135.

Buzatu, A. (2022). *Advanced Persistant Treat Groups Increasingly Destabilize Peace and Security in Cyberspace*. Teoksessa Shackelford, S., Douzet, F. & Ankersen, C. (Toim.) *Cyber Peace*. Cambridge: Cambrige University Press.

Chapple, V. & Seidl, D. (2015). *Cyberwarfare: Information operations in a connected world.* Burlington: Jonas & Barlett Learning

Clauzewitz, C. (1998). *Sodankäynnistä.* (H. Eskelinen, suom.) Smedjebacken: Art House.

Delerue F. (2020). *Cyber Operations and International Law.* Cambridge: Cambridge University Press.

European Comission. (2013). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Joint Communication To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, Brussels, 7.2.2013, JOIN(2013) 1 final.* Saatavissa: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001 Luettu 28.01.2024.

Friis, K. & Ringsmose, J. (Toim.) (2016). *Conflict in Cyberspace: Theoretical, stradegic and legal persperctives.* Abington: Routledge.

Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security. The MIT Press Journals.* 38(2). s. 41-73.

Gaycken, S. (2019). *Understanding offense in Cybersecurity.* Teoksessa Gaycken, S. (Toim.). *Cyber Defense -Politics, Operations and Capacity Building: CYBEF 2018, Nato Science for Peace and Security Series E: Human and Societal Dynamics – Vol. 147.* Amsterdam: IOS Press.

Gill, T., van Haaster, J. & Roorda, M. (2017). *Some legal and operational considerations regarding remote warfare: drones and cyber warfare revisited.* Teoksessa Ohlin, J (Toim.). *Reseach Handbook on Remote Warfare.* Gheltenham: Edward Elgar Publishing Limited.

Corbin, J & Strauss, A. (1990). Grounded Theory Research: Procedures, Canons, and Evaluative Criteria. *Qualitative Sociology*, Vol. 13(1), 1990. s. 3-20.

Goldsmith, J. (2013). How Cyber Changes the Laws of War. *The European journal of International Law. Oxford University Press*. 24(1) s. 129-138.

Green, J. (Toim.) (2015). *Cyberwarfare: A multidisciplinary analysis.* Abingdon: Routledge.

Harle, V. (Toim.) (2010). *Näkökulmia kansainvälisen politiikan tutkimukseen.* 3. uudistettu painos. Niini Finland: Tampere

Healey J. (Toim.) (2013). *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012.* Cyber Conflict Studies Association*:* USA

Hejase, H., Fayyad-Kazan, H. & Moukadem, I. (2020). Advanced Persistant Threats (APT): An Awareness Review. *Journal of Economics and Economic Education Research. Volume 21, Issue 6.* December 2020. s. 1-8.

Hendriksen, A. (2016). *Politics and the development of legal norms in cyber space.* Teoksessa Friis, K. & Ringsmose, J. (Toim). *Conflict in cyber space: Theoretical, stradegic and legal perspectives.* Abingdon: Routledge.

Heywood, A. (2019). *Politics.* 5th edition. Red Globe Press: London.

Hocking, B. & Smith, M. (1990). *World Politics: An Introduction to International Relations.* Hertfordshire: Harvester Wheatsheaf.

Hodges, D. & Creese, S. (2015). *Understanding cyber-attacks.* Teoksessa Green, J. (Toim.). *Cyber warfare: A multidisciplinary analysis.* Abington: Routledge. s. 33-60

Havu, E. & Höyhtiö, M. (2023). *Yritysten ja julkisten toimijoiden yhteistyö verkoistoituneen yhteiskunnan puolustamisessa – Laaja-alaisen vaikuttamisen huomioiminen kybertoimintaympäristössä.* Teoksessa Palokangas, M. (Toim.). *Sodan usvaa II: Sodankäynnin laaja-alaisuus.* Helsinki: Maanpuolustuskorkeakoulu.

International Court of Justice. (1986). Case Concerning Military And Paramilitary Activities in and Against Nicaragua (Nicaragua V. United States of America), Merits, Judgment of 27 June 1986. The Hague: International Court of Justice.

International Law Commission. (2001). Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, 2001. New York & Geneva: United Nations.

Josefsson, A., Anderson, J., Norlander, A. & Marcusson, B. (2019). Mission Command when waging cyber operations. Teoksessa G. Wijers, S. Brinkkemper & T. Wasserman (toim.), *Ingår i: 24th International Command and Control Research & Technology Symposium (ICCRTS)*, 2019, Vol. Topic 2. International Command and Control Institute.

Järvinen, P. (2018). *Kyberuhkia ja somesotaa; Digiaikana sinäkin olet etulinjassa.* Jyväskylä: Docendo Oy.

Kari, M. (2019). *Russian stradegic culture in Cyberspace: Theory of Stradegic Culture -a tool to Explain Russia's Cyber Threat Perception and Response to Cyber Threats.* Doctor's thesis. Jyväskylä: University of Jyväskylä

Kettani, H., & Wainwright, P. (2019). On the Top Threats to Cyber Systems. Teoksessa: *2019 IEEE 2nd international Conference on information and Computer technologies (ICICT). 14 – 17 March, 2019.* Kahului, Hawaii, USA. s. 175-179.

Kielitoimiston sanakirja. (2022). Politiikka. Haettu 29.02.2023 osoitteesta https://www.kielitoimistonsanakirja.fi/#/politiikka?searchMode=all

Laari, T. (2019). *#Kyberpuolustus, Kyberkäsikirja puolustusvoimien henkilöstölle.* Helsinki: Maanpuolustuskorkeakoulu.

Lehto, M. (2019). *Kybermaailman ilmiöitä ja määrittelyjä.* (Versio 11.0). Jyväskylä: Jyväskylän Yliopisto.

Leitzel, C. & Hillebrand, G. (2022). *Stradegic Cyberspace Operations Guide.* Carlisle, Us Army War Collage.

Lemieux, F. (toim.) (2015). *Current and emerging trends in cyber operations: Policy, Stradegy and Practice*. Basingstoke: Palgrave Macmillan. s. 1-15

Mačák, K. (2021). Unblurring the lines: military cyber operation and international law. *Journal of Cyber policy. Volume 6, Issue 3.* December 2021. s. 411-428.

Maness, R. & Valeriano, B. (2016a). *Cyber splillover conflicts: Transitions from cyber conflict to conventional foreign policy disputes?* Teoksessa Friis, K. &

Ringsmose, J. (Toim.). *Conflict in Cyberspace: Theoretical, stradegic and legal persperctives.* Abington: Routledge. s.45-65.

Ministry of Foreign Affairs, Italy. (2021). *Iitalian Position Paper on 'International Law And Cyberspace'.* Saatavissa: https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf Luettu 27.01.2024.

Metsämuronen, J. (2008). *Laadullisen tutkimuksen perusteet.* Jyväskylä: Gummerus Kirjapaino Oy. s. 16-29.

Palojärvi, P. (2009). *A Battle in Bits and Bytes: Computer Network attacks and the Law of Armed Conflict.* Helsinki: Hakapaino Oy.

Rahman, N., Sairi, I., Zizi, N. & khalid, F. (2020). The importance of Cybersecurity Education in School. *International Journal of Information and Education Technology. Volume 10, Issue 5.* May 2021. s. 378-382.

Rid, T. (2013). *Cyber war will not take place.* Lontoo: Hurst & Company.

Rowe, N. (2015). *The attribution of cyber warfare.* Teoksessa Green, J. (Toim.). *Cyber warfare: A multidisciplinary analysis.* Abington: Routledge. s. 61-72.

Sanastokeskus. (2018). *Kyberturvallisuuden sanasto.* Helsinki: Huoltovarmuuskeskus.

Sari, A. (2019). Turkish national cyber-firewall to mitigate countrywide cyber-attacks. *Computers and Electrical Engineering Volume 73.* January 2019. s. 128-144.

Shaw, M. (2021). *International Law*. Ninth edition. Cambridge: Cambridge University Press. s. 735-738.

Solis, G. (2022). *The Law of Armed Conflict: International Humanitarian Law in War.* 3rd edition. Cambrideg: Cambridege University Press.

Steed, D. (2015). *The stradegic inplications of cyber warfare*. Teoksessa Green, J. (Toim.). *Cyber warfare: A multidisciplinary analysis.* Abington: Routledge. s. 73-95.

Schmitt, M (Toim). (2017). *Tallinn Manual 2.0. on the Internatioanal Law Applicable to Cyber Operations / Prepared by the international Groups of Experts at the Invitation of the NATO Cooperative Cyber Centre of Excelence*. (Second Edition). New York: Cambridge University Press.

Takamaa, K. (2023). Johtava sotilaslakimies. Henkilökohtainen haastattelu. Helsinki, 06.12.2023.

The Federal Government of Germany. (2021). *On the Application of International Law in Cyberspace, Position Paper – March 2021*. Saatavissa: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf Luettu 27.01.2024.

Tsagourias, N. & Farrell, M. (2020). Cyber attribution: technical and legal approaches and Challenges. *The European Journal of International Law Volume 31, Issue 3.* s. 941-967

Ulkoasiainministeriö. (2021). *International law and cyberspace Finland's national positions.* Saatavissa: https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727 Luettu 27.01.2024.

United Nations. (1945). *The Charter of the United Nations.* Saatavissa: https://www.icj-cij.org/en/charter-of-the-united-nations Luettu: 05.08.2022

Valtioneuvosto (2018). *Valtioneuvoston päätös huoltovarmuuden tavoitteista (1048/2018)*. Helsinki; Valtioneuvosto.

Woltag, J.-C. (2015). *Cyber Warfare*. Teoksessa Lachenmann, F. & Wolfrum, R. (Toim.) (2017). *The Law of Armed Conflict and the Use of Force: The Max Planck Encyclopedia of Public International Law*. Oxford: Oxford University press. s. 313-321.

Zolotukhin, M., Hämäläinen, T., Kokkonen, T. & Siltanen, J. (2016). Increasing Web Service Availability by Detecting Application-Layer DDoS Attacks in Encrypted Traffic. *2016 23rd Conference on Telecommunications (ICT).* Jyväskylä: Jyväskylän Yliopisto & Jamk University of Applied Sciences.

LIITE 1: LUETTELO TUTKIMUKSEN SUORITTAMISEEN KÄYTETYISTÄ ARTIKKELEISTA JA MUISTA LÄHTEISTÄ

Akbariavaz, K., Tehrani, M. & Sabaruddin, J. (2020). Cyberattacks and the Prohibition of the Use of Force under Humanitarian Law with Reference to the Tallinn Manual. Teoksessa: Eze, T., Speakman, L. & Onwubiko, C. (Toim.) *Proceedings of the 19th European Conference on Cyber Warfare and Security, ECCWS 2020. 25- 26 June 2020.* Online. s. 451-458.

Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Research,* January 2021. s. 1-15.

Aslanoglu, R. & Tekir, S. (2012). Recent Cyberwar Spectrum and its Analysis. Teoksessa: Filiol, E. & Erra, R. (Toim.) *Proceedings of the 11th European Conference on Information Warfare and Security, ECIW 2012. 5-6 July 2012.* Laval: France. s. 45-52.

Barbosa, J. (2020a). Cyber Alliances and Proxy Cyber Warfare. Teoksessa Payne, B. & Wu, H. (Toim.). *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020. 12-13 March 2020.* Norfolk: USA. s. 33-38.

Barbosa, J. (2020b). Cyber Warfare: Can there be Small Cyber Military Powers? Teoksessa Payne, B. & Wu, H. (Toim.). *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020. 12-13 March 2020.* Norfolk: USA. s. 37-46.

Boyte, K. (2017). A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare. *International Journal of Cyber Warfare and Terrorism. Volume 7, Issue 2.* s. 54-69.

Burita, L. (2020). Analysis of Reports on Cyber Threats and Attacks Using Text Analytical Software. Teoksessa: Eze, T., Speakman, L. & Onwubiko, C. (Toim.) *Proceedings of the 19th European Conference on Cyber Warfare and Security, ECCWS 2020. 25- 26 June 2020.* Online. s. 50-60.

Cole, B. & Noel, G. (2021). Nation-State Perspectives on Information Operations and the Impact on Relative Advantage. Teoksessa Lopez, J., Siraj, A. & Perumalla, K. (Toim.) *Proceedings of the 16th International Conference on Cyber Warfare and Security, ICCWS 2021. 25 – 26 February 2021.* Online. s. 48-54.

Czosseck, C. (2013). State Actors and their Proxies in Cyberspace. Teoksessa Ziolkowski, K. (Toim.) *Peacetime Regime for State activities in Cyberspace.* Tallinn: NATO CCD COE publification. s. 1-30.

Darraj, E., Sample, C. & Cowley, J. (2017). Information Operations: The use of Information Weapons in the 2016 US Presidential Election. Teoksessa Scanlon, M. & Le-Khac, N. (Toim.) *Proceedings of the 16th European Conference on Cyber Warfare and Security, ECCWS 2017. 29 – 30 June 2017.* Dublin: Ireland. s. 92-101.

Dupuy, A., Iftimie, I., Nussbaum, D. & Pickl, S. (2020). Cyber as a Hybrid Threat to NATO's Operational Energy Security. Teoksessa: Eze, T., Speakman, L. & Onwubiko, C. (Toim.) *Proceedings of the 19th European Conference on Cyber Warfare and Security, ECCWS 2020. 25- 26 June 2020.* Online. s. 98-106.

Frantis, P. (2020). Cyberwar as a New Type of War? Teoksessa Payne, B. & Wu, H. (Toim.). *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020. 12-13 March 2020.* Norfolk: USA. s. 182-186.

Gisel, L. & Olejnik, L. (Toim.) (2018). *The Potential Human Cost of Cyber Operations.* (Report on the ICRC Expert Meeting in Geneva, 14-16 Nov. 2018). Geneva: The International Committee of the Red Cross.

Granåsen, D. & Jaitner, M. (2019). The Offensive Cyber Operations Playbook. Teoksessa: Cruz, T. & Simoes, P. (Toim.) *Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019. 4 - 5 July 2019.* Coimbra: Portugal. s. 194-201.

Greiman, V. (2017). Cyberwarfare and the Winds of Change in World Politics. Teoksessa Scanlon, M. & Le-Khac, N. (Toim.) *Proceedings of the 16th European Conference on Cyber Warfare and Security, ECCWS 2017. 29 – 30 June 2017.* Dublin: Ireland. s. 146-152.

Greiman, V. (2019). The Winds of Change in World Politics and the Impact on Cyber Stability. *International Journal of Cyber Warfare and Terrorism (2019), Vol.9 (4).*

Guitton, C. (2013). Modelling Attribution. Teoksessa Kuusisto, R. & Kurkinen, E. (Toim,) *Proceedings of the 12th European Conference on Information Warfare and Security ECIW 2013.* University of Jyväskylä, Finland. s. 91-97.

Gunneriusson, H. & Ottis, R. (2013). Cyberspace from the Hybrid Threat Perspective. Teoksessa Kuusisto, R. & Kurkinen, E. (Toim,) *Proceedings of the 12th European Conference on Information Warfare and Security ECIW 2013.* University of Jyväskylä, Finland. s. 98-105.

Huskaj, G., Iftimie, I. & Wilson, R. (2020). Designing Attack Infrastructure for Offensive Cyberspace Operations. Teoksessa: Eze, T., Speakman, L. & Onwubiko, C. (Toim.) *Proceedings of the 19th European Conference on Cyber Warfare and Security, ECCWS 2020. 25- 26 June 2020.* Sonning Common: Academic Conferences and Publishing International Ltd. s. 473-482.

Izycki, E. & Colli, R. (2019). Protection of Critical Infrastructure in National Cyber Security Strategies. Teoksessa: Cruz, T. & Simoes, P. (Toim.) *Proceedings of the 18th European Conference on Cyber Warfare and Security, ECCWS 2019. 4 - 5 July 2019.* Coimbra: Portugal. s. 219-228.

Izycki, E. & Vianna, E. (2021).Critical Infrastructure: A Battlefield for Cyber Warfare? Teoksessa Lopez, J., Siraj, A. & Perumalla, K. (Toim.) *Proceedings of the 16th International Conference on Cyber Warfare and Security, ICCWS 2021. 25 – 26 February 2021. Online.* s. 454-464.

Karlzén, H. (2020) Usefulness of Cyber Attribution Indicators. Teoksessa: Eze, T., Speakman, L. & Onwubiko, C. (Toim.) *Proceedings of the 19th European Conference on Cyber Warfare and Security, ECCWS 2020. 25- 26 June 2020.* Online. s. 168-176.

Kello, L. (2013). The Meaning of the Cyber Revolution. *International Security (2013), Vol. 38 (2).* s. 7-40.

Kiviharju, M. & huttunen, M. (2020). Turning the Asymmetry Around: Tactical Principles of Warfare in the Cyber Domain. Teoksessa: Eze, T., Speakman, L. & Onwubiko, C. (Toim.) *Proceedings of the 19th European Conference on Cyber Warfare and Security, ECCWS 2020. 25- 26 June 2020.* Online. s.177-185.

Kiviharju, M., Huttunen, M. & Kantola, H. (2020). Finnish View on the Combat Functions in the Cyber Domain. Teoksessa: Eze, T., Speakman, L. & Onwubiko, C. (Toim.) *Proceedings of the 19th European Conference on Cyber Warfare and Security, ECCWS 2020. 25- 26 June 2020.* Online. s. 186-194.

Kong, J., Lim, J., & Gon, K. (2019). The All-Purpose Sword: North Korea's Cyber Operations and Strategies. *Proceedings of the 11th International Conference on Cyber Conflict. 28-31 May 2019.* s. 123-134.

Kostyuk, N., Powell, S. & Skach, M. (2018). Determinants of the Cyber Escalation Ladder. *The Cyber Defense Review, Vol. 3 (1).* s. 123-134.

Kostyuk, N. & Zhukov, Y. (2019). Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal of Conflict Resolution, Vol. 63(2).* s. 317-347.

Kyoung, J., Sung, M. and Joshua, J. (2017). A Case Study of the 2016 Korean Cyber Command Compromise. Teoksessa Scanlon, M. & Le-Khac, N. (Toim.) *Proceedings of the 16th European Conference on Cyber Warfare and Security, ECCWS 2017. 29 – 30 June 2017.* Dublin: Ireland. s. 315-321.

Lahmann Henning. (2020). *Unilateral Remedies to Cyber Operation: Self-defense, countermeasures, necessity and the question of attribution.* Cambridge, Cambridge Univeristy Press. s. 8-9.

Lee, Y., Kwon, H., Lee, J. & Shin, D. (2015). Development of Countermeasures against North Korean Cyberterrorism through Research Case Studies. *The Korean Journal of Defense Analysis Vol. 27 (1).* s. 71–86.

Lemay, A., Knight, S., Fernandez, J. & Leblanc, S. (2016). The Sound a Rattling Cyber-Sabre Makes: Cases Studies in Cyber Power Projection. Teoksessa: Koch, R. & Rodosek, G. (Toim.) *Proceedings of the 15th European Conference on Cyber Warfare and Security, ECCWS 2016. 7 – 8 July 2016.* Munich: Germany. s. 191-197.

Lindsay, J. (2015). The Impact of China on Cybersecurity: Fiction and Friction. *International Security 39(3).* s. 7-47.

Mancuso, V. Strang, A., Funke, G. & Finomore, V. (2014). Human factors of cyber attacks: a Framework for human-centered research. Teoksessa *Proceedings of the Human Factors and Ergonomics Society 58th Annual Meeting – 2014, 27–31 October 2014*. Chicago: USA. s. 437-441

Maness, R. & Valeriano, B. (2016B). The Impact of Cyber Conflict on International Interactions. *Armed Forces & Society, Vol. 42(2).* S. 301-323.

Martins, R. (2018). Punching Above Their Digital Weight: Why Iran is Developing Cyberwarfare Capabilities Far Beyond Expectations. *International Journal of Cyber Warfare and Terrorism, Vol, 8(2).* s. 32-46.

Mattila, J. & Parkinson, S. (2017). Evolution of Military Information Security. Teoksessa Scanlon, M. & Le-Khac, N. (Toim.) *Proceedings of the 16th European Conference on Cyber Warfare and Security, ECCWS 2017. 29 – 30 June 2017.* Dublin: Ireland. s. 610–618.

Maybaum, M. (2013). Technical Methods, Technoques, Tools, and Effects of Cyber Operations. Teoksessa Ziolkowski, K. (Toim.) *Peacetime Regime for State activities in Cyberspace.* Tallinn: NATO CCD COE publification. s. 103-131.

Mueller, R. (2019). *Report On The Investigation Into Russian Interference In The 2016 Presidential Election, Vol 1.* (Submitted Pursuant to 28 C.F.R. § 600.8(c)). Washington, D.C.: U.S. Department of Justice.

Nye, J. (2017). Deterrence and Dissuasion in Cyberspace. *International Security (2017), Vol. 41 (3).* s. 44–71.

Payne, B. & Mienie, E. (2019). The Impact of Cyber-Physical Warfare on Global Human Security. *International Journal of Cyber Warfare and Terrorism, Vol. 9 (3).* s. 36-50.

Phihelgas, M. (2013). Back-Tracing and Anonymity in Cyberspace. Teoksessa Ziolkowski, K. (Toim.) *Peacetime Regime for State activities in Cyberspace.* Tallinn: NATO CCD COE publification. s. 31-60.

Ristolainen, M. (2017). Should 'RuNet 2020' be Taken Seriously? Contradictory Views About Cybersecurity Between Russia and the West. Teoksessa Scanlon, M. & Le-Khac, N. (Toim.) *Proceedings of the 16th European Conference on Cyber Warfare and Security, ECCWS 2017. 29 – 30 June 2017.* Dublin: Ireland. s. 370-379.

Schmitt, M. (2021). Foreign Cyber Interference in Elections. *97 International Law Studies 739 (2021).* s. 740-764.

Valtioneuvosto. (2013). *Suomen kyberturvallisuusstrategia* (Valtioneuvoston periaatepäätös 24.1.2013). Forssa: Forssa print.

Watney, M. (2014) Challenges Pertaining to Cyber War under International Law. Teoksessa *Proceedings of the Third International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2014. 29 April - 1 May 2014.* Beirut: Lebanon. s. 1-5.

Ween, A., Dortmans, P., Thakur, N. & Rowe, C. (2019). Framing cyber warfare: an analyst's perspective. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology, Vol. 16(3).* s. 335–345.