Eero Oksala

KYBERSUOJAJOUKKOJEN PUOLUSTUKSELLISET KYBEROPERAATIOT

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Oksala, Eero
Kybersuojajoukkojen puolustukselliset kyberoperaatiot
Jyväskylä: Jyväskylän yliopisto, 2024, 113 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Moilanen, Panu

Suomen geopoliittinen asema, erityisesti Nato-jäsenyys ja jännitteet Venäjän kanssa, ovat useiden viranomaislähteiden ja julkisten raporttien mukaan lisänneet kriittiseen infrastruktuuriin kohdistuvaa tiedustelun ja vaikuttamisen uhkaa kybertoimintaympäristössä. Myös kansainvälisesti on tuotu laajasti ilmi yhteiskunnallisesti elintärkeisiin toimintoihin kohdistuvan uhkatason nousu. Naton liittolais- ja kumppanimaita onkin vastannut uhkatason nousuun ja toteutuneisiin kyberhyökkäyksiin toimeenpanemalla valtion tietoverkoissa kybersuojajoukkojen puolustustuksellisilla kyberoperaatioita, joilla on pyritty suojaamaan ja turvaamaan tietoverkkojen käytettävyys. Tässä tutkimuksessa tarkasteltiin kybersuojajoukkojen puolustuksellisia kyberoperaatioita kriittisen infrastruktuurin suojaamisen ja turvaamisen näkökulmasta. Tutkimusongelmana oli luoda operatiivisen ja teknis-taktisen tason toimintatapamalli kybersuojajoukkojen puolustuksellisten kyberoperaatioiden suunnittelun ja toimeenpanon viitekehyksessä. Ongelman ratkaisussa käytettiin suunnittelutieteellistä metodologiaa, jonka kautta tunnistettiin eri tasojen toimijoita, operaation vaiheita ja kybersuojajoukkojen toimenpiteitä. Tutkimuksen keskeisenä tavoitteena oli luoda aikaisemman kirjallisuuden ja tutkimusten pohjalta tutkimustietoa energiatoimialan toimijoiden ja kybersuojajoukkojen mukaisen operoinnin yhtenäistämiseksi. Tutkimuksen alussa luotiin perusta ja kuvaus energiatoimialan toimijoista. Tämän jälkeen esiteltiin Yhdysvaltojen, Euroopan Unionin ja Naton kybersuojajoukot ja niiden toimintaperiaatteet. Kuvattujen kokonaisuuksien perusteella luotiin toimintatapamallit operatiiviselle ja teknis-taktiselle tasolle, jotka pohjautuivat aineistolähtöisessä sisällönanalyysissä tunnistettuun tutkimukseen ja kirjallisuuteen. Kerätyn tiedon luotettavuutta varmennettiin asiantuntijahaastatteluiden avulla, joiden kautta varmistuttiin tunnistettujen kokonaisuuksien soveltumisesta myös Suomen toimintaympäristöön. Asiantuntijahaastatteluissa seitsemälle asiantuntijalle toteutettiin puolistrukturoitu teemahaastattelu. Tutkimuksen tuloksena syntyi operatiivisen ja teknis-taktisen tason yleistason toimintatapamallikuvaus, joka perustuu aikaisempaan tutkimukseen ja asiantuntijoiden kehitysesityksiin toimintatapamallin eri tasojen mukaisten kokonaisuuksien suhteen. Kehitetyn toimintatapamallin suurimmaksi merkitykseksi arvioitiin olevan sen yksinkertaisuus, jonka tunnistettiin mahdollistavan pohjan jatkotutkimukselle. Lisäksi luodun toimintatapamallin vaiheistus ja toimijoiden tunnistaminen arvioitiin edistävän valtionhallinnon ja yhteiskunnan tilannetietoisuutta ja valmiutta kansallisissa tai kansainvälisissä häiriötilaneissa.

Asiasanat: Kriittinen infrastruktuuri, energiatoimiala, kybersuojajoukko, puolustuksellinen kyberoperaatio, toimintatapamalli.

ABSTRACT

Oksala, Eero
Defensive Cyber Operations of Cyber Protection Teams
Jyväskylä: University of Jyväskylä, 2024, 113 pp.
Cyber Security, Master's Thesis
Supervisor: Moilanen, Panu

Finland's geopolitical position, in particular its NATO membership and tensions with Russia, have, according to several authorities and public reports, increased the threat level of intelligence and influence operations on critical infrastructure in the cyber domain. Increased threats to the vital functions of societies have also been highlighted by multiple global security and intelligence organisations. NATO allies and partners have responded to the increased threat level and the cyber attacks that have occurred by conducting Defensive Cyber Operations by national or multinational Cyber Protection Teams on state networks in order to protect and secure the critical networks and to analyse cyber attacks that have already occurred. This study examined Defensive Cyber Operations conducted by the Cyber Protection Teams from the perspective of protecting and securing the energy sector. The key objective of the study was to build on previous literature and research to generate research evidence on the interconnections between energy industry actors and Cyber Protection Teams operations. Expert interviews were used to verify the reliability of the research data. The research problem was to establish an operational and technical-tactical level Standard Operational Procedure in the framework of planning and execution of Defensive Cyber Operations by Cyber Protection Teams. To solve the problem, Design Science Research methodology was used to identify the actors at the levels described, the phases of the operation and the required actions. The study started with a baseline and operational-level description of the actors in the environment of the critical infrastructure and energy sector. This was followed by an introduction to the US, European Union and NATO Cyber Protection Teams and their operational procedures. Based on the described overviews, a Standard Operational Procedure was created at the operational and technical-tactical levels, based on the research and literature identified through a qualitative material-based content analysis. A semi-structured interview was then conducted with seven operational and technical experts to improve the developed Standard Operational Procedures. The research resulted in a generic operational and technical-tactical level Standard Operational Procedure, based on previous research and the experts' suggestions for the development of the procedures various levels of entities. The main value of the procedure developed was considered to be its simplicity, which was seen to introduce a basis for further research and development. In addition, the phasing of the developed procedure and the identification of measures and actors were considered to contribute to the situational awareness and preparedness of the government and society in case of national or international emergencies.

Keywords: Critical Infrastructure, Energy Sector, Cyber Protection Teams, CPT, Defensive Cyber Operations, Standard Operational Procedure

KUVIOT

TAULUKOT

SISÄLLYS

1 ENERGIATOIMIALAN DIGITAALINEN LUONNE

1.1 Tutkimuksen kohde ja tarkoitus

Tämä tutkimus kohdistuu kriittisen infrastruktuurin ja yhteiskunnan elintärkeiden toimintojen kyberturvallisuuden kehittämiseen ja turvaamiseen, sekä kansallisen ja kansainvälisen yhteistyön ja johtamisrakenteiden selkeyttämiseen. Tutkimukseen johtanut tilannekehitys pohjautuu geopoliittiseen tilanteeseen ja kriittisen infrastruktuuria kohtaan lisääntyneeseen uhkaan, sekä yhteiskunnan elintärkeiden toimintojen verkottumisen keskinäisriippuvuuteen. Suomen geopoliittinen asema, erityisesti sen Nato-jäsenyys ja jännitteet Venäjän kanssa, ovat lisänneet kriittiseen infrastruktuuriin kohdistuvaa tiedustelua ja vaikuttamista sekä fyysisessä että kybertoimintaympäristössä (Supo, 2023).

Tutkimuksen lähtökohta on Naton kehittämä CIP-käsite (engl. Critical Infrastructure Protection), joka tarkastelee kriittisen infrastruktuurin turvallisuutta energiatoimialan suojaamisen ja sen mukaisten järjestelyiden näkökulmasta (Kruszka, Klósak & Muzolf, 2019). Asian ajankohtaisuutta kuvaa kansallisesti muun muassa Suojelupoliisin vuosikatsaus (Supo, 2023) ja Sisäministeriön kansallisen riskiarvio (Sisäministeriö, 2023), jonka mukaan energiatoimialaan ja sen mukaiseen infrastruktuuriin kohdistuva kyberoperaatioiden uhkataso on kohonnut. Kansainvälisesti ajankohtaisuutta kuvaa muun muassa Yhdysvaltain ja Saksan tiedusteluviranomaisten esiintuoma energiatoimialaa kohtaan kasvava kiinnostus, sekä Tanskan viranomaisten ilmoitus maan historian laajimmasta ja vakavimmasta kyberhyökkäyksestä, joka oli kohdistettu 22 tanskalaista energiatoimialan yritystä ja organisaatiota kohtaan (SektorCERT, 2023). Suomen ja Ruotsin Nato-jäsenyys korostaa tutkimuksen ajankohtaisuutta, sillä Naton kesällä 2022 päivittämä strateginen konsepti tuo liittouman ydintehtävien viitekehyksessä vahvasti ilmi yhteiskunnan kriisinkestävyyden merkitystä osana valtioiden kansallista puolustuskykyä. Häiriötilanteissa ja poikkeusoloissa sotilaallisen suorituskyvyn varmistaminen edellyttääkin myös yhteiskunnan elintärkeiden toimintojen turvaamista (Sisäministeriö, ei pvm.). Venäjän aloittama hyökkäyssota Ukrainassa onkin osoittanut, kuinka merkittävä kohde energiatoimiala ja sen mukainen infrastruktuuri on (Kukkola, 2024).

1.2 Tutkimuksen tavoitteet ja tutkimuskysymykset

Tutkimuksen keskeisenä tavoitteena on luoda uutta tutkimustietoa kriittisen infrastruktuurin toimijoiden kyberturvallisuuden johtamisen ja viranomaisyhteistyön kehittämisen näkökulmasta. Tähän pyritään esittelemällä kansainvälisten kybersuojajoukkojen käyttöperiaatteita osana kriittisen infrastruktuurin suojaamista, samalla pyrkien arvioimaan mahdollisten kansallisten kybersuojajoukkojen vaiheistusta vastaavanlaisien operaatioiden suorittamisen näkökulmasta. Tavoitteena on luoda kirjallisuuden, tutkimusten, ohjeiden ja teemahaastatteluiden pohjalta toimintatapamalli operatiivisen ja taktis-teknisen tason toiminnoista, operaation vaiheista ja suoritettavista toimenpiteistä. Selkeän vaiheistuksen, sekä toimenpiteiden ja toimijoiden tunnistaminen arvioidaan edistävän valtionhallinnon ja yhteiskunnan tilannetietoisuutta ja valmiutta häiriötilaneissa ja poikkeusoloissa, tai laajassa kyberpoikkeamassa ja proaktiivsessa uhkalähtöisessä toiminnassa. Tutkimuksessa hyödynnetään aikaisempaa kansallista tutkimusprofiilia, huomioimalla toimintatapamallien kehittämisessä strategisia, operatiivisia ja taktisia kyberturvallisuuden näkökulmia (Pöyhönen, 2020, s. 22). Tutkimusongelmana on pyrkiä luomaan kokonaisvaltainen toimintatapamalli puolustuksellisten kyberoperaatioiden suunnittelun ja toimeenpanon mahdollistamiseksi kriittisen infrastruktuurin kohdearkkitehtuurissa.

Edgar & Manz (2017, s. 65) mukaan tieteellinen prosessi alkaa kysymyksellä, joka voi olla yleisluontoinen tai erittäin spesifi ja voi saada inspiraationsa aiemmasta työstä tai arkisista tapahtumista. Pääkysymyksen muodostaminen on heidän mukaansa tutkimuksen ydin. Tässä tutkimuksessa vastataan seuraavaan pääkysymykseen:

- Minkälaisella prosessilla mahdollistetaan kybersuojajoukkojen puolustuksellisen kyberoperaation toimeenpaneminen?

Lisäksi vastataan seuraaviin alakysymyksiin:

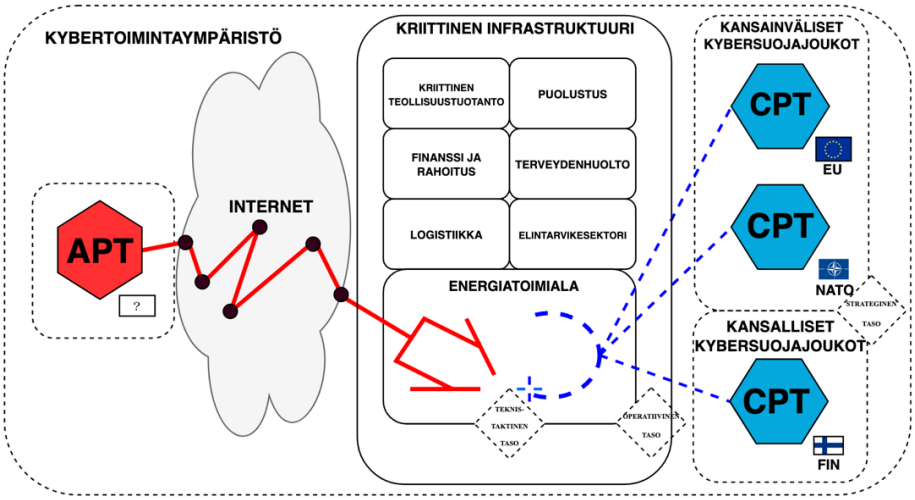
- Mikä on valtionhallinnon johtamisen rakenne kybersuojajoukkojen puolustuksellisen kyberoperaation käynnistämisessä?
- Mitä toimintatapamalleja tulee huomioida kybersuojajoukkojen toteuttaman puolustuksellisten kyberoperaatioiden toimeenpanossa?
- Mitä johtamisen ja ohjauksen rakenteita, malleja ja lainsäädäntöä tulisi luoda tutkimuksen viitekehyksen saavuttamiseksi?

1.3 Tutkimusalueen kuvaus

Tutkimusalueen kuvauksessa käytetään useita kriittistä infrastruktuuria käsitteleviä julkisia selvityksiä ja raportteja, sekä kansallisen kyberturvallisuuden selvityshankkeiden loppuraportteja, joiden kautta muodostetaan teoreettinen tausta kansallisen kriittisen infrastruktuurin toimijoille ja toimintaympäristölle (Lehto, Limnéll, Innola, Pöyhönen, Rusi, & Salminen, 2017; Lehto, Limnéll, Kokkomäki, Pöyhönen & Salminen, 2018; Pöyhönen, Rajamäki, Ruoslahti &

Lehto, 2020; Pöyhönen, 2020; katso myös Vankka, Ahvenainen, Lantto, Hakkarainen, Vestama, Heinäaro, Timonen & Zaerens, 2014; Vankka, Eronen, Häyhtiö, Pöyhönen & Zaerens, 2023). Tutkimukset on esitelty kappaleessa 1.5. Lisäksi kybersuojajoukkojen toimintaa kuvataan eri valtioiden asevoimien, organisaatioiden ja tutkimuslaitosten julkaisujen kautta, joiden pohjalta muodostetaan teoreettinen tausta joukkojen operoinin vaiheistukselle, sekä luodaan ymmärrys joukkojen käyttämistä taktiikoista ja tekniikoista (Trent, Hoffman & Beltz, 2016; Trent, Hoffman, Merritt, & Smith, 2019; katso myös DOA, 2021; DOD, 2014).

Kansallisten ja kansainvälisten tutkimusten ja julkaisujen pohjalta muodostettiin perusanalyysin (engl. Problem Situation) mukainen peruskuva (engl. Rich Picture), jonka avulla on pyritty havainnollistamaan käsiteltävää ongelma-aluetta ja tutkimuskysymysten taustoja (Monk & Howard, 1998). Lisäksi kuvan avulla on pyritty esittämään tutkimuksen keskeisimmät entiteetit, rakenteet ja näkökulmat, sekä kuvaamaan strategisten, operatiivisten ja teknis-taktisten prosessien sijainnit kokonaiskuvassa. Tutkimusalueen peruskuva on esitetty kuviossa 1, jonka kokonaisuudet on kuvattu laajemmin liitteessä 1. Peruskuvassa on hyödynnetty McCroskeyn & Mockin (2017), sekä Vargan, Winkelholzin & Träber-Burdinin (2019) esityksiä kybertoimintaympäristöön sovellettavasta Naton APP-6:n taktisten merkkien symbologiasta. APP-6 on Naton standardi (Standardization Agreement STANAG) taktisille karttamerkeille, jotka on suunniteltu johtamisen, tilannekuvan ja yhteistoiminnan yhtenäistämiseksi (NATO, 2011). Lisäksi peruskuvassa kriittistä infrastruktuuria on käsitelty Pöyhösen & Lehdon (2017) esittämän kriittisen infrastruktuurin toimintaympäristön hierarkisesta rakenteesta, koostuen energiatoimialasta, tiedonsiirtoverkoista ja kriittisistä palveluista. Pöyhösen & Lehdon mukainen toimintaympäristökuvaus on esitetty tarkemmin kappaleessa 2.1.

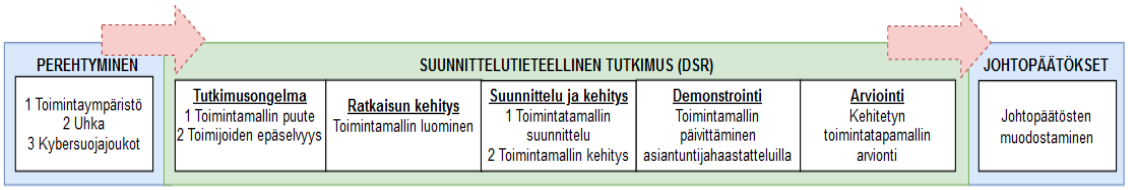


KUVIO 1 Tutkimuksen perusanalyysin (Problem Situation) mukainen peruskuva (Rich Picture), jolla havainnollistetaan tutkimusaluetta. Merkkien ja lyhenteiden tarkemmat kuvaukset on esitetty liitteessä 1. Sinisillä katkoviivoilla on pyritty havainnollistamaan tutkimuksen ongelma-aluetta, johon pyritään selvittämään vastaus. Katkoviivat kuvaavat kansallisten tai kansainvälisten kybersuojajoukkojen tosiasiallisia mahdollisuuksia toimeenpanna puolustuksellisia kyberoperaatioita kohdeympäristössä.

1.4 Tutkimuksen rakenne ja rajaukset

Tutkimuksen rakenne koostuu seitsemästä pääluvusta. Teoriaosuudet koostuvat kriittisen infrastruktuurin sekä energiatoimialan toimintaympäristöanalyysistä ja uhka-arviosta, sekä kybersuojajoukkojen rakenteesta ja operaatioiden toimintaperiaatteista. Tutkimuksen empiirinen osuus koostuu toimintatapamallin kehittämisestä, sekä tutkimuksessa kehitettävän toimintatapamallin päivittämisestä ja validoinnista asiantuntijahaastatteluiden avulla. Lopuksi kuvataan tutkimuksen johtopäätökset, jossa esitellään tuotetun toimintatapamallin yhteenveto, arvioidaan toimintatapamallin luotettavuutta, sekä esitellään tutkimuksen aikana havaitut jatkotutkimustarpeet.

Tutkimustulokset pohjautuvat tutkimuksessa käytettyn suunnittelututkimuksen vaiheistukseen (Design Science Research, myöhemmin DSR), jonka tunnistettiin mahdollistavan johdonmukaisen tutkimuksen toteuttamisen. Tutkimuksen rakenne sidottuna DSR:n prosessiin on esitetty kuviossa 2 (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007; kts. myös Herbert, 1996). Tutkimusmenetelmät on kuvattu kappaleessa 4.



KUVIO 2 Tutkimuksen rakenne ja viitekehys sidottuna suunnittelututkimuksen (DSR) tutkimusmenetelmän vaiheistukseen (Peffers ym., 2017; kts. myös Herbert, S., 1996).

Luku **yksi** pitää sisällään tutkimuksen keskeisimmät lähtökohdat ja menetelmät, luoden teoreettisen pohjan tutkimuksen toimeenpanolle. Luvussa on aikaisemman tutkimuksen pohjalta korostettu tarvetta strategisen, operatiivisen ja taktisen johtamisen kehittämiselle sekä elintärkeiden toimintojen turvaamisen edistämiselle.

Luku **kaksi** käsittelee kriittistä infrastruktuuria ja energiatoimialaa käsitteenä, pyrkien korostamaan toimintaympäristöanalyysin ja uhka-arvion kautta niiden yhteiskunnallista merkitystä, sekä niitä kohtaan kohdistuvien uhkien vaikutuksia yhteiskunnan elintärkeille toiminnoille. Lisäksi luvussa tuodaan ilmi toimialojen kansalliset päätoimijat ja vastuuviranomaiset.

Luvussa **kolme** kuvataan Yhdysvaltain asevoimien, Euroopan Unionin ja Naton kybersuojajoukkojen toimintaa ja rakennetta, sekä joukkojen toimintatapamalleja ja operoinnin periaatteita. Lisäksi luvussa tuodaan ilmi monikansallisten kybersuojajoukkojen käyttöönoton periaatteet ja huomiot.

Luku **neljä** koostuu tutkimuksen viitekehyksen ja tutkimusmenetelmän esittelystä. Lisäksi luvussa käsitellään tutkimuksen aineistonkeruu- ja analyysimenetelmiä, sekä kuvataan toteutettujen teemahaastatteluiden toteutus.

Luku **viisi** on tutkimuksen empiirinen osuus, koostuen toimintatapamallin kehittämisestä teorian ja teemahaastatteluiden pohjalta. Toimintatapamallin

kehittämisen jälkeen luvussa kuvataan teemahaastatteluiden havaintoja ja analyysejä, joiden kautta esitettävää toimintatapamallia päivitetään.

Luku **kuusi** koostuu tutkimuksen johtopäätöksistä ja pohdinnasta, käsittäen kehitetyn toimintatapamallin tarkastelun tutkimusongelman ja tutkimustuloksen luotettavuuden viitekehyksessä. Lisäksi luvussa tuodaan esityksiä jatkotutkimusaiheista.

Liitteessä **yksi** on esitetty perusanalyysin mukainen peruskuva tutkimuksen aihealueen toimintaympäristöstä. Liitteessä **kaksi** on CPT:n toimintaperiaatteita ja tehtävän rakennetta kuvaava toimintatapamalli (Trent ym., 2019, s. 130). Liitteessä **kolme** on ”PESCO CRRT Incident Report”, joka sisältää CRRT:n neuvoston puheenjohtajalle esitettävän tukipyynnön (Vasiliauskaitė & Šakūnas, 2018, s. 31). Liitteessä **neljä** on tiedote tutkimuksesta. Liitteessä **viisi** on esitetty viimeisen kommentointivaiheen saatekirje. Liitteessä **kuusi** on teemahaastatteluiden osakokonaisuudet ja apukysymykset. Liitteessä **seitsemän** on tutkimuksen toimintatapamallin luonnos. Liitteessä **kahdeksan** on tutkimustuloksen toimintatapamalli.

1.5 Aihealueen aikaisemmat tutkimukset

Kansallisen kriittisen infrastruktuurin suojaamista on tutkittu Jyväskylän yliopistossa osana kriittisen infrastruktuurin suojaamiseen ja kyberpuolustuksen ilmiöihin liittyvää kyberturvallisuuden tutkimusohjelmaa, jonka tuloksena edistettiin yhteiskunnan huoltovarmuuskriittisten organisaatioiden kybertuvallisuutta (Lehto ym., 2017; Lehto ym., 2018; Pöyhönen ym., 2017). Lisäksi Jyväskylän yliopiston alla on julkaistu useita aihealuetta käsitteleviä väitöskirjatutkimusta (Pöyhönen, 2020; Puuska, 2021), sekä Pro Gradu- (Mustonen, 2021) ja kandidaatintutkielmaa (Tams, 2020; Lipsanen, 2019; Virtanen, 2019; Kuokkanen, 2020).

Lehto ym. (2017) tutkivat tutkimushankkeessa ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” vuoden 2013 kyberturvallisuusstrategiassa asetettujen tulosten saavuttamista, sekä vuoden 2020 kyberturvallisuuden kansallista tavoitetilaa. Tutkimuksen perusteella Suomi ei ollut edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa. Tutkimuksessa tunnistettuja kehittämiskohteita olivatkin muun muassa strategisen johtamisen kehittäminen, kansainvälisen toiminnan tehostaminen, elintärkeiden toimintojen turvaamisen edistäminen ja lainsäädännön kehittäminen (Lehto ym., 2017).

Lehto ym. (2018) tutkivat tutkimushankkeessa ”Kyberturvallisuuden strateginen johtaminen Suomessa” kyberturvallisuuden strategista johtajuutta ja sen toteuttamista kokonaisturvallisuuden vastuumallissa, häiriötilanteiden hallintamallin toteuttamista laajoissa kyberturvallisuuden häiriötilanteissa, kyberturvallisuuden strategisen johtamisen organisointia, sekä valtionhallinnon kyberturvallisuuden johtamisen rakennetta. Tutkimuksen tuloksena tunnistettiin tarve strategisen tason johtamismallille, joka toimisi kansallisen varautumisen perustana, mahdollistaen erilaisten normaaliaikojen ja poikkeusolojen vakavien ja laajamittaisten häiriötilanteiden johtamisen sekä voimavarojen ja toimintatapojen yhteensovittamisen. Tutkimuksessa esitellyt

mallit eivät tuoneet ilmi kokonaisvaltaista ratkaisua kyberturvallisuuden strategisen johtamisen toteuttamiseksi. Esitettyjen johtamismallien käyttöönotto todettiin edellyttävän syvällisempää analyysiä muun muassa kyberturvallisuuden johtamisrakenteista ja toimivaltuuksista (Lehto ym., 2018).

Jouni Pöyhönen & Martti Lehto (2017) tutkivat, kuinka nykyaikaisen yhteiskunnan toimivuus nojaa kriittisten infrastruktuurin eri toimijoiden ja sektoreiden yhteistyöhön, mikä heidän mukaansa on yhä riippuvaisempi luotettavasta sähköjärjestelmästä. Tutkimuksessa tutkittiinkin energiatoimijoiden prosesseja kyberturvallisuuden mukaisen poikkeamanhallinnan ja johtamisen viitekehyksessä. Heidän havaintojen mukaan energiayhtiöiden on kehitettävä toimiaan sekä strategisella, operatiivisella kuin myös taktis-teknisellä tasolla. Tutkimuksen mukaan energiatoimialan toimijoiden tulisi ylläpitää tehokkaita ja testattuja toimintatapamalleja ja prosesseja, jotka mahdollistavat tehokkaan toiminnan kaikilla tasoilla (Pöyhönen ym., 2017).

Jouni Pöyhönen (2020) tutki Jyväskylän yliopiston väitöskirjatutkimuksessaan kansallisen kriittisen infrastruktuurin kuuluvien yritysten ja organisaatioiden kykyä kehittää kyberturvallisuuden maturiteettia johtamisen pohjalta. Tutkimuksen keskiössä oli kyberturvallisuuden johtamis- ja kehittämismallit, jotka keskittyivät systeemimetodologian pohjalta toimintatapamallien ja -prosessien jatkuvuuden hallintaan ja luottamuksen ylläpitämiseen. Tutkimuksessaan Pöyhönen korostaa, että kriittisen infrastruktuurin toimijoiden ihmiset, prosessit ja teknologiat ovat avainasemassa kyberturvallisuuden kyvykkyyksien rakentamisessa. Väitöskirja vastaa kokonaisvaltaisella systeemitarkastelulla siihen, kuinka johtaa ja kehittää kyberturvallisuutta kriittisen infrastruktuurin organisaatioissa. Tällä kuvataan pyrittävän parantamaan kansallisen kriittisen infrastruktuurin suojausta ja edistämään kyberomavaraisuutta, kokonaisturvallisuutta, huoltovarmuutta sekä kansallista ja organisaatiokohtaista kilpailuetua. Pöyhösen tutkimus tarjoaa myös muita konkreettisia toimintamalleja ja -suunnitelmia kyberturvallisuuden parantamiseksi eri kriittisen infrastruktuurin toimijoiden organisaatioissa.

Trent, Hoffman & Smith (2019) kuvaavat tutkimuksessaan "Modelling the Cognitive Work of Cyber Protection Teams" kybersuojajoukkojen (Cyber Protection Teams, CPT) tehtäviä puolustuksellisissa kyberoperaatioissa. Tutkimuksessaan he kuvaavat kybersuojajoukkojen taktiikoita ja tekniikoita, joiden pohjalta tutkimuksessa luodaan deskriptiivisen toimintatapamalli. Tutkimuksessa kuvaillaan kattavasti kybersuojajoukkojen puolustuksellisten kyberoperaatioiden eri vaiheita. Trent ym. (2019, s. 130) kehittämä toimintatapamalli on esitetty liitteessä 2.

Trent, Hoffman & Beltz (2016) tutkivat tutkimuksessaan "An Empirical Assessment of Cyberspace Network Mapping Capabilities" kybersodankäynnin tutkimuksen ja kehityksen haasteita, jotka kuvataan johtuvan rajoitetusta tiedonjaosta operatiivisten sidosryhmien ja tutkijoiden välillä. Tutkimuksen projekti oli osa U.S. Cyber Command (USCYBERCOM) kehitys- ja kokeilutoimintaa, ja siinä keskityttiin arvioimaan tietoverkkojen kartoituskyvyn toiminnallista soveltuvuutta kybersuojajoukkojen toiminnassa. Tutkimuksessa kuvataan, kuinka Trent ym. kehittivät ja sovelsivat erilaisia mittareita työkalujen kykyjen arviointiin, pyrkien tukemaan päätöksentekoa operatiivisissa ympäristöissä.

1.6 Tutkimuksen määritelmät

1.6.1 Puolustukselliset kyberoperaatiot

Puolustuksellinen kyberoperaatio on operaatiotyyppi, joka voidaan toimeenpanna reaktiivisesti havaittaessa poikkeama, tai proaktiivisesti uhkatiedustelun perusteella (Laari ym., 2019, s. 58). Laarin ym. mukaan (kts. myös DOA, 2021, s. 32–33) operaatiotyyppi voidaan jakaa kahteen osaan, käsittäen puolustukselliset suojatoimet (Internal Defensive Measures, DCO-IDM) ja puolustukselliset vastatoimet (Responsive Actions, DCO-RA). Puolustukselliset suojatoimet voidaan jakaa edelleen valvontaan (engl. screen), rajoittamiseen (engl. contain), puhdistamiseen (engl. clear) sekä palautumiseen (engl. Secure; Laari ym., 2019, s. 60). Tässä tutkimuksessa käsitellään ainoastaan puolustuksellisia suojatoimia.

Puolustuksellisten suojatoimien (DCO-IDM) tavoitteena on tunnistaa uhkatoimijan luvaton toiminta, mahdollinen jalansija ja lateraalinen liike, tai muu turvallisuuspoikkeama. Poikkeaman tunnistamisen jälkeen toimija tai uhkaava toiminta estetään, eristetään tai poistetaan tietojärjestelmistä. (Laari ym., 2019, s. 60). Kuvattu toiminta on pääsääntöisesti reaktiivista, jonka myötä se toteutetaan muun muassa digitaalisen forensiikan keinoin (Digital Forensics & Incident Response, DFIR). Digitaalinen forensiikka on prosessi, jossa kerätään, analysoidaan ja raportoidaan digitaalisia tietoja tavalla, joka on oikeudellisesti hyväksyttävää. Se käsittää erikoistekniikoiden käytön sähköisten tietojen palauttamiseen, todentamiseen ja analysointiin tapauksissa, jotka liittyvät muun muassa tietomurtoon tai tietokoneen muuhun haitalliseen hyväksikäyttöön (Pande & Prasad, 2016, s. 1-3). Puolustukselliset suojatoimet voivat myös olla luonteeltaan proaktiivisia suojaustoimia, eli niin sanottua uhkanmetsästystä (engl. Threat Hunting; Ekstorm, B., 2022, s. 27.). Uhkanmetsästys on proaktiivinen prosessi, jonka tarkoituksena on etsiä uhkia organisaation tietojärjestelmistä kyberuhkatiedustelun (engl Cyber Threat Intelligence) tuottamien indikaattoreiden avulla (Jiawei, Zhang, Jianyi & Gongshen, 2019, s. 1).

Tässä tutkimuksessa puolustuksellisilla kyberoperaatioilla tarkoitetaan puolustuksellisia suojaustoimia (DCO-IDM), jotka käynnistyvät havaittaessa poikkeamia tai kun uhkatiedustelun perusteella tunnistetaan potentiaalinen uhka. Suojaustoimenpiteet kuvataan tutkimuksen viitekehyksessä toimenpiteiksi, jotka voivat olla joko reaktiivista DFIR-toimintaa tai proaktiivista uhkanmetsästystä.

1.6.2 Strateginen taso

Strategisella tasolla toimivat yleisesti valtiohallinnon korkeimman tason päätöksentekijät. Lehdon ym. (2017, s. 38) mukaan kyberturvallisuuden strategista tasoa johtaakin Suomessa valtioneuvosto, joka määrittelee poliittisen ja strategisen tason linjaukset ja päättää käytettävistä resursseista ja toimintaedellytyksistä. Ministeriöiden kuvataan vastaavan muun muassa hallinnonalojen kyberturvallisuuden kehittämisestä ja häiriötilanteiden hallinnasta (Lehto ym., 2017, s. 28). Strategiselle tasolle keskeiseksi kuvataan myös johtaminen, joka Lehto ym. (2018, s. 27) mukaan sisältää

kybertoimintaympäristön turvaamisesta johdettujen tavoitteiden tunnistamisen, ja niiden asettamisen, sekä toiminnan ja varautumisen yhteensovittamisen. Heidän mukaansa (2018, s. 12) kansallinen kyberturvallisuuden strateginen johtaminen muodostuukin kahdesta kokonaisuudesta, jotka ovat varautumisen ja laajamittaisten häiriötilanteiden hallinnan johtaminen niin normaali- kuin myös poikkeusoloissa. He kuvaavat varautumisen koostuvan yhteisten toimintatapamallien, yhteistyöverkostojen ja kyvykkyyksien tuntemisena ja kehittämisenä, sekä kansainvälisen kyberturvallisuustoiminnan ohjaamisena. Heidän mukaansa hitauselementti korostuu valtionhallinnon prosessissa, sillä toimintaympäristöä kohtaan kohdistuvat uhkat vaativat proaktiivista reagointia.

Tässä tutkimuksessa strategisella tasolla kuvataan toimijoita, jotka vastaavat kysymyksiin 'miksi' ja 'mitä' tehdään, pyrkien määrittämään toiminnan suuntaa ja tavoitteita (Pöyhönen ym, 2017, s. 335; Terho, 2009, s. 48). Osa tutkimuksessa käsiteltävistä ministeriöistä ja muista toimijoista toimivat myös strategisen tasolla, mutta tutkimuksen viitekehyksessä näiden toimijoiden toimintaa tarkastellaan pääasiallisesti operatiivisen tason näkökulmasta.

1.6.3 Operatiivinen taso

Terhon (2009, s. 48) mukaan operatiivinen taso koostuu toimeenpantavien operaatioiden suunnittelusta, johtamisesta, ylläpitämisestä, arvioimisesta ja mukauttamisesta strategisten tavoitteiden saavuttamiseksi. Pöyhönen ym. (2017, s. 335-336) mukaan operatiivisen tason konkreettiset toimenpiteet kohdistuvat kyvykkyyksien käytön prosessien kehittämiseen, tietoturvaratkaisujen varmistamiseen ja jatkuvuuden sekä palautumissuunnitelmien luomiseen. Tavoitteena on heidän mukaansa tunnistaa toimintaprosessit, luokitella ne ja seurata niiden käytettävyyttä jatkuvasti, tukien siten toimintaprosessien jatkuvuuden varmistamista.

Tässä tutkimuksessa operatiivista tasoa tarkastellaan valtakunnallisena päätöksentekoprosessina kybersuojajoukkojen käyttöönoton ja sen mukaisen viranomaissuunnittelun ja toimeenpanon suhteen. Tutkimuksen viitekehyksessä tällä tasolla kuvataan, 'missä' ja 'mitä' vastaan toimitaan ja 'millä' strategialla (Terho, 2009, s. 48). Lisäksi tutkimuksen mukaisella operatiivisella tasolla vastataan myös 'miten' suoritettavat toimenpiteet toteutetaan (Pöyhönen ym. 2017, s. 334). Tutkimuksella pyrkitäänkin tunnistamaan kyberoperaatioiden toimeenpanoon liittyvät toimivaltaiset viranomaiset ja muut toimijat. Lisäksi operatiivisen tason näkökulmasta tutkimuksen tavoitteena on pyrkiä luomaan operatiivisen tason toimivaltaiselle viranomaiselle teknis-taktisen tason kuvaus toimeenpantavasta operaatioista, mahdollistaen toimeenpantavien kyberoperaatioiden kokonaisvaltaisen suunnittelun ja johtamisen.

1.6.4 Teknis-taktinen taso

Teknis-taktisella tasolla kuvataan toimeenpantavan strategisella tasolla määriteltyjä ja operatiivisella tasolla suunniteltuja tavoitteellisia toimintoja (Pöyhönen ym., 2017, s. 334). Pöyhösen mukaan tasoon liittyvät käytännön toimenpiteet ICT-järjestelmien ja -laitteiden, tietoverkkojen sekä niiden käytön suojaamiseksi, sisältäen lisäksi uhkien ja haavoittuvuuksien tunnistamisen ja kyberturvallisuusriskien hallinnan (Pöyhönen, 2020, s. 149-151). Lisäksi

Pöyhösen ym. (2017) mukaan teknillis-taktisella tasolla toimivien järjestelmien ja prosessien tulee noudattaa logistiikkaa ja hallintaa yhdistävää kehystä. Tehokkaita tuloksia kuvataan saavutettavan, mikäli toimintoja käsitellään ja hallitaan toisiinsa liittyvinä prosesseina, jotka toimivat yhtenäisenä järjestelmänä (Pöyhönen ym., 2017, s. 336). Heidän mukaansa (2017, s. 336-340) tärkeää on myös tunnistaa uhkat ja haavoittuvuudet, sekä ylläpitää reaaliaikaista tilannekuvaa.

Tässä tutkimuksessa teknis-taktisella tasolla tarkoitetaan operaatioiden vaiheita ja yksittäisiä taktiikoita, tekniikoita ja toimintamalleja. Tutkimuksen viitekehyksessä teknis-taktista tasoa tarkastellaan kybersuojajoukkojen toimeenpanemien puolustuksellisten kyberoperaatioiden vaiheistuksen, menetelmien ja niiden mukaisten huomioiden näkökulmasta. Tavoitteena on pyrkiä luomaan teorian pohjalta kuvaus operaatioiden toimeenpanosta operatiiviselle ja strategiselle tasolle, mahdollistaen operaatioiden kokonaisuuden ymmärtämisen.

2 KRIITTINEN INFRASTRUKTUURI JA ENERGIA-TOIMIALA

Tässä luvussa käsitellään Suomen kriittisen infrastruktuurin ja energiatoimialan toimintaympäristöä ja sitä kohtaan kohdistuvia uhkia. Osion tarkoituksena on vastata kysymykseen: ”Mikä on valtionhallinnon johtamisen rakenne kybersuojajoukkojen puolustuksellisen kyberoperaation käynnistämisessä?”. Luvun tavoitteena on luoda teoreettinen käsitys kriittisestä infrastruktuurista ja energiatoimialasta sekä niiden toimijoista ja vastuuviranomaisista.

Luku on jaettu kahteen alalukuun, joista ensimmäisessä käsitellään kriittisen infrastuktuurin ja sen mukaisen energiatoimialan toimintaympäristöä. Toisessa alaluvussa käsitellään toimintaympäristöjä kohtaan kohdistuvia uhkia.

2.1 Toimintaympäristöanalyysi

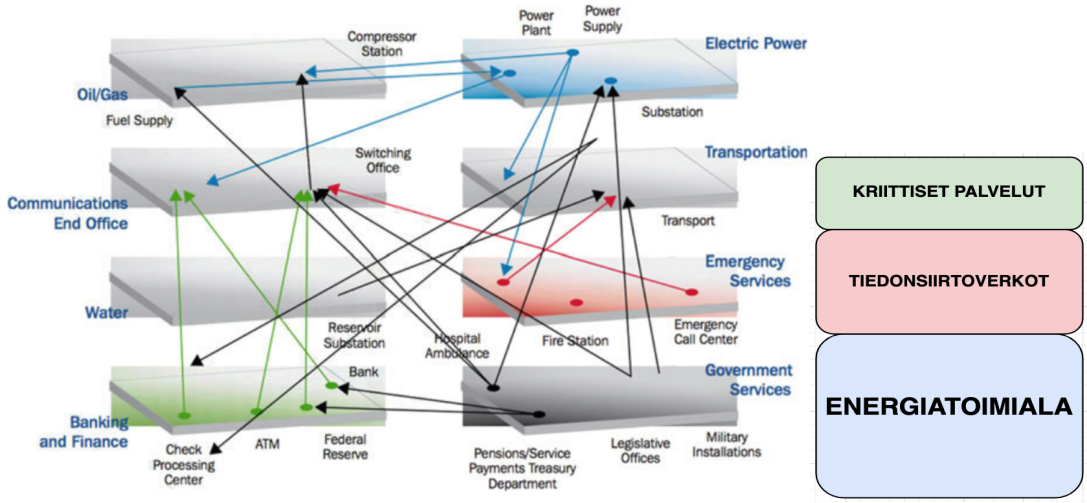
Tässä alaluvussa tarkastellaan kriittisen infrastruktuurin sekä energiatoimialan toimijoiden ja rakenteiden teoreettisia perusteita. Tarkastelun päämääränä on perustella teoreettisin argumentein malli, joka kuvaa kyseisten alojen entiteettejä ja prosesseja. Tutkimuksen luotettavuuden näkökulmasta on kuitenkin merkittävää huomioida, että eri valtiolliset kontekstit määrittelevät kriittisen infrastruktuurin toimijat ja sektorit vaihtelevasti. Vaikka tämä tutkimus ei keskity eri määritelmien vertailevaan analyysiin, se tunnustaa näiden määritelmien olemassaolon ja potentiaalisen vaikutuksen tutkimuksen kontekstiin (Hagelstam, 2005, s. 16).

2.1.1 Kriittinen infrastruktuuri

Hagelstamin (2005, s. 15) mukaan useilla valtioilla on nykypäivänä kriittisen infrastruktuurin toimintaympäristöstä tarkka määritelmä, jossa ilmenee sen toimintaympäristön eri osat, yhteiskunnallinen tärkeys sekä kriittisimmät uhkat. Eri valtioiden määritelmät eivät itsessään eroa toisistaan, mutta niiden sisältämät toiminnot ja järjestelmät vaihtelevat. Huoltovarmuuskeskuksen (HVK) mukaan Suomen kriittinen infrastruktuuri koostu fyysistä laitoksista ja niiden perusrakenteista, sekä laitteista, palveluista ja niihin liittyvistä

toiminnoista, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämiseksi (HVK, 2023). Yleisesti ottaen kriittisellä infrastruktuurilla voidaan kuitenkin nähdä tarkoitettavan yhteiskunnan toiminnalle välttämättömiä fyysisiä ja tietojärjestelmäpohjaisia palveluita ja toimintoja, joiden häiriöt ja katkokset vaikuttaisivat välittömästi yhteiskunnan normaaliin toimintaan (Turvallisuuskomitea, 2017; Supo, 2022).

Pöyhönen ym. (2017) ovat tunnistaneet kriittisen infrastruktuurin riippuvuuden energiatoimialasta ja sähköverkostosta, joka heidän mukaansa luo pohjan kriittisen infrastruktuurin ja sen palveluiden ja järjestelmien käytettävyydelle. Kuviossa 3 on esitetty Lehdon ja Neitaanmäen (2022, s. 5) kuvaus kriittisen infrastruktuurin keskinäisriippuvainen kohdearkkitehtuuri, sekä Pöyhösen ym. (2017) kuvaus kriittisen infrastruktuurin riippuvuus energiatoimialasta ja sähkövoimajärjestelmästä, jotka muodostavat pohjan tietoverkkojen toiminnalle, sekä palvelutason järjestelmien tiedon käytettävyydelle (Pöyhönen ym., 2017, s. 39).



KUVIO 3 Kriittisen infrastruktuurin keskinäisriippuvainen kohdearkkitehtuuri (Lehto, 2022, s. 5), sekä kriittisen infrastruktuurin riippuvuus energiatoimialasta (Pöyhönen ym., 2017).

Kriittisen infrastruktuurin toimintaympäristön verkottumista, keskinäisriippuvuutta ja turvaamista (engl. Critical Infrastructure Protection, CIP) voidaan Hagelstamin (2005) mukaan tarkastella myös poliittisesta, taloudellisesta ja teknisestä ulottuvuudesta (Hagelstam, 2005; kts. myös Lehto ym., 2022, s. 4-5):

- **Poliittinen ulottuvuus** koostuu kansallisesta lainsäädännöstä ja turvallisuustarpeista, sekä näihin liittyvästä kansainvälisestä yhteistyöstä ja intresseistä turvata järjestelmää.
- **Taloudellinen ulottuvuus** koostuu yrityksistä ja muista toimijoista, jotka ovat osa järjestelmän rakentamista, omistamista ja hallinnoimista. Lisäksi ulottuvuus sisältää turvallisuuskustannusten oikeudenmukaisen jaon.
- **Tekninen ulottuvuus** koostuu tekniikan kehittymisestä ja sen hyödyntämisestä osana toimintaympäristön turvaamista. Ulottuvuus sisältää myös kaikki ne ratkaisut ja toimenpiteet, joita valtiot ja yritykset tekevät suojatakseen toimintaympäristöä.

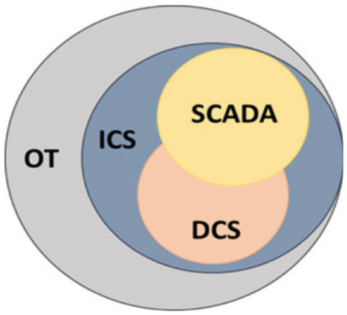
Kriittisen infrastruktuurin toimintoja tulee myös tarkastella yhteiskunnan elintärkeiden toimintojen (YETT) näkökulmasta. Niitä ei tule kuitenkaan yhdistää suoraan kriittiseen infrastruktuuriin, sillä YETT koostuu infrastruktuurin lisäksi johtamisen rakenteista, valtion kansainvälisestä toiminnasta, puolustuskyvystä, sisäisestä turvallisuudesta, taloudesta ja huoltovarmuudesta, väestön toimintakyvystä ja palveluista sekä henkisestä kriisinkestävyydestä (Turvallisuuskomitea, 2017; kts. myös Kuokkanen, 2020, s. 20). Näitä toimintoja johtaa, valvoo ja yhteensovittaa **valtioneuvosto** sekä toimivaltaiset **vastuuministeriöt** omalla hallinnonalalla. Yhteiskunnan elintärkeiden toimintojen ja kriittisen infrastruktuurin välisessä kokonaisuudessa korostuukin vastuuministeriöiden toiminta, jotka vastaavat toimialan palveluita kohtaan kohdistuvien uhkien, haavoittuvuuksien ja riskien tunnistamisesta, sekä ennakoivan tiedon ylläpitämisestä yhteistyössä huoltovarmuusorganisaation (HVO) kanssa (Lehto ym., 2018, s. 14). HVO koostuu HVK:sta ja sen hallituksesta, huoltovarmuusneuvostosta sekä eri toimialojen sektoreista ja pooleista (HVK, D, 2023). HVO:n rakenne on esitetty yksityiskohtaisemmin kappaleessa 2.1.2.

Pöyhönen ym. (2020, s. 2) myös korostavat, kuinka kriittisen infrastruktuurin organisaatiot pitävät yhteyttä Kyberturvallisuuskeskukseen tietoturvaloukkausten suhteen. Poikkeamanhallinnassa ja toiminnan turvaamisessa kuvataankin pyrittävän hyödyntämään toimialan yhteistyöverkostoja, sekä viranomais- ja liiketoimintaverkostoja. Keskeiset huoltovarmuuskriittiset toimijat ja palveluntarjoajat ovatkin velvoitettuja NIS-direktiivin nojalla ilmoittamaan verkko- ja tietojärjestelmien tietoturvapoikkeamista oman toimialan valvontaviranomaisille. Direktiivi edellyttää organisaatioilta ilmoitusvelvollisuuden lisäksi muun muassa riskienhallintaa ja yhteistyötä kansallisten viranomaisten kanssa (Aleksiev, 2023). Tietoturvaloukkauksista voi ilmoittaa myös Kyberturvallisuuskeskukselle, joka mahdollistaa toimijoille tilanneavun ja luottamusverkoston tietoturvatapausten selvittämiseen (KTK, 2022).

Suurin osa Suomen kriittisestä infrastruktuurista on yksityisen sektorin omistuksessa, joista jokainen vastaa oman infrastruktuurinsa suojaamisesta (HVK, 2023). Kriittisen infrastruktuurin julkisen ja yksityisen sektorin hajanaisuus muodostaakin keskinäisriippuvaisen arkkitehtuurikokonaisuuden, jota kohtaan kohdistuvat hyökkäykset moninkertaistuvat kokonaisuuden kompleksisuuden takia (Pöyhönen, Rajamäki, Nuojua & Lehto, 2021, s. 2). Kokonaisuuden tehokas hallinta kuvataan vaativan tiivistä yhteistyötä eri viranomaisten ja yritysten välillä, jossa muun muassa Pöyhösen (2020, s. 117) mukaan Suomi on tunnustettu edelläkävijäksi (kts. myös Lehto ym., 2018, s. 24). PPP-toimintana (engl. Public, Private, Partnership) tunnettu yhteistyön kuvastaan edistävän tilannetietoisuutta ja parantavan koko yhteiskunnan kykyä mukautua ja kestää muuttuvissa toimintaympäristöissä (Pöyhönen, 2020, s. 117).

Kriittisen infrastruktuurin laaja-alaisen verkottumisen johdosta useille toimijoille on yhteistä riippuvuus toimijoiden tarpeeseen tuotettujen ohjausjärjestelmien toimivuudesta osana palveluiden tuottamista. Neitaanmäen ym. (2022, s. 5) mukaan nämä kansallisen kriittisen infrastruktuurin verkkoarkkitehtuurin pääkomponentit, eli ohjausjärjestelmät, voidaan nähdä jakautuvan neljään osaan: teollisuuden ohjausjärjestelmiin (engl. Industrial Control System, ICS), valvonta-, ohjaus- ja datankeruujärjestelmiin (engl.

Supervisory Control and Data Acquisition, SCADA), hajautettuihin automaatiojärjestelmiin (engl. Distributed Control Systems, DCS) ja OT-järjestelmiin (engl. Operational Technology, OT). Neitaanmäen ym. (2022, s. 6) kuvaus järjestelmien hierarkkisesta toimintaympäristöstä ja sen pääkomponenttien kuvaukset on esitetty kuviossa 4. Heidän mukaansa OT-järjestelmät on kattotermi, joka sisältää kaikki kriittisen infrastruktuurin toimijoiden operatiiviset järjestelmät. Neitaanmäki ym. (2022) kuvaavat ICS:n sisältävän niin SCADA-järjestelmät, kuin myös DCS-järjestelmät.

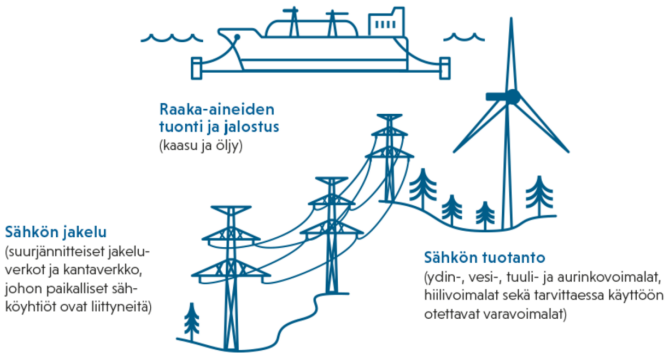


Järjestelmä	Kuvaus
OT	Ohjelmoitavat järjestelmät tai laitteet, jotka vuorovaikuttavat fyysisen ympäristön kanssa ja havaitsevat tai aiheuttavat suoria muutoksia valvomalla ja/tai ohjaamalla laitteita, prosesseja ja tapahtumia. (NIST A, ei päivämäärää)
ICS	Tietojärjestelmä teollisten prosessien, kuten valmistuksen, tuotteen käsittelyn, tuotannon ja jakelun hallintaan, sisältäen valvontajärjestelmiä, tiedonhankintaa ja pienempiä paikallisia prosesseja ohjaavia ohjelmallisia logiikkaohjaimia (NIST B, ei päivämäärää).
SCADA	Tietokonejärjestelmä, joka kerää ja käsittelee tietoja sekä soveltaa toiminnallisia ohjauksia pitkän matkan päästä. Tyypillisesti käytössä sähkön siirrossa ja jakelussa sekä putkistojärjestelmissä (NIST C, ei päivämäärää)
DCS	Ohjausjärjestelmä, jossa älykkyys on hajautettu ohjattavan prosessin ympärille, eikä keskitetty yhteen yksikköön (NIST D, ei päivämäärää)

KUVIO 4 Kuvaus kriittisen infrastruktuurin pääkomponenteista (Lehto, 2022, s. 6; kts. myös Securicon, 2019), sekä niiden yleiskuvaukset (NIST A, B, C, D, ei pvm).

2.1.2 Energiatoimiala

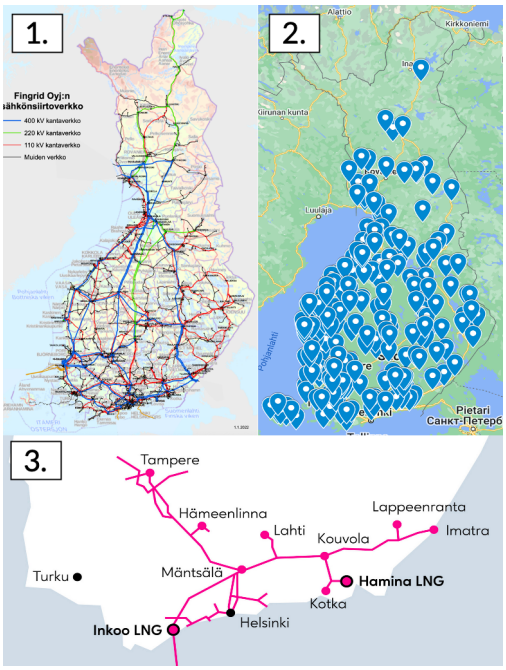
Suomalainen energiatoimiala koostuu sähkönjakeluverkosta, voimalaitoksista ja sähkön kuluttajista (Fingrid A, ei pvm; kts. myös Pöyhönen ym., 2017, s. 332; Heinäaro, 2014). Toimintaympäristön kuvaus on esitetty kuviossa 5 (Supo, 2022).



KUVIO 5 Suomalaisen energiatoimialan toimintaympäristö (Supo, 2022).

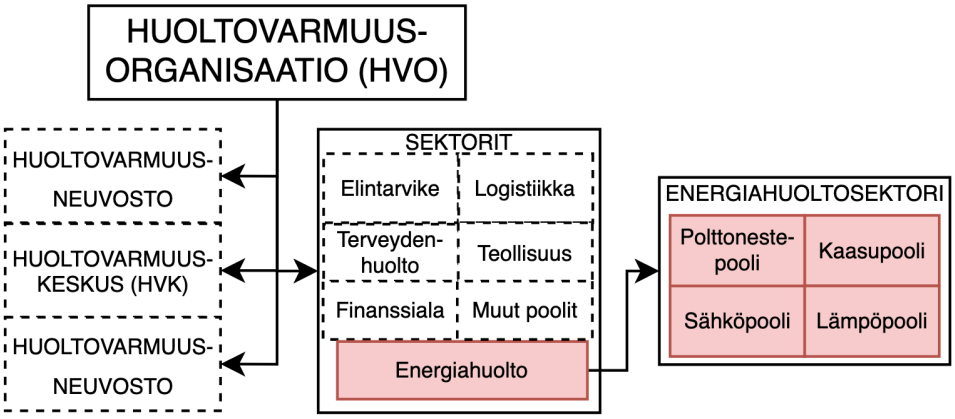
Sähkönjakeluverkko muodostuu suurjännitteisestä jakeluverkosta ja kantaverkosta, johon paikalliset sähköyhtiöt ovat liittyneitä. Suomen sähköverkot ovat myös osa pohjoismaista sähköjärjestelmää. Naapurimaista tuotava ja voimalaitoksilla tuotettava sähkö kuvataan siirrettävän Fingrid Oyj:n hallinnoimassa kantaverkossa ja paikallisten sähköverkkoyhtiöiden hallinnoimissa alueverkoissa kaikkialle Suomeen (STK, ei pvm.). **Voimalaitokset** koostuvat ydin-, vesi- tuuli- ja aurinkovoimaloista,

hiilivoimaloista ja tarvittaessa käyttöön otettavista varavoimaloista. Suomessa voimalaitoksia on yli 400, joiden toiminnasta vastaa noin 120 eri toimijaa ja yritystä (Fingrid B, ei pvm; kts. myös Pöyhönen ym., 2017, s. 332-333). Yhteiskunnan turvallisuusstrategian mukaan (Turvallisuuskomitea, 2017, s. 63-64) energiatoimialan toimintaympäristön turvallisuus keskittyy polttoaine- ja voimahuollon turvaamiseen, joiden turvaamisesta vastaa **Työ- ja elinkeinoministeriö**, johtaen hallinnonalansa varautumista ja sisällyttäen periaatepäätöksen vaatimat toimenpiteet suunnitteluun ja toimeenpanoon hallinnonalansa toiminnassa ja taloudessa (Lehto ym., 2018, s. 14). Lisäksi Työ- ja elinkeinoministeriö toimii energiatoimialan **vastuuministeriönä** (Turvallisuuskomitea, 2017, s. 63-64). Sähkömarkkinoiden ja siirtoverkkotoiminnan varautumisen valvonnasta vastaa **Energiavirasto**, joka varmistaa energiajärjestelmän osa-alueiden toiminnan (Turvallisuuskomitea, 2017, s. 63-64). Viranomaistoiminta kohdistuukin energiatoimialan jatkuvuuden varmistamiseen, kun taas energiatoimialan yritysten vastuulla ovat konkreettisten turvatoimien toteuttaminen ja toimeenpano (Turvallisuuskomitea, 2017, s. 63). Esimerkiksi **Fingrid Oyj** huolehtii kantaverkon hallinnasta, valvonnasta sekä sen ylläpidosta ja kehittämisestä (Fingrid A, ei pvm.), kun taas **Gasgrid Finland Oyj** vastaa kaasunsiirrosta, siirtoinfrastruktuurin ylläpidosta ja kehittämisestä. **Energiayhtiöt** puolestaan vastaavat energianjakelun luotettavuudesta, toimien lainsäädännön asettamien suuntaviivojen ja vaatimusten mukaisesti (Turvallisuuskomitea, 2017, s. 64). Fingrid Oyj:n ja energiayhtiöiden maantieteellinen toiminta-alue on esitetty kuviossa 6.



KUVIO 6 Suomen energiatoimialan toimintaympäristö voidaan nähdä jakautuvan valtakunnalliseen sähköverkostoon, voimalaitoksiin ja kuluttajiin (Fingrid, 2022; Heinäaro, 2014, s. 29.) Kuvassa on esitetty Fingrid Oyj:n sähkönsiirtoverkosto (Kohta 1; Fingrid, 2022), Suomen yli 400 voimalaitoksen pääpiirteiset sijainnit (Kohta 2; Fingrid B, ei pvm.), sekä sekä Gasgrid Finland Oyj:n maakaasuverkosto, koostuen toisiinsa liitetyistä maakaasuputkista (Gasgrid, ei pvm.).

Suomessa energiatoimialan toimintaympäristön toimijat ovat osa **energiahuoltosektoria**, joka muodostaa yhden Huoltovarmuusorganisaation sektoreista. **Huoltovarmuusorganisaatio** (HVO) on valtakunnallinen verkosto, joka turvaa huoltovarmuuden kannalta kriittisten organisaatioiden toimintaedellytykset kaikissa olosuhteissa (Huoltovarmuuskeskus B, ei pvm.). HVO:n energiahuoltosektorin tehtävänä on kaasun, lämmön, sähkön ja öljyn saatavuuden turvaaminen, sekä huoltovarmuuden ja jatkuvuudenhallinnan ylläpitäminen ja kehittämisen energiatoimialan yritysten ja organisaatioiden verkostossa (HVK, A, 2023; Valtioneuvosto, 2022, s. 28-30 ja 37-38) . Energiahuoltosektorin toiminta jakautuu neljään **pooliin**, jotka vastaavat omien poolien varautumis- ja valmiussuunnittelusta poikkeus- ja normaaliolojen vakavia häiriötilanteita varten. HVO:n mukaisten sektorien ja poolien hierarkkinen rakenne on esitetty kuviossa 7 (Valtioneuvosto, 2022).



KUVIO 7 Huoltovarmuusorganisaation ja energiahuoltosektorin rakenne (Valtioneuvosto, 2022).

2.2 Uhka-arvio

Kyberuhka voidaan nähdä kuvaavan tilannetta, tapahtumaa tai toimintaa, joka realisoituessa vahingoittaa, häiritsee tai estää verkko- ja tietojärjestelmien käytön, vaikuttaen niiden suoriin tai välillisiin käyttäjiin, tai muulla tavoin vaikuttaa näihin haitallisesti. Vaikuttamisen lopullisena tavoitteena voi olla pyrkimys vahingoittaa, tuhota tai estää tietoverkon, -järjestelmän tai päätelaiteen tietosisällön käyttö kokonaisuudessaan (Pöyhönen, 2018, s. 32.). Kybervaikuttamiseksi konkretisoitunut kyberuhka voi pahimmillaan vaarantaa yhteiskunnan elintärkeän toiminnon, tai toimintoihin vaadittavan kriittisen infrastruktuurin saatavuuden, eheyden tai luottamuksellisuuden (Valtioneuvosto, 2022, s. 21).

Lehdon mukaan (2022, s. 6-9; katso myös Neitaanmäki ym., 2021, s. 133-136) jakavat kyberuhkat kuusitasoiseen malliin, joka on heidän laajennettu muokkaus Caveltyn (2010) esittämästä alkuperäisestä viisitasoisesta rakennemallista. Lehdon (2022) ja Neitaanmäen ym. (2022) mukainen kuusitasoinen malli on esitetty taulukossa 1. Tässä tutkimuksessa keskitytään kybervakoilun, -sabotaasin tai -sodankäynnin muodostamaan uhkaan, jonka

tavoitteena voi olla epävakauden aiheuttaminen, offensiivisten kybersuorituskykyjen testaaminen, taistelutilan valmistelu tai suora vaikuttaminen (Neitaanmäki ym., 2022, s. 6-9).

TAULUKKO 1 Kyberuhkien kuusitasoinen malli (Lehto, 2022, s. 6-9; katso myös Neitaanmäki ym., 2021, s. 133-136).

TASO	UHKA	KUVAUS
1	Kybervandalismi	Sisältää hakkeroinnin, haktivismin ja kyberparveilun, jotka saavat julkisuudessa näkyvyyttä, mutta ovat vaikutuksilta lyhytaikaisia ja usein vaarattomia
2	Kyberrikollisuus	Tietotekniikkaan tai tietoverkkoihin kohdistettavat rikokset, tai tietotekniikkaa ja tietoverkkoja hyväksi käyttäen suoritettavat rikokset. Jakautuu yleisesti tietoverkkosidonnaisiin ja tietoverkkoavusteisiin rikoksiin.
3	Kybervakoilu	Internetissä, tietoverkoissa, ohjelmistoissa, tai tietokoneissa suoritettavat toimet, joiden avulla hankitaan sensitiivistä, yksityisoikeudellista tai turvaluokiteltua tietoa valtioilta, hallituksilta, kilpailijoilta tai yksityisiltä ihmisiltä poliittisen, taloudellisen tai sotilaallisen edun saavuttamiseksi.
4	Kyberterrorismi	Hyökkäykset, joissa tietoverkkoja käytetään kriittisiin informaatiojärjestelmiin vaikuttamiseen ja niiden kontrollointiin. Tavoitteena voi olla pelon levittäminen, vahingon tuottaminen ja poliittinen painostus
5	Kybersabotaasi	Valtiollisen toimijan tai sen tukeman ryhmittymän toiminta sodan alemmalla tasolla. Tavoitteena voi olla epävakauden aiheuttaminen, offensiivisten kybersuorituskykyjen testaaminen tai taistelutilan valmistelu. Uhkan voidaan nähdä kohdistuvan pääasiallisesti yhteiskunnan elintärkeitä toimintoja kohtaan
6	Kybersodankäynti	Termiä käytetään hyvin laajasti kuvaamaan valtiollisen toimijan operaatioita kybermaailmassa. Varsinainen kybersodankäynti edellyttää valtioiden välistä sotatilaa, jossa kyberoperaatiot ovat osa muita sotilaallisia operaatioita. Uhkan voidaan nähdä kohdistuvan pääasiallisesti yhteiskunnan elintärkeitä toimintoja kohtaan.

Tietojärjestelmien ja -laitteiden jatkuvasti julkitulevat haavoittuvuudet ovat Pöyhösen (2018, s. 32) mukaan merkittävin syy kyberuhkien muodostumiselle tietoverkoissa, -järjestelmissä tai päätelaitteissa. Hän korostaa, kuinka haavoittuvuuksia on usein vaikea havaita ja torjua, uhkatoimijoiden pyrkiessä muodostetun jalansijan piilottamisen ja vaikuttamiseen mahdollisesti vasta pitkällä aikavälillä. Pöyhönen ei tutkimuksessaan kuvaa pelkästään teknisiä

haavoittuvuuksia, vaan myös organisaatioiden toimintaprosesseja, jotka muodostavat organisaatioiden toiminnan perustan (Pöyhönen, 2017, s. 33). Hän kuvaa, kuinka hyökkääjät pyrkivätkin hyödyntämään myös muun muassa hallinnollisten prosessien heikkouksia oman toiminnan edistämiseksi. Myös Euroopan Unionin kyberturvallisuusvirasto tuo vuosittaisessaan raportissaan ilmi, kuinka organisaatioiden on erityisen tärkeää tunnistaa operatiivisen tason toimintaprosesseihin kohdistuvat uhkat (ENISA, 2017, s. 15).

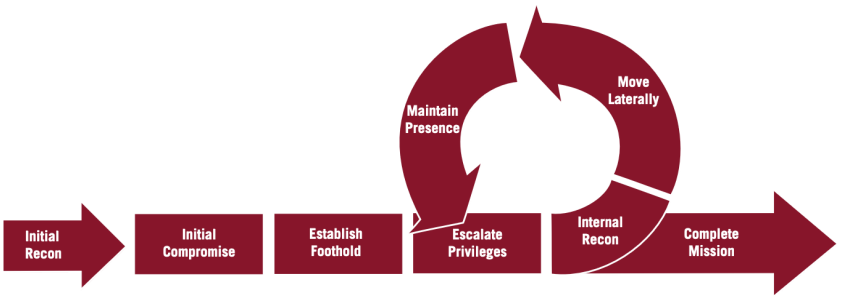
2.2.1 Kriittinen infrastruktuuri

Kriittistä infrastruktuuria kohtaan kohdistuvan uhkan ajankohtaisuus korostuu Venäjän käynnistämän Ukrainan hyökkäyssodan, sekä Suomen ja Ruotsin Nato-jäsenyyden myötä. Muun muassa Suojelupoliisin kansallisen turvallisuuden katsauksen (2023) mukaan kriittiseen infrastruktuuriin kohdistuva tiedustelu ja vaikuttamisen uhka on kohonnut sekä fyysisessä että kyberympäristössä (Supo, 2023; Sisäministeriö, 2023). Tiedusteluyritysten kohteena ovat Suojelupoliisin mukaan (2023) muun muassa kriittisen infrastruktuurin toimijoiden toiminta sekä puolustuskykyyn liittyvät kohteet. Vaikuttamisen keinot voisivat realisoituessa aiheuttaa laajoja häiriöitä, taloudellisia menetyksiä ja jopa kansallisen turvallisuuden vaarantumista (Sisäministeriö, 2023).

Toimintaympäristön muutos on johtanut yhteiskunnan turvallisuuteen vaikuttavien turvallisuusuhkien ja epävarmuustekijöiden kasvamiseen. Digitalisaation myötä uhkan ennakkovaroitusaika on lyhentynyt reaaliaikaiseksi, asettaen haasteita ennakkoon tehtäville varautumistoimenpiteille, päätöksenteolle ja viranomaisten toimintavalmiudelle sekä viranomaisyhteistyön sujuvuudelle (Sisäministeriö, 2022, s. 13). Sähköisten järjestelmien ja palveluiden keskinäisriippuvuuksien vuoksi vikojen ja häiriöiden ketjuuntuminen ja kertautuminen ovat merkittävä uhka. Realisoituvat uhkat voivat myös olla peräisin Suomesta tai Suomen ulkopuolelta, vaikuttaa Suomen alueelle tai sen ulkopuolelle, sekä ilmetä itsenäisinä, samanaikaisina tai toistensa jatkumoina (sama, s. 13-14). Uhan kohteina voivat myös olla energia-, elintarvike-, vesi- ja terveydenhuolto, tai tietovarannot, liikenteen solmukohdat, viestintäjärjestelmät, logistiikka. Sähköisten palveluiden häiriöt voivat aiheuttaa häiriöitä myös fyysisiin palveluihin, kuten vedenjakeluun (Valtioneuvosto, s. 21).

Neitaanmäen ym. (2022, s. 3) mukaan kybertoimintaympäristön merkittävimmät uhkat kohdistuvatkin kriittistä infrastruktuuria kohtaan. He jakavat kriittistä infrastruktuuria kohtaan kohdistuvat uhkat kohdistamattomiin ja kohdistettuihin hyökkäyksiin. Kohdistamattomat hyökkäykset kuvataan laajoiksi hyökkäyksiksi, jossa toiminta kohdistetaan mahdollisimman moneen julkisen verkon kautta saavutettavaan palveluun, laitteeseen tai käyttäjään. Toiminta ei kuvata organisoiduksi, vaan opportunistiseksi ja sattumanvaraiseksi. Kohdistetuissa hyökkäyksissä (engl. Advanced Persistent Threat, APT) hyökkäyksen kohde on Neitaanmäen ym. mukaan valittu tarkasti. APT-ryhmillä tarkoitetaan muun muassa valtiollisia toimijoita, järjestäytyneitä rikollisryhmiä ja kyberterroristejä, joilla on käyttö edistynyttä osaamista ja resursseja kyberoperaatioiden toimeenpanemiseksi. APT-ryhmien kyberoperaatioissa pyritään kerätyn tiedustelutiedon pohjalta tunnistamaan kohteen heikkouksia ja haavoittuvuuksia, joita hyödyntämällä pyritään kohteeseen vaikuttamiseen niin sanotun kybertappoketjun mukaisesti,

alkaen kohteen tiedustelusta ja päättyen asetetun tehtävän saavuttamiseen. Kybertappoketjun kuvaus on esitetty kuviossa 8 (Mandiant, 2013, s. 27; kts. myös Oksala, Heikkinen, Vulli & Lehtinen, 2023; Hutchins, Cloppert & Amin, 2011).



KUVIO 8 Kyberuhkamalli on kyberhyökkäystä mallintava menetelmä, joka perustuu kyberhyökkäyksen ketjutettuun vaiheistukseen. Hyökkäys tulee edetä ketjun alusta loppuun hyökkäyksen lopullisen tavoitteen saavuttamiseksi. Vaikuttamalla ketjun johonkin osaan kyetään hyökkääjän toimintaa rajoittamaan tai estämään (Mandiant, 2013, 27; kts. myös Oksala ym., 2023; Hutchins ym., 2011).

Kohdistetut hyökkäykset käynnistyvät kohteen tiedustelusta, jonka tavoitteena on mahdollistaa operaation toimintaedellytykset. Tiedustelun jälkeen hyökkääjä pyrkii tunkeutumaan maalitetun kohteen tietojärjestelmään teknisten menetelmien avulla, tai niiden kautta (Laari, Flyktman, Härmä, Timonen & Tuovinen, 2019, s. 34-36). Teknisten menetelmien uhka koostuu järjestelmissä olevien haavoittuvuuksien hyväksikäytöstä, kun taas teknisen järjestelmän kautta muodostuva uhka voi koostua käyttäjän manipuloinnista (engl. social engineering), jossa hyödynnetään teknisiä järjestelmiä kohteen lähestymisessä (Laari ym, 2019, s. 34-35). Molemmat uhkat voivat koostua tai johtaa haittaohjelmien levittämiseen ja käyttöön, jonka kautta uhkatoimija pyrkii muodostamaan jalansijan verkkoympäristöön, mahdollistaen operaation jatkuvuuden varmistamisen (Hutchins ym., 2011). Tämän jälkeen uhkatoimija pyrkii kohottamaan käyttöoikeuksiaan ja liikkumaan lateraalisesti kohdeverkossa. Lopullisena tavoitteena voi olla tiedustelutiedon kerääminen iteratiivisena prosessina, tai suora kohdejärjestelmään vaikuttaminen. Neitaanmäen ym. (2022) mukaan kriittisen infrastruktuuriin kohdistetun kybersabotaasin lopullisena tavoitteena voisi olla piilotettujen takaporttien (engl. Back door) tai tappokytkimien (engl. Kill Switch tai Logic Bomb) asennuttaminen. Haitalliset asennukset voitaisiin aktivoida määritettyyn aikaan tai määritettyjen olosuhteiden täyttyessä, kiistäen palveluiden käytettävyyden kybersodankäynnin tavoitteiden mahdollistamiseksi (Neitaanmäki ym., 2022, s. 35-36).

Neitaanmäki ym. (2022, s. 125) korostavat, kuinka eri uhkamallit mahdollistavat kyberoperaatioden jakamisen tunnistettaviin vaiheisiin, jonka avulla mahdollistetaan uhkatoimijoiden operaation seuraavien vaihdeiden tunnistaminen, sekä tulevien kyberhyökkäysten vaikutuksen rajoittaminen. Xing, Li, Jiang, & Jia (2021, s. 185) kuitenkin korostavat, kuinka erilaisia kyberuhkia ja uhkatoimijoiden toimintamenetelmiä sekä taktiikoita tai tekniikoita on loputon määrä, asettaen haasteita niiden täydelle torjumiselle. Heidän (2021, s. 187) mukaan kriittistä infrastruktuuria kohtaan räätälöidyt

haittaohjelmat ovat erittäin edistyneitä ja voivat hyödyntää toiminnan piilottamisessa muun muassa nollapäivähaavoittuvuuksia tai koneoppimismenetelmiä. Lisäksi Xing ym. (2021) korostavat, kuinka APT-ryhmien räätälöidyt haittaohjelmat ovat usein pitkäkestoista, mahdollistaen uhkatoimijalle pääsyn kohdejärjestelmään jopa useita vuosia etukäteen. Kolmantena he (Xing ym. 2021) korostavat, kuinka kriittistä infrastruktuuria kohtaan räätälöidyt haittaohjelmat on tuotettu aiheuttamaan erittäin suuria vahinkoja (Xing ym. 2021, s. 188).

2.2.2 Energiatoimiala

Venäjän vuonna 2022 aloittama hyökkäyssota Ukrainaan on muuttanut energiatoimialan toimintaympäristöä pitkäksi aikaa, voimistaen energian hinnan nousua, samalla haastaen energian huoltovarmuutta (Sisäministeriö, 2022, s. 21). Sisäministeriön kansallisen riskiarvion (2023) mukaan energiainfrastruktuuriin kohdistuva hybridi- ja kyberoperaatioiden uhkataso on kasvanut erityisesti Venäjän aloittaman hyökkäyssodan vuoksi, minkä lisäksi Naton liittolais- ja kumppanimaiden tiedustelu- ja turvallisuuspalvelut ovat aktiivisesti varoittaneet energiainfrastruktuuria ja –toimialaa kohtaan kasvaneesta uhkasta kybertoimintaympäristössä (Smalley, 2023; Martin, 2023; Топалов, 2023). Myös digitaalisen turvallisuuden toimija Thales on vuosiraportissaan (2023) nostanut energiasektorin yhdeksi eniten kohdistettuja hyökkäyksiä kokevaksi kriittisen infrastruktuurin toimialaksi, johtuen kiinnostuksesta toiminnallisiin teknologioihin (OT-verkot), teollisuuden ohjausjärjestelmiin (ICS) ja niiden mukaisiin SCADA-järjestelmiin (Thales, 2023, s. 22). Lehto ym. (2017, s. 16) korostavatkin, kuinka jatkuvien kohdistettujen hyökkäysten takana on usein jokin valtiollinen toimija tai valtion kanssa hyvin läheisesti toimiva rikollisryhmittymä. Huomionarvoista on myös, kuinka Yhdysvaltain tiedusteluviranomaiset (engl. Office of The Director of National Intelligence, ODNI) ovat tuoneet vuosiraportissaan (2023) ilmi, kuinka Kiinalla olisi lähes varmasti kyky häiritä kybervaikuttamisen keinoin Yhdysvaltojen energiasaantia, aiheuttaen muun muassa polttoaineiden saannin vakavia häiriöitä (ODNI, 2023).

Energiatoimialaa kohtaan kohdistuvat uhkat voidaan nähdä koostuvan voimalaitosten logistiikan häiritsemisestä, hyökkäyksistä sähköjärjestelmän ohjaus- ja säätöjärjestelmiin, tai raaka-ainetoimitusten, siirto- ja jakeluverkkojen tai niiden välisten muuntamo- ja kytkinasemien mukaisten toimitusreittien vahingoittamisesta fyysisin toimenpitein (Lewis, 2015; Pöyhönen, 2020, s. 114). Onnistuneet häiriöt voidaan nähdä johtavan sähkön saannin suurhäiriöhin, sekä polttoaineen saannin vakaviin häiriöihin (Sisäministeriö, 2022, s. 54-60). Toteutuessaan **sähköjärjestelmän suurhäiriö** voidaan arvioida vaikuttavan kansalaisten arkielämän toimivuuteen, kansallisen infrastruktuurin ja sen mukaisten rakennusten lämmitykseen, useiden kriittisten palvelujen saatavuuteen sekä esimerkiksi elintarvikehuoltoon. Suurhäiriön seurauksena teollisuuden prosessit lähes varmasti pysähtyisivät tietoverkkojen toimimattomuuden ja liikenteen häiriöiden seurauksena, minkä lisäksi viranomaisten toiminta hankaloituisi merkittävästi (Sisäministeriö, 2022, s. 54). **Polttoaineen saannin vakavalla häiriöllä** olisi erittäin todennäköisesti merkittävä vaikutus väestön toimintakyvylle ja palveluille, taloudelle, infrastruktuurille ja huoltovarmuudelle, sekä sisäiselle turvallisuudelle (Sisäministeriö, 2022, s. 59).

Vaikka energiatoimialan kyberkypsyystaso on yleisesti hyvä, ovat toimialaa kohtaan kohdistuvat uhkat sen keskeisestä roolista valtioiden välisessä vaikuttamisessa ja konflikteissa niin merkittäviä, että yritysten oma varautuminen ei välttämättä riitä (HVK, 2022, s. 28). Toimialan merkittävyys korostuukin sähkön tuotannon ja jakelun häiriötilanteiden osalta, vaikuttaen yhteiskunnan toimintaan välittömämmin ja laajemmin kuin monien muiden kriittisten sektoreiden häiriötilanteet (Supo, 2022). Tällaisten häiriötilanteiden kuvataan voivan syntyä tunnistamattomasta sähköverkon ja tietoliikenneverkon keskinäisvaikutuksesta tai kyberhyökkäyksestä kantaverkkoa tai jakeluverkkoja ohjaaviin järjestelmiin. Teknologian kehitys kasvattaakin energiatoimialan hyökkäyspinta-alaa uusien teknelogisten rajapintojen ja integraatioiden kautta, samalla luoden uusia uhkavektoreita IT- ja OT-ympäristöjen välillä (HVK, 2023, s. 28). Infrastruktuurin ohjausjärjestelmän tahalliset tai tahattomat ja suorat tai epäsuorat verkkoyhteydet voivat altistaa järjestelmät hyökkäyksille. Esimerkiksi ohjausjärjestelmien verkot voivat olla yhteydessä yrityksen liiketoimintaverkkoon, joka puolestaan on yhteydessä julkiseen verkkoon (Neitaanmäki ym., 2022, s. 21-23).

Taulukossa 2 on esitetty kahdeksan toisistaan poikkeavaa kybertapahtumaa, jotka ovat suoraan tai välillisesti muodostaneet uhkan energiatoimialan toiminnalle. Tapaukset ovat esimerkkejä teknisin menetelmin toteutetusta, sekä teknisten järjestelmien kautta muodostuvasta kyberuhkasta. Molempien uhkakuvien avulla on pyritty luomaan pääsy kohdeorganisaation kohdearkkitehtuuriin, pyrkien vaikuttamaan OT-järjestelmien toimintaan, kuin myös varastamaan käyttäjätietoja mahdollisten tulevien operaatioiden mahdollistamiseksi.

TAULUKKO 2 Tapausesimerkkejä energiatoimialaan kohdistuneista kyberhyökkäyksien menetelmistä ja tavoitteista.

TAPAHTUMA	KUVAUS
Tanskan energiatoimiala (2023)	Toukokuussa 2023 Tanskan energiasektorin 22 eri toimijaa kohtaan kohdistettiin maan historian laajin kyberhyökkäys, jossa hyödynnettiin palomuurien kriittistä haavoittuvuutta, mahdollistaen pääsyn energiatoimijoiden kohdearkkitehtuuriin. Hyökkäyksen kohteet oli tarkkaan koordinoitu, uhaten laajasti Tanskan sähkö- ja lämpöhuoltoa. Nopeiden ja tehokkaiden vastatoimien ansiosta merkittävät toiminnalliset häiriöt saatiin estettyä ja kriittinen infrastruktuuri turvattua (SektorCERT, 2023). Vaikuttamisyrityksen takana on arvioitu olleen uhkatoimija Sandworm, mutta tätä on kyseenalaistettu toisten tietoturvatalojen toimesta (Forescout Research, 2024).
Ukrainan sähköverkko (2022)	Vuonna 2022 uhkatoimija Sandworm suoritti osana Venäjän aloittamaa hyökkäyssotaa kyberhyökkäyksen Ukrainan kriittisen infrastruktuurin SCADA-järjestelmään, aiheuttaen merkittäviä häiriöitä sähkönjakeluun. Sähkökatkosten aikana suoritettiin maanlaajuisia ohjusiskuja Ukrainan muuta kriittistä infrastruktuuria kohtaan. Hyökkäyksessä uhkatoimija onnistui luomaan pääsyn OT-ympäristöön, jossa SCADA-järjestelmiä hallinnoitiin, mahdollistaen sähköjärjestelmien sulakeiden tilaan vaikuttamisen. Lisäksi

	kohdearkkitehtuurissa levitettiin CADDYWIPER-haittaohjelmaa. Digitaalisten analyysien tuloksena ei ole tunnistettu hyökkäyksen alkuperäistä hyökkäysvektoria (Proska, Wolfram, Wilson, Black, Lunden, Kapellmann, Brubaker, Mclellan & Sistrunk, 2023).
Colonial Pipeline (2021)	Suuri yhdysvaltalainen energiayhtiö Colonial Pipeline joutui kiristyshaittaohjelman kohteeksi, jonka leviäminen alkoi yhdestä vuotaneesta salasanasta. Hyökkäys kohdistui Yhdysvaltain suurimpaan polttoainelinjastoon, pakottaen yhtiön sulkemaan koko polttoaineenjakeluputkistonsa. Hyökkäyksellä oli merkittävä vaikutus polttoainejakeluun Yhdysvaltojen itärannikolla. Hyökkäyksen takana on arvioitu olleen rikollisryhmä DarkSide (Congressional Research Service, 2021).
TRITON (2017)	Tapahtumassa tunnistamaton uhkatoimija onnistuneesti muodosti etäyhteyden hallintatyöasemalle ja levitti sen kautta kohdearkkitehtuurissa TRITON-haittaohjelmaa, joka oli suunniteltu öljy- ja kaasutuotannossa käytettyjen ICS-järjestelmien SIS-kontrollereihin (engl. Safety Instrumented Systems, SIS) vaikuttamiseen. TRITON-haittaohjelman käyttö johti joidenkin SIS-kontrollerien siirtymisen virhetilaan, joka automaattisesti pysäytti tuotantoprosessin ja lisävahinkojen muodostumisen (Johnson, Caban, Krotofil, Scali, Brubaker, & Glyer, 2023).
Ukrainan sähköverkko (2015 & 2016)	Joulukuussa 2015 ja 2016 kohdistettiin merkittäviä kyberhyökkäyksiä Ukrainan sähköverkkoa kohtaan, onnistuen tilapäisesti vaikuttamaan sähköyhtiöiden toimittajaverkostoon, mahdollistaen sähköjen katkaisun laajalta alueelta. Sähköverkon kannalta keskeiset tietokoneet onnistuttiin saastuttamaan haittaohjelmilla, samalla mahdollistaen myös vaikuttamisen energiayhtiöiden ICS -järjestelmiin. Arvioiden mukaan hyökkäykset saivat alkunsa kohdennettujen tietojenkalastelujen kautta kerättyjen kirjautumistietojen avulla (CISA, 2021; Slowik, 2019).
Norjan energiatoimiala (2014)	Vuonna 2014 Norjan öljy- ja energiasektorin useita kymmeniä yrityksiä kohtaan kohdistettiin laaja hyökkäyskampanja, jossa hyödynnettiin yritysten avainhenkilöille kohdennettuja tietojenkalasteluviestejä. Viestien avulla levitettiin haitallisia liitetiedostoja, jotka sisälsivät haittaohjelman. Haittaohjelma pyrki muodostamaan yhteyden hyökkääjän hallussa olevalle komentopalvelimelle ja välittämään sille varastetut salasanat. Laajat toiminnalliset häiriöt saatiin estettyä ja kriittinen infrastruktuuri turvattua (Muller, Gjesvik, & Friis, 2018).
Saudi-Aramco (2012)	Vuonna 2012 Saudi-Arabian kansallinen öljy- ja kaasuyhtiö Saudi Aramco joutui laajan kyberhyökkäyksen kohteeksi, kun SHAMOON-haittaohjelma saastutti noin 30 000 yhtiön tietokonetta, tuhoten tietoja ja tehden tietokonejärjestelmistä käyttökelvottomia. Haittaohjelma tuhosi tiedostoja, aiheuttaen merkittäviä häiriöitä yhtiön liiketoiminnassa. Hyökkäys sai alkunsa, kun uhkatoimija onnistui

	muodostamaan pääsyn yksittäiseen päätelaitteeseen, joka oli yhteydessä Aramcon sisäisen tietoverkkoon (Alshathry, 2017)
Stuxnet (2010)	Iranin Natanzin ydinlaitoksta kohtaan tunnistettiin vuonna 2010 kohdistetun hienostunut kyberhyökkäys (Stuxnet). Hyökkäys toteutettiin käyttämällä monimutkaista tietokonevirusohjelmaa, joka levisi todennäköisesti USB-tikkujen kautta ja hyödynsi useita nollapäivähaavoittuvuuksia. Stuxnet vioitti ydinlaitoksen sentrifugeja manipuloimalla niiden ohjausjärjestelmiä. Hyökkäys onnistui kuitenkin vain osittain, aiheuttaen viivästyksiä Iranin ydinohjelmassa. Hyökkäys oli kohdistettu erityisesti teollisuuden ohjausjärjestelmiin, eritoten ICS ja SCADA-järjestelmiin. Stuxnet on ensimmäinen esimerkki teollisuusympäristön ohjauslaitteiden manipulointiin suunnitelluista haittaohjelmista. Hyökkäyksen erityisyys oli siinä, että se oli suunniteltu tunnistamaan ja aktivoitumaan vain erittäin tarkasti määritellyissä teollisuuslaitoksissa. Kun nämä ehdot eivät täyttyneet, Stuxnet pysyi passiivisena ja vahingoittamattomana (De Falco, 2012).

Tapaukset ovat esimerkkejä siitä, kuinka kybervakoilun, kybersabotaasin ja kybersodankäynnin eri vaiheet ilmentyvät reaalimaailman energiatoimialaa kohdistuneissa hyökkäyksissä. Kybersabotaasin päämääränä on usein yhteiskunnan elintärkeiden toimintojen häiritseminen, epävakauden aiheuttaminen tai offensiivisten kybersuorituskykyjen testaaminen. Tämä näkyy selkeästi esimerkiksi Ukrainan sähköverkkoihin vaikuttamisessa, joilla oli välillinen vaikutus koko yhteiskunnan elintärkeiden toimintojen ylläpitämiseen, ja kansalaisten turvallisuuteen. Myös Colonial Pipelineen kohdistettu kiristyshaittaohjelmahyökkäys on esimerkki siitä, kuinka rikollisjärjestötkin voivat toteuttaa kybersabotaasia, joko valtion ohjaamana tai omien taloudellisten intressien edistämiseksi. Näiden tapausten kautta korostuu kyberuhkien monimuotoisuus ja niiden potentiaali aiheuttaa merkittäviä vahinkoja kriittiselle infrastruktuurille, joko välillisesti energiatoimialan kautta, mutta myös suoraan. Eri vaiheissa onnistuneet tai torjutut hyökkäykset kuvaavat siitä, kuinka tärkeää on ymmärtää ja ennakoida kyberuhkia proaktiivisesti, sekä kehittää tehokkaita prosesseja niiden torjumiseksi, niin strategisella, operatiivisella, kuin teknis-taktisella tasolla.

3 KYBERSUOJAJOUKOT JA NIIDEN TOIMINTAPERIAATTEET

Tässä luvussa käsitellään Yhdysvaltain asevoimien Cyber Protection Teamin (myöhemmin CPT) sekä Euroopan Unionin Cyber Rapid Response Teamin (myöhemmin CRRT) toimintamenetelmiä operatiivisella ja taktisella tasolla. Osion tarkoitus on vastata kysymykseen: ”Mitä toimintatapamalleja tulee huomioida kybersuojajoukkojen toteuttaman puolustuksellisten kyberoperaatioiden toimeenpanossa?”. Tämän luvun painopiste on pyrkiä tunnistamaan tutkittavien kybersuojajoukkojen operatiivisen ja teknis-taktisen tason toimintatapamallit, jotka kuvaavat kybersuojajoukkojen käyttöönoton eri vaiheita, sekä joukkojen operointia.

3.1 Yhdysvaltain asevoimat

3.1.1 USCYBERCOM

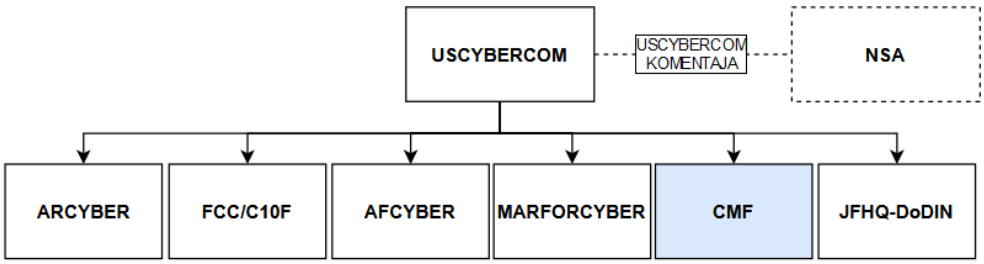
U.S. Cyber Command (USCYBERCOM) on Yhdysvaltain puolustusministeriön (Department of Defense, DOD) alainen, puolustushaaratasoinen kyberjohtoporras, joka vastaa Yhdysvaltojen asevoimien toteuttamien sotilaallisten kyberoperaatioiden suunnittelusta ja koordinoinnista, sekä ohjaa puolustushallinnon tietoverkkojen toimintaa ja puolustusta yhteistyössä kansainvälisten kumppanimaiden kanssa (USCYBERCOM, 2018). USCYBERCOM:in keskeisimmät tehtävät ovat DOD:n tietoverkkojen puolustaminen, Yhdysvaltojen kansallisten ja kansainvälisten operaatioiden tukeminen, sekä Yhdysvaltojen sotilaallisen kybersuorituskykyjen ylläpitäminen ja kehittäminen. Lisäksi USCYBERCOM ylläpitää kykyä toteuttaa hyökkääviä kyberoperaatioita omien tietoverkkojen ulkopuolella (Leitzel & Hillebrand, 2018, s. 136). USCYBERCOM:in alaisuuteen kuuluu puolustushaarojen omat kyberjohtoportaat (ARCYBER; FCC/C10F; AFCYBER; MARFORCYBER), kansallisten intressien toteuttamisesta kybertoimintaympäristössä vastaavaa Cyber Mission Force (CMF), sekä DOD:n tietoverkkojen ylläpidosta ja turvallisuudesta vastaava esikuntarakenne (JFHQ-DODIN; USCYBERCOM, ei pvm). On myös huomion arvoista, että

USCYBERCOM:in virassa toimiva komentaja toimii myös Yhdysvaltain turvallisuusviraston (National Security Agency, NSA) pääjohtajana (NSA, ei pvm). Toimijoiden täydelliset kuvaukset on esitetty Taulukossa 3.

TAULUKKO 3 USCYBERCOM:n kyberjohtoportaat ja esikuntarakenteet.

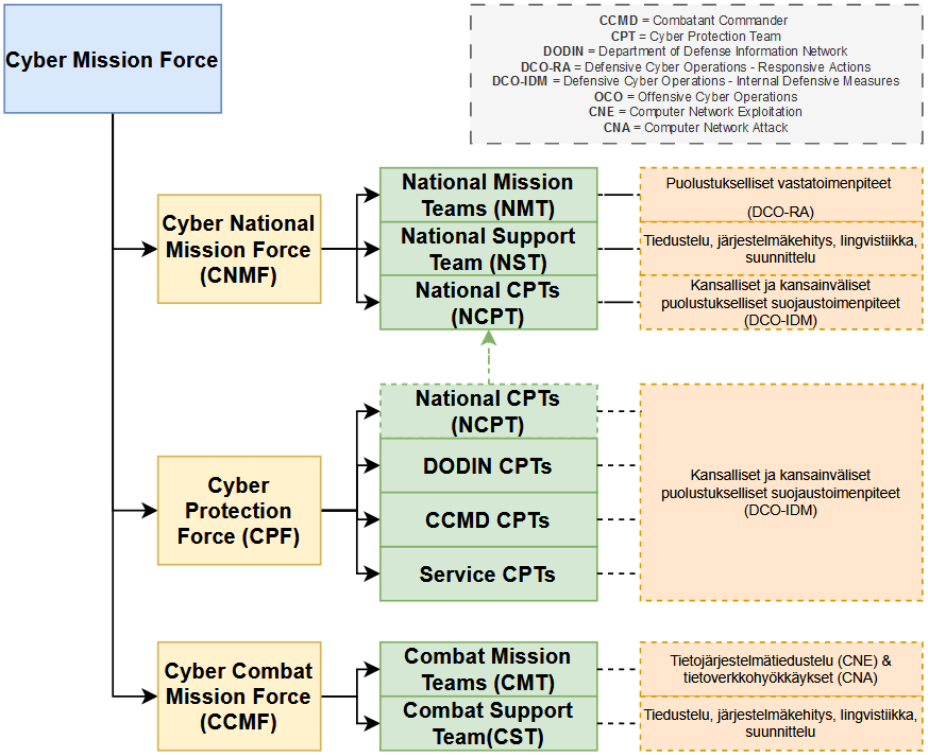
USCYBERCOM	United States Cyber Command	Puolustushaaratasoinen kyberjohtoporras
NSA	National Security Agency	Kansallinen turvallisuusvirasto
ARCYBER	Army Cyber Command	Maavoimien kyberjohtoporras
FCC/C10	U.S. Fleet Cyber Command/U.S. TENTH Fleet	Merivoimien kyberjohtoporras
AFCYBER	16th Air Force / Air Forces Cyber	Ilmavoimien kyberjohtoporras
MARFORCYBER	Marine Corps Forces Cyber Command	Merijalkaväen kyberjohtoporras
CMF	Cyber Mission Force	Kansallisten kyberjoukkojen alajohtoporras
JFHQ-DoDIN	Joint Forces Headquarters – Department of Defence	Puolustusministeriön kyberjoukkojen alajohtoporras

USCYBERCOM:in alajohtoportaiden hierarkinen joukkorakenne on esitetty kuviossa 9 (USCYBERCOM, ei pvm.). Käsillä olevan tutkimuksen tarkastelun kohteena on CMF:n joukkorakenne ja sen joukkojen toimintaperiaatteet, minkä myötä puolustushaarojen alaisia joukkorakenteita ei käsitellä erikseen. On kuitenkin huomioitavaa, kuinka Yhdysvaltain kansalliskaartilla (National Guard) on myös omia kybersuojajoukkoja, jotka vastaavat osavaltioiden paikallisista kyberoperaatioista, tarjoten kriittisen infrastruktuurin suojaamiseen keskittyvää nopeaa tukea ja asiantuntemusta. Yhdysvaltain kansalliskaartin reserviläisistä koostuvat kybersuojajoukot voivat toimia sekä maavoimien (Army National Guard) että ilmavoimien (Air National Guard) alaisuudessa, riippuen osavaltiosta ja spesifisistä organisaatiojärjestelyistä (Ebrahimi, Leithner, Lowham, & Tiscareño, 2020; kts. myös NGB, 2015).



KUVIO 9 USCYBERCOM on Yhdysvaltain puolustusministeriön alainen kyberjohtoporras, joka koordinoi alajohtoportaiden toimeenpanemia sotilaallisia kyberoperaatioita (USCYBERCOM, 2018). Tutkimus on rajattu käsittelemään 34 vain CMF:n joukkokokonaisuutta. USCYBERCOM:n komentaja toimii myös Yhdysvaltain kansallisen turvallisuusviraston (NSA) johtajana.

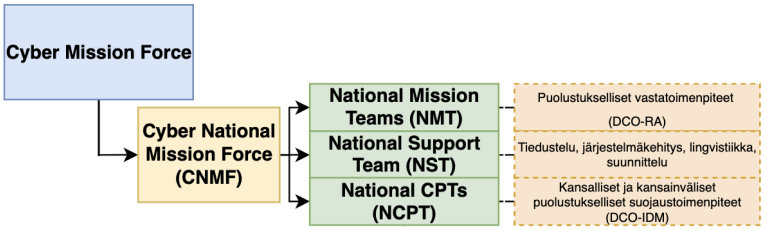
Cyber Mission Force (CNF) toimeenpanee ja koordinoi USCYBERCOM:n ohjaamat hyökkäykselliset (Offensive Cyber Operations, OCO) ja puolustukselliset kyberoperaatiot (Defensive Cyber Operations, DCO), sekä johtamisjärjestelmäoperaatiot (Department of Defense Information Network Operations, DODIN OPS; USCYBERCOM A, 2022). Puolustushaarojen kyberjohtoportaiden tehtävänä onkin tarjota CMF:lle operoivia joukkoja mainittujen operaatioiden toteuttamsiseksi (Ebrahimi, Leithner, Lowham, Tiscareño, 2020, s. 11). CMF:lle jaetut operaatiovastuut on jaettu edelleen kolmelle alajohtoportaalle (CNMF, CPF, ja CCMF), jotka vastaavat omaan toimialan mukaisten kyberoperaatioiden toteuttamisesta (DOA, 2021, s. 114-117). CNF:n joukkorakenne on esitetty kuviossa 10.



KUVIO 10 Cyber Mission Force:n (CMF) joukkorakenne (DOA, 2021, s. 118).

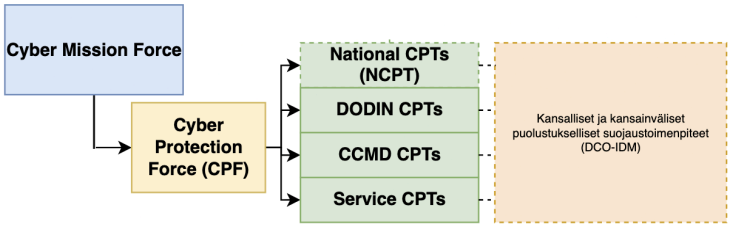
Cyber National Mission Force (*CNMF*) koostuu kansallisten tehtävien joukoista (National Mission Team, NMT), kansallisista tukijoukoista (National Support Teams, NST), sekä kansallisista kybersuojajoukoista (National CPT, *NCPT; DOA, 2021, s. 117).* Joukkojen pääasiallisena tehtävänä on suorittaa puolustuksellisia suojatoimia (DCO-IDM) Yhdysvaltain puolustusministeriön tietoverkoissa (DODIN), sekä erikseen valtuutettuna DODIN:n tietoverkkojen ulkopuolella. Puolustuksellisissa suojaustoimissa uhkatoimija pyritään etsimään, sen mahdollinen toiminta pyritään estämään tai eristämään, minkä jälkeen uhkatoimija pyritään poistamaan omista tietojärjestelmistä (Laari ym., 2019, s. 55-60). Lisäksi joukon tehtävänä on erikseen valtuutettuna suorittaa puolustuksellisia vastatoimia (DCO-RA) neutraaleissa tai vastustajan tietoverkoissa (DOA, 2021, s. 117). Puolustuksellisissa vastatoimissa (DCO-RA) aktiiviset vastatoimenpiteet kohdistetaan neutraaliin tai vastustajan verkkoon, jossa uhkatoimijan toimintaedellytykset pyritään kiistämään aktiivisin

vastatoimenpitein (Laari ym., 2019, s. 58-60). CNMF:n joukkorakenne ja pääasialliset tehtävät on esitetty kuviossa 11 (DOA, 2021, s. 118).



KUVIO 11 Cyber National Mission Force:n (CNMF) joukkorakenne ja pääasialliset tehtävät (DOA, 2021, s. 118).

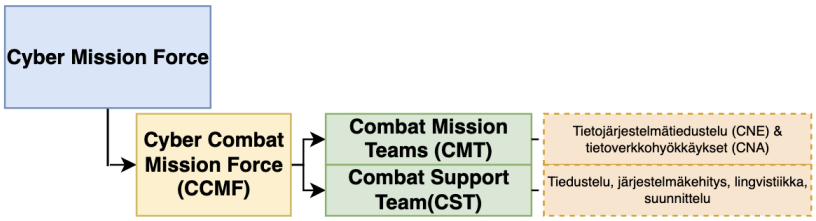
Cyber Protection Force (CPF) koostuu kansallisista kybersuojajoukoista (National CPT, NCPT), Yhdysvaltain puolustusministeriön kybersuojajoukoista (DODIN CPT), rintamakomentajan kybersuojajoukoista (Combatant Commander CPT, CCMD CPT), sekä puolustushaarojen kybersuojajoukoista (Service CPT; DOA, 2021, s. 118). Joukkojen pääasiallisena tehtävänä on toteuttaa puolustuksellisia suojatoimia (DCO-IDM) Yhdysvaltain puolustusministeriön tietoverkoissa (DODIN), sekä erikseen valtuutettuna DODIN:n tietoverkkojen ulkopuolella. Kybersuojajoukkojen käyttö perustuu kohdistettujen kybertoimintaympäristöjen puolustamiseen yhteistoiminnassa kohdearkkitehtuurien omistajien, ylläpitäjien ja käyttäjien kanssa (DOA, 2021, s. 116). CPF:n joukkorakenne ja pääasialliset tehtävät on estietty kuviossa 12. CPT-joukkojen operoinnin toimintaperiaatteita on kuvattu tarkemmin kappaleessa 3.1.2.



KUVIO 12 Cyber Protection Forcen (CPF) joukkorakenne ja pääasialliset tehtävät (DOA, 2021, s. 118).

Cyber Combat Mission Force (CCMF) koostuu taistelutehtävän mukaisista joukoista (Combat Mission Teams, CMT) sekä taistelutuen mukaisista joukoista (Combat Support Team, CST). Joukkojen pääasiallisena tehtävänä on suorittaa hyökkäyksellisiä kyberoperaatioita neutraaleissa ja vastustajan verkoissa (DOA, 2021). Hyökkäyksellisillä operaatioilla (OCO) tavoitellaan kohdejärjestelmän tuhoamista (destroy), lamauttamista, (disrupt), järjestelmien toiminnan häirintää (degrade) ja toiminnan tai palvelun saatavuuden rajoittamista (deny). Tavoitteena voi myös olla harahauttaminen (decieve; Hutchins, Cloppert, Amin, 2012; Kiviharju, M., Huttunen, M. & Kantola, H., 2021). Joukon hyökkäykselliset kyberoperaatiot koostuvat tietojärjestelmätiedustelusta (Computer Network Exploitation, CNE) ja tietoverkkohyökkäyksistä (Computer Network Attack, CNA). CNE:llä tarkoitetaan tietoteknisin menetelmin suoritettavaa tietojen hankkimista valtion ulkopuolella olevasta

tietojärjestelmästä (Monte, 2015, s. 1-5; 590/2019). CNA:lla tarkoitaan hyökkäyksellistä kyberoperaatiota, jonka tavoitteena on tietoverkkojen tai -järjestelmien, ICT-laitteiden tai datan tuhoaminen, lamauttaminen tai käytön häiritseminen (Monte, 2015, s. 2). CCMF:n joukkorakenne ja pääasialliset tehtävät on esitetty kuviossa 13.



KUVIO 13 Cyber Combat Mission Force:n (CCMF) joukkorakenne ja pääasialliset tehtävät (DOA, 2021, s. 118).

3.1.2 Cyber Protection Teams (CPT)

Kybersuojajoukot (CPT) ovat alueellisesti ja paikallisesti liikkuvia kyberpuolustuksen joukkoja, jotka ovat erikoistuneet kybertaistelutilan valmisteluun ja kyberavainkohteiden (Key Cyber Terrain) hallintaan ja suojaamiseen, sekä operaatiovarmuuden takaamiseen (Molle, 2016, s. 33). Kyberavainkohteet ovat kybertoimintaympäristön fyysisen, loogisen tai sosiaalisen kerroksen hallitsevia kohdearkkitehtuurin maastonkohtia, jotka mahdollistavat taistelutilan hallinnan ja etulyöntiaseman vastapuoleen nähden (Raymond, Conti, Cross & Nowatkowski, 2016, s. 287). Operointivarmuus tarkoittaa toimenpiteitä, joita toteutetaan tehtävään käytettävien järjestelmien, tietoverkkojen, verkkoinfrastruktuurin jatkuvuudenhallinnan toteuttamiseksi ja ylläpitämiseksi kaikissa olosuhteissa (Molle, 2016, s. 5). Lisäksi CPT:t jakavat uhkatietoa eri viranomaisten ja kriittisten toimijoiden kesken tunnistetuista haittaohjelmista ja haavoittuvuuksien hyväksikäytön vaarantumisindikaattoreista (DOD, 2014, s. 10). CPT:n pääasialliset tehtävät koostuvat uhkanmetsästyksestä, uhkien torjunnasta ja emuloinnista, sekä kyberoperointia tukevista tukitehtävävistä, kuten haavoittuvuustestauksesta ja haavoittuvuuksien hallinnasta (DOD, 2014, s. 9-10). Keskeisimmät tehtäväkokonaisuudet voidaan nähdä jakautuvan seuraavasti (Trent, Hoffman & Beltz, 2016, s. 4):

- Tietoverkon kriittisimpien assettien tunnistaminen;
- Kohdeverkon verkkorajapintojen funktioiden tunnistaminen;
- Hyökkäysvektoreiden tunnistaminen ja hyväksikäyttö;
- Tietoverkon haavoittuvuuksien tunnistaminen ja hyväksikäyttö;
- Verkkokonfiguraatioiden muutosten tunnistaminen;
- Verkkoliikenteen uudelleenohjauksen määrittäminen.

Cyber Mission Force (CMF) koostuu täydessä operatiivisessa valmiudessa 68 CPT:stä (Trent, Hoffman, Merritt & Smith, 2019, s. 125). Nämä joukot jakautuvat edelleen Cyber Protection Force:n (CPF) alle aikaisemmin esitetyn kuvion 10 mukaisesti. Lisäksi Yhdysvaltain maavoimien käytössä on 11 kansalliskaartin CPT:tä (National Guard CPT), sekä maavoimien reserviläisistä

koostuvaa 10 CPT:tä, joiden tarkoitus on suojata, torjua ja estää kansallista kriittistä infrastruktuuria kohtaan kohdistuvat kyberhyökkäykset (Ebrahimi ym., 2020, s. 12). Yhden CPT-joukon kokonaisvahvuus on täydessä operatiivisessa valmiudessa (Full Operational Capacity, FOC) 39 henkilöä, joista vähintään 34 paikkaa tulee olla miehitettynä ja koulutettuna (Ebrahimi ym., 2020, s. 26). Täyden operatiivisen valmiuden saavuttanut joukko jakautuu viiteen ryhmään, joista jokaisella on omat erikoisalan mukaiset tehtävät ja vastuut. Joukolla on myös johtorakenne, joka koostuu joukon johtajasta (CPT Chief), operaatioupseerista (Operations Officer) sekä kybersuunnittelijasta (Cyberwarfare Planner). CPT:n operoivien ryhmien rakenne ja tehtävät on esitetty Taulukossa 4 (Caton, 2019, s. 7; Stoney ym., 2019, s. 125). Stoney Trent ym. (2016, s. 8) kuvaavat myös tutkimuksessaan lyhyesti CPT:n toimintaa partiotasolla. Yhden CPT-partion kuvataan koostuvan kahdesta operaattorista, joista toinen käyttää valittuja työkaluja ja toinen toimii avustajana, luoden hypoteeseja, tutkii ja esittää seuraavia aliverkkoja kartoitettavaksi, pyrkii tunnistamaan rajoituksia ja niiden mukaisia päätöksentekopisteitä, sekä ylläpitää tilannekuvaa verkon topologian kartoituksesta.

TAULUKKO 4 CPT on tavanomaisesti jaettu viiteen ryhmään, jotka suorittavat oman erikoisalan mukaisia tehtäviä (Caton, 2019, s. 7; Trent ym., 2019, s. 125).

Ryhmän nimi	Kuvaus	Tehtävä
The Mission Protection Squad	Blue Team	Puolustukselliset suojatoimet (DCO-IDM)
The Discovery and Counter-Cyber Infiltration Squad	Hunt Team	Uhkanmetsästys ja mahdolliset vastatoimet omissa tietoverkoissa
The Cyber Threat Emulation Squad	Red Team	Uhkasimulointi ja penetraatiotestaus
Cyber Support Squad	Green Team	Tekninen tuki tehtävien jatkuvuuden mahdollistamiseksi
The Inspection Forces/Cyber Readiness Squad	White Team	CPT:n suorituskykyjen ja operatiivisen valmiuden arviointi

3.1.3 Hunt Forward -operaatiot

Yhdysvaltain asevoimien USCYBERCOM:n Cyber National Mission Force:n (CNMF) toteuttamat "Hunt Forward" -operaatiot (HFO, myöhemmin HF-operaatiot) ovat tiedustelulähtöisiä kyberoperaatioita (engl. Intelligence-Driven Incident Response; USCYBERCOM, A, 2023; Kapelanski, 2023), joita toteutetaan pyynnöstä yhdessä liittolais- ja kumppanimaiden kanssa. Operaatioiden tavoitteena on pyrkiä seuraamaan ja tunnistamaan ystävällismielisen tietoverkon haavoittuvuuksia ja niiden hyväksikäyttöyrityksiä, haittaohjelmia sekä muita epäilyttäviä ilmiöitä (USCYBERCOM, B, 2022). Operaatiot perustuvat Yhdysvaltain puolustusministeriön kyberstrategiaan, jonka mukaan Yhdysvallat turvaa kybertoimintaympäristöä ja kehittää kyvykkyyksiä yhdessä liittolais- ja kumppanimaiden kanssa, samalla laajentaen mahdollisuuksia mahdollisille yhteisoperaatioille kybertoimintaympäristössä (DOD, 2023). Huomioin arvoista onkin, kuinka HF-operaatiot ovat saaneet erillismaininnan kyberstrategiassa, jonka mukaan kyseiset operaatiot ovat luoneet ja vahvistaneet tiedonvaihdon kyvykkyyksiä lukuisien valtioiden kanssa, sekä kasvattaneet liittolais- ja kumppanimaiden kyberresilienssiä paljastamalla vihamielinen toiminta ystävällismielisissä tietoverkoissa (sama, 2023, s. 12). Operaatioiden avulla onkin kyetty paljastamaan uhkatoimijoiden useita

taktiikoita, tekniikoita, hyökkäystyökaluja ja haittaohjelmia, joiden havaitseminen Yhdysvalloista käsin ei olisi ollut mahdollista. Kerättyä tietoa on myös jaettu tietoturvayrityksille, mahdollistaen laajemman kansallisen kokonaishyödyn saavuttamisen (Rollins, 2023). Operaation sopimukseen kuuluukin molemminpuolinen tiedon jakaminen, jolloin molemmat osapuolet voivat hyödyntää operaation kokemuksia oman kyberturvallisuuden kehittämiseksi.

CNMF on toteuttanut vuoteen 2023 mennessä 50 operaatiota 24 eri maassa ja 77 eri tietoverkossa (Nakasone, 2023). On kuitenkin huomionarvoista, että operaatioita tai niiden tuloksia ei tuoda julkisuuteen ilman isäntämaan tahtoa, jonka myötä kaikki tukea vastaanottaneet maat eivät ole julkisesti tiedossa. Naton liittolaismaista muun muassa Viro, Latvia, Liettua, Albania, Kroatia ja Montenegro, sekä kumppanimaista Ukraina ovat tulleet julkisuuteen operaatioiden toimeenpanosta ja isäntämaana toimimisesta (USCYBERCOM, 2020; sama, A, 2023; sama, C, 2022; sama, B, 2023; sama, C, 2023, sama, D, 2022; CNMF, A, 2022, CNMF, B, 2022; Nakasone & Sulmeyer, 2020). Osa julkitulleista operaatoista ja niiden tapahtumista on esitetty Taulukossa 5.

TAULUKKO 5 USCYBERCOM:n HF-operaatioita Naton liittolais- ja kumppanimaissa.

KOHDEMAA	KUVAUS
Viro	Virossa toteutettu HF-operaatio toimeenpantiin Viron asevoimien tietoverkoissa 23. syyskuuta ja 6. marraskuuta 2020 välisenä aikana (USCYBERCOM, 2020). Operaatio oli osa Yhdysvaltojen vuoden 2020 presidentinvaalien turvaamista, jonka tavoitteena oli pyrkiä tunnistamaan proaktiivisesti mahdolliset uhkat ja vaikutusyritykset, joita nähtiin Yhdysvaltojen vuoden 2016 presidentinvaaleissa (Vavra, 2020). Venäjän tunnistettiin tuolloin vaikuttaneen vaalien luottamuksellisuuteen, pyrkien horjuttamaan yhdysvaltalaisvetoista liberaalista demokratiaa ja presidenttiehdokas Hilary Clintonin uskottavuutta ja luotettavuutta presidentin virassa, samalla vahvistaen presidenttiehdokas Donald Trumpin todennäköisyyttä virkaan nimittämisen suhteen (NIC, 2017, s. 7). Vaalien jälkeen arvioitiin todennäköiseksi, että Venäjä hyödyntäisi vastaavia menetelmiä myös tulevaisuuden vaalivaikuttamisessa (sama, s. 8).
Latvia	Latviassa vuonna 2023 toteutettu kolmen kuukauden kestävä HF-operaatio toimeenpantiin valtion kriittisen infrastruktuurin tietoverkoissa yhteistyössä Latvian CERT.LV3 ja Kanadan asevoimien kanssa (USCYBERCOM, A, 2023). Yhdysvaltojen CNMF-joukkojen osalta operaation osallistui 12 henkilöä (Matishak, 2023). Operaatiosta teki poikkeuksellisen se, että se toimeenpantiin yhteisoperaationa Kanadan asevoimien kanssa, jonka mukanaolo perustui sen asemaan Latvian Adazin alueella sijaitsevassa Naton monikansallinen pataljoonan taisteluosastossa, joka on Kanadan johtama 1 400 sotilaan taisteluosasto (Kadettikunta, ei pvm.).
	Liettuassa toteutettiin vuonna 2022 yhteistyössä USCYBERCOM:n CNMF-joukkojen kanssa kolme kuukautta

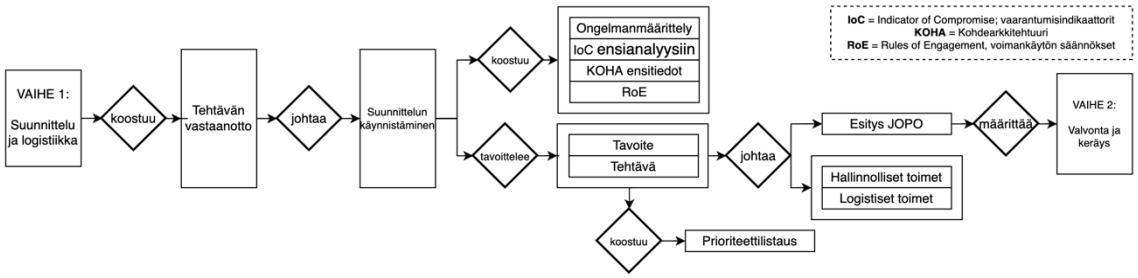
Liettua	kestänyt HF-operaatio Liettuan kansallisen puolustuksen järjestelmissä, sekä ulkoministeriön tietoverkoissa (USCYBERCOM, C, 2022). Operaatio julistettiin toimeenpantavaksi vastauksena Baltian maita kohtaan kasvanutta uhkaa vastaan, joka eskaloitui Venäjän Ukrainassa vuonna 2022 aloittaman hyökkäyssodan myötä (Hartman, 2022). CNMF-joukot toimeenpanivat Liettuassa vuonna 2023 myös toisen kaksi kuukautta kestäneen HF-operaation. Yhdysvaltalaisten operoivien joukkojen vahvuutena oli tuolloin noin 20 henkilöä. Operaation tavoitteena oli pyrkiä tunnistamaan ja estämään Liettuan sisäministeriön alaisen informaatioteknologia- ja viestintäosaston tietoverkoissa mahdollisesti toimeenpantava vihamielinen toiminta, sekä tunnistamaan tietoverkon palveluiden ja järjestelmien mahdollisesti hyväksikäytettävät haavoittuvuudet (Seldin, 2023).
Albania	Albaniassa toimeenpantiin vuonna 2023 kolme kuukautta kestänyt HF-operaatio osana Albanian valtionhallinnolle osoitettua Yhdysvaltojen tukea, Iranin kohdistettua Albaniaa kohtaan lamauttavia kyberhyökkäyksiä vuoden 2022 heinäkuussa ja syyskuussa (USCYBERCOM, C, 2023). Yhdysvaltojen kyberturvallisuusviranomaisen CISA:n mukaan iranilaiset uhkatoimijat olivat muodostaneet jalansijan Albanian valtionhallinnon kohdearkkitehtuuriin jo 14 kuukautta ennen heinäkuun vaikuttamisoperaation toimeenpanoa. Vaikuttamisoperaation seurauksena uhkatoimijat onnistuivat laajasti levinneen tuhoavan haittaohjelman avulla kiistämään Albanian valtionhallinon tietojärjestelmien ja palveluiden käytettävyyden (CISA, 2022). Vastaavanlainen hyökkäys toimeenpantiin myös syyskuussa, jonka seurauksena Yhdysvaltain valtionhallinto tiedotti ryhtyvänsä vastatoimiin Nato-liittolaismaan kohdearkkitehtuurin suojaamiseksi (The White House, 2022). Hyökkäykset johtivat kriittiseen tarkasteluun siitä, olisiko tapahtumien johdosta mahdollista toimeenpanna Naton 5. artiklan mukaisia Naton liittolaismaiden kollektiivisen puolustuksen vastatoimenpiteitä (Miller, 2022), joka määrittää Naton jäsenvaltioiden velvoitteen puolustaa muita jäsenvaltioita (Nato, A, 2023).
Ukraina	Yhdysvaltojen ja Ukrainan yhteisvoimat toteuttivat 2022–2024 yhteisen, kolme kuukautta kestäneen puolustuksellisen kyberoperaation Ukrainan kansallisen kriittisen infrastruktuurin tietoverkkojen turvaamiseksi. Operaatioon osallistui Yhdysvaltojen suurin kybersuojajoukkue, joka suoritti uhkanmetsästystä vihamielisen kybertoiminnan tunnistamiseksi Ukrainan verkoista Venäjän hyökkäyssodan käynnistymiseen asti. Puolustustoimien lisäksi Yhdysvaltojen kyberusojajoukko tarjosi Yhdysvalloista etäanalyysiä ja neuvontatukea. Operaatiosta kerättyä uhatietoja jaettiin myös Yhdysvaltojen turvallisuusviranomaisille ja -yrityksille (CNMF, A, 2022).

3.1.4 CPT:n taktiikat, tekniikat ja toimintatapamallit

Trent ym. (2019) tutkivat CPT-kybersuojajoukkojen tehtävärakennetta virtauskaavioiden kautta, joiden pohjalta he pyrkivät yksinkertaistamaan tehtävän dokumentointia, luomaan tarkastuslistaa ja koulutusmateriaalia, helpottamaan ja virtaviivaistamaan päätöksentekoa sekä tunnistamaan kyvykkyyksien vahvuuksia ja puutteita. Tutkimuksiaan varten he haastattelivat 50 vapaaehtoista, jotka työskentelivät eri puolustushaarojen edustajina 19 eri CPT:ssä (maavoimat: 8; merivoimat: 4; merijalkaväki: 4; ilmavoimat: 3). Tutkimuksen lähtökohta perustui asiantuntijakokemuksien pohjalta laadittuun ensivaiheen virtauskaavioon, jossa toimenpiteitä ei sidottu vaiheisiin, vaan ne pyrittiin tuomaan esiin tehtävän kokonaiskuvan mahdollistamiseksi. Ensimmäisen vaiheen virtauskaaviota kehitettiin puolustushaarojen CPT:n asiantuntijoiden kanssa, jonka tuloksena tutkijat kehittivät useiden iteraatiokierrosten pohjalta lopullisen CPT:n toimintaperiaatteita ja tehtävän rakennetta kuvaavan virtauskaavion, joka on esitetty Liitteessä 2 (Trentin ym., 2019, s. 130).

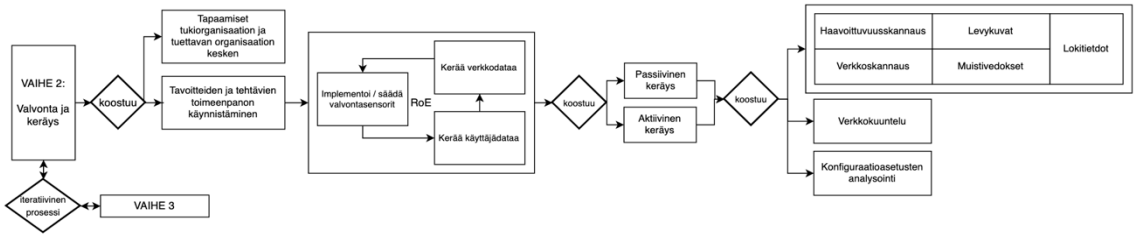
CPT:n operaatiot voidaan nähdä Trentin ym. (2019) toteuttaman tutkimuksen pohjalta jakautuvan neljään osaan. Ensimmäinen vaihe koostuu suunnittelusta ja logistisesta vaiheesta (Planning & Logistics); toinen vaihe on valvonta ja keräys (Monitoring & Collecting); kolmas vaihe koostuu analyysistä ja synteesin muodostamisesta (Analysis & Synthesis); ja viimeinen vaihe koostuu raportoinnista ja tehtävän päättämisestä (Closure). Virtauskaavion yläosasta ilmenee myös virtausviiva, joka kuvaa jatkuvaa tiedonvaihtoprosessia oman tukiorganisaation, tuettavan organisaation ja tiedustelun kesken. Myös kuvion alaosassa sijaitseva virtausviiva kuvaa vastaavasti riskiarvioinnin olevan jatkuvaa. Tutkijat (Trentin ym., 2019, s. 130) tuovat myös ilmi kehityksessä olevan CPT CONOPS:in (Concept of Operations), jonka mainitaan rakentuvan neljään vaiheeseen: Tutki (Survey), suojaa (Secure), puolusta (Protect) ja palaudu (Recover). He tuovat kuitenkin ilmi asiantuntijoiden näkemyksen siitä, kuinka kyseinen vaiheistus ei ole suoranaisesti sopiva, sillä se ei huomioi kokonaisuutta.

Trentin ym. tutkimuksen mukaisen toimintatapamallin ensimmäisen vaiheen kuvataan koostuvan tehtävän vastaanotosta ja suunnittelun käynnistämisestä. Suunnittelun kuvataan pohjautuvan ongelmanmäärittelyyn, vaarantumisindikaattoreiden ensianalyysiin, kohdearkkitehtuurin ensitiedon keräämisen, sekä voimankäytön säännösten määrittelyyn. Suunnittelun pohjalta kuvataan tuotettavan operaation tavoitteet ja tehtävälistaus, joka koostuu kohteiden prioriteetin määrittelystä. Viimeisessä vaiheessa toimeenpantavat tavoitteet ja tehtävät kuvataan esitettävän ylemmälle johtoportaalle, minkä lisäksi käynnistetään logistiset ja hallinnolliset toimenpiteet (Trent ym., 2019, s. 130). Trent ym. (2019) mukainen tulkinta operaation ensimmäisetä vaiheesta on esitetty kuviossa 14.



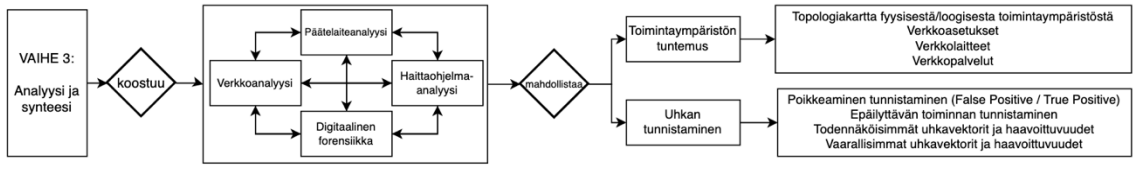
KUVIO 14 Trent ym. (2019) tulkinta operaation ensimmäisestä vaiheesta.

Operaation toinen vaihe kuvataan sisältävän tapaamisia tukiorganisaation ja tuettavan organisaation kanssa, minkä lisäksi vaiheessa kuvataan käynnistettävän operaatioin ensimmäisen vaiheen mukaisten tavoitteiden ja tehtävien toimeenpano. Tämän kuvataan koostuvan valvontasensorien asentamisesta, joka käynnistää iteratiivisen prosessin tiedonkeräyksen suhteen. Tiedonkeräystä kuvataan toteutettavan aktiivisesti ja passiivisesti, koostuen verkkokuuntelusta, konfiguraatioasetusten tutkimisesta, haavoittuvuusskannauksista, sekä levykuvien, muistivedosten ja lokitietojen keräämisestä (Trent ym., 2019, s. 130). Stoney Trentin ja muiden (2019) mukainen tulkinta operaation toisesta vaiheesta esitetty kuviossa 15.



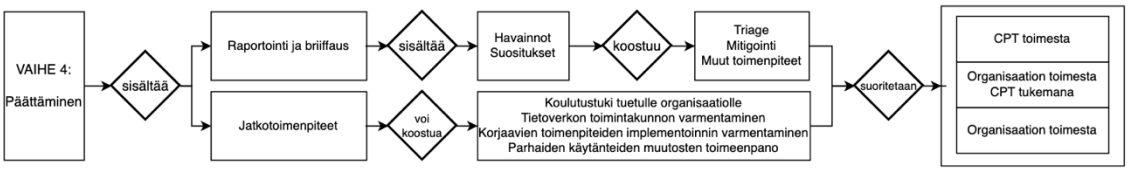
KUVIO 15 Trent ym. (2019) tulkinta operaation toisesta vaiheesta.

Operaation kolmas vaihe kuvataan Trentin ym. (2019) mukaan koostuvan iteratiivisesta analyysiprosessista, joka käsittää verkkoanalyysin, päätelaiteanalyysin, haittaohjelma-analyysin sekä digitaalisen forensiikan tutkimukset. Iteratiivisen analyysiprosessin kuvataan johtavan toimintaympäristön ja uhkan tuntemukseen. Toimintaympäristön tuntemus kuvataan loogiseksi tai fyysiseksi kartaksi, joka sisältää tiedot verkkoasetuksista, -laitteista- ja palveluista. Uhkan tuntemuksen kuvataan koostuvan poikkeamien, epäilyttävän toiminnan ja potentiaalisimpien uhkavektoreiden ja haavoittuvuuksien tunnistamisesta (Trentin ym., 2019). Trentin ym. (2019) mukainen tulkinta operaatioiden kolmannesta vaiheesta on esitetty kuviossa 16.



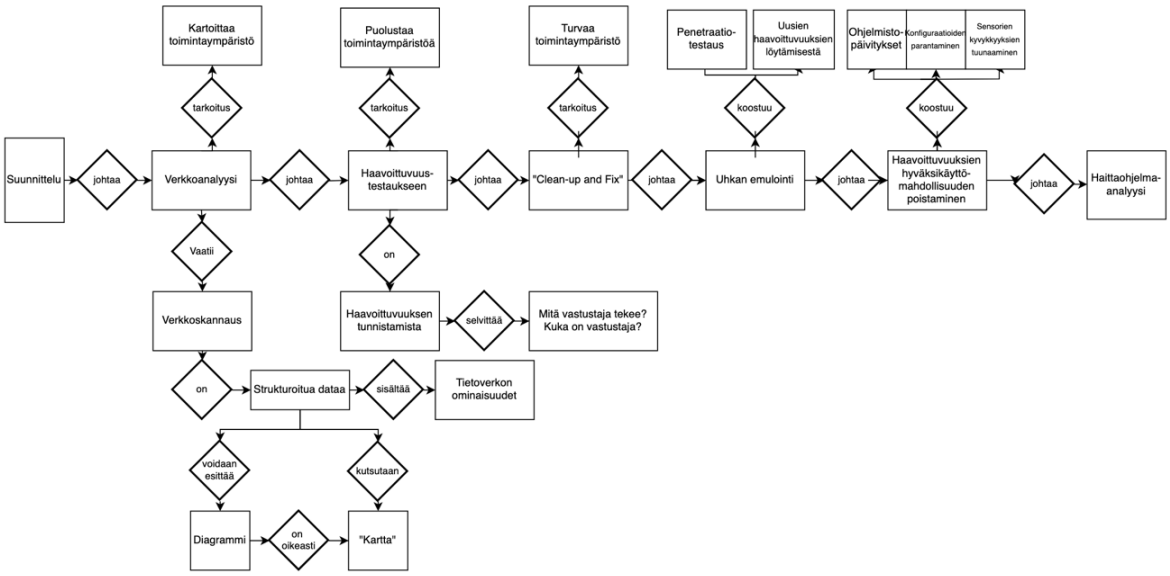
KUVIO 16 Trent ym. (2019) tulkinta operaation kolmannesta vaiheesta.

Neljännen vaiheen kuvataan koostuvan tunnistetuista poikkeamahavainnoista ja suosituksista niiden korjaamiseksi joko organisaation toimesta itsenäisesti, CPT:n tukemana tai CPT:n toimesta. Lisäksi vaiheen kuvataan koostuvan jatkotoimenpiteistä, jotka voivat olla koulutustuki tuettavalle organisaatiolle, tietoverkon toimintakunnon varmentaminen, suoritettujen korjaavien toimenpiteiden implementoinnin varmentaminen tai parhaiden käytänteiden muutosten toimeenpaneminen (Trent ym., 2019). Stoney Trentin ja muiden (2019) tulkinta operaation neljännestä vaiheesta on esitetty kuviossa 17.



KUVIO 17 Trent ym. (2019) tulkinta operaation neljännestä vaiheesta.

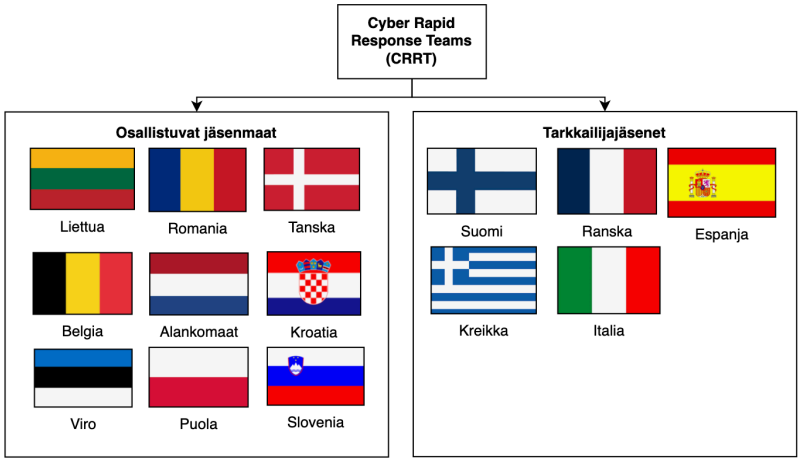
CPT:n yksityiskohtaisempia taktiikoita, tekniikoita ja proseduureja on selvitetty Trent ym. (2016) tutkimuksessa, jossa he selvittivät CPT:n näkemyksiä ja kykyä tuottaa operaatioiden aikana kohdeympäristöistä topologiakarttoja, joista ilmenisi kybertoimintaympäristön fyysisen ja loogisen kartan mukaisesti kohdearkkitehtuurin aliverkot, laitteiden määrä, kohdeympäristön laitteet, palvelut ja käyttöjärjestelmät, avoimet portit, ulkoiset yhteydet, käyttäjäoikeudet ja –roolit, sekä verkkokonfiguraatiot (Trent ym., 2016, s. 2). Tutkimuksessa haastateltiin 24 asiantuntijaa eri puolustushaaroista, jotka korostivat suuresti tarvetta verkkoympäristön kuvaamiselle karttapohjan mukaiseksi kokonaisuudeksi. Lisäksi tutkimuksen tuloksena tuotettiin CPT:n mukainen virtauskaavio, jonka voidaan nähdä toimivan yksityiskohtaisempana kuvauksena Trent ym. (2019) esittämän CPT:n operoinnin vaiheista. Trent ym. (2016, s. 5) kehittämä CPT:n työprosessi on esitetty kuviossa 18.



KUVIO 18 CPT:n operoinnin prosessikuvaus (Trent ym., 2016, s. 5).

3.2 Euroopan Unioni

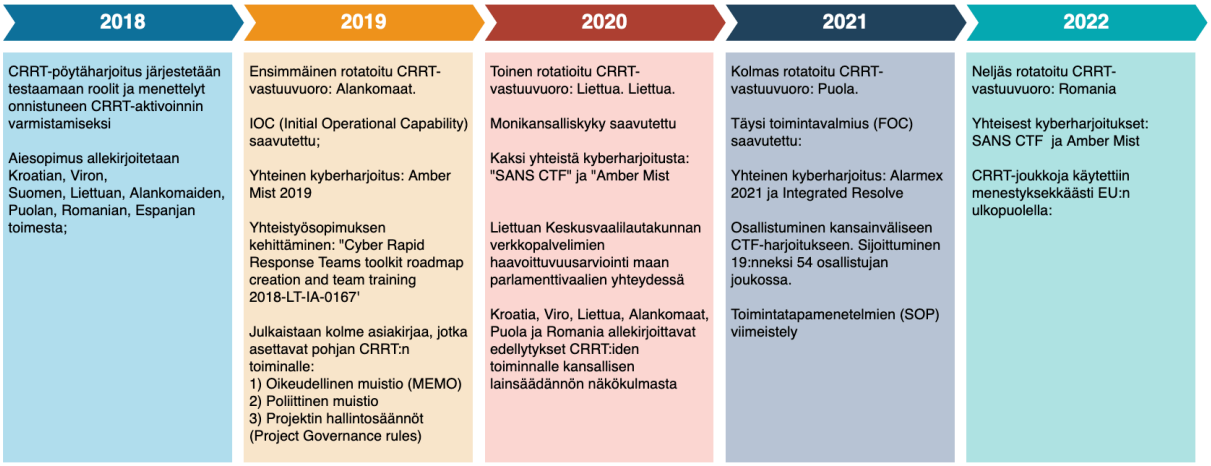
Vuonna 2018 Euroopan parlamentti vaati päätöslauselmassaan, että kyberpuolustusta vahvistettaisiin perustamalla nopean kybertoiminnan joukot (Cyber Rapid Response Team, CRRT; Vainio, 2018). Tämän seurauksena Euroopan Unionin (EU) pysyvän rakenteellisen puolustusyhteistyösopimuksen (PESCO) mukainen kyberpuolustushanke ”Cyber Rapid Response Teams and Mutual Assistance in Cyber Security” käynnistettiin Liettuan toimesta vuonna 2018 (Galinec, Steingartner & Zebić, 2019). Hanke on Liettuan koordinoima, minkä lisäksi hankkeen osallisina on Belgia, Kroatia, Viro, Alankomaat, Puola, Romania, Slovenia ja Tanska (CRRT, 2023). CRRT:n toiminta perustuu jäsenvaltioiden vapaaehtoisuuteen, johon osallistuu vain osa jäsenmaista pääosin puolustushallinnon alalta. Suomi on mukana tarkkailijajäsenenä (Valtioneuvosto, A, 2023). Hankkeelle on poikkeuksellista se, että se mahdollistaa tiedonvaihdon lisäksi myös suoran henkilöstöresurssien rotatoinnin (Pozzi, 2022, s. 2). Hankkeen jäsen- ja tarkkailijamaat on esitetty kuviossa 16.



KUVIO 19 Euroopan Unionin puolustusyhteistyösopimuksen (PESCO) mukaisen ”Cyber Rapid Response Teams and Mutual Assistance in Cyber Security” –kyberpuolustushankeen jäsen- ja tarkkalijamaat (CRRT, 2023).

Hankkeen tarkoitus on kehittää jäsenmaiden kyberkyvykkyyksiä ja valmiuksia kyberpoikkeaman hallinnassa ja sen ennaltaehkäisemisessä (CRRT, 2023). Hankkeen mukainen suorituskyky perustuu jäsenmaiden yhteistyöhön, sekä parhaiden käytänteiden ja toimintamallien harjaannuttamiseen. Osallistujamaat delegoivatkin tiettyjen eri alojen asiantuntijoita yhteiseen rotatoivaan joukkoon, joka kykenee vastaamaan monialaisiin poikkeamatilanteisiin (sama, 2023). Rotatoinnista vastaavaksi valitaan vuosittain yksi jäsenmaa, jonka tehtävänä on toimeenpanna CRRT:n yhteinen vuosisuunnitelma, joka koostuu yhteistapaamisien järjestämisestä jäsenvaltioiden sekä mahdollisten avustettavien maiden kanssa, vuosittaisen rotaatioharjoituksen järjestämisestä, sekä toimeenpantavien kokonaisuuksien koordinoinnista (sama, 2023). Vuosittaiset rotaatiot ja niiden mukaiset suunnittelu- ja toimeenpanotilaisuudet ovatkin mahdollistaneet joukon poliittisen tuen varmistamisen (Political Support), hallinnollisten sääntöjen laatimisen (Governance Rules),

lakiperusteisten toimintaperiaatteiden varmistamisen (Establishment of Legal Basis for Provision), vakioitujen toimintaohjeiden laatimisen (Standard Operating Procedures), työkalujen luomisen (Cybertoolkit), harjoitusten toimeenpanon sekä toiminnan taloudellisen tuen varmistamisen (sama, 2023). Vuoteen 2022 mennessä suoritetut toimenpiteet on esitetty kuviossa 20.

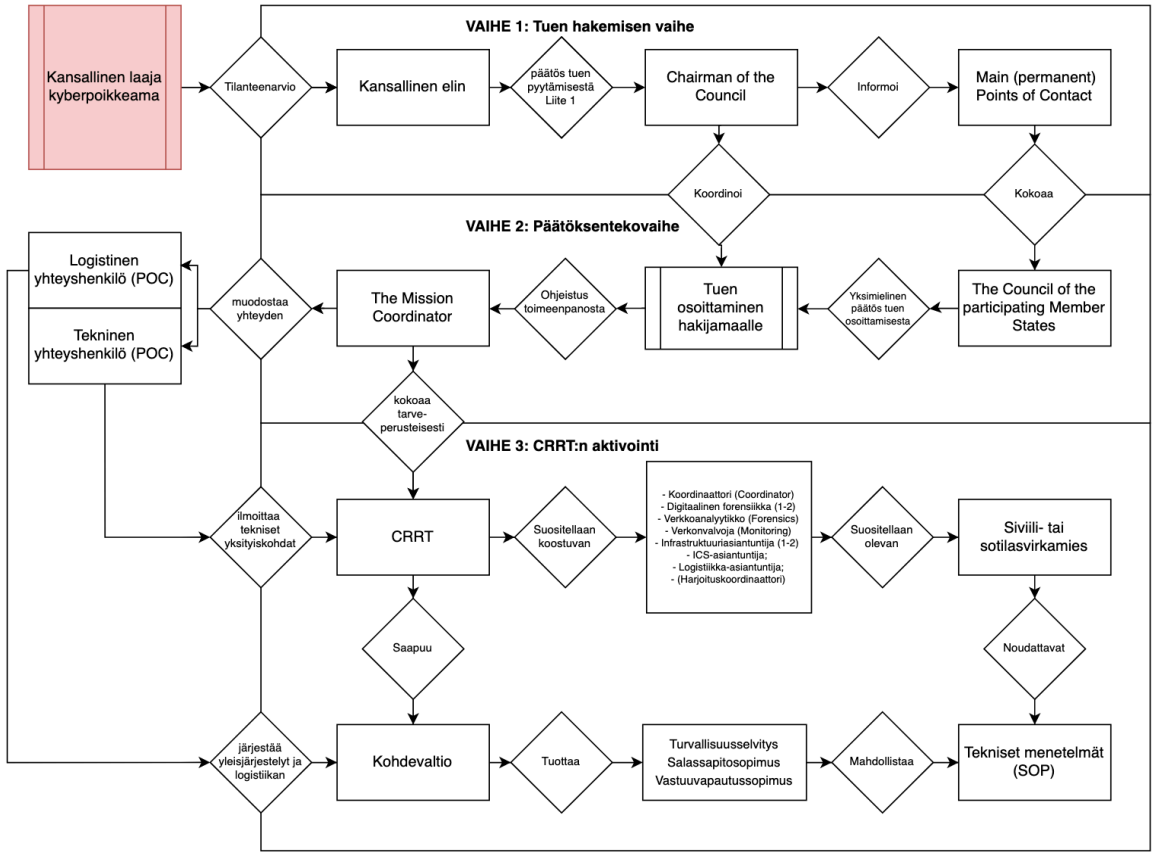


KUVIO 20 CRRT:n julkaistu toiminta vuoden 2018-2022 välillä (CRRT, 2023).

3.2.1 Cyber Rapid Response Teams (CRRT)

CRRT:n ensimmäinen harjoitus oli vuonna 2018 järjestetty Amber Mist -pöytäharjoitus (Table Top Exercise), jossa käsiteltiin CRRT:n toimeenpanemien operaatioiden mukaisia johtamisprosesseja ja muita hallinnollisia kokonaisuuksia (Vasiliauskaitė & Šakūnas, 2018). Ensimmäinen toiminnallinen yhteisharjoitus toimeenpantiin vuonna 2019, jonka tavoitteena oli harjaannuttaa joukkoa kriittisessä infrastruktuurissa toimeenpantavassa puolustuksellisissa kyberoperaatioissa, joissa pyrittiin uhkien tunnistamiseen, arviointiin, estämiseen ja neutralisointiin (Ministry of National Defence of Lithuania, 2019). Harjoituksista kehitettiin CRRT:n toimintoja ja prosesseja kuvaavia muistioita, jotka ovat ainoat julkiset toimintaa kuvaavat asiakirjat. Muistioiden mukaan CRRT:n toimeenpanemat operaatiot voivat olla reaktiivisia, joilla vastataan jäsenmaiden tai EU:n instituutioiden ilmoittamiin käynnissä oleviin laajoihin kyberpoikkeamiin, tai proaktiivisia ja ennaltaehkäiseviä, joilla suojataan ja mahdollistetaan tietojärjestelmien käytettävyys yleisen uhkatason noustessa (sama, 2018, s. 29). Esimerkiksi Venäjän hyökkäys Ukrainaan johti vuonna 2022 Euroopan Unionin päätökseen mobilisoida CRRT ensimmäistä kertaa, osana Ukrainalle osoitettua kansainvälistä tukea. Operaation lähetettiin yhteisellä päätöksellä noin 10 asiantuntijaa Kroatiasta, Virosta, Liettuasta, Alankomaista, Puolasta ja Romaniasta (Cerulus, 2022). Päätös lähettämisestä tehtiin Ukrainan pyynnöstä, joka oli saanut tiedustelutiedon pohjalta ennakkovaroituksen tulevasta kybervaikuttamisesta osana Venäjän sodan aloitusta (CERT-UA, 2022). Ukraina esittikin pyynnön asiantuntijaryhmästä, joka suorittaisi haavoittuvuuksien evalvuointia Ukrainan kriittisimmissä tietoverkoissa ja -järjestelmissä, sekä osoittaisi teknistä kalustoa ja ohjelmistoja kyberpuolustuksellisen infrastruktuurin vahvistamiseksi (Cerulus, 2022).

CRRT:n toimintaa kuvaavan muistion perusteella (Vasiliauskaitė & Šakūnas, 2018) joukon toimeenpanemat operaatiot voidaan nähdä jakautuvan kolmeen vaiheeseen, koostuen tuen hakemisen vaiheesta, päätöksentekovaiheesta ja CRRT:n aktiivivaiheesta. Joukkojen käyttöönoton prosessi on esitetty kuviossa 18.



KUVIO 21 CRRT -joukkojen käyttöönoton prosessikuvaus (Vasiliauskaitė & Šakūnas, 2018).

Joukkojen käyttöönoton toimenpiteet käynnistyvät vastaanottajamaan tukipyynnöstä, joka esitetään CRRT:n neuvoston puheenjohtajalle vastaanottajamaan korkeimman valtiollisen kyberturvallisuudesta vastaavan viraston tai instituution toimesta (Vasiliauskaitė & Šakūnas, 2018, s. 15). Tuen hakeminen tapahtuu asiakirjalla, joka on esitetty Liitteessä 3. Tukipyynnön vastaanottamisen jälkeen neuvoston puheenjohtaja informoi jäsenmaiden yhteyshenkilöitä, jonka seurauksena toimeenpannaan seuraavan vaiheen mukainen neuvoston kokous, jossa tulee saada yksimielinen päätös tuenosoituksesta hakijamaalle. Kollektiivisen päätöksenteon jälkeen neuvoston puheenjohtaja käynnistää tuen koordinoinnin, ja ohjeistaa neuvoston tehtäväkoordinaattoria CRRT:n mukaisenasiantuntijaryhmän kokoamisesta. CRRT:n mukainen asiantuntijaryhmä voi olla ennaltamääritetty, tai ryhmä voidaan koota erikseen määritellyistä jäsenmaiden rotatoivista joukoista, joista määritetään tapahtumakohtaisesti ryhmän jäsenet tilanteen ja tehtävän mukaan (sama, 2018, s. 22). Lisäksi tehtäväkoordinaattori muodostaa yhteyden kohdemaan logistisiin ja teknisiin yhteyshenkilöihin, jotka koordinoivat tekniset ja logistiset yleisjärjestelyt CRRT:n toiminnan mahdollistamiseksi.

Aktiivivaihe alkaa, kun CRRT-joukot saapuvat kohdemaahan. Joukot voivat koostuvat eri jäsenmaiden asiantuntijoista, joiden osaaminen on valikoitu vastaamaan kohdemaan tarpeita ja kyberuhkia. Joukkoon voi kuulua muun muassa tehtäväkoordinaattori, haittaohjelma- ja verkkortutkijat, verkonvalvontaan erikoistuneet asiantuntijat, infrastruktuuri- ja verkkoasiantuntijat sekä teollisen ohjausjärjestelmän (ICS) spesialisti, jotka operoivaat yhteistyössä kohdemaan teknisen ja logistisen yhteyshenkilön kanssa. Lisäksi kuvataan hyödylliseksi, että joukoissa on sekä siviili- että sotilastaustan omaavia asiantuntijoita, mikä mahdollistaa monipuolisen osaamisen hyödyntämisen ja parantaa yhteistyötä eri organisaatioiden välillä (Vasiliauskaitė & Šakūnas, 2018).

CRRT:n operointi kohdemaassa kuvataan vaativan useita valmisteluja ja sopimuksia, jotka takaavat joukkojen toiminnan tehokkuuden ja turvallisuuden. Ensinnäkin, kohdemaan on varmistettava joukkojen saapumisen logistiikka, mukaan lukien lentokenttäkuljetukset, majoitus ja työskentelytilat. CRRT:n onnistunut operointi kuvataan edellyttävän myös, että joukoilla on riittävät turvallisuusluokitukset, jotta he voivat käsitellä arkaluonteista tietoa. Lisäksi kuvataan tärkeäksi, että CRRT allekirjoittaa salassapitosopimuksen, jolla joukot sitoutuvat olemaan paljastamatta herkkää tietoa, johon he voivat törmätä tehtäviensä aikana. Kohdemaan on myös annettava vastuuvapauslauseke mahdollisista vahingoista, joita CRRT:n toimet voivat aiheuttaa operaation aikana (Eglė Vasiliauskaitė & Šakūnas, 2018).

CRRT:n tehtävänä on ensisijaisesti tukea isäntämaata kyberuhkien hallinnassa, mukaan lukien haittaohjelmien leviämisen estämisessä kriittisten palveluiden palauttamisessa ja kyberhyökkäysten analysoinnissa. Joukkojen toiminta perustuu tiiviiseen yhteistyöhön isäntämaan kanssa, ja ne toimivat kohdemaan kyberturvallisuudesta vastaavan kansallisen instituution mandaatin puitteissa. Toiminnassa kuvataan tärkeäksi, että CRRT:llä on pääsy tarvittaviin tietoihin ja järjestelmiin, jotta he voivat suorittaa tehtävänsä tehokkaasti (sama, 2018).

3.3 NATO

Pohjois-Atlantin liitto (The North Atlantic Treaty Organization, Nato), on perustettu takaamaan jäsenvaltioidensa turvallisuus poliittisen ja sotilaallisen yhteistyön kautta (Nato, A, 2023). Nato on tunnustanut kyberavaruuden kasvavan merkityksen nykyaikaisessa sodankäynnissä ja kansainvälisessä turvallisuudessa, mikä on johtanut liittouman kyberpuolustuksen strategian kehittämiseen. Tämän strategian ytimessä on liittouman omien verkkojen suojaaminen, tehokas toiminta kyberavaruudessa, jäsenvaltioiden kansallisen kyberresilienssin tukeminen ja alusta poliittiselle konsultaatiolle sekä kollektiiviselle toiminnalle (Nato, A, 2023; Nato, B, 2023). Liittolaismaat ovat sitoutuneet parantamaan tiedonvaihtoa ja keskinäistä apua kyberhyökkäysten ehkäisemisessä, lieventämisessä, toipumisessa ja niihin vastaamisessa (Nato, B, 2023).

Nato tekee yhteistyötä muun muassa Euroopan unionin (EU), Yhdistyneiden kansakuntien (YK) ja Euroopan turvallisuus- ja yhteistyöjärjestön (ETYJ) kanssa kyberpuolustuksessa (Nato, B, 2023). Kyberpuolustus onkin yksi vahvistuneen yhteistyön alueista Naton ja EU:n

välillä osana näiden kahden organisaation yhä koordinoidumpia pyrkimyksiä torjua sotilaallisiin ja kriittisen infrastruktuurin kohteisiin kohdistettavaa hybridivaikuttamista. Kollektiivista kyberturvallisuutta korostettiin myös yhtenä merkittävänä aiheena Naton Vilnan huippukokouksessa 11.-12. heinäkuuta 2023, jonka yhteydessä pilotoitiin Virtual Cyber Incident Support Capability -kyvykkyyttä (VCISC), joka on liittouman tuorein pyrkimys jäsenvaltioiden kyberpuolustuskyvykkyyksien vahvistamiseen (Martin, 2023; Nato, B, 2023). VCISC mukaisten RRT-joukkojen (Rapid Response Team) toimintatapojen rajoitetusta dokumentoinnista, tutkimuksista ja julkisuudesta johtuen joukkojen toimintatapamalleja ei ole kuvattu tässä tutkimuksessa. Tutkimuksen viitekehyksen näkökulmasta joukot ovat kuitenkin merkittävä osa kyberpuolustuksen kehitystä Naton toiminnan näkökulmasta, jonka myötä niiden toimintaa on esitelty lyhyesti tässä tutkimuksessa.

3.3.1 Virtual Cyber Incident Support Capability (VCISC)

Virtual Cyber Incident Support Capability (VCISC) on suunniteltu tukemaan jäsenvaltioita vastaamaan merkittäviin haitallisiin kyberaktiivisuuksiin tarjoamalla oikea-aikaista teknistä tukea ja asiantuntemusta. Kyky perustuu jäsenvaltioiden vapaaehtoiseen osallistumiseen ja mahdollistaa nopean reagoinnin kyberhyökkäyksiin, vähentäen niiden potentiaalista vahinkoa ja parantaen koko liittouman kybersietoisuutta (Luckenbaugh, 2023). Pilotointi Vilnan kokouksessa osoitti VCISC:n merkityksen ja potentiaalin käytännössä. Kokouksen aikana 11 maata, mukaan lukien Albania, Belgia, Viro, Puola, Alankomaat, Norja, Slovenia, Slovakia, Espanja, Turkki ja kokouksen isäntämaa Liettua, yhdistivät voimansa ja tarjosivat virtuaalista teknistä tukea Liettuan kansalliselle kyberturvallisuuskeskukselle mahdollisten kohdistettujen hyökkäysten varalta (Rousi & Bordelon, 2023). Tämä osoitti, kuinka VCISC voi toimia tehokkaana välineenä kansallisten kyberturvallisuuspyrkimysten tukemisessa ja kuinka jäsenvaltiot voivat yhdessä vastata kyberuhkiin nopeasti ja koordinoidusti (Nato, B, 2023; Roussi ym., 2023).

VCISC:n pilotointi Vilnan huippukokouksessa voidaan nähdä korostavan liitouman sitoutumista kyberuhkien torjuntaan ja jäsenvaltioiden kyberturvallisuusvalmiuksien vahvistamiseen. Se on konkreettinen askel kohti yhteistyöhön perustuvaa lähestymistapaa kyberpuolustuksessa, joka kattaa sekä teknisen tuen että poliittisen konsultaation, varmistaen Naton ja sen jäsenvaltioiden kyvyn vastata nopeasti ja tehokkaasti kyberuhkiin. Vaikka VCISC on tuore suorituskyky eikä sen prosesseista tai toiminnoista ole vielä julkisesti saatavilla paljon tietoa, se on erittäin merkittävä osa kyberpuolustuksen kehitystä Naton toiminnan näkökulmasta. Naton ylläpitämän VCISC:n kehittäminen ja käyttöönotto korostaakin kasvavaa kiinnostusta CPT ja CRRT -tyyppisten joukkojen suorituskyvyn kehittämiseen ja käyttöönottoon.

4 TUTKIMUS JA SEN MENETELMÄT

Tässä luvussa käsitellään tutkimuksessa käytettyjä tutkimusmenetelmiä sekä -ongelmia ja analyysimenetelmiä. Lisäksi esitellään tutkimuksen hypoteesit, aineistot ja tutkimuksen teemahaastatteluiden menetelmät ja toteutuksen periaatteet. Lopuksi suoritetaan tulosten luotettavuuden ja eettisyyden arviointi. Tutkimus toteutettiin laadullisena tutkimuksena, joka mahdollisti kartoittavat tutkimuksen toteuttamisen. Kartoittavan tutkimuksen keinoin pyrittiin tunnistamaan eri muuttujia muissa maissa toteutettujen vastaavien operaatioiden eri vaiheista (Kaplan & Maxwell, 2005, s. 40-55).

Tuomen & Sarajärven (2018) mukaan teorian rooli on laadullisessa tutkimuksessa kiistaton, mikä tekee sen käytön välttämättömäksi. Tutkimusprosessin alkuvaiheessa kävikin ilmeiseksi, että suomenkielisessä tutkimuksissa ei ole aikaisemmin käsitelty kybersuojajoukkojen käyttöä osana kriittisen infrastruktuurin suojaamista, vaikka useat länsimaat ovat toteuttaneet yhteisiä kyberoperaatioita kriittisen infrastuktuurin tietoverkoissa (USCYBERCOM, 2020). Näin ollen aihealueella oli huomattava vaje niin tutkimuksesta kuin myös teoriasta, erityisesti suhteutettuna kriittisen infrastruktuurin toimintaympäristöön ja sen suojaamiseen, tukien aihealueen valintaa suomenkielisen teorian ja osaamisen kehittämiseksi.

4.1 Tutkimusongelma ja hypoteesit

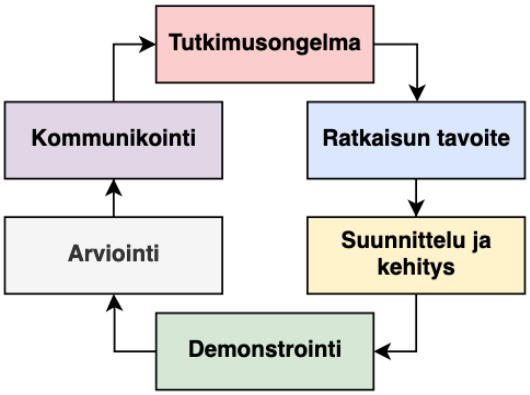
Tutkimusongelmaksi tunnistettiin tarve luoda kokonaisvaltainen toimintatapamalli kybersuojajoukkojen toteuttamien puolustuksellisten kyberoperaatioiden suunnittelun ja toimeenpanon mahdollistamiseksi kriittisen infrastruktuurin kohdearkkitehtuurissa operatiivisella ja teknis-taktisella tasolla, samalla huomioiden strategisen tason vaatimukset. Tutkimusongelma muodostettiin aineistolähtöisellä sisällönanalyysilla aikaisemmasta tutkimustiedosta, jonka pohjalta tuotettiin tutkimusongelmaan vastaavan toimintatapamallin luonnos. Teoriapohjaista toimintatapamallin luonnosta kehitettiin 7 asiantuntijahaastattelun kautta kerättyjen tietojen, havaintojen ja palautteen pohjalta.

Edgar ym. (2017, s. 69) mukaan tutkijan tulee teoretisoida ja luoda hypoteesi, joka olisi olemassa, jos teoria pitäisi paikkansa. Hypoteesi muodostaa heidän mukaansa tutkimusongelman ytimen. Hypoteesi

määritellään ennakoivaksi lausumaksi järjestelmän käyttäytymisestä, joka on testattavissa todistein (Edgar ym., 2017, s. 69–70). Bodeau, Graubart & Heinbockel (2013, s. 13) täydentävät, että hypoteesin tulee ottaa huomioon uhkiin, teknologiaan ja toimintaan liittyvät näkökohdat, kuten läsnä olevat uhkat, käytettävät teknologiat ja organisaation roolit ja vastuut. Näin ollen hypoteesi voidaan kuvata tarkaksi ennusteeksi, joka perustuu nykyiseen tietoon ja sisältää teknisiä, uhkiin liittyviä ja toiminnallisia komponentteja, ja sen paikkansapitävyys voidaan testata. Tämän tutkimuksen hypoteesina oli, että kehitettävällä toimintatapamallilla kyetään kuvaamaan kybersuojajoukkojen käyttöönottoprosessia operatiivisella ja teknis-taktisella tasolla, sekä tunnistamaan tapahtumat, toimijat, toimenpiteet ja rajoitukset operaation suunnittelun ja toimeenpanon osalta. Toisena hypoteesina oli, että nykytilassa viranomaisilla ei ole riittäviä toimintaedellytyksiä toimeenpanna kansallisten tai kansainvälisten kybersuojajoukkojen kyberoperaatiota kansallisen kriittisen infrastruktuurin suojaamisen näkökulmasta. Jälkimmäisen hypoteesin perusteeksi tunnistettiin, että toteutetun sisällönanalyysin perusteella lainsäädäntöä ei ole ajanmukaistettu kyberturvallisuuden vaatimuksia vastaaviksi. Muun muassa Lehdon ym. (2017, s. 36) mukaan lainsäädännön tulisikin antaa eri alojen toimivaltaisille viranomaisille riittävät toimivaltuudet toteuttaa yhteiskunnan elintärkeiden toimintojen suojaamista kyberuhkia vastaan, joka ei heidän mukaansa toteudu tällä hetkellä.

4.2 Tutkimusmenetelmät

Remus & Wiener kuvaavat (2008, s. 25–52), kuinka tietojärjestelmien tutkimusalueella on alettu yhä enemmän suosia monimenetelmällisiä lähestymistapoja. Heidän näkemyksensä mukaan erilaisten menetelmien yhdistäminen mahdollistaa monipuolisista lähteistä saatujen tietojen vertailemisen ja vahvistamisen, mikä voi parantaa tutkimusten luotettavuutta. Tämä käsitys on linjassa myös tämän tutkimuksen valittujen metodien kanssa, joissa on käytetty sekä tietojärjestelmien, että havainnollistavien tutkimusten menetelmiä (Hevner, Salvatore, Jinsoo & Sudha, 2004, s. 75). Tutkimuksessa päädyttiinkin käyttämään suunnittelutieteellistä metodologiaa (Design Science Research, DSR; Peffers ym., 2008). Peffersin ym. (2008) tutkimus kuvaa kuusi vaihetta DSR:lle: **1) ongelman tunnistaminen** ja tutkimuksen tarve, jossa määritetään ja perustellaan tutkimusongelma; **2) ratkaisun tavoitteiden määrittäminen**, jossa ongelmaan hahmotellaan realistiset ratkaisutavoitteet; **3) suunnittelu ja kehitys**, jossa luodaan ongelman ratkaisemiseen tarkoitettu tuote; **4) demonstraatio**, jossa tuotteen ratkaisukyky osoitetaan; **5) arviointi**, jossa vertaillaan tavoitteita saavutettuihin tuloksiin ja tarvittaessa palataan tuotteen kehitysvaiheeseen; **6) kommunikointi**, jossa tuloksista kerrotaan sekä muille tutkijoille että yleisölle. Peffersin ym. (2008) kuvaus DSR:n prosessikehikosta on esitetty kuviossa 19.



KUVIO 22 Suunnittelutieteellisen metodologian (DSR) vaiheistus (Peffers ym., 2008).

Peffers ym. (2008) kuvaavat, kuinka DSR:n tutkimusprosessissa ei ole pakko edetä lineaarisesti vaiheesta 1 vaiheeseen 6. He esittävät neljä vaihtoehtoista lähestymistapaa. Nämä lähestymistavat voivat olla:

- Ongelmalähtöisiä, jolloin prosessi aloitetaan tunnistamalla ja motivoiden tutkimusongelma;
- Tavoitelähtöisiä, jolloin tavoitteet määritellään ongelman perusteella ja lähtökohtana on artefaktin kehittämisen tarve;
- Suunnittelu- ja kehityskeskeisiä, joissa lähtökohtana on olemassa oleva artefakti, jonka pohjalta luodaan uusi ratkaisu; tai
- Asiakas- ja kontekstilähtöisiä, joissa prosessi alkaa artefaktin demonstroinnista ja pohjautuu käytännön ratkaisun havainnointiin.

Käsillä oleva tutkimus toteutettiin tavoitelähtöisenä suunnitteluttutkimuksena, jonka tavoitteena oli pyrkiä kehittämään toimintatapamalli, artefakti, kybersuojajoukkojen operatiivisen ja teknis-taktisen tason suunnittelun mahdollistamiseksi. Artefaktin kehittäminen ei Hevnerin ym. (2004) mukaan kuitenkaan usein tähtää täysimittaisen sovelluksen luomiseen, vaan sen keskeinen tehtävä on ideoiden generointi sekä käytänteiden ja teknisten potentiaalien määrittely. Lisäksi Peffers ym. (2008) korostavat, kuinka DSR:n avulla voidaan pyrkiä tuottamaan tutkimusongelmaan vastaava konkreettinen lopputuote ja mahdollisesti todentaa sen toimivuus käytännössä.

DSR:n vaihtoehtoiseksi metodologiaksi tunnistettiin konstruktiivinen tutkimusote (Constructive Research Approach, CRA) jonka avulla tunnistettiin myös mahdolliseksi kehittää ratkaisumalleja tai -tuotteita vastaamaan käytännön ongelman tarpeita, samalla lisäten ymmärrystä niiden toiminnasta (Kasanen, Lukka, & Siitonen, 1993; Lukka, 2003). Piirainen & Gonzales (2013) ovatkin tutkimuksessaan verranneet DSR:n ja CRA:n välisiä yhtäläisyyksiä ja eroja. Heidän tutkimuksensa perusteella arvioitiin, että DSR keskittyy tutkimuksen näkökulmasta paremmin luomaan täysin uusia, innovatiivisia ratkaisuja ongelmiin, CRA:n keskittyessä käytännöllisten ratkaisujen luomiseen olemassa oleville ongelmille. Lisäksi heidän mukaansa CRA:ssa, toisin kuin DSR:ssä, on tuloksen ilmentäminen olennainen osa tutkimusprosessia. Koska käsillä olevan tutkimuksen artifaktia ei ole mahdollista suoranaisesti ilmentää, koettiin DSR:n mahdollistavan kattavamman toimintatapamallin kehittäminen, mahdollistaen tutkimuksen keskittämisen artefaktin suunnitteluun ja kehittämiseen (Piirainen & Gonzales, 2013, s. 40-43).

4.3 Tutkimuksen vaiheistus

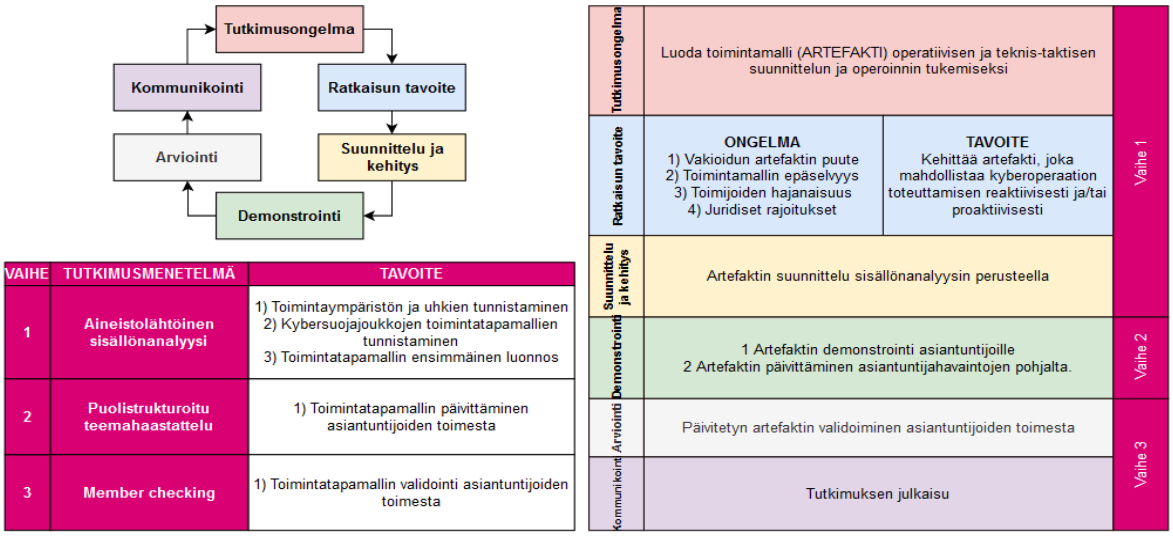
Peffersin ym. (2007) esittämän DSR:n vaiheiden ympärille laadittiin oma kolmiosainen vaiheistus, perustuen eri tutkimus- ja aineistonkeruumenetelmien tehokkalle ja vaiheistetulle käytölle. Tutkimuksen vaiheet on esitetty kuviossa 20. Tutkimuksen aineistonkeruu toteutettiin perinteisen kirjallisuustutkimuksen menetelmin. Tuomen ja Sarajärven (2018) mukaan teoreettisessa kirjallisuustutkimuksessa keskeiseksi kysymykseksi nousee uskottavuus, joka kiteytyy siihen, kuinka johdonmukaisesti ja pätevästi argumentaatio rakennetaan ja lähdeaineistoa hyödynnetään. Heidän mukaansa argumentaation näkökulmasta korostuvat lähdevalinnat, joiden tulee olla aiheen kannalta merkittäviä. Tutkittavasta aihealueesta ei kuitenkaan ollut olemassa aikaisempaa kansallista tutkimusta, minkä lisäksi kansainvälinen tutkimus koostui ainoastaan yksittäisistä avoimesti saatavilla olevista julkaisuista. Näin ollen tutkimuksen alussa oli ilmeistä, että aihealueen tutkiminen tulisi vaatimaan julkaistujen tutkimusten lisäksi eri valtioiden asevoimien ohjesääntöjen ja julkaisujen hyödyntämistä osana tutkimuksen rakentamista.

VAIHE	TUTKIMUSMENETELMÄ	TAVOITE
1	Aineistolähtöinen sisällönanalyysi	1) Toimintaympäristön ja uhkien tunnistaminen 2) Kybersuojajoukkojen toimintatapamallien tunnistaminen 3) Toimintatapamallin ensimmäinen luonnos
2	Puolistrukturoitu teemahaastattelu	1) Toimintatapamallin päivittäminen asiantuntijoiden toimesta
3	Member checking	1) Toimintatapamallin validointi asiantuntijoiden toimesta

KUVIO 23 Tutkimusmenetelmien vaiheistus.

Tutkimuksen kolmiosaisen vaiheistuksen **ensimmäisessä vaiheessa** toteutettiin aineistolähtöinen sisällönanalyysi, joka pohjautui eri lähteistä kerättyihin tutkimuksiin, ohjeistuksiin ja kuvauksiin. Sisällönanalyysin tarkoituksena oli luoda syvällinen ymmärrys empiirisen osan esittämille tuloksille sekä niiden taustalla oleville tekijöille ja ilmiöille. Kerätyn aineiston avulla muodostettiin teoreettinen ymmärrys kriittisen infrastruktuurin ja energiatoimialan toimintaympäristöstä ja uhkista operatiivisella tasolla (kappale 2), sekä kybersuojajoukoista ja niiden toimintatapamalleista taktis-teknisellä tasolla (kappale 3). Kerättyjen tietojen pohjalta muodostettiin tutkimuksessa kehitettävän toimintatapamallin ensimmäinen versio. Tutkimuksen **toisessa vaiheessa** toimeenpantiin seitsemän puolistrukturoitua teemahaastattelua. Haastatteluihin osallistui kriittisen infrastruktuurin toimintojen edustajia, valtionhallinnon virkamiehiä sekä muita teknisiä asiantuntijoita. Haastateltaville asiantuntijoille luvattiin täysi anonymiteetti. Haastatteluiden teemat käsittelivät kybersuojajoukkoja ja niiden käyttöperiaatteita strategisella, operatiivisella ja taktis-teknisellä tasolla, mukaillen CATWOE-analyysin perusperiaatteita (Bergvall-Kåreborn, Mirijamdotter & Basden, 2004).

CATWOE-analyysi on kuudesta elementistä koostuva työkalu, joka auttaa ymmärtämään ja arvioimaan erilaisia päätöksenteon ja ongelmanratkaisun näkökulmia. Analyysin avulla pyrittiin tunnistamaan kybersuojajoukkojen käyttöönoton toimijoita, toimintatapoja ja prosesseja ja muita vaikuttavia tekijöitä. Tutkimuksen **kolmannessa vaiheessa** aineistolähtöisen sisällönanalyysin ja asiantuntijahaastatteluiden pohjalta kehitetty toimintatapamalli toimitettiin validoitavaksi ja arvioitavaksi haastatteluihin osallistuneille asiantuntijoille, mahdollistaen viimeisten huomioiden esittämisen. Tällä pyrittiin varmistamaan haastatteluiden asiantuntijoiden näkemysten oikeinymmärrys, sekä kehitetyn toimintatapamallin luotettavuus. Asiantuntijoille tarjottiin kolmen viikon aikaikkuna tutustua ja kommentoida lopullista toimintatapamallia. Tutkimuksen kokonaisuus ja tutkimusmenetelmien vaiheistus sidottuna DSR:n vaiheistukseen on esitetty kuviossa 21 (Peffers ym., 2007).



KUVIO 24 Peffersin ja muiden (2008) malli DSR:n prosessista, sekä prosessikehikon vaiheiden soveltaminen käsillä olevaan tutkimukseen.

4.4 Haastatteluiden toteutus

Hirsjärvi, Remes & Sajavaara (2009, s. 208) kuvaavat, kuinka teemahaastatteluille on tyypillistä, että käsiteltävät asiakokonaisuudet ovat etukäteen haastattelijan tiedossa, kysymysten muotoilun ja esitysjärjestyksen vaihdellessa haastatteluiden kulun mukaisesti. Tuomen ja Sarajärven (2018) mukaan tämä korostaa haastateltavien omia tulkintoja, kokemusta ja toimintatapoja, antaen vastauksille syvällisempää merkitystä. Heidän mukaansa haastatteluiden toteuttamisen heikkous on niihin käytettävä aika ja johtopäätösten luotettavuus. Hirsjärvi ym. (2009, s. 207) korostavat myös niiden konteksti- ja tilannesidonnaisuutta.

Tässä tutkimuksessa tuotettu pääaineisto pohjautui puolistrukturoiduissa teemahaastatteluista kerätyille tiedoille ja havainnoille. Haastattelut etenivät etukäteen valittujen teemojen mukaisesti, samalla käsitellen tarkentavia ja syventäviä kysymyksiä haastateltavien vastausten perusteella (Tuomi &

Sarajärvi, 2018, s. 85-87). Haastateltavat edustivat julkisen sektorin viranomaisia ja yksityisen sektorin ammattilaisia, joilla tunnistettiin olevan osaamista eri organisaatioiden ja tasojen johtamis- ja asiantuntijatehtävistä. Haastatteluiden avulla kerätty tieto arvioitiin luotettavaksi, perustuen haastateltavien asemaan, koulutukseen ja asiantuntijuuteen. Koska haastatteluiden tarkoituksena oli pyrkiä kuvaamaan ja luomaan tulkintoja ja ymmärrystä ennestään tutkimattomista ilmiöistä, valikoitui haastateltaviksi henkilöitä, joilla arvioitiin ja tunnistettiin olevan entuudestaan paljon tuntemusta tutkittavan aiheen mukaisesta toimintaympäristöstä ja toimintatapamenetelmistä. Henkilöt profiloitiin julkisten lähteiden tiedonhankinnan perusteella soveltuviksi asiantuntijahaastatteluun, minkä lisäksi haastatteluiden päätteeksi haastateltavilta tiedusteltiin muita mahdollisesti haastateltaviksi soveltuvia henkilöitä. Henkilöitä ei suoranaisesti haastateltu organisaatioiden edustajina, vaan haastattelut painottuivat asiantuntemuksen ja kokemuksen mukaisiin havaintoihin toimintaympäristöstä.

Haastatteluja toteutettiin yhteensä seitsemän asiantuntijan kanssa. Haastatteluiden toteutuksessa hyödynnettiin ennalta laadittua haastattelurunkoa, jonka toteutuksessa hyödynnettiin CATWOE-analyysiä, joka määrittelee systeemitasolla asiakkuuden, toimijat, muutosprosessit, näkökulmat, omistajat ja toimintaympäristön (Pöyhönen, 2020, s. 100). Haastattelurunko koostui kuudesta osakokonaisuudesta ja 15 niiden käsittelyä tukevasta apukysymyksestä. Osakokonaisuudet ja niiden mukaiset apukysymykset on esitetty liitteessä 6. Haastateltaville toimitettiin myös etukäteen tutkimuksen ensimmäisessä vaiheessa kehitetty toimintatapamalli, joka käsitti operatiivisen ja teknis-taktisen tason vaiheistuksen joukkojen käyttöönotosta ja suoritettavista toimenpiteistä.

Haastattelut toteutettiin etähaastatteluina tammi-maaliskuussa 2024. Haastatteluihin varattiin aikaa yksi tunti haastateltavaa kohden, mutta todellisuudessa haastatteluijen kestot vaihtelivat 60 minuutista 90 minuuttiin, riippuen käytössä olevasta ylimääräisestä ajasta. Ennen haastatteluiden toteuttamista haastateltavia toimitettiin suostumus haastatteluun osallistumisesta, jossa anottiin lupaa tutkimustulosten käyttöön osana Pro Gradu -tutkielmaa. Lisäksi suostumuksella varmistuttiin luvasta nauhoittaa haastattelu. Haastateltaville välitetyn kirjallisen suostumuksen pohja on esitetty liitteessä 4. Haastatteluissa hyödynnettiin äänitallentamisen mahdollistavaa kokoussovellusta, jonka tallenteille suoritettiin litterointi ja anonymisointi henkilö- ja organisaatiotietojen osalta, mahdollistaen niiden jatkokäsittely julkisen tutkimuksen puitteissa. Haastatteluiden ja litteroinnin aikana kiinnitettiin myös erityishuomiota haastatteluiden sisältöön turvaluokituksen näkökulmasta, jolla varmistuttiin aineiston jatkokäsittelystä julkisen tutkimuksen puitteissa.

Pöyhösen mukaan (2020, 105) eri vallankäyttötasoille voi muodostua toisistaan poikkeavia näkökulmia ja odotuksia toimintatapamallien kehityksen suhteen, sekä toiminnan resursseista, menetelmistä ja aikatauluista, johtaen haasteisiin linjauksista ja toimenpiteistä päätettäessä. Tästä johtuen haastateltaville jaettiin ennakkoon toimintatapamalli sekä esitettävät kysymykset kokonaisuuden ja aihealueen ennenaikaisen hahmottamisen mahdollistamiseksi, sekä yhteisten lähtökohtien mahdollistamiseksi. Ennakkoon jaettu materiaali ei suoranaisesti näkynyt haastatteluissa, sillä jokaisen haastattelun alussa pidettiin noin 20 minuutin yleisesittely tutkimusaiheen mukaisesta viitekehyksestä, toimintatapamallista ja

aikaisemmista havainnoista ja toimintatapamallin muutoksista. Ennakkomateriaaliin tutustumista ei haastateltavilta erikseen vaadittu, minkä myötä haastateltavien ennakkoymmärrys vaihteli aihealueen osalta. Havainnon mukaan ennalta laadittu esitysmateriaali olikin kriittinen haastattelun toteutumisen osalta, mikä itsessään herätti tarpeeksi keskustelua toimintatapamallin kehitysideoiden suhteen. Tämän myötä ennalta laadittuja kysymyksiä ei suoranaisesti hyödynnetty haastatteluissa, sillä esittelymateriaalin pohjalta heräsi keskustelua, jonka kautta keskustelua ohjattiin muodostamaan vastauksia nousseisiin kokonaisuuksiin, joiden oikeinymmärrys varmistettiin haastateltavilta tasaisin väliajoin. Lisäksi haastatteluiden lopussa kerätyt huomiot vedettiin yhteen, ja niiden oikeinymmärrys varmistettiin. Havaintojen mukaan kysymyksiin vastattiin erittäin spesifisti, mikä mahdollisti haastattelijalle jatkokysymysten esittämisen toimintatapamallin yksityiskohtaisen kehittämisen suhteen.

4.5 Luotettavuuden ja eettisyyden tarkastelu

Luotettavuuskysymykset voidaan nähdä Saaranen-Kauppisen & Puusniekan (A, B, 2006) mukaan koostuvan validiteetista ja realabiliteetista. Validiteetti määrittää heidän mukaansa tutkimuksen pätevyyden, sekä tulosten päätelmien "oikeellisuuden". Lisäksi he kuvaavat, kuinka tutkimuksessa voi ilmetä virheitä esimerkiksi tutkijan nähdessä tarkasteltavien kokonaisuuksien suhteita tai periaatteita virheellisesti. Reliabiliteetti taas Saaranen-Kauppisen & Puusniekan (2006) mukaan ilmaisee sen, miten luotettavasti ja toistettavasti käytetty tutkimus- tai mittausmenetelmä mittaa tutkittavaa ilmiötä. Mikään tutkimus ei kuitenkaan heidän mukaansa pysty tuottamaan täydellistä ymmärrystä siinä käsitellyistä asioista.

Tässä tutkimuksessa luotettavuuteen ja eettisyyteen pyrittiin sen kaikissa vaiheissa, pyrkien tarkastelemaan aihetta ennakkoluulottomasti ja objektiivisesta näkökulmasta. Luotettavuuteen panostaminen näkyi teemahaastatteluissa keskusteluiden nauhoittamisella sekä litteroinnin kaksinkertaisella läpikäynnillä, jolla pyrittiin vähentämään väärintulkintoja tai muita epähuomioita. Haastateltaville luvattiin täysi anonymiteetti, minkä lisäksi haastateltavilta pyydettiin kirjallinen suostumus haastatteluun osallistumisesta. Tutkimuksen lopussa haastateltaville toimitettiin teemahaastatteluiden pohjalta tuotettu toimintatapamalli. Tarkoituksena oli tuottaa DSR:n mukainen kehitetyn artefaktin arviointi, minkä lisäksi haastateltaville annettiin ennen tutkimuksen julkaisua mahdollisuus täydentää ja kommentoida tutkimuksen toimintatapamallin kehityksen tuloksena esiin nousseita asioita. Viimeisen kommenttikierroksen saatekirje on esitetty liitteessä 5.

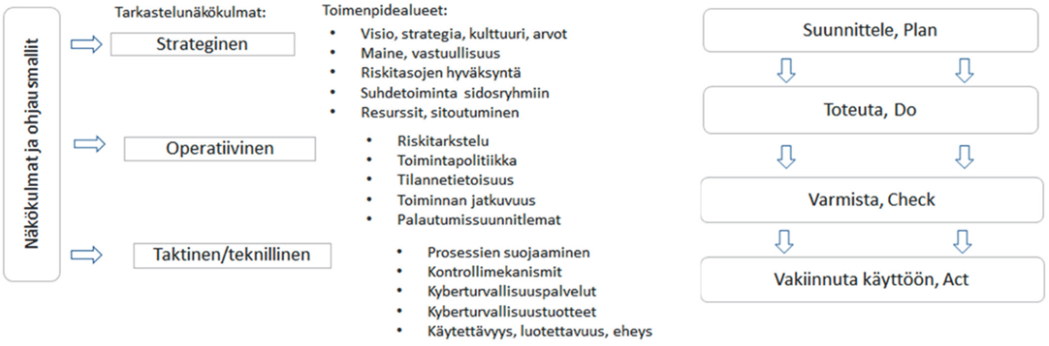
5 KYBERSUOJAJOUKKOJEN PUOLUSTUKSELLISTEN KYBEROPERAATIOIDEN TOIMINTATAPAMALLI

Tässä luvussa käsitellään kybersuojajoukkojen käyttöönoton toimintamenetelmiä operatiivisella tasolla, sekä kybersuojajoukkojen toimenpiteitä taktis-teknisellä tasolla. Osion tarkoitus on vastata tutkimuksen pääkysymykseen: "Minkälaisella prosessilla mahdollistetaan kybersuojajoukkojen puolustuksellisen kyberoperaation toimeenpaneminen?". Tämän luvun painopiste onkin pyrkiä luomaan operatiivisen ja taktisen tason toimintatapamalli, joka kuvaa prosessia kybersuojajoukkojen käyttöönoton eri vaiheissa.

Tämä luku rakentuu siten, että aluksi esitellään aineistolähtöisen sisällönanalyysin pohjalta kehitetty toimintatapamalli, jonka jälkeen esitetään asiantuntijoiden näkemyksien ja palautteen pohjalta kehitetty toimintatapamalli, joka toimii tutkimustuloksena. Luvussa kehitetyt toimintatapamallit on esitetty myös liitteissä, josta niiden yksityiskohtaisempi tarkastelu on mahdollista. Liitteessä 7 on kehitetty alkuperäinen malli. Liitteessä 8 on esitetty haastatteluiden pohjalta kehitetty toimintamalli, joka toimii tutkimuksen lopullisena toimintatapamallina.

5.1 Toimintatapamallin kehittäminen

Tutkimuksessa kehitetetyn toimintatapamallin kehitettämiseen ja päivitettämiseen hyödynnettiin Pöyhösen (2020) kyberturvallisuuden kehitystoimenpiteiden implementointikehystä, jonka arvioitiin mahdollistavan tarkastelunäkökulmat strategiselta, operatiiviselta, sekä teknis-takniselta tasolta, johtaen toiminnan suunnitteluun, toteutukseen, varmistukseen ja käyttöönvakiinnuttamiseen (Pöyhönen, 2020, s. 181). Mallin tunnistettiinkin auttavan ottamaan huomioon kybersuojajoukkojen puolustuksellisten kyberoperaatioiden eri vaiheet alkaen suunnittelusta toteutukseen, tarkistukseen ja vakiinnuttamiseen. Lisäksi mallin avulla onnistuttiin löytämään rajapinta operatiivisen ja teknis-taktisen tason välillä. Toimintatapamallin kehityksessä hyödynnetty kehitystoimenpiteiden implementointikehys on esitetty kuviossa 20 (Pöyhönen, 2020, s. 181).

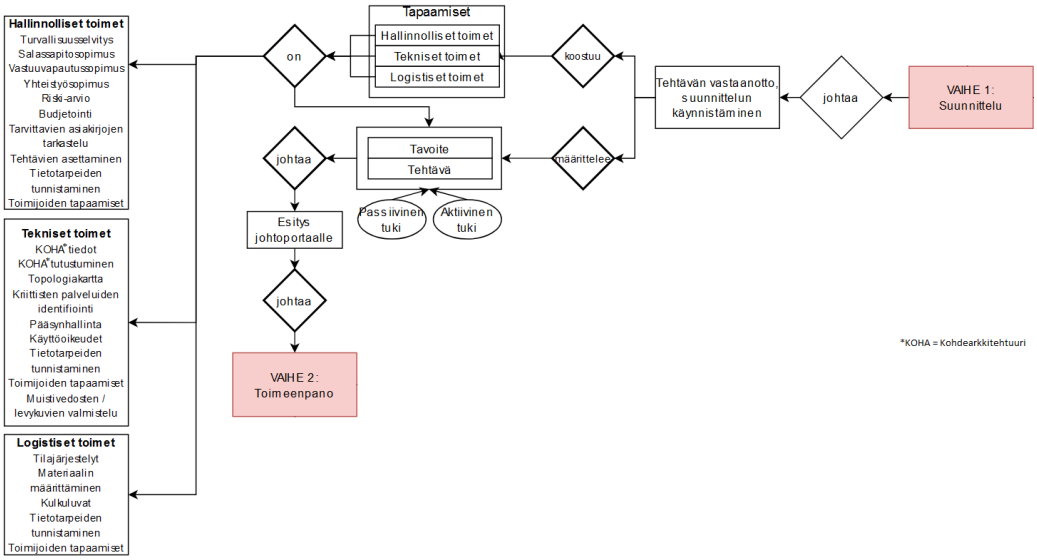


KUVIO 25 Tutkimuksessa kehitetyn toimintatapamallin viitekehyksenä hyödynnettiin Pöyhösen (2020, s. 181) kuvausta kyberturvallisuuden kehitystoimenpiteiden implementoinnista.

Toimintatapamallin suunnittelu käynnistettiin teknis-taktiselta tasolta, joka perustui Trentin ym. (2016, 2019) esityksiin CPT:n toimintatapamalleista. Lisäksi taktis-teknisen tason toimintatapamallin kehityksessä huomioitiin Pöyhösen (2020) kehitystoimenpiteiden mukaisesti prosessit, kontrollimekanismit sekä kyberturvallisuuspalvelut ja -tuotteet. Näiden tuottamiseen arvioitiin kyettävän kattavammin teknis-taktisen tason ensimmäisessä vaiheessa, jolloin operaation toimintaedellytykset sovitaan. Teknis-taktisen tason jälkeen siirryttiin kehittämään operatiivisen tason toimintatapamallia, joka perustui EU:n CRRT-joukkojen käyttöönottoprosessin mukaisiin huomioihin (Vasiliauskaitė & Šakūnas, 2018). Lisäksi operatiivisen tason kehittämisessä huomioitiin toimintaympäristöanalyysin tuloksena tunnistettujen vastuuviranomaisten vastuualueita kriittisen infrastruktuurin ja energiatoimialan suhteen. Näin ollen vaiheessa luotujen viranomaisten vastuualueiden ja rajapintojen varmentaminen tunnistettiin olevan vaiheen tärkein kehittämiskohde. Haastatteluiden toimeenpanoa edeltävä toimintatapamalli on esitetty Liitteessä 7.

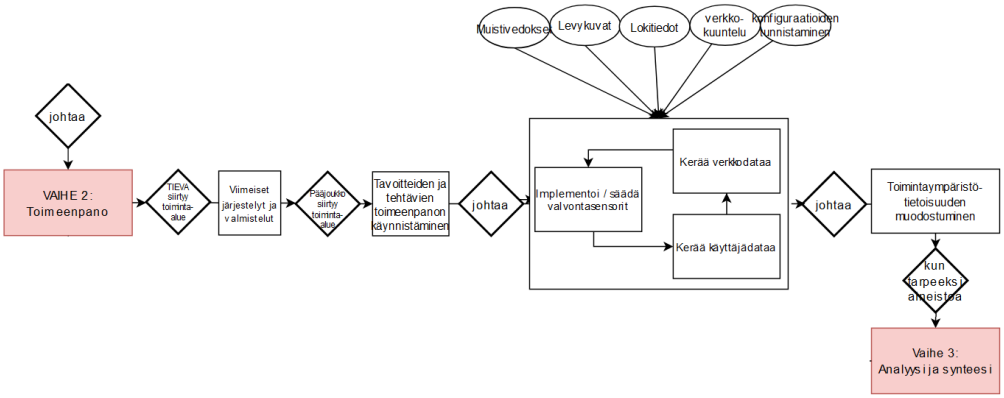
5.1.1 Teknis-taktisen tason toimintatapamallin kehittäminen

Taktis-teknisen tason ensimmäisen vaiheen suunnittelu käynnistettiin Yhdysvaltain USCYBERCOM:n CPT-joukkojen tehtäväarakenteen pohjalta. CPT-joukkojen tehtäväarakenne on esitetty kattavammin tutkimuksen kappaleessa 3.1.4. Tehtäväarakenteen tuottamisessa pyrittiin hyödyntämään Trentin ym. (2016; 2019) tutkimia CPT:n taktiikoita, tekniikoita ja proseduureja. Heidän esittämään rakenteeseen lisättiin kuitenkin ongelmanmäärittelyn, ensianalyysin, kohdearkkitehtuurin ensitietojen ja toimivaltuuksien (engl. Rules of Engagement, ROE) tilalle hallinnolliset toimet, tekniset toimet ja logistiset toimet, joiden olemassaolo tunnistettiin Euroopan Unionin CRRT -joukkojen käytön periaatteista. Tämän kautta luotiin kattavampi kuvaus tarpeellisista kokonaisuuksista, jotka arvioitiin mahdollistavan yksinkertaisemman vastuunjaon operatiivisella tasolla. Lisäksi tehtäviin ja tavoitteisiin lisättiin päätösvaihe passiivisen tai aktiivisen tuen osoittamisesta asiakkaalle. Edellä mainitussa tehtävässä CPT ei operoi itsenäisesti, vaan ohjeistaa tuettavaa asiakasta toimenpiteiden suorittamiseen, ja jälkimmäisessä CPT operoi itsenäisesti. Teknis-taktisen tason ensimmäisen vaiheen toimintatapamalliluonnos on esitetty kuviossa 26.



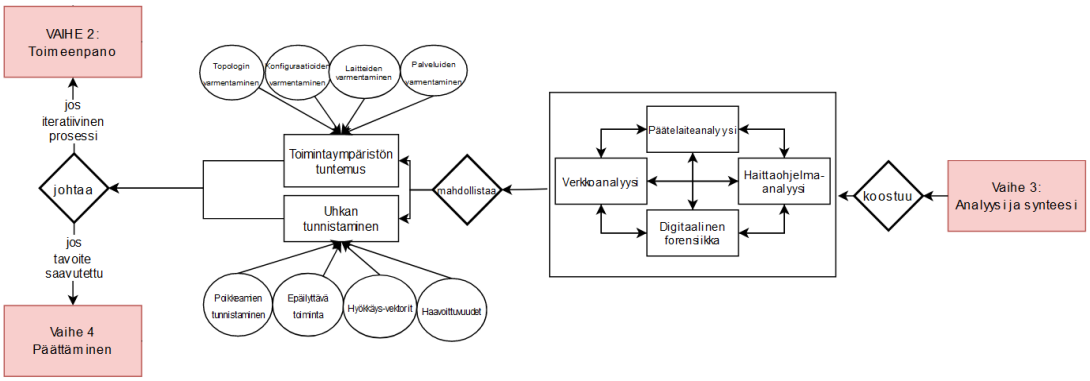
KUVIO 26 Teknis-taktisen tason vaiheen 1 ensimmäinen toimintatapamalliluonnos ennen haastatteluiden toteuttamista.

Kehitettävän toimintatapamallin teknis-taktisen tason operaation toisen vaiheen kehittämisessä hyödynnettiin vastaavasti Trentin ym. (2016, 2019) kuvausta CPT-toimintatapamallista. Vaiheistuksesta poistettiin tapaamiset asiakkaan kanssa, sillä se sisällytettiin ensimmäisen vaiheen hallinnollisten, teknisten ja logististen toimien kokonaisuuteen. Vaiheistukseen lisättiin kuitenkin niin kutsutun ”tiedustelu- ja valmisteluosaston” (TIEVA) siirtyminen toiminta-alueelle ennen pääjoukkoja, mahdollistaen toimintaympäristöön tutustumisen ja viimeisten järjestelyiden toteuttamisen ennen pääjoukon siirtymistä tehtäväalueelle (Maavoimien esikunta, 2008, s. 80-81). Lisäksi Trentin ym. esittämään kuvaukseen yhdistettiin keräys- ja analyysimenetelmät yhdeksi kokonaisuudeksi, jonka nähtiin kuvaavan toimintaa yksinkertaisemmin. Näiden tuloksena arvioitiin johtavan toimintaympäristötietoisuuden muodostumiseen, eli ymmärrykseen verkkoarkkitehtuurin teknisestä ympäristöstä ja sen käytöstä, käyttäjistä ja prosesseista. Tarpeellisen aineistomäärän ja toimintaympäristötietoisuuden jälkeen operaation arvioitiin siirtyvän kolmanteen vaiheeseen. Teknis-taktisen tason toisen vaiheen toimintatapamalliluonnos on esitetty kuviossa 27.



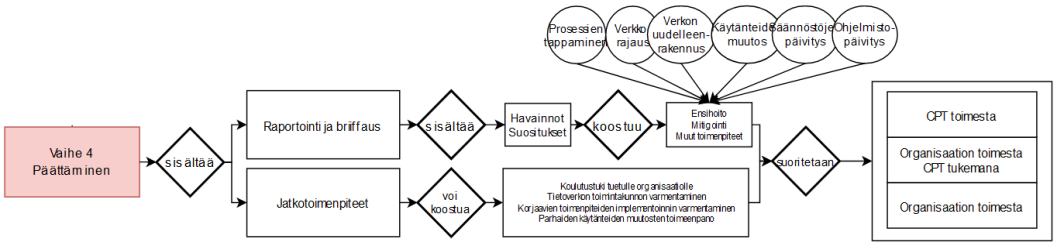
KUVIO 27 Teknis-taktisen tason vaiheen 2 ensimmäinen toimintatapamalliluonnos ennen haastatteluiden toteuttamista.

Teknis-taktisen tason kolmannen vaiheen kehittämisessä hyödynnettiin jälleen Trentin ym. (2016, 2019) kuvausta CPT-toimintatapamallista, joka perustui iteratiiviseen prosessiin vaiheen 2 välillä ennen siirtymistä vaiheeseen 4. Vaiheeseen ei tehty huomattavia muutoksia Trentin ja muiden esittämän mallin suhteen. Teknis-taktisen tason kolmannen vaiheen toimintatapamalliluonnos on esitetty kuviossa 28.



KUVIO 28 Teknis-taktisen tason vaiheen 3 ensimmäinen toimintatapamalliluonnos ennen haastatteluiden toteuttamista.

Myös teknis-taktisen tason neljännen vaiheen kehittäminen pohjautui Trentin ym. (2016; 2019) esittämään malliin, joka koostui raportointiin ja jatkotoimenpiteiden esittämisestä. Kuitenkin, laaditussa mallissa havaintoihin ja suosituksiin lisättiin tarkemmat kuvaukset ensihoidosta, mitigoinnista ja muista toimenpiteistä, jotka tunnistettiin olevan Trentin ym. (2016) kuvaus hyväksikäyttömahdollisuuksien poistamisen suhteen. Toimintatapamallin vaiheessa säilytettiin Trentin alkuperäisen mallin mukaisesti korjaustoimenpiteiden suorittaminen joko asiakkaan toimesta itsenäisesti, CPT:n tukemana tai CPT:n toimesta. Teknis-taktisen tason neljännen vaiheen toimintatapamalliluonnos on esitetty kuviossa 29.



KUVIO 29 Teknis-taktisen tason vaiheen 4 ensimmäinen toimintatapamalliluonnos ennen haastatteluiden toteuttamista.

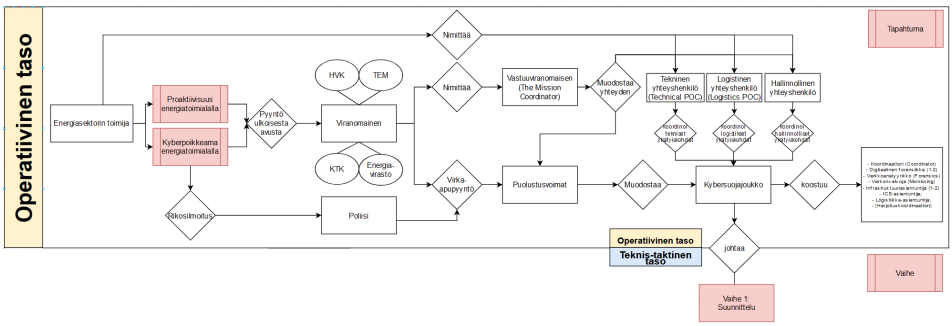
5.1.2 Operatiivisen tason toimintatapamallin kehittäminen

Operatiivisen tason toimintatapamallin kehittäminen perustui toimintaympäristöanalyysin tuloksena (kappale 2.1) tunnistettujen kriittisen infrastruktuurin ja energiatoimialan suojaamisen vastuuviranomaisten vastuualueisiin, sekä EU:n CRRT-joukkojen käyttöönottoprosessin mukaisiin huomioihin (kappale 3.2). Operatiivisen tason toimintatapamallin luonnos on esitetty kuviossa 30.

Joukkojen käyttöönoton tilanne jaettiin kahteen tapahtumaan, joista ensimmäinen on energiasektorin toimijan itsenäinen ja proaktiivinen tahto toteuttaa puolustuksellinen kyberoperaatio kohdearkkitehtuurissa, jälkimmäisen ollessa poikkeamalähtöinen tapahtuma, johtaen reaktiivisesti operaation toteuttamiseen. Lisäksi jälkimmäisessä tapauksessa olisi taustalla jo tehty rikosilmoitus, joka todennäköisesti perustuisi muun muassa Rikoslain[1] 38. lukuun, joka käsittelee tieto- ja viestintärikoksia.

Toimintaympäristöanalyysin perusteella (kts. kappale 2) toiminnan koordinointiin osallistuviksi viranomaisiksi tunnistettiin Huoltovarmuuskeskus (HVK), Työ- ja elinkeinoministeriö (TEM), Kyberturvallisuuskeskus (KTK) ja Energiavirasto. Kerätyn aineiston pohjalta HVK:n tunnistettiin vastaavan yhteiskunnan elintärkeiden toimintojen, kuten energian tuotannon, siirron ja jakelujärjestelmien ylläpidosta ja turvaamisesta, minkä myötä se arvioitiin keskeiseksi toimijaksi energiasektorin huoltovarmuuden turvaamisessa. TEM:n tunnistettiin energiatoimialan vastuuministeriöksi, vastaten energiatoimialan varautumisesta ja turvaamisesta, sisältäen myös toimenpiteet toiminnan suunnitteluun ja toimeenpanoon. KTK tehtäväksi tunnistettiin vastata kriittisen infrastruktuurin, mukaan lukien energiatoimialan, kyberturvallisuuden tukemisesta ja kyberuhkien hallinnasta osana toimintaympäristön suojaamista ja toiminnan jatkuvuuden varmistamista. Energiaviraston osalta tunnistettiin, että se vastaa sähkömarkkinoiden ja siirtoverkkotoiminnan tehokkuuden sekä varautumisen valvonnasta, varmistaen energiajärjestelmän kaikkien osa-alueiden sujuvan ja turvallisen toiminnan. Lisäksi Energiavirasto tunnistettiin energiatoimialan vastuuviranomaiseksi.

Puolustusvoimien ei tunnistettu julkisten lähteiden perusteella omaavan kybersuojajoukkojen mukaista joukkorakennetta. Tutkimuksen viitekehyksessä sen tunnistettiin kuitenkin olevan ainoa toimija, joka mahdollistaisi CPT- tai RRT-joukkojen mukaisen sotilas- ja virkamiesrakenteen. Lisäksi Puolustusvoimien arvioitiin kykenevän teoreettisesti käyttämään myös reserviläisiä operaatioiden toiminnassa Yhdysvaltain kansalliskaartin mukaisten CPT-joukkojen mukaisesti. Näin ollen tutkimuksen toimintatapamallin viitekehys rakennettiin Puolustusvoimien ympärille. Kybersuojajoukkojen rakenne muodostettiin CPT ja CRRT -joukkorakenteen pohjalta, koostuen yleisjohtajasta tai koordinaattorista, sekä useista eri asiantuntijoista, jotka tunnistettiin erikoistuneen muun muassa digitaaliseen forensiikkaan, verkkovalvontaan ja -analyysin, infrastruktuuriin ja OT-ympäristöön, sekä yleiseen logistiikkaan (Vasiliauskaitė & Šakūnas, 2018).

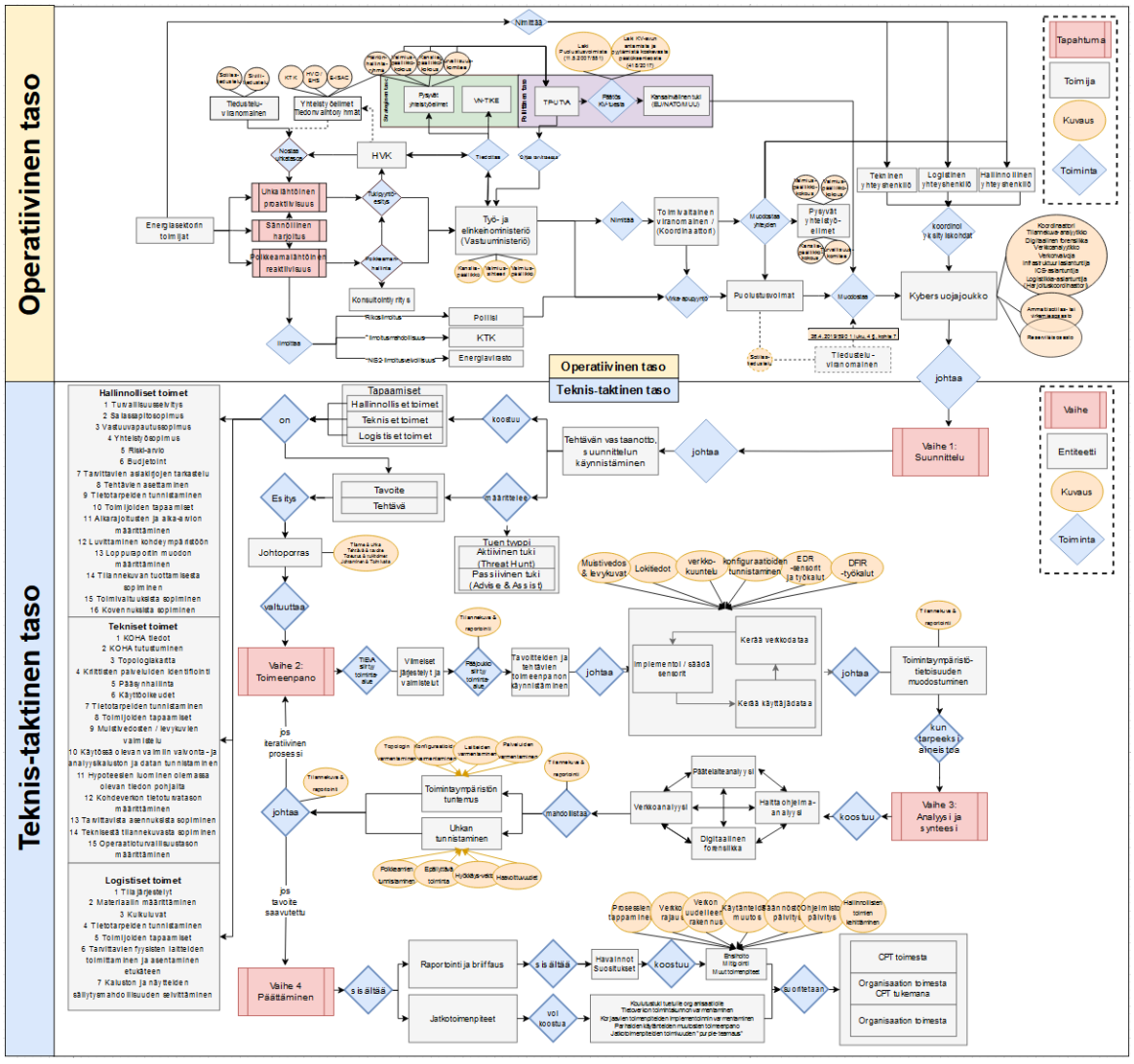


KUVIO 30 Operatiivisen tason toimintatapamalliluonnos.

[1] Rikoslaki 39/1889

5.2 Toimintatapamallin päivittäminen

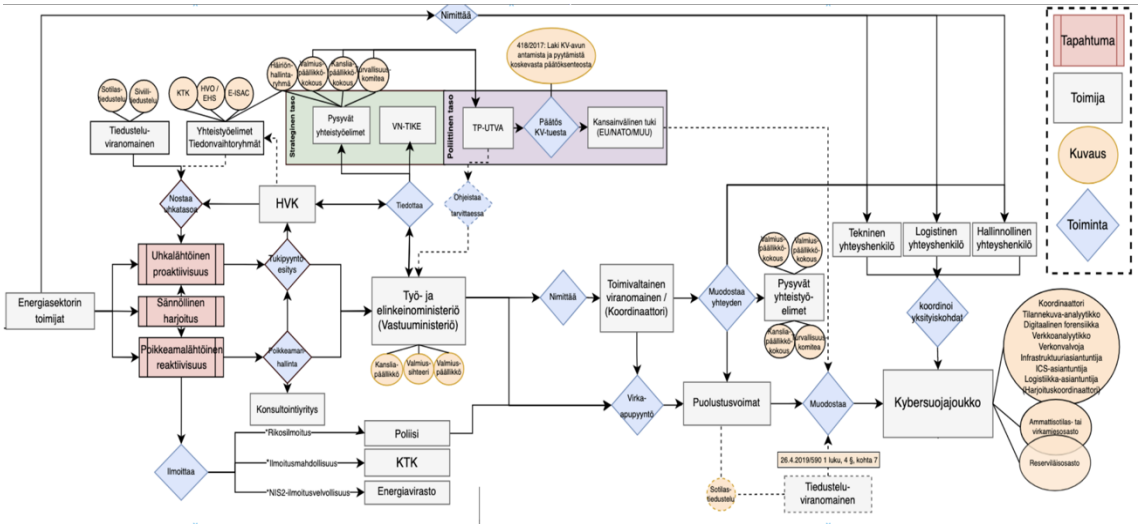
Tässä luvussa on esitetty tutkimuksessa kehitettävän toimintatapamallin päivitetty versio, joka perustuu vuoden 2024 aikana toimeenpantuun seitsemään asiantuntijahaastatteluun, joiden kautta kerättiin havaintoja toimintatapamallin operatiivisen ja teknis-taktisen tason huomioista ja mahdollisesti kehitettävistä kokonaisuuksista. Alaluvuissa on esitetty erikseen ja yksityiskohtaisemmin operatiivisen ja teknis-taktisen tason toimintatapamallien päivitykset, jotka pohjautuvat asiantuntijahaastatteluiden havaintoihin ja keskusteluihin, sekä näistä johdettuihin lähteisiin. Haastatteluiden pohjalta kehitetty lopullinen toimintatapamalli on esitetty kuviossa 25 ja liitteessä 8. Haastatteluissa käytetty haastattelurunko ja haastattelusta tiedottaminen on esitetty liitteessä 4.



KUVIO 31 Haastatteluiden pohjalta kehitetty lopullinen toimintatapamalli. Kuvio on esitetty yksityiskohtaisemmin liitteessä 8.

5.2.1 Operatiivisen tason toimintatapamallin päivittäminen

Kybersuojajoukkojen toimeenpanemien operaatioiden lähtötilannetta operatiivisella tasolla päivitettiin kolmeen eri tapahtumaan, koostuen uhkalähtöisistä proaktiivista operaatioista, poikkeamalähtöisistä reaktiivisista operaatioista, mutta myös näitä mukailevista, ennalta sovituista ja säännöllisistä harjoitustapahtumista. Yleisesti ottaen operatiivisen tason toimintatapamallin tehtiin useita päivityksiä toimijoiden, kuvausten ja toiminnan osalta, minkä lisäksi kuvaukseen lisätiin strateginen ja poliittinen taso, joilla tunnistettiin olevan pääasialliset päätöksentekoelimet. Operatiivisen tason päivitetty toimintatapamalli on esitetty kuviossa 26.

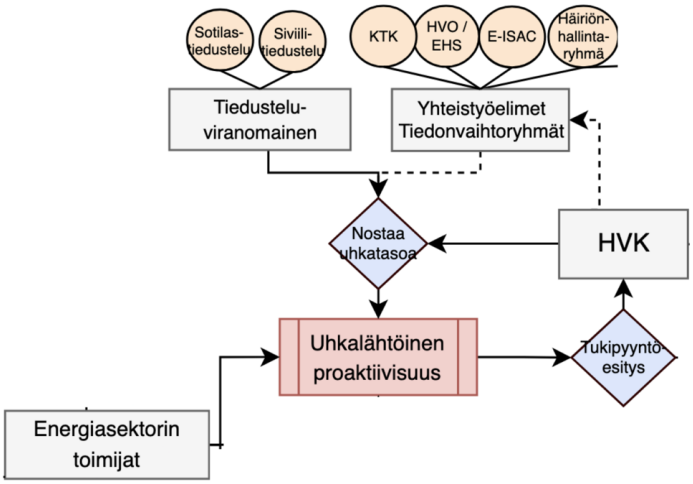


KUVIO 32 Operatiivisen tason toimintatapamallin päivitetty versio tapahtumien, toimijoiden, kuvausten ja toiminnan osalta.

Uhkalähtöisen proaktiivisen toiminnan osalta vapaaehtoiset yhteistyöelimet ja tiedonvaihtoryhmät tunnistettiin keskusteluissa keskeisiksi toimijoiksi uhkatason muutosten ja tilanneymmärryksen muodostamisessa. Huoltovarmuuskeskus (HVK) erottui keskeisenä koordinaattorina huoltovarmuuden uhkatason säätelijänä, joka toimi vastuuministeriön (TEM) ja Huoltovarmuusorganisaation (HVO) energiahuoltosektorin välisessä rajapinnassa. Uhkalähtöisen tilannekuvan muodostaminen ja tiedon jakaminen tunnistettiin liittyvän vahvasti HVO:n toimintaan, kun taas proaktiiviset toimenpiteet ja poikkeamien hallinta kuvattiin kytkeytyvän HVK:n rooliin varautumisen tehostamisessa ja huoltovarmuuden uhkatason säätelyssä. VIRT-häiriönhallintaryhmät ja ISAC-tiedonvaihtoryhmät tunnistettiin edistävän myös ennakollista tietoisuutta uhista jakamalla suodatettua tietoa riskeistä. Lisäksi keskusteluissa korostettiin sähköyhtiöiden kyberasiantuntijoiden muodostamia pienempiä tiedonvaihtoryhmiä, joissa toimijoiden kuvattiin vaihtavan avoimesti tietoa kybertilanteesta, ylittäen yritysten taloudellisen kilpailulliset rajat yleisen turvallisuuden varmistamiseksi. Tämä yhteistyö ja tiedonvaihto energiasektorilla nähtiin keskeiseksi uhkalähtöisen proaktiivisen toiminnan edistämisessä. Myös tiedusteluviranomaisten rooli nähtiin merkittävänä uhkavaroitusten tuottajana osana uhkatasojen säätelyä. Tiedusteluviranomaisten arviot uhkista, esimerkiksi valtiollisiin toimijoihin

yhdistetystä haitallisesta verkkoliikenteestä, tunnistettiin erittäin tärkeäksi uhkatasoa sääteleväksi ja mahdollisesti proaktiivisiin toimiin johtavaksi elementiksi. Tapausesimerkkeinä keskusteluissa nostettiin Suojelupoliisin kansallisen turvallisuuden vuosikatsaukset ja Venäjän hyökkäyssota Ukrainassa, jonka seurauksena kriittisen infrastruktuurin toimijoita on varoitettu kohonneesta vakoilu- ja kyberuhkasta ja kehoitettu kohottamaan valmiutta.

Haastatteluissa energiatoimialaa kohtaan kohdistuvien uhkien ei arvioitu kohdistuvan välttämättä suoraan kriittisen infrastruktuurin OT-verkkoympäristöön, vaan välillisesti energiatoimijan IT-toimistoverkkoon tai sen alihankintaketjuihin. Kohdennettu tiedonhankinta energiatoimijan hallinnollisesta IT-toimistoverkkoympäristöstä arvioitiin muodostavan uhkavektorin järjestelmiin, prosesseihin, tai henkilöstöön liittyvän herkän tiedon varastamiseksi. Kyseisten tietojen kautta arvioitiin mahdolliseksi pyrkiä luomaan ymmärrys tulevan vaikuttamisoperaation painopisteestä jalansijan asennuttamiseksi ja operaatioiden vaikuttamisvaiheen toteuttamiseksi. Kyseistä tietoa ei välttämättä yrityksen toimesta tunnistettaisi turvallisuusluokitelluksi tiedoksi, sillä yritykset eivät suoraan sovella asetusta asiakirjojen turvallisuusluokittelusta (1101/2019[2]), joka on suunnattu valtionhallinnon toimijoille. Yritykset noudattavat kuitenkin vähintään omia turvallisuusstandardeja ja -käytäntöjä, jotka todennäköisesti perustuvat alalla vakioituun standardiin- tai käytäntöön. Energiatoimialan uhkaksi tunnistettiin myös alihankintaketjujen muodostamat uhkat. Suomea kuvattiin keskenään verkottuneeksi maaksi, minkä lisäksi kriittisen infrastruktuurin huollon ja ylläpidon tunnistettiin olevan usein ulkoistettua toimintaa, mahdollistaen toimijoiden resurssien keskittämisen kriittisen infrastruktuurin mukaiseen tuotantoon ja palveluun. Lisäksi uhkaksi tunnistettiin OT- ja IT-tietoverkkojen konfiguraatiovirheet, joiden kautta voisi mahdollisesti muodosta verkkorajapinta julkisesti saatavilla oleviin tietoverkkoihin ilman, että yrityksen oma ylläpito-osasto havaitsee rajapinnan virheellistä muodostumista. Uhkalähtöisen proaktiivisen operaation käynnistymistä kuvaava toimintatapamallin on esitetty kuviossa 27.



KUVIO 33 Uhkalähtöisen proaktiivisen operaation käynnistymistä kuvaava toimintatapamalli ja sen mukaiset toimijat.

[2] Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019)

Poikkeamalähtöisen reaktiivisen toiminnan osalta haastatteluissa korostui Huoltovarmuuskeskuksen rooli uhkatilanteiden hallinnassa ja laajemman tilannekoordinoinnin toteuttamisessa, toimien yhteistyössä vastuuministeriön (TEM) sekä muiden keskeisten huoltovarmuuskriittisten toimijoiden kanssa. Lisäksi haastatteluissa nousi esiin NIS [3] - ja NIS2-direktiivien mukaiset ilmoitusvelvollisuudet toimialan valvontaviranomaiselle, sekä ilmoitus Kyberturvallisuuskeskukselle (Kyberturvallisuuskeskus, ei päivämäärää) ja tarvittaessa poliisille, mikäli tapauksessa oli rikosepäily. NIS-direktiivin mukaan keskeisten huoltovarmuuskriittisten toimijoiden ja palveluntarjoajien on ilmoitettava verkko- ja tietojärjestelmässä olevista tietoturvapoikkeamista toimialansa valvontaviranomaiselle, jossa energiatoimialalla valvontaviranomaisena toimii Energiavirasto (Kyberturvallisuuskeskus, ei päivämäärää). NIS2-direktiivin kuvattiin laajentavan ilmoitusvelvollisuutta, sisällyttämällä tietoturvapoikkeamien ilmoitusvelvollisuuden piiriin suuremman joukon organisaatioita sekä tiukentamalla ilmoitusprosesseja ja -aikatauluja[4].

Keskustelussa nousi myös esiin CER-direktiivi[5], jonka 9. artiklassa velvoitetaan EU:n jäsenvaltioita perustamaan tai nimeämään yhden tai useamman toimivaltaisen viranomaisen ja keskitetyn yhteyspisteen (Euroopan parlamentti & neuvosto, 2022). Sisäministeriön (2024) lausuntopyynnön luonnoksessa hallituksen direktiivin täytäntöönpanoesityksessä on esitetty, että ”yhteyspistetoiminnan” mukaisia tehtäviä jaetaan Huoltovarmuuskeskukselle, Valtioneuvoston tilannekeskukselle ja yhteensovittamistehtävää hoitavalle sisäministeriölle. Lakiluonnoksessa ei kuitenkaan nimetä yhtä kansallista keskitettyä yhteyspistettä, jonka myötä se ei tällä hetkellä mahdollista direktiivin mukaista säätämistä kokonaisuutena. Huoltovarmuuskeskuksen tunnistettiinkin esittäneen Sisäministeriön lausuntopyynnössä (Sisäministeriö, 2024), että lakiesityksen 8 § nimi muutettaisiin muotoon ”kansallinen keskitetty yhteyspiste”, ja että Huoltovarmuuskeskus nimettäisiin direktiivin 9. artiklan mukaiseksi yhteyspisteeksi, sekä että sille säädettäisiin 9. artiklan mukaiset yhteyspisteen tehtävät. Sisäministeriön lausuntopyynnön edetessä sen mukaisen keskitetyn yhteyspisteen muodostumisella tunnistettiin olevan mahdollinen vaikutus tutkimuksessa kehitettyyn toimintatapamalliin, jota ei tutkimuksen aikana kyetty arvioimaan[6].

Poikkeamalähtöisten toimenpiteiden käynnistämisen osalta haastatteluissa nousi myös esille, kuinka useat yritykset koordinoivat kyberpoikkeamatilanteet usein kaupallisten konsultointiyritysten kanssa. Keskusteluissa korostuikin, kuinka tietyt palvelut, kuten poikkeamiin vastaaminen (engl. Incident Response), ovat alueita, joilla yksityisen ja julkisen sektorin tarjonta voisi toimintatapamallin mukaisessa toiminnassa mennä päällekkäin tai muodostua vapaata markkinaa ja kilpailua rikkovaksi tai vaarantavaksi tilanteeksi, riippuen miten valtiolliset sekä yksityiset toimijat ja tuotannonalat osallistuisivat poikkeamanhallintaan. Keskusteluissa kuitenkin korostui, kuinka tällä hetkellä tähän ei ole

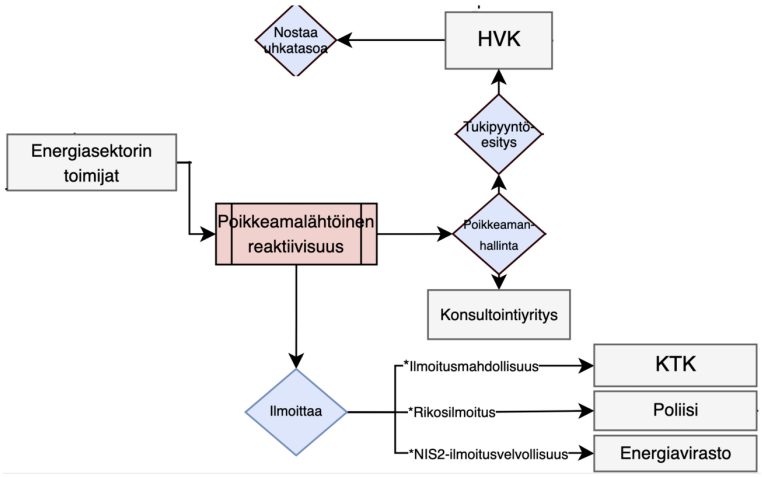
[3] The Network and Information Systems Regulations (NIS)

[4] NIS2-direktiivi astui voimaan 16. tammikuuta 2023, ja jäsenvaltioiden on saatettava direktiivin vaatimukset osaksi kansallista lainsäädäntöään viimeistään 17. lokakuuta 2024. Tutkimuksen aikana virallista päätöstä NIS2-direktiivin voimaantulosta ei ole tehty, mutta sillä tunnistettiin olevan mahdollinen vaikutus kehitettävään toimintatapamalliin.

[5] The Critical Entities Resilience Directive (CER)

[6] Lausunto- ja lakiesitys on tutkimuksen aikana vielä kesken.

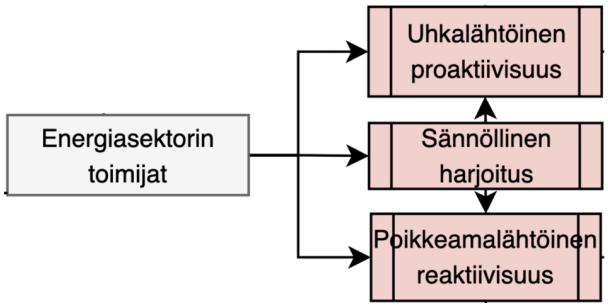
suoranaisesti vaaraa, koska kuvatun laatuista julkista toimijaa ei ole Suomessa. Haastatteluissa nousi esiin myös konsulttiyritysten toiminnan nopeus kyberturvallisuusongelmien ratkaisemisessa, minkä arvioitiin ylittävän normaalioloissa kybersuojajoukkojen käyttöönotto- ja operaatioiden toimeenpanoviiveen. Konsulttiyritysten kuvattiin tarjoavan "Battle Tested" osaamista 2–6 tunnin kuluessa poikkeamailmoituksesta, jonka kuvattiin mahdollistavan ongelmakohtien tunnistamisen tavalla, jota satunnaisemmin laajojen poikkeamatilanteiden parissa työskentelevät eivät välttämättä kykenisi ennakoimaan. Haastatteluissa tunnistettiin kuitenkin tilanteita, joissa kaupallisten konsulttiyritysten käyttö ei ole soveliasta tai mahdollista. Näistä erityisesti kansallista turvallisuutta vaarantavat laajat ja monialaiset poikkeamanhallintatilanteet sekä vihamielisen toiminnan taustalle tunnistettu valtiollinen toiminta ja tarve yhdistää toimet laajempaan ulko- ja turvallisuuspoliittiseen kontekstiin nähtiin tilanteiksi, joissa julkisen organisaation kybersuojajoukkojen käyttö oli perusteltua. Konsulttiyritysten tunnistettin mahdollistavan asiantuntevan teknisen avun tarjoamisen, mutta niiden kyky puuttua ja tunnistaa vihamielisen toiminnan juurisyy tai tavoite, tai estää valtakunnalliset lisävahingot nähtiin lähes olemattomaksi. Toimintaa kuvattiinkin tietoturvalähtöiseksi, jolloin kytkös ulko- ja turvallisuuspolitiikkaan tai viranomaisen operatiiviseen kontekstiin arvioitiin jäävän täysin puutteelliseksi. Lisäksi konsultointipalveluita kuvattiin tarjottavan poikkeamahallinnan palveluvarautumisen etukäteissopimuksena (engl Incident Response Retainer), rajoittaen palveluntarjontaa laajamittaisissa kansainvälisissä poikkeamanhallintatilanteissa, jotka vaativat samanaikaista toimintaa useassa kohteessa. Poikkeamalähtöisen reaktiivisen operaation käynnistymistä kuvaava toimintatapamallin on esitetty kuviossa 34.



KUVIO 34 Poikkeamalähtöisen reaktiivisen operaation käynnistymistä kuvaava toimintatapamalli ja sen mukaiset toimijat.

Haastatteluissa tunnistettiin myös mahdollisuus toteuttaa kybersuojajoukkojen puolustuksellisia kyberoperaatioita osana ennalta sovittua harjoituskokonaisuutta, jossa kybersuojajoukot suorittaisivat säännöllisiä turvallisuustarkastuksia kriittisen infrastruktuurin osalta. Tapausesimerkeiksi nostettiin Yhdysvaltain kansalliskaartin CPT-joukkojen harjoitukset, joissa osavaltioiden reserviläisistä pääosin koostuvat paikallisjoukot suorittavat säännöllisiä harjoituksia kriittisen infrastruktuurin toimijoiden kanssa ilman

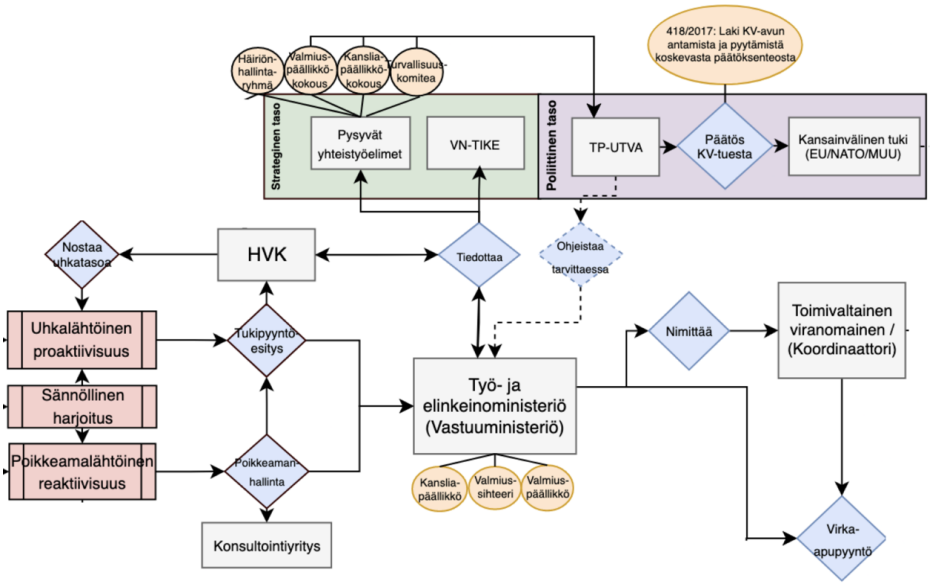
suoraa uhkaa (Jessica Roles, 2023). Säännöllisten harjoitusten kuvattiin mahdollistavan kriittisten toimintojen suunnitelmallisen läpikäyntiin, toimintaympäristöön tutustumiseen ja hallinnollisten toimien ennenaikainen sopiminen. Tämän nähtiin korostavan sotilaallisesti kriittisen infrastruktuurin turvallisuuden merkitystä (engl. Critical Infrastructure Protection, CIP; Military Critical Infrastructure, MCI; Mission Vital Infrastructure, MVI) ja sen laajentunutta käsitettä, jonka nähtiin sisältävän enemmän kuin pelkästään puolustusteollisuuden tai logistiikkainfrastruktuurin palvelut ja järjestelmät. Harjoituskokonaisuudesta johdettava toimintatapamalli on esitetty kuviossa 29.



KUVIO 35 Kybersuojajoukkojen ennalta suunniteltu, määräaikaistyyppinen harjoituskokonaisuus nähtiin voivan olevan joko uhkalähtöinen tai poikkeamalähtöinen harjoitus, joka perustuisi erillisiin juridisesti sovittuihin sopimuksiin kriittisen infrastruktuurin toimijoiden välillä. Harjoituksessa kuvattiin kyettävän käyvän suunnitelmallisesti läpi kriittisen infrastruktuurin toimijoita ja niiden turvallisuutta, mahdollistaen toimintaympäristöön tutustumisen ja hallinnollisten asiakirjojen valmistelun ennenaikaisesti.

Haastatteluissa korostui Työ- ja elinkeinoministeriön merkittävä rooli vastuuministeriönä erityisesti voima- ja polttoainehuollon turvaamisessa sekä energiatoimialan laajassa poikkeamanhallinnassa. Toiminnan ytimessä kuvattiin olevan muun muassa Valtioneuvoston ohjesäännön (3.4.2003/262) ja Yhteiskunnan turvallisuusstrategian (Turvallisuuskomitea, 2017) mukainen vastuunjakomalli, jossa määritellään vastuuministeriöt häiriö- ja poikkeustilanteissa. Näissä tilanteissa kuvattiin mahdolliseksi tarpeeksi kutsua koolle kansliapäällikkökokous tai ylimääräinen valmiuspäällikkökokous, jossa ensin mainitussa otettaisiin johtoasema operatiivisen päätöksenteon ja toiminnan koordinoinnin suhteen. Turvallisuuskomitean toiminnan kuvattiin toimivan tärkeänä varautumisen foorumina, mutta kansliapäällikkökokouksen johtoasema operatiivisessa päätöksenteossa ja toiminnan koordinoinnissa koettiin poikkeamanhallinan osalta ensisijaisen tärkeäksi. Näin ollen, tutkimuksen kontekstissa nostettiin esille, kuinka monitasoista yhteistyötä ja koordinointia tarvitaan häiriötilanteiden hallinnassa, minkä operatiivisen johtamisen keskiössä on kansliapäällikkökokous, kun taas Turvallisuuskomitea todettiin keskittyvän ennakoivaan varautumiseen. Haastatteluissa korostettiin myös TP-UTVA:n tai mahdollisuutta ohjeistaa tapahtuman tilannekuvan ja sen tarpeen määrittelyssä ja vastatoimenpiteiden koordinoinnissa, kuitenkin korostaen Työ- ja elinkeinoministeriön ensisijaista vastuuta vastuuministeriönä, jonka toimintaa muiden tahojen nähtiin tukevan. Keskustelut heijastivat ajatusta, että yhteistoimintamallissa ja Yhteiskunnan turvallisuusstrategiassa (Turvallisuuskomitea, 2017) on selkeä vastuunjakomekanismi, joka voi muuttua tilanteen hallinnan edetessä tai jos esimerkiksi Poliisin käynnistää tapauksesta

rikostutkinnan. Vastuuministeriönä toimivan Työ- ja elinkeinoministeriön toimintaa kuvaava toimintatapamalli on esitetty kuviossa 36.



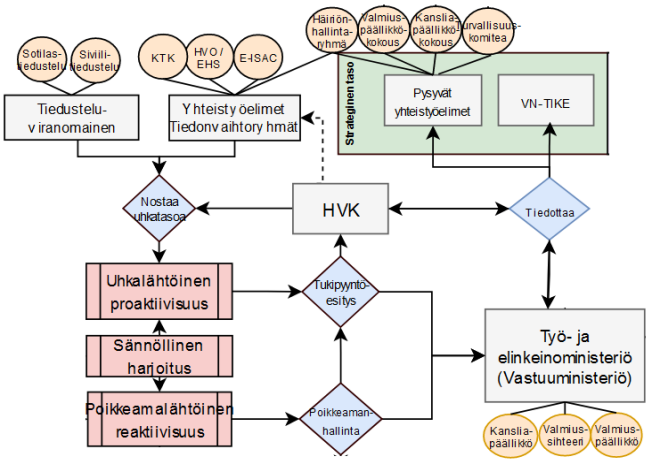
KUVIO 36 Vastuuministeriönä toimivan Työ- ja elinkeinoministeriön toimintaa kuvaava toimintatapamalli.

Haastatteluissa korostettiin, kuinka COVID-19-pandemian[7], Balticconnector-kaasuputken katkeamisen[8] ja psykoterapiakeskus Vastaamon tietomurron[9] kaltaisissa poikkeamatilanteissa valtiollinen reagointi rakentuu monitasoiselle yhteistyölle ja vastuunjaolle eri hallinnonalojen ja toimijoiden kesken. Näissä yhteyksissä kansliapäällikkö- ja valmiuspäällikkökokousten merkitys nähtiin korostuvan keskeisinä yhteistyö- ja päätöksentekofoorumeina, joissa määriteltiin, kuka kriisitilanteissa toimintaa johtaa ja miten vastuut jaetaan. Haastatteluissa tuotiin myös esille, että kokouksissa ei suoranaisesti päätetä aktiivisista toimenpiteistä, mutta ovat avainasemassa yhteistyön ja vastuunjaon määrittämisessä.

COVID-19-pandemian osalta haastatteluissa korostettiin havaintoja siitä, kuinka nopeasti tunnistettiin tarve laajentaa kansliapäällikkökokoukseen osallistuvien hallinnonalojen ja organisaatioiden määrää. Vastaamon tapauksen puolestaan korostettiin alleviivaavan, kuinka kyberpoikkeamien monialaiset seuraukset voivat ulottua useille hallinnonaloille, johtaen vastuun ja toimivallan määrittelyn haasteellisuuteen. Näissä esimerkeissä korostettiin, että yhteistyö ja valmiuden koordinointi eri toimijoiden kesken on kriittistä kriisitilanteiden tehokkaassa hallinnassa, ja että yhteistyörakenteet

[7] COVID-19 oli koronaviruspandemia, joka alkoi vuoden 2019 lopussa Wuhanista, Kiinasta, ja levisi maailmanlaajuiseksi terveyskriisiksi.
[8] Balticconnector-kaasuputki katkesi laahaavan ankkurin johdosta Suomenlahdella 8. lokakuuta 2023, keskeyttäen kaasunsiirron Suomen ja Viron välillä.
[9] Tietomurrossa asiakastietojärjestelmästä varastettiin tuhansien ihmisten potilaskertomuksia. Tapahtuma koostui usean viranomaisen ja ministeriön yhteystyöstä, yhteensovittamisesta ja avustamisesta. Kokonaisuudessa oli osallisena Keskusrikospoliisi, Liikenne- ja Viestintäministeriön Kyberturvallisuuskeskus, Sosiaali- ja Terveysministeriön keskusvirasto Valvira sekä Valtioneuvosto. Tämän lisäksi teknisessä tutkinnassa osallisena oli konsultointiyrityksiä (Hakoniemi, Jussi-Pekka, 2021).

mahdollistavat joustavan reagoinnin laajoihin ja monimutkaisiin haasteisiin. Balticconnector-kaasuputken vaurioitumisen yhteydessä haastatteluissa korostui tiedonvaihdon ja koordinoinnin tärkeys Huoltovarmuuskeskuksen (HVK), huoltovarmuusorganisaation, energiatoimijoiden ja Työ- ja elinkeinoministeriön (TEM) välillä. Tämä monitahoinen yhteistyö nähtiin keskeisenä energiasektorin kriisinhallinnassa, toimien HVK:n, TEM:n ja energiatoimijoiden välisenä rajapintana. Tapauksessa korostui HVK:n rooli tiedottamisessa ja varautumistasojen nostattamisen ohjeistamisessa huoltovarmuuskriittisille yrityksille, sillä Balticconnector-kaasuputken poikkeamatapauksen seurauksena HVK kehotti huoltovarmuuskriittisiä yrityksiä varautumaan mahdollisiin uhkiin kriittisen infrastruktuurin osalta. Lisäksi HVK:n nähtiin olevan keskeinen toimija myös TEM:n tiedottamisessa ja toiminnan operatiivisessa koordinoinnissa. Tämän nähtiin toimivan proaktiivisena välineenä, mahdollistaen reagoinnin muuttuviin turvallisuustilanteisiin. Turvallisuustilanteen muuttuessa HVK:n tehtäväksi kuvattiinkin tilannetiedon ja ohjeiden jakaminen huoltovarmuuskriittisille yrityksille sekä elinkeinoelämän ja julkisen sektorin varautumisyhteistyön edesauttaminen. HVK:n toiminta toimintatapamallin viitekehyksessä on esitetty kuviossa 31.



KUVIO 37 Huoltovarmuuskeskuksen keskeinen toiminta uhkalähtöisessä ja poikkeamalähtöisessä toiminnassa.

Keskusteltaessa virka-avun vastaanottamisesta ja antamisesta, nousi haastatteluissa esille, kuinka lainsäädäntö ei määrittele selkeästi, ketkä kaikki ovat oikeutettuja pyytämään ja saamaan virka-apua. Kybersuojajoukkojen käyttöönoton osalta keskustelussa nousikin esille viranomaisen pyynnöstä tai rikosilmoituksesta johdettavan virka-avun rooli kybersuojajoukkojen käyttöönotossa. Toiminnan perustavanlaatuiseksi rajoitukseksi tunnistettiinkin Puolustusvoimien virka-avun osoittaminen Poliisille, Työ- ja elinkeinoministeriölle, Kyberturvallisuuskeskukselle, Energiavirastolle ja Huoltovarmuuskeskuksen toimivaltaisen viranomaiselle. Puolustusvoimien toiseksi tehtäväalueeksi on määritetty muiden viranomaisten tukeminen ja virka-avun antaminen muun muassa yleisen järjestyksen ja turvallisuuden ylläpitämiseksi ja yhteiskunnan turvaamiseksi (11.5.2007/551[10]). Puolustusvoimat voi kuitenkin osoittaa tukea

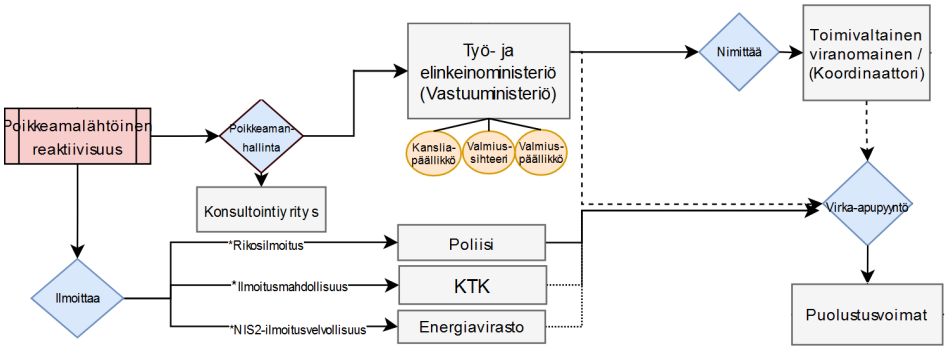
[10] Laki Puolustusvoimista (11.5.2007/551)

puolustusvoimien muihin tehtäviin kuulumattomaan ja erittelemättömään tehtävään. Tämä tulisi kyseeseen, jos kansallinen turvallisuus edellyttäisi Puolustusvoimien hallussa olevaa materiaalia, henkilöstöä ja osaamista, mitä toimivaltaisilta viranomaisilta puuttuu (Liesinen, Karinen & Lahtinen, 2017, s. 4-6). Poliisin osalta virka-avun antaminen kuvattiin mahdolliseksi, mutta sen soveltuvuus uhkalähtöiseen proaktiivisuuteen nähtiin epätodennäköiseksi. Kuitenkin poliisin tukeminen poikkeamalähtöisessä reaktiivisessa toiminnassa nähtiin juridisesti mahdolliseksi osana lakia Puolustusvoimien virka-avusta poliisille (20.5.2022/342[11]), jonka 1. luvun 2 §:n mukaan puolustusvoimien on annettava poliisille virka-apua muun muassa kaluston, välineistön, tai Puolustusvoimien asiantuntija-avun luovuttamiseksi tilapäisesti poliisin käyttöön. Puolustusvoimien virka-avun antaminen Kyberturvallisuuskeskukselle tunnistettiin erittäin haastavaksi, sillä Liikenne- ja viestintävirastolla on oikeus HE 61/2018[12] nojalla saada täysimittaista virka-apua ainoastaan poliisilta, Tullilta ja Rajavartiolaitokselta, Puolustusvoimilta saadun virka-avun rajautuessa ainoastaan radioviestinnän häiriöiden syiden selvittämiseen. Energiaviraston osalta virka-avun vastaanottaminen tunnistettiin puuttuvan kokonaan laista (13.12.2013/870[13]). Työ ja elinkeinoministeriölle ja toimivaltaiselle viranomaiselle tarjottavan tuen osalta tarkasteltiin hallintolakia (6.6.2003/434[14]), jonka 2. luvun 10 §:n mukaan viranomaisen on toimivaltansa rajoissa ja asian vaatimassa laajuudessa avustettava toista viranomaista tämän pyynnöstä hallintotehtävän hoitamisessa sekä muutoinkin pyrittävä edistämään viranomaisten välistä yhteistyötä. Lain yhteydessä tunnistettiin kuitenkin todettavan, että viranomaisten välisestä virka-avusta säädetään erikseen. Keskusteluiden pohjalta virka-avun osoittaminen tunnistettiinkin erittäin rajoitetuksi, mutta mahdolliseksi, mikäli yhteiskunnan turvaaminen edellyttäisi toimivaltaisilta viranomaisilta puuttuvaa henkilöstöä, materiaalia ja osaamista (Liesinen, Karinen & Lahtinen, 2017, s. 4-6).

Keskusteluissa nousi myös esille, kuinka virka-apu on aina luonteeltaan tilapäistä ja ehdollista, eikä sen varaan voida rakentaa jatkuvaa yhteistoimintaa. Näin ollen nähtiin toimintaa tukevaksi, että uhkalähtöinen ja poikkeamalähtöinen operointi kulkisi tarvittaessa virka-apupyynnöstä erillistä toimintalinjaa pitkin, perustuen toiminnan koordinointiin vastuuministeriöiden kanssa, sekä toiminnan käynnistämiseen kriittisen infrastruktuurin toimijoiden kanssa ennalta sovittujen ja juridisesti hyväksyttyjen sopimusten pohjalta. Toimintaa kuvattiin sopimusmalliehtoiseksi toiminnaksi, jossa olisi ennalta sovittu kriittisen infrastruktuurin toimijoiden kanssa tuesta esimerkiksi laajojen poikkeamien tai kyberuhkien torjunnan suhteen, jolloin toiminta olisi vakioitua ja harjoiteltua, eikä erillistä virka-apuprosessia tarvittaisi. Lisäksi ongelmana nähtiin, että virka-avun osoittaminen ja vastaanottaminen tapahtuu pääasiallisesti viranomaiselta toiselle viranomaiselle, vaikka lopullisena kohteena olisikin yksittäinen yritys. Virka-avun suoraa osoittamista yksittäiselle yritykselle ei nykylainsäädännön nojalla nähty suoranaisesti mahdolliseksi, ellei kyseessä olisi esimerkiksi Puolustusvoimien strateginen kumppani. Suuressa kuvassa lainsäädäntö tunnistettiinkin olevan rikki, määrittelemätön ja vajavainen. Virka-avun ja toimivallan ohessa haastatteluissa korostuikin tarve kehittää lainsäädäntöä niin, että se palvelisi paremmin normaalioloja, mutta myös kriisilainsäädännön

[11] Laki Puolustusvoimien virka-avusta poliisille (20.5.2022/342)
[12] Hallituksen esitys eduskunnalle laiksi Liikenne- ja viestintäviraston perustamisesta, Liikennevirastosta annetun lain muuttamisesta ja eräiksi niihin liittyviksi laeiksi
[13] Laki Energiavirastosta (13.12.2013/870)
[14] Hallintolaki (6.6.2003/434)

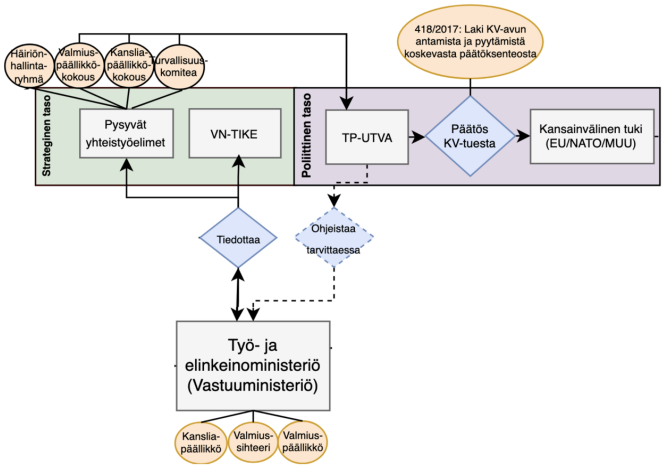
mukaisen valmiuslain (29.12.2011/1552[15]) ja huoltovarmuuden turvaamisen lain (18.12.1992/1390[16]) mukaisia viitekehyksiä. Haastateltavat painottivat, että kriisilainsäädännön tarkoitus on tarjota lisätoimivaltuuksia poikkeuksellisissa tilanteissa, mutta sen ulkopuolella on tärkeää, että normaaliolojen sääntely ja roolitukset ovat selkeät ja toimivat. Tämän tunnistettiin korostuvan kyberuhkien kaltaisten haasteiden ennakoivaa käsittelyä lainsäädännössä ja varautumisessa. Lisäksi haastatteluissa mainittiin hallitusohjelman sisältävän kirjauksen valmiuslain kehittämiseksi, mikä viittaa poikkeusolojen lisäksi tunnistettua tarvetta vahvistaa normaaliolojen lainsäädännöllistä kehystä, roolitusta ja hallinnollista varautumista. Myös huoltovarmuus nähtiin laaja-alaisena kokonaisuutena, joka perustuu paitsi lainsäädäntöön, mutta myös hallinnolliseen varautumiseen, yritysten jatkuvuuden hallintaan, riskienhallintaan ja sopimuksiin. Virka-apuprosessia kuvaava toimintatapamalli on esitetty kuviossa 38.



KUVIO 38 Virka-apuprosessia kuvaava toimintatapamalli

Haastatteluissa korostettiin poliittisen tason Tasavallan Presidentin ja hallituksen ulko- ja turvallisuuspoliittisen ministerivaliokunnan (TP-UTVA) roolia poliittisena päätöksentekoelimenä, jonka nähtiin vastaanottavan tietoa ministereiltä ja ministeriöiden kansliapäällikkökokouksista, sekä muun muassa Turvallisuusneuvoston edustajilta. Valtioneuvoston tilannekeskuksen (VN-TIKE) tehtäväksi ei tunnistettu nostaa asioita TP-UTVA:n agendalle, vaan tiedottaminen todettiin tapahtuvan edellä mainittujen toimielimien kautta, joiden nähtiin ohjaavan operatiivista päätöksentekoa ja evästävän strategisia toimenpiteitä ja päätöksiä. TP-UTVA:n tunnistettiinkin käsittelevän tapahtumaa korkeimmalla poliittisella tasolla, jonka toiminta poikkeamanhallinnassa koettiin moninaisena. Haastatteluissa TP-UTVA nähtiin toimielimenä, joka voi "siunata" toimet ja selkeyttää toimivaltuuksia. TP-UTVA:n tunnistettiin myös päätöksentekoelimenä kansainvälisen tuen vastaanottamisen suhteen. Suurimmaksi osaksi sen roolista kuvattiin kuitenkin vain olla tietoinen tapahtumista ja mahdollisesti osallistua keskusteluun kohonneen uhkan aikana. TP-UTVA:n toimintaa kuvaava toimintatapamalli on esitetty kuviossa 39.

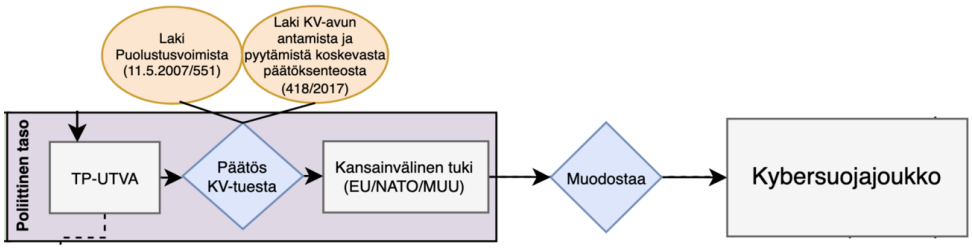
[15] Valmiuslaki (29.12.2011/1552)
[16] Laki huoltovarmuuden turvaamisesta (18.12.1992/1390)



KUVIO 39 TP-UTVA:n toimintaa kuvaava toimintatapamalli.

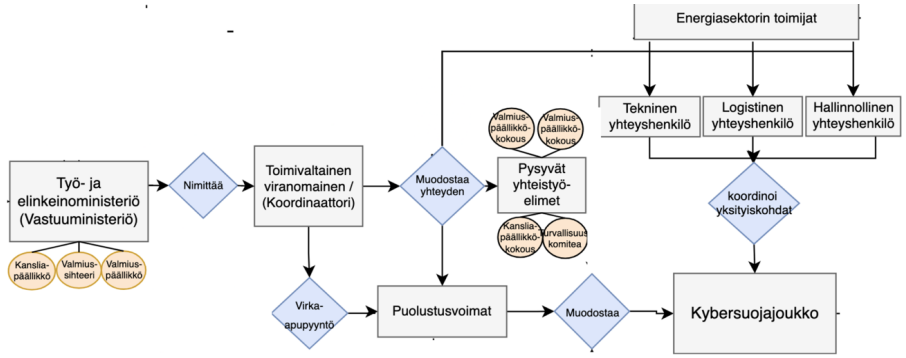
Kansainvälisen (KV) tuen vastaanottamiseen ja antamiseen liittyen keskusteluissa korostettiin Puolustusvoimien toimintaa säätelevän lainsäädännön, kuten Puolustusvoimista annetun lain (11.5.2007/551[17]) 2. luvun 12 c §:n sekä kansainvälisen avun antamisesta ja pyytämisestä koskevan lain (418/2017[18]), merkitystä. Näiden lakien nähtiin mahdollistavan oikeudellisen perustan kansainvälisen avun vastaanottamiselle, antamiselle, yhteistoiminnalle sekä muulle kansainväliselle toiminnalle. Keskusteluissa tunnistettiin myös haasteet, jotka liittyvät kansainvälisten joukkojen teknis-taktisen operoinnin toimivaltuuksiin ja Suomen lainsäädännön soveltamiseen kansallisten joukkojen tavoin. Lisäksi tunnistettiin haasteita, jotka voivat muodostua ongelmaksi erityisesti tietosuojan ja turvaluokitellun tiedon siirtämisen osalta, johtuen EU:n tiukasta tietosuojalainsäädännöstä. Hallinnollisesti merkittäväksi nähtiinkin tietosuojan ja turvaluokitellun tiedon siirtäminen Suomen rajojen ulkopuolelle liittolais- tai kumppanimaahan. Tämän arvioitiin korostuvan erityisesti tilanteessa, jossa tiedonsiirto ja sen käsittely tapahtuu EU:n tai Euroopan talousalueen (ETA) ulkopuolella. Kansainvälisten kybersuojajoukkojen teknisen analyysikyvyn arvioitiin olevan parhaimmillaan joukkojen kotimaassa, missä niiden käytössä olevat resurssit arvioitiin paremmaksi. Tämän myötä keskusteluissa arvioitiin todennäköiseksi, että tuen vastaanottaminen vaatisi myös kerättyjen uhkatietojen ja muiden näytteiden siirtoa ulkomaille. Tämän nähtiin nostavan esiin tarpeen tasapainottaa kansainvälisen yhteistyön hyödyt ja tietosuojaan liittyvät velvoitteet, mikä vaatii huolellista suunnittelua ja sopimista tietojen käsittelystä kansainvälisissä operaatioissa. Kansainvälisten joukkojen toimintaa kuvaava toimintatapamalli on esitetty kuviossa 40.

[17] Laki Puolustusvoimista (11.5.2007/551)
[18] Laki kansainvälistä apua, yhteistoimintaa tai muuta kansainvälistä toimintaa koskevasta päätöksenteosta (28.6.2017/418). Lakia on muutettu vuonna 2023 osana Hallituksen esitystä HE 193/2022



KUVIO 40 Kansainvälisten joukkojen toimintaa kuvaava toimintatapamalli.

Haastatteluiden perusteella vastuuministeriön päätöksellä toimeenpantavaa operatiivista koordinointia tunnistettiin toteuttavan niin sanottu ”toimivaltainen viranomainen”. Toimijan tunnistettiin olevan tilanteesta riippuen vaihteleva ja erikseen määritettävä, sillä yllättäviin ja kompleksisiin koko valtakuntaa koskeviin häiriötilanteisiin ei ole määritelty selkeää johto- tai koordinaatiovastuuta yhdellekään viranomaiselle (Koistinen, 2021, s. 4). Toimivaltaisen viranomainen tunnistettiin johtavan TEM:n valtuuttamaa operatiivista toimintaa, käynnistäen häiriötilanteen hallintaan liittyvät toimenpiteet, samalla vastaten tilanteen tiedottamisesta sovittujen käytäntöjen mukaisesti. Muiden viranomaiset sekä valtion ja kuntien laitosten kuvattiin osallistuvan toimintaan antamalla muun muassa virka-apua tilanteen hallinnan edellyttämässä laajuudessa (Turvallisuuskomitea, 2017, s. 15). Lisäksi toimivaltaisen viranomainen tunnistettiin hyödyntävän tukenaan pysyviä päätöksentekoelimiä. Tällaisiksi tunnistettiin olevan valmiuspäällikkö- ja kansliapäällikkökokous valtioneuvostotasolla ja Turvallisuuskomitea valtioneuvoston tukena, sekä Huoltovarmuuskeskus huoltovarmuuden ja Kyberturvallisuuskeskus kybertilannekuvan osalta. Lisäksi tukena tunnistettiin olevan ministeriöiden ja hallinnonalojen valmiustoimikunnat, alueelliset valmiustoimikunnat sekä kuntien valmiussuunnittelun johtoryhmät (Turvallisuuskomitea, 2017, s. 28). Huoltovarmuuskeskuksen tunnistettiin myös kykenevän toimimaan toimivaltaisena viranomainen (Huoltovarmuuskeskus, 2023, D). Toimintatapamallin viitekehyksessä toimivaltaisena viranomaisena arvioitiinkin toimivan Huoltovarmuuskeskus, joka todennäköisesti nimitettäisiin toimivaltaisen viranomaisen koordinoivaan asemaan Työ- ja elinkeinoministeriön valtuuttamana. Operatiivisen johtovastuun tunnistettiin säilyvän vastuuministeriöllä, toimivaltaisen viranomaisen toiminnan painottuessa yleistilanteen koordinointiin ja toimijoiden toiminnan yhteensovittamiseen. Tutkimuksen viitekehyksen mukaisissa tapauksissa toimivaltaisen viranomaisen tehtäväksi tunnistettiinkin esittää tarvittaessa virka-apu pyyntö esimerkiksi Puolustusvoimille, minkä lisäksi tunnistettiin tarve muodostaa yhteys ja koordinointivalmius kohteena olevan energiatoimijan määrittämien teknisen, hallinnollisen ja logistisen yhteyshenkilöiden kanssa, pyrkien yhteensovittamaan toiminta virka-avun mukaiselle kybersuojajoukolle. Toimivaltaisen viranomaisen toimintaa kuvaava toimintatapamalli on esitetty kuviossa 41.



KUVIO 41 Toimivaltaisen viranomaisen toimintaa kuvaava toimintatapamalli.

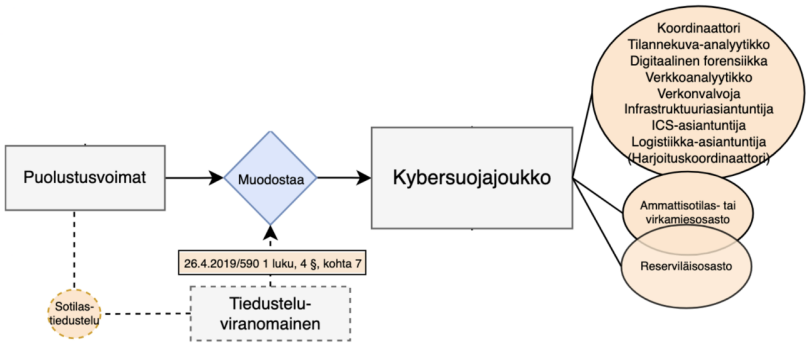
Haastatteluissa nousi esille, että Puolustusvoimien kybersuojajoukon rooli tiedusteluviranomaisen tukemisessa voisi olla juridisesti mahdollista, viitaten sotilastiedustelulain 590/2019[19] 1. luvun 4 §:n, jonka mukaan sotilastiedustelun kohteena on vieraan valtion toiminta tai muu toiminta, joka vakavasti uhkaa Suomen maanpuolustusta tai vaarantaa yhteiskunnan elintärkeitä toimintoja. Kybersuojajoukon toimivalta voisi juridisesti perustella 590/2019[20] 8. luvun 90 §:ä, jonka mukaan tiedustelumenetelmien käyttöön riittävän koulutuksen saanut Puolustusvoimien virkamies voi käyttää sotilastiedusteluviranomaisen ohjauksessa ja valvonnassa kyseisessä laissa määriteltyjä tiedonhankintamenetelmiä. Tällaisen tuen arvioitiin tukevan uhkalähtöistä toimintaa, jossa Puolustusvoimien kybersuojajoukot voisivat antaa teknistä tukea, mahdollistaen tiiviimmän yhteistyön ilman virallisia virka-apupyyntöjä. Myös reserviläisten käyttölle ei tunnistettu suoria rajoituksia, sillä 590/2019[21] 8. luvun mukaisesti asevelvollisuuslain (1438/2007[22]) mukaisessa kertausharjoituksessa oleva riittävän koulutuksen saanut reserviläinen saa avustaa sotilastiedusteluviranomaista muun muassa teknisten tietojen käsittelyssä. Siviilitiedustelun osalta yhteistyö tunnistettiin monimutkaisemmaksi, kyseisen toiminnan painottuessa sisäministeriön ohjaukseen.

Kybersuojajoukon kokoamista tarkasteltiin haastatteluissa myös reserviläisistä koostuvan joukon toimivaltuuksien näkökulmasta. Reserviläisistä koostettavan kybersuojajoukon toiminnan kuvattiin perustuvan päivitettyyn lakiin vapaaehtoisesta maanpuolustuksesta (346/2022[23]), jonka mukaan Puolustusvoimat voi käyttää vapaaehtoisiin harjoituksiin sitoutuneita henkilöitä puolustusvoimista annetussa laissa (551/2007[24]) tarkoitettuihin virka-aputehtäviin 342/2022[25] mukaisesti. Suomen kansalainen voi antaa lain vapaaehtoisesta maanpuolustuksesta (11.5.2007/556[26]) mukaisesti Puolustusvoimille kirjallisen sitoumuksen siitä, että hän osallistuu Puolustusvoimien vapaaehtoisiin harjoituksiin sekä sen mukaisiin virka-aputehtäviin. Reserviläisten käyttö kuvattiinkin perustuvan joko vapaaehtoiseen kertausharjoitukseen (VEH), jonne Puolustusvoimat kutsuisi

[19] Laki sotilastiedustelusta (590/2019)
[20] Laki sotilastiedustelusta (590/2019)
[21] Laki sotilastiedustelusta (590/2019)
[22] Asevelvollisuuslaki (1438/2007)
[23] Laki vapaaehtoisesta maanpuolustuksesta annetun lain 23 §:n muuttamisesta (346/2022)
[24] Laki puolustusvoimista (551/2007)
[25] Laki Puolustusvoimien virka-avusta poliisille (342/2022)
[26] Laki vapaaehtoisesta maanpuolustuksesta (11.5.2007/556)

11.5.2007/556 [27] mukaisen sitoumuksen antaneet reserviläiset, tai kertausharjoitukseen (KH), johon lähetettäisiin kutsu vähintään kolme kuukautta ennen harjoituksen alkamista (28.12.2007/1438[28]).

Kybersuojajoukon kokoonpanon osalta haastatteluissa korostui, että kokoonpanoon tulisi päivittää myös tilannekuva-analyytikon tehtävä, jonka keskeisenä toiminnallisuutena tunnistettiin tarve tuottaa tilannekuvaa sekä joukolle itselleen, mutta erityisesti tuettavalle organisaatiolle ja sen avainhenkilöille. Tämän kautta tunnistettiin mahdollistettavan päätöksenteon tuki ja toimenpiteiden luvittaminen, sillä yllättävien tilanteiden päätöksenteko ja toimenpiteiden luvitus nähtiin mahdollisesti edellyttävän jopa toimitusjohtajan tai valvovan viranomaisen hyväksyntää, mikäli vaarana olisi tuotantoprosessin häiriintyminen. Tämän myötä painotettiinkin, että kybersuojajoukon tehokkuus ei perustu pelkästään "hakkeriporukan" toimintaan, vaan vaatii erikseen omistautunutta osaamista tilannekuvallisen toiminnan muodossa, jolla voidaan varmistaa asianmukainen viestintä ja ylemmän johdon tietoisuuden ylläpitäminen. Kybersuojajoukkojen toiminnan kuvaus ja joukon koostumus on esitetty kuviossa 42.

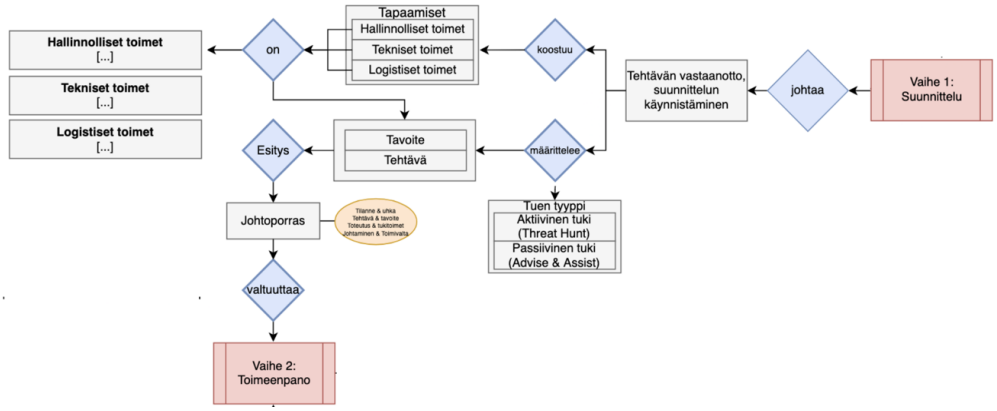


KUVIO 42 Kybersuojajoukkojen nähtiin koostuvan eri alojen asiantuntijoista, jotka tunnsitettiin kykenevän olevan ammattisotilaita, siviilivirkamiehiä tai reserviläisiä.

5.2.2 Teknis-taktisen tason toimintatapamallin päivittäminen

Teknis-taktisen tason mukaisen operoinnin ensimmäisen vaiheen kokonaisuudesta tunnistettiin huomioita niin hallinnollisten, teknisten ja logististen toimien osalta, sekä johtoportaalle esitettävien kokonaisuuksien suhteen. Tehtävän vastaanoton ja suunnittelun käynnistämisen yhteydessä tunnistettiin tarve määritellä kybersuojajoukkojen tuen tyyppi, jonka nähtiin jakautuvan aktiiviseen tai passiiviseen tukeen. Aktiivisen tuen nähtiin koostuvan uhkanmetsästyksestä tai digitaalisesta forensiikasta ja poikkeamanhallinnasta (Digital Forensics & Incident Response, DFIR), jossa kybersuojajoukko operoi itsenäisesti asiakkaan valtuuttamin toimivaltuuksin. Passiivisessa tuessa tunnistettiin toimenpiteeksi tukea asiakasta ohjein, neuvoin ja koulutuksin, ilman kytkeytymistä kohdeverkkoon datan keräämiseksi, tai sen käsittelyksi ja analysoimiseksi (Advise & Assist). Suunnitteluvaiheen toimintatapamallin kuvaus on esitetty kuviossa 37.

[27] Laki vapaaehtoisesta maanpuolustuksesta (11.5.2007/556)
[28] Asevelvollisuuslaki (28.12.2007/1438)

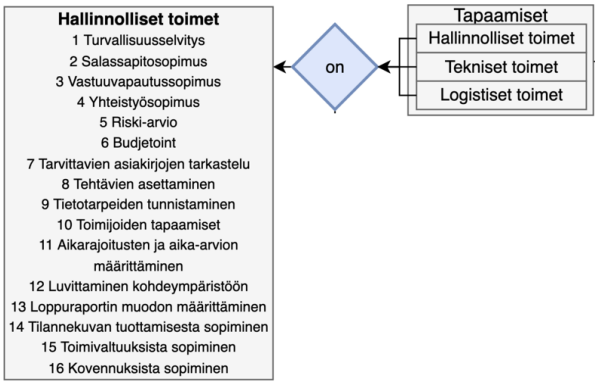


KUVIO 43 Ensimmäisen vaiheen (”Suunnittelu”) toimintatapamallin kuvaus.

Hallinnollisten toimien keskusteluissa korostui, kuinka asiakkaan tulee yhdessä kybersuojajoukon kanssa sopia tarvittavat luvitukset ja turvallisuusselvitykset, käytettävissä oleva aika ja resurssit, sekä tuotettavan loppuraportin muoto ja sisältö. OT-ympäristön automaatiossa perusperiaateeksi tunnistettiin, että järjestelmien ja prosessien ohjattavuus ja valvontakyky on säilyttävä kaikissa tilanteissa, tai muuten tuotantoprosessi tulee ajaa turvalliseen tilaan prosessi- ja henkilöturvallisuuden säilyttämiseksi. Näin ollen teknisen operoinnin tilannekuva tunnistettiin kriittiseksi organisaation päätöksenteon ja turvallisuuden kannalta. Turvallisuuden säilyminen tunnistettiin kyettävän varmistamaan operaation aikaisella teknisen tilannekuvan tuottamisella, sillä tuettava organisaatio ja sen mukainen liiketoiminta tunnistettiin olevan vastuussa päätöksenteosta operaation kaikissa vaiheissa. Lisäksi kybersuojajoukolle tunnistettiin vaatimukseksi tehdä asiakkaan toimesta selväksi toimivalta päätöksenteon suhteen, eli keneltä ja missä vaiheessa suoritettavat toimenpiteet valtuutetaan, jos niitä ei ole erillisessä toimivaltataulukossa määritetty ennen operaation käynnistämistä. Lisäksi korostettiin kuinka päätöksentekijä ei voi olla henkilöriippuvainen, vaan rooliriippuvainen, mahdollistaen laajemman tavoitettavuuden ja toiminnan jatkuvuuden turvaamisen. Tämän nähtiin edistävän nopeaa ja perusteltua päätöksentekokykyä ja tavoitettavuutta, sekä turvallisuuden ja toiminnan jatkuvuutta. Lisäksi korostettiin kybersuojajoukkojen ennalta sovittua toimivaltaa ja luvitusprosesseja, mahdollistaen joustavuutta ja tarvittaessa tarvetta nopealle kytkeytymiselle ja oikeuksille järjestelmiin, erityisesti laajoissa poikkeamanhallintatilanteissa. Hallinnollisten toimien osalta korostettiin myös tarvetta määritellä rajapiste, jos toiminnan nähtiin vaikuttavan tuotantoprosessin toimintaan, vaatien tuotantoprosessin keskeyttämistä ja tuotannon irrottamista muusta infrastruktuurista. Tämän kuvatiin mahdollistuvan “checklistinä” tai “toimivaltaa kuvaavana RACI-taulukkona”, jotta toimininnan rajat kyettäisiin yhteensovittamaan asiakkaan ja kybersuojajoukon kesken. Havaintona tuotiinkin ilmi, kuinka tuettavien organisaatioiden tulisi ennakoida ja valmistautua poikkeaviin luvitusprosesseihin ja luoda mahdollisuuksien mukaan tarvittavat sopimukset jo ennaltasovituin menetelmin.

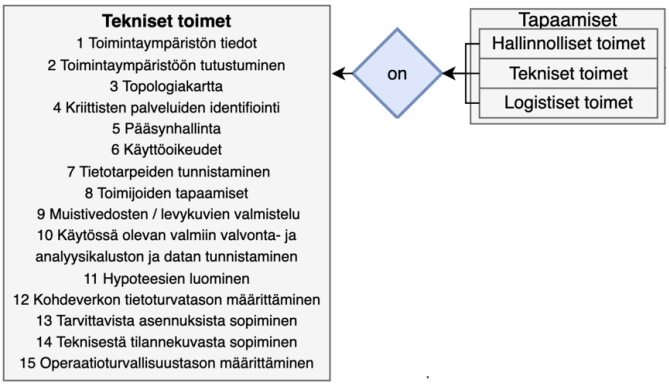
Lisäksi haastatteluissa tuli esille, että kybersuojauksen projektimaisten lähestymistapojen yhteydessä on tärkeää määrittää selkeästi uhkat, käytettävät analyysimenetelmät ja tunnistaa saatavilla oleva data. Tämän nähtiin auttavan hypoteesien rakentamisessa ja toimintamenetelmien esittämisessä

johtoportaalle, korostetaan vaiheen lopullista “tilannetta ja uhkaa”, “tehtävää ja tavoitetta”, “toteutusta ja tukitoimia”, sekä “johtamista ja toimivaltaa”. Haastatteluissa nousi esille myös turvallisuusselvitysten ajoituksen merkitys, ehdottaen niiden tekemistä etukäteen erityisesti silloin, kun käsitellään sensitiivistä dataa. Tämän nähtiin vähentävän viivästyksiä prosesseissa ja mahdollistaa nopeamman toimintavalmiuden. Ensimmäisessä vaiheessa huomioitavat hallinnolliset toimet on esitetty kuviossa 44.



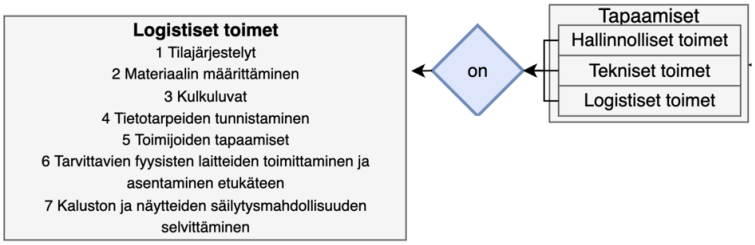
KUVIO 44 Teknis-taktisen tason mukaisen operaation ensimmäisessä vaiheessa huomioitavat hallinnolliset toimet.

Teknisten toimien osalta tunnistettiin keskeiseksi sopia toimintamenetelmistäja tarvittaessa asentaa erityisiä sensoreita ja agentteja kohdeverkon palvelimille ja päätelaitteille, jotta operaation keräys- ja analyysivaiheen datan luotettavuus kyettäisiin varmistamaan. Lisäksi ennenaikainen harjaantuminen tuntemattoman verkon haltuunottoon suhteen tunnistettiin kriittiseksi. Kohdeympäristön etukäteisvalmisteluilla ja -tuntemuksella tunnistettiin mahdolliseksi varmistaa operaation tehokkuus ja toimeenpanonopeus. Etukäteisvalmistelun osalta tunnistettiin myös kriittiseksi vastaanottaa asiakkaalta kohdeverkon topologiakartta, mahdollistaen operaation teknisen tilannekuvan ylläpitämisen ja toiminnan vaiheiden seuraamisen. Tätä havaintoa tukee Trent ym. (2016) tutkimuksen viitekehys. Lisäksi teknisten toimien osalta uhkalähtöisen proaktiivisen toiminnan keskeiseksi tekijäksi nousi operaatioturvallisuuden korostaminen, jonka avulla tunnistettiin mahdolliseksi ennakoida mahdollisten uhkatoimijoiden vastatoimenpiteitä jälkien peittämisen suhteen. Operaatioiden suunnitteluvaiheen tärkeäksi päätöksentekovaiheeksi tunnistettiinkin toimintatavan määrittäminen operaation salaamisen ja harhauttamisen suhteen, sillä joukkojen, teknologioiden ja sensorien käyttöönoton todettiin paljastavan operaatiot, johtaen mahdollisesti uhkatoimijan vastatoimenpiteisiin. Ensimmäisessä vaiheessa huomioitavat tekniset toimet on esitetty kuviossa 45.



KUVIO 45 Teknis-taktisen tason mukaisen operaation ensimmäisessä vaiheessa huomioitavat tekniset toimet.

Logististen toimien osalta keskusteluissa korostettiin tarvetta määritellä tarve ja toimintatavat mahdollisten erillisten fyysisten laitteiden toimittamiselle tai asennukselle suoraan operointitiloihin datan keräämistä ja käsittelyä varten. Erillisille laitteile tunnistettiin tarve erityisesti silloin, jos kyseessä on esimerkiksi turvaluokitellun tiedon keräystä ja käsittelyä. Toimenpiteillä tunnistettiin mahdolliseksi varmistaa, että operaatiokriittistä lokidataa on kyetty keräämään turvallisesti, estäen sen siirtämisen operaatioalueen ulkopuolelle. Tämän tunnistettiin korostavan logististen valmistelujen kriittistä roolia herkän tiedon suojaamisessa operaation aikana. Lisäksi tunnistettiin tarve selvittää operointitiloissa käytettävän laitteiston ja datan säilyttämismahdollisuus tilaturvallisuuden näkökulmasta. Ensimmäisessä vaiheessa huomioitavat logistiset toimet on esitetty kuviossa 46.

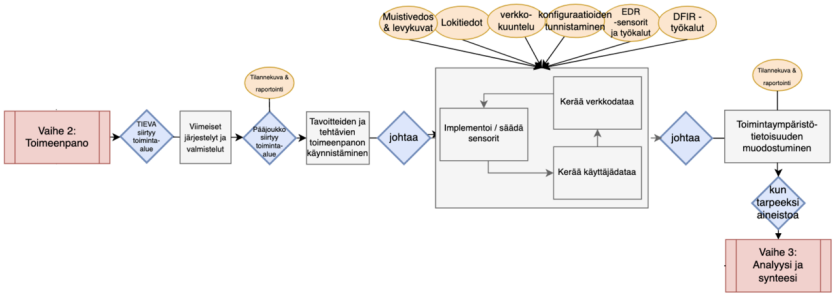


KUVIO 46 Teknis-taktisen tason mukaisen operaation ensimmäisessä vaiheessa huomioitavat logistiset toimet.

Toisen vaiheen muutoksia toimintatapaprosessiin tehtiin tavoitteiden ja tehtävien toimeenpanon käynnistämisen osalta. Ennen kyseisten toimenpiteiden käynnistämistä tunnistettiin tilanteen mahdollistaessa tarve ns. tiedustelu- ja valmisteluosastolle (TIEVA), jonka toiminnaksi kuvattiin saapuminen toiminta-alueelle useita tunteja tai päiviä ennen pääjoukkoa. Joukon tehtäväksi tunnistettiin pyrkimys muodostamaa yhteys tukihenkilöihin, sekä tunnistamaan kohdeympäristön kriittiset pisteet ja valmistella toimintaympäristöä siten, että pääjoukko pääsee saapuessaan käynnistämään operaation. Näiden yhteydessä tunnistettiin myös tarve jatkuvalle tilannekuvan muodostamiselle ja raportoinnille, jonka tunnistettiin mahdollistavan nopeampi päätöksenteko ja tilanneymmärrys. OT-ympäristön osalta korostettiin, että hetkellinen katkos operaation aikana saattaa OT-ympäristön mukaisessa teollisuusprosessissa konkretisoitua vas-

ta usean viikon kuluttua, mahdollisesti aiheuttaen kriittisiä ongelmia tuotantoprosessin sujuvuudessa. Tilannekuvan tuottamiselle tunnistettiinkin tarve olla integroitu osa kybersuojajoukon kokoonpanoa.

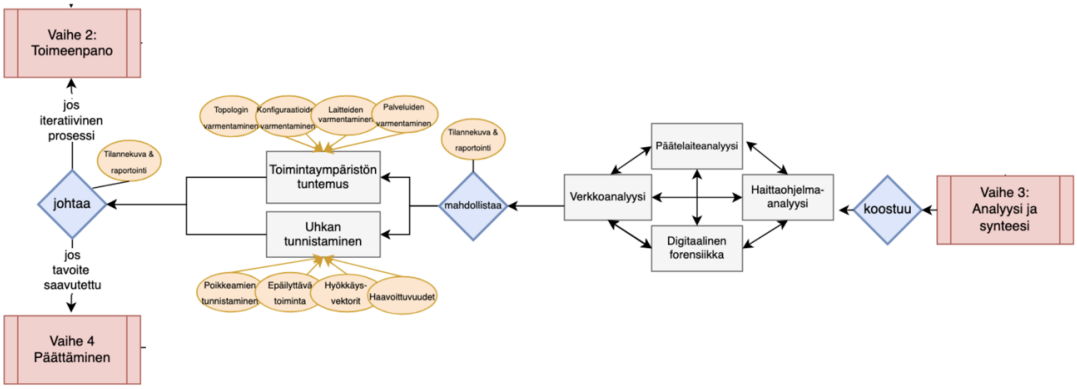
Operaation toisen vaiheen mukaisen datan keräyksen osalta haastatteluissa korostui, että uhkanmetsästysoperaatioissa erityisesti EDR[29]-sensorien DFIR-työkalujen käyttö on merkittävästi tehokkaampaa kuin perinteisen muistivedosten ja levykuvien kerääminen. EDR-dataa pidettiin erittäin hyödyllisenä, sillä sen kuvattiin mahdollistavan tiedon keräämisen päätelaitteilta snapshot-menetelmällä, jonka kuvattiin olevan hyödyllisempää kuin suurten datamäärien kerääminen ja analysointi. Tämän lisäksi SYSMON-työkalun asentaminen kaikkiin laitteisiin nostettiin esiin kustannustehokkaana ja menetelmänä tehostaa forensista tutkintaa, kyeten tallentamaan tietoja, jotka eivät yleensä tallennu perinteiseen forensiikkamateriaaliin. Sysmonin passiivinen luonne, eli datan kerääminen ilman aktiivisia toimenpiteitä, koettiin hyödyllisenä, erityisesti tilanteissa, joissa EDR-teknologioita ei voida asentaa. Tällaisen datan keräämisen kuvattiin mahdollistavan tehokkaamman uhkien tunnistamisen, mahdollistaen nopean reagoinnin epäilyttäviin toimintoihin, johtaen kohdennettujen muisti- ja levykuvien talteenoton tarkempaa analysointia varten. Toimeenpanovaiheen toimintatapamalli on esitetty kuviossa 47.



KUVIO 47 Operaation toisen vaiheen (Toimeenpano) toimintatapamalli.

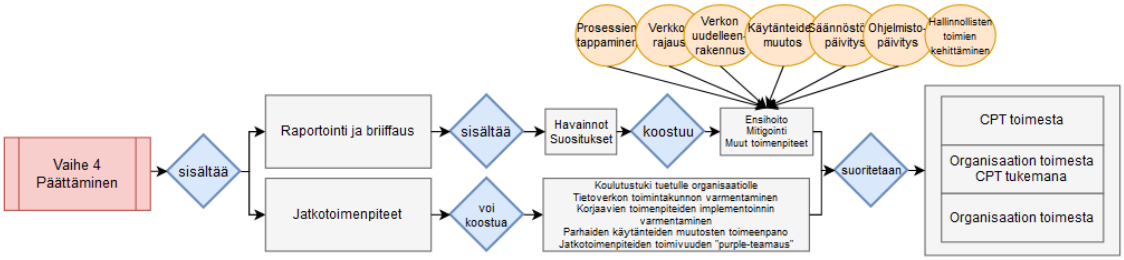
Kolmannen vaiheen osalta tunnistettiin tarve jatkuvalle tilannekuvan muodostamiselle ja raportoinnille, jolla tunnistettiin mahdollistavan tilanneymmärryksen muodostuminen tuettavalle organisaatiolle, mutta myös kybersuojajoukolle itselle. Yleisesti ottaen kolmannen vaiheen analyysin tulokset tunnistettiin perustuvan operaation toisessa vaiheessa kerättävään dataan, johon palattiin iteratiivisesti niin kauan, kunnes ensimmäisessä vaiheessa asetettu tavoite olisi saavutettu tai käytettävissä oleva aika loppuisi. Operaation kolmannen vaiheen mukainen toimintatapamalli on esitetty kuviossa 48.

[29] EDR-sensori (Endpoint Detection and Response) on turvallisuustyökalu, joka asennetaan päätelaitteisiin keräämään ja analysoimaan tietoturvauhkia reaaliajassa,



KUVIO 48 Operaation kolmannen vaiheen (Analyysi ja synteesi) mukainen toimintatapamalli, jonka tunnistettiin jatkuvan joko iteratiivisesti, tai päättyen tavoitteen saavuttamisen tai käytettävissä olevan ajan loppumisen jälkeen.

Neljännen vaiheen ja operaation päättämisen osalta haastatteluissa korostettiin, että havaitun toiminnan toistaminen uhkasimuloinnin keinoin on keskeistä toteutettavien korjaustoimenpiteiden tehokkuuden varmistamiseksi. Haastateltavat näkivät, että korjaustoimenpiteiden jälkeen on olennaista suorittaa penetraatiotestaus, jossa aiemmin käytetyt tekniikat ajetaan uudestaan läpi. Tämän prosessin kuvattiin varmistavan korjaustoimenpiteiden tehokkuus. Lisäksi testausprosessin kuvattiin tarjoavan toimeksiantajalle mahdollisuuden "Purple Teamaukseen", eli mahdollisuudeksi yhdistää hyökkääjän (Red Team) ja puolustajan (Blue Team) toimintatapoja ja tietotaitoa koulutuksen omaisessa yhteistyöllisessä prosessissa. Operaation neljännen vaiheen mukainen toimintatapamalli on esitetty kuviossa 49.



KUVIO 49 Neljännen vaiheen osalta korostettiin tarvetta suoritettujen toimenpiteiden toimivuuden varmistamiselle ”Purple Teamauksen” kautta.

5.3 Toimintatapamallin johtopäätökset

5.3.1 Operatiivisen tason johtopäätökset

Operatiivisen tason osalta päivityksiä alkuperäiseen toimintatapamalliin tehtiin operaatioiden lähtötilanteiden, toimijoiden roolien ja prosessien osalta. Lisäksi kokonaisuuteen lisättiin kuvaukset strategisen ja poliittinen tason toimijoista. Uhkalähtöisen operaation osalta keskeisiksi toimijoiksi nousivat tiedonvaihtoryhmät ja yhteistyöelimet. Tiedusteluviranomaisten rooli korostui

myös uhkavaroitusten tuottajana. Uhkalähtöisen tilannekuvan muodostaminen ja tiedon jakaminen tunnistettiin liittyvän vahvasti HVO:n toimintaan, kun taas proaktiiviset toimenpiteet ja poikkeamien hallinta kuvattiin kytkeytyvän HVK:n rooliin varautumisen tehostamisessa ja huoltovarmuuden uhkatason säätelyssä. Reaktiivisen operaation osalta tunnistettiin useita toimijoita, joille tunnistettiin tarve ja mahdollisuus ilmoittaa laajasta kyberpoikkeamasta. Toiminnan osalta korostui Huoltovarmuuskeskuksen rooli uhkatilanteiden hallinnassa ja laajemman tilannekoordinoinnin toteuttamisessa, toimien yhteistyössä vastuuministeriön (TEM) sekä muiden keskeisten huoltovarmuuskriittisten toimijoiden kanssa. Lisäksi tunnistettiin eri tilanteita konsultipalveluiden käytölle ja käyttämättömyydelle poikkeamanhallintatilanteessa, mutta myös tilanteita, joissa kaupalliset palvelut eivät ole soveltuvia, vaatien valtiollisen toimijan mukaista kybersuojajoukkoa.

COVID-19-pandemian, Balticconnector-kaasuputken ja Vastaamon tietomurron kaltaisissa poikkeamatilanteissa valtiollinen reagointi tunnistettiin rakentuvan monitasoiselle yhteistyölle eri hallinnonalojen kesken. Kuvauksissa korostui Työ- ja elinkeinoministeriön merkittävä rooli vastuuministeriönä erityisesti voima- ja polttoainehuollon turvaamisessa sekä energiatoimialan laajassa poikkeamanhallinnassa. Kansliapäällikkökokouksen johtoasema operatiivisessa päätöksenteossa ja toiminnan koordinoinnissa koettiin poikkeamanhallinan osalta ensisijaisen tärkeäksi. TP-UTVA:n roolia korostettiin poliittisena päätöksentekoelimenä, jonka nähtiin vastaanottavan tietoa ministereiltä ja ministeriöiden kansliapäällikkökokouksista, sekä muun muassa Turvallisuusneuvoston edustajilta. TP-UTVA:n osalta kybersuojajoukkojen toiminta korostui erityisesti kansainvälisen tuen vastaanottamisen viitekehyksessä, jossa TP-UTVA:n nähtiin valtuuttavan toimet, selkeyttävän toimivaltuuksia sekä tehden strategisen tason päätöksiä kansainvälisen yhteistyön ja tuen hyödyntämisestä. Kansainvälisen tuen vastaanottamisessa tunnistettiin keskeiseksi kyky tasapainottaa tuen hyödyt ja mahdolliset haasteet, kuten tietosuojan ja turvaluokitellun tiedon siirtämisen kysymykset.

Virka-avun antamisen ja vastaanottamisen suhteen keskeiseksi havainnoksi nousi lainsäädännön ja käytännön rajoitteiden monimutkaisuus, jonka nähtiin vaikuttavan viranomaisten väliseen yhteistyöhön. Virka-apua säätelevän lainsäädännön tunnistettiin määrittelevän tiukasti edellytykset ja muodon virka-avun antamiselle ja vastaanottamiselle, minkä tunnistettiin rajoittavan joustavuutta ja nopeaa toimintaa. Erityisesti Puolustusvoimien rooli virka-avun antajana tunnistettiin rajoitetuksi. Toisaalta havaittiin myös, että virka-avun mekanismien kehittämisen tarve on tunnistettu, ja pyrkimykset suuntautuvat kohti lainsäädännön selkiyttämistä ja toimivaltuuksien laajentamista. Tavoitteeksi tunnistettiinkin tehokkaampi ja ketterämpi viranomaisten välinen yhteistyö, erityisesti kriittisen infrastruktuurin suojaamisessa kyberuhkilta. Tämän tunnistettiin edellyttävän paitsi lainsäädännöllisiä muutoksia, mutta myös käytäntöjen ja prosessien uudelleenarviointia, jotta yhteiskunnan elintärkeiden toimintojen jatkuvuus ja turvallisuus kyetään varmistamaan. Lisäksi kybersuojajoukon kokoonpanon osalta tunnistettiin tarve päivittää joukon rakenteeseen tilannekuva-analyytikon tehtävä, jonka keskeisenä toiminnallisuutena tunnistettiin tarve tuottaa operaatiosta tilannekuvaa. Yleisesti ottaen kybersuojajoukon toiminnan tunnistettiin mahdollistuvan joko sotilas- tai siviilivirkamiesten, tai reserviläisten toimintana.

5.3.2 Teknis-taktisen tason johtopäätökset

Teknis-taktisen tason toimintatapamallin mukaisessa operoinnissa päivityksiä tehtiin hallinnollisten, teknisten ja logististen toimien sekä johtoportaalle esitettävien kokonaisuuksien osalta. Kybersuojajoukkojen osalta määritteltiin aktiivinen ja passiivinen tuki, minkä lisäksi korostettiin muun muassa tarvetta sopia asiakkaan kanssa luvituksista ja turvallisuusselvityksistä, mahdollisesti asennettavista lokiagenteista sekä operointitilassa käytettävistä erillistyöasemista ja -palvelimista. OT-ympäristön prosessien ja järjestelmien ohjattavuuden ja valvontakyvyn säilyttäminen tunnistettiin kriittiseksi, jonka turvallisuudesta tuli varmistui operaation jokaisessa vaiheessa.

Toisen vaiheen osalta tavoitteiden ja tehtävien toimeenpanon käynnistäminen tunnistettiin vaativan tiedustelu- ja valmisteluosaston ennakollista toimintaa. Tämän tunnistettiin mahdollistavan pääjoukon tehokkaamman operaation käynnistämisen. Lisäksi havainnoissa korostettiin kohdeympäristön kriittisten pisteiden tunnistamista ja tilannekuvan jatkuvaa ylläpitämistä ja jakamista. Myös datan keräyksessä korostettiin tarvetta EDR-sensorien DFIR-työkalujen käyttöön, jonka kautta arvioitiin mahdollsitettavan levykuvien ja muistivedosten keräyksen painopisteen tunnistaminen.

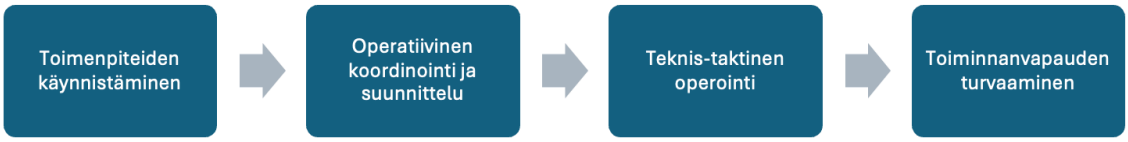
Kolmannessa vaiheessa korostettiin jatkuvan tilannekuvan muodostamista ja raportointia. Lisäksi korostettiin analyysin tuloksen perustuvan operaation toiseessa vaiheessa kerätyn datan laatuun, jonka keräämistä todettiin jatkettavan iteratiivisesti niin kauan, että operaatiossa käytettävä aika loppuu, tai tavoite saavutetaan.

Operaation päättämisen yhteydessä tunnsitettiin tarve korjaustoimenpiteiden varmistamiseen uhkasimuloinnin ja penetraatiotestauksen kautta. Korjaustoimenpiteiden tehokkuuden varmistaminen ja "Purple Teamauksen" mahdollistaminen korostettiin tärkeäksi, mahdollistaen hyökkääjän toimintatapojen tunnistamiseen ja puolustajan toimintatapojen kouluttamiseen ja tehostamiseen.

6 JOHTOPÄÄTÖKSET

6.1 Kehitetyn toimintatapamallin yhteenveto

Tutkimuksessa kehitetyn kybersuojajoukkojen puolustuksellisten kyberoperaatioiden toimintatapamallin yhteenvetona voidaan todeta, että tutkimuksessa kuvatun operatiivisen ja teknis-taktisen tason toimenpiteet puolustuksellisten kyberoperaatioiden toimeenpanossa vaatii moniulotteista ja monitasoista prosessia, vaatien eri tasojen koordinoinnin yhdistämistä sekä strategisen ja poliittisen tason päätöksentekoa. Tutkimuksen pääkysymykseksi oli asetettu "Minkälaisella prosessilla mahdollistetaan kybersuojajoukkojen puolustuksellisen kyberoperaation toimeenpaneminen?". Vastaus pääkysymykseen on esitetty kuviossa 50, minkä lisäksi tutkimuksessa kehitetty toimintatapamallia voidaan tarkastella yksityiskohtaisempana vastauksena tutkimuksen pääkysymykseen. Tutkimuksessa kehitetty toimintatapamalli on esitetty liitteessä 8.



KUVIO 50 Tutkimuksen pääkysymyksen vastaus.

Tutkimuksen pääkysymyksen vastausta voidaan tarkastella jakamalla tutkimustuloksen mukainen kokonaisuus neljään vaiheeseen.

1) **Toimenpiteiden käynnistäminen:** Puolustuksellisten kyberoperaatioiden tarve tunnistetaan joko uhkalähtöisesti, ennakoiden mahdollisia riskejä ja pyrkien estämään ongelmat ennen niiden esiintymistä, tai poikkeamalähtöisesti, reagoiden jo ilmenneisiin ongelmiin. Tässä vaiheessa keskeistä on uhkien ja poikkeamien tunnistaminen sekä päätös puolustuksellisen toimenpiteen aloittamisesta.
2) **Operatiivinen koordinointi ja suunnittelu:** Tässä vaiheessa tapahtuu kybersuojajoukkojen, muiden viranomaisten ja

potentiaalisesti kansainvälisten kumppaneiden välinen koordinointi. Suunnittelussa huomioidaan sekä strategiset että poliittiset näkökulmat, määritellen operaation tavoitteet, toimintamallit ja vastuut. Koordinoinnissa varmistetaan, että toimenpiteet ovat linjassa yleisempien turvallisuuspoliittisten tavoitteiden kanssa ja että kaikki osapuolet ovat tietoisia rooleistaan ja toimintalinjoista. Toiminnassa noudatetaan kansallista lainsäädäntöä virka-avun vastaanottamisen ja sen osoittamisen suhteen.

3) **Teknis-taktinen operointi**:
    a. **Vaihe 1, Suunnittelu:** Tässä alivaiheessa laaditaan yksityiskohtainen suunnitelma operaation toteutuksesta, määritellään tarvittavat resurssit, tehtävät ja tavoitteet.
    b. **Vaihe 2, Toimeenpano**: Toteutetaan suunnitellut toimenpiteet käytännössä. Tämä vaihe käsittää varsinaiset operatiiviset toimet, kuten tunkeutumisen eston, tiedonkeruun ja mahdollisten haavoittuvuuksien paikallistamisen.
    c. **Vaihe 3, Analyysi ja synteesi**: Toimenpiteiden vaikutusten ja kerätyn datan analysointi. Tässä vaiheessa arvioidaan operaation onnistumista ja kerätään ymmärrystä jatkotoimenpiteitä varten.
    d. **Vaihe 4, Päättäminen**: Operaation virallinen päättäminen ja siirtyminen jälkihoitoon. Tässä vaiheessa määritellään tarvittavat jatkotoimenpiteet ja raportoidaan operaation tulokset asianosaisille.
4) **Toiminnanvapauden turvaaminen:** Operaation päätyttyä kybersuojajoukot esittävät mahdolliset korjaustoimenpiteet turvattavalle kohteelle, jotta sen normaali toiminta voidaan jatkaa turvallisesti. Vaiheessa varmistetaan, että kohde on suojattu tulevia kyberuhkia vastaan ja että se pystyy jatkamaan toimintaansa vahvistetuin turvallisuustoimin.

Tutkimuksen ensimmäiseksi apukysymykseksi oli asetettu “Mikä on valtionhallinnon johtamisen rakenne kybersuojajoukkojen puolustuksellisen kyberoperaation käynnistämisessä”. Tutkimustuloksen perusteella valtionhallinnon johtamisen rakenne kybersuojajoukkojen puolustuksellisen kyberoperaation käynnistämisessä perustuu toimivaltuuksien ja vastuiden selkeään jakoon TEM:n, HVK:n ja useiden muiden eri viranomaisten ja organisaatioiden välillä. Työ- ja elinkeinoministeriön tunnistettiin toimivan energiatoimialan vastuuministeriönä, koordinoiden toimintaa yhdessä operatiivisen, strategisen ja poliittisen toimijoiden kanssa. Operatiivisen tason koordinointi ja päätöksenteko tunnistettiin tukeutuvan kansliapäällikkökokouksien johtoasemaan ja TP-UTVA:n rooliin poliittisena päätöksentekoelimenä. Lisäksi tutkimuksessa tunnistettiin HVK:n rooli energiatoimialaa kohdistuvan uhkatason mukaisessa koordinoinnissa. Kansainvälisen tuen vastaanottamisen ja antamisen prosesseja tunnistettiin ohjattavan poliittisella tasolla, jotka mukailevat useaa eri lainsäädäntöä.

Tutkimuksen toisena apukysymyksenä oli “Mitä toimintatapamalleja tulee huomioida kybersuojajoukkojen toteuttaman puolustuksellisten kyberoperaatioiden toimeenpanossa?” Tutkimustuloksena tunnistettiin, että

kybersuojajoukkojen toimeenpanemissa puolustuksellisissa kyberoperaatioissa tulee huomioida useita toimintatapamalleja, jotka kattavat teknis-taktisen tason operoinnin, sekä uhkalähtöisen ja poikkeamalähtöisen toiminnan. Nämä mallit korostavat tarvetta ennakolliselle suunnittelulle, resurssien tehokkaalle käytölle, jatkuvan tilannekuvan muodostamiselle ja yhteistyölle eri toimijoiden välillä niin operatiivisella, strategisella ja poliittisella tasolla, luoden pohjan teknis-tason operoinnille.

Tutkimuksen kolmanneksi apukysymykseksi oli asetettu: "Mitä johtamisen ja ohjauksen rakenteita, malleja ja lainsäädäntöä tulisi luoda tutkimuksen viitekehyksen saavuttamiseksi?". Kybersuojajoukkojen toiminnan tehokkuuden maksimoimiseksi ja operaatioiden onnistuneeksi toimeenpanemiseksi on tarpeellista kehittää johtamisen ja ohjauksen rakenteita, malleja sekä lainsäädäntöä. Tutkimuksessa korostui virka-avun antamisen ja vastaanottamisen lainsäädännöllisten rajoitteiden selkeyttäminen. Lisäksi tutkimuksessa tunnistettiin mahdollisuus tarkastella sopimusmalliehtoista toimintaa, sekä määritellä kansainvälisen yhteistyön tietosuojaan liittyvien haasteiden toimintamenetelmät.

Tutkimustuloksen lopullisena yhteenvetona voidaan todeta, että kybersuojajoukkojen puolustuksellisen kyberoperaation toimeenpaneminen on monimutkainen prosessi, joka vaatii eri tasojen tiivistä yhteistyötä, selkeää lainsäädäntöä ja toimintamalleja, sekä kykyä mukautua nopeasti muuttuviin uhkakuviin ja operatiivisiin olosuhteisiin. Lisäksi tulee korostaa, että päätöksenteon nopeus, luvitusprosessien joustavuus sekä ennakollinen valmistautuminen ja harjoittelu ovat olennaisia tekijöitä operaation onnistuneessa toimeenpanossa.

6.2 Havainnot ja käytännön hyödynnettävyys

Tutkimuksen aikana kävi ilmeiseksi, että Suomessa ei ole olemassa vakituista toimijaa, joka voisi toimia kybersuojajoukon taustalla toimivana organisaationa. Eräs haastateltava tiivisti kysymyksen seuraavasti:

> Tullaan siihen tilanteeseen, että tän tyyppinen toiminta kokonaisuudessa puuttuu. Jos seuraava kysymys on, että missä se pitäisi olla, niin tässä palataan siihen, että miten tän tyyppinen toiminta pitäisi organisoida strategisella tasolla Suomessa, jotta tällaiselle toiminnalle löytyisi kotipaikka […]. Mahdollisuus, mitä joissakin maissa on, että [OPERATIIVINEN JOHTAMINEN] on paikallisessa Prime Minister Officessa tai Valtioneuvoston kansliassa. Jos oletetaan, että meillä olisi sen tyyppinen rakennelma kuin Israelissa on, kun siellä se kyberturvallisuuden strateginen johtoyksikkö on osana pääministerin kansliaa, niin se käynnistäisi tämmöisessä uhkatilanteessa ne toimenpiteet ja hankkisi tarvittavat resurssit siviiliorganisaatioista ja asevoimilta.

Havainnon voidaan nähdä toimivan keskustelunavauksena sille, että olisiko Suomeen tarvetta perustaa kriittisen infrastruktuurin kyberturvallisuuden valvontaan ja vastatoimiin erikoistunut viranomainen, verrattavissa Israelin kyberturvallisuuden strategisen johtoyksikön malliin tai Yhdysvaltain Cybersecurity and Infrastructure Security Agency:n (CISA). Tämän tarpeen voisi nähdä olevan erityisen ilmeinen, kun otetaan huomioon kyberuhkien kasvava määrä ja yhteiskunnan jatkuva digitalisoituminen ja verkottuminen.

Toisena tutkimuksen havaintona on, kuinka Suomen Nato-jäsenyys saattaa asettaa tulevaisuudessa uusia tarpeita valtiollisten kyberkyvykkyyksien käytölle osana liittouman kollektiivista puolustusta. Suomelle VCISC:n kaltaisen toiminnan mahdollinen tulevaisuuden osallistuminen korostaa entisestään tarvetta luoda kyberturvallisuuden operatiivista toimintaa tukeva rakennelma. Tämän voitaisiin nähdä parantavan Suomen valmiuksia vastata nopeasti ja koordinoidusti kyberuhkiin sekä kansallisella että kansainvälisellä tasolla. Lisäksi Suomen Nato-jäsenyyden kautta tunnistettiin tarve muutokselle Suomen strategisessa kulttuurissa kansainvälisen tuen vastaanottamisen suhteen. Tutkimuksen asiantuntijahaastatteluissa tuotiin esiin erityisesti VSISC-toiminnan herättämä mahdollinen laaja yhteiskunnallinen keskustelu kansainvälisen avun antamisesta ja vastaanottamisesta, ja kuinka Suomi on historiallisesti korostanut omavaraisuutta ja selviytymistä omilla resursseilla. Nato-jäsenyyden myötä tämä itsenäisyyden asetelma on kuitenkin kääntymässä, vaatien mahdollisesti merkittävää kulttuurista muutosta ja valmiutta toimia osana kansainvälistä yhteisöä. Tämä tarkoittaa tarvetta valmistaua vastaanottamaan kansainvälistä tukea, mutta myös aktiivisesti osallistumaan ja antamaan tukea muille jäsenvaltioille, rakentaen luottamusta ja yhteistyötä liittolaisten kesken.

Kolmantena havaintona tutkimuksen voidaan nähdä nostavan esiin, kuinka virka-avun selkeyttäminen ja sen tarkempi juridinen määrittely ovat keskeisiä tekijöitä viranomaisten ja kriittisen infrastruktuurin toimijoiden välisen yhteistyön tehostamisessa kybertoimintaympäristössä. Selkeät vastuunjaot, ennakoiva valmistautuminen ja lainsäädännön kehittäminen tunnistettiin mahdollistavan nopean ja koordinoidun reagoinnin, vahvistaen yhteiskunnan kykyä suojautua kyberuhkilta. Erityisesti tarpeeksi lainsäädännön selkeyttämiseen ja toimivaltuuksien laajentamiseen tunnistettiin olevan, kun toiminnan tavoitteena on proaktiivinen toiminta kriittisen infrastruktuurin turvaamiseksi.

6.3 Tutkimustulosten luotettavuuden arviointi

Tämän tutkimuksen tulosten luotettavuuden näkökulmasta tulee huomioida tutkimuksessa kehitetyn toimintatapamallin yleismaailmallinen lähestymistapa tulosten esittämiseen. Tämän lähestymistavan arvioitiin mahdollistavan kriittisen infrastruktuurin yksityiskohtaisten tietojen ja toimintojen suojauksen, minkä nähtiin vahvistavan tutkimuksen eettistä perustaa. Tutkimuksen toimintatapamallin operatiivisen tason kokonaisuuden rakentaminen Puolustusvoimien toiminnan ympärille keskittyi ainoastaan virka-apuun ja joukkojen perustamiseen ja operointiin julkisen tutkimuksen pohjalta, osoittaen harkittua lähestymistapaa arkaluontoisen tiedon vahingollisessa paljastamisessa. Teknis-taktisen tason olta Puolustusvoimia ei eroteltu toiminnasta, vaan toimintaa kuvattiin yleisluontoisesti aikaisempien tutkimusten mukaisesti. Tutkimuksen julkisen julkaisukelpoisuuden varmistamiseksi haastatteluissa ei haastateltu suoraan Puolustusvoimien alaisessa virassa palvelevia henkilöitä, minkä johdosta on mahdollista, että näkemykset voivat olla eroavia Puolustusvoimissa palvelevien henkilöiden käsityksiin. Valittu toimintamenetelmän tunnistettiin myös saattavan johtaa yleistettävien johtopäätösten ja kriittisen infrastruktuurin toimintaa koskevan

syvällisen ymmärryksen rajoittumiseen. Tämän arvioitiin asettavan mahdollisesti rajoituksia tutkimuksen tulosten syvyydelle, mutta samalla sen tunnistettiin korostavan tutkimuksen tarkoituksenmukaista varovaisuutta ja eettisiä harkintoja tiedonhallinnan suhteen. Tutkimuksen nojautuminen aikaisempaan tutkimukseen ja säännölliset viittaukset niihin arvioitiinkin tarjoavat vankan perustan käytetyille toimintatapakuvauksille, minkä on arvioitu lisäävän sen luotettavuutta. Viittausten johdonmukainen käyttö arvioitiin tukevan tutkimuksen läpinäkyvyyttä, samalla mahdollistaen tulosten verifiointimahdollisuuden. Tutkimuksen viimeisessä vaiheessa, validoitaessa tutkimustulosta asiantuntijoiden toimesta, kävi kuitenkin ilmeiseksi, kuinka toimintaa oli kuvattu laajasti eri alojen asiantuntijoiden toimesta, jonka myötä tutkimustuloksen mukaisessa kokonaisuudessa voisi olla todennäköisesti eroavaisuuksia yksityiskohtaisen koordinoinnin suhteen. Toimintatapamallin tunnistettiin kuitenkin toimivan yleismallisena kuvauksena toimintaympäristöstä ja sen mukaisista toimijoista, joka mahdollistaa aihealueen yksityiskohtaisemman suunnittelun toimijoiden omien prosessien mukaisesti. Tutkimustuloksen luotettavuuden näkökulmasta toimintatapamalli arvioitiin käytettäväksi mallipohjana, vaatien kuitenkin yksittäisiä soveltamiskokonaisuuksia eri toimijoiden suhteen, jotka eivät välttämättä ole käytettävissä osana julkista tutkimusta.

Tutkimuksen aikana tuli myös ilmeiseksi, kuinka Liikenne- ja viestintäministeriöön sijoitetun valtion kyberturvallisuusjohtajan toiminto muutetiin valtion kyberturvallisuusjohtajan toimistoksi vuodenvaihteessa 2023-2024. Muutoksella on pyritty vastaamaan laajemmin kyberturvallisuuteen liittyvään valtioneuvostotason ennakointiin ja varautumiseen. Tutkimuksen toteuttamisen aikana tästä ei kuitenkaan ollut saatavilla tietoa julkisista lähteistä, jonka myötä kokonaisuus jätettiin tutkimuksen ulkopuolelle. Lisäksi toiminnan tunnistettiin painottuvan vahvasti strategiselle tasolle, joka ei mukaillut tutkimuksen rajausta. Valtion kyberturvallisuusjohtajan toimiston tulevaisuuden tehtävillä arvioitiin kuitenkin olevan mahdollisesti vaikutuksia tutkimuksessa kehitetyn strategisen tason kokonaisuuden osalta. Lisäksi muita kehitetyn toimintatapamallin luottamukseen vaikuttavia tekijöitä tunnistettiin olevan CER- ja NIS2-direktiivien mukaiset kokonaisuudet, joiden lakiesitykset ovat tutkimuksen aikana vielä kesken. Näillä arvioitiin olevan mahdollisesti vaikutuksia operatiivisen tason toimintoihin muun muassa keskitettyjen yhteyspisteiden muodostumisen osalta.

6.4 Jatkotutkimusaiheet

Tutkimuksen havaintojen perusteella voisi olla tarvetta tarkastella mahdollisuutta perustaa erikoistunut viranomainen kriittisen infrastruktuurin kyberturvallisuuden valvontaan ja vastatoimiin. Jatkotutkimusaiheeksi esitetäänkin selvityksen toimeenpano siitä, miten tällainen viranomainen voitaisiin Suomessa perustaa ja integroida olemassa olevaan operatiiviseen toimintaan. Lisäksi selvityksessä tulisi tarkastella kyseisen perustettavan toiminnon juridisia, organisatoorisia ja operatiivisia puitteita. Toiminta voisi myös tarkastella valtion kyberturvallisuusjohtajan toimiston näkökulmasta, ja sen mahdollisuudesta muodostaa niin sanottu “kybernyrkki”. Suomen Nato-jäsenyyden osalta olisi tarpeen tutkia täysjäsenyyden konkreettisiä vaikutuksia

kyberpuolustusstrategiaan ja operatiivisen yhteistyön mekanismeihin liittolaisten kesken. Myös tutkimuksessa havaitut virka-avun puutteet ja epäselvyydet kybertoimintaympäristössä voitaisiin nähdä jatkotutkimusaiheena. Tutkimuksessa voitaisiin pyrkiä selvittämään virka-avun toimeenpanon prosessien selkeyttämiseen vaadittavai toimia ja muita lainsäädännön kehittämisen kokonaisuuksia. Jatkotutkimus voisi myös pureutua siihen, miten eri viranomaisten välisen yhteistyön ja vastuunjaon parannukset voidaan saavuttaa tehokkaan ja joustavan reagoinnin mahdollistamiseksi kyberuhkiin. Viimeisenä esitettävänä jatkotutkimusaiheena nähtäisiin tarpeelliseksi tarkastella kehitetyn toimintatapamallin mukaista toimintaympäristöä yksittäisten toimijoiden näkökulmasta siten, että toimijat tuottaisivat itsenäisesti oman toimintaympäristön mukaisen kuvauksen. Tämä on arvioitu mahdollistavan toimintaympäristöjen yksityiskohtaisemman vertailun, sillä toimijoiden kuvaukset perustuisivat jo lähtökohtatilanteessa organisaatioiden omiin näkemyksiin, eikä taustalla olisi tutkijan itsenäisesti tuottamaa toimintatapamallia. Tämän on kuitenkin tunnistettu tuottavan huomattaa lisätyötä tutkimukseen osallistuville organisaatioille, minkä lisäksi tutkimus tuottaisi todennäköisesti turvaluokitellun tutkimustuloksen, jonka myötä sen voisi epätodennäköisesti tuottaa osana korkeakoulujen opinnäytetöitä, vaan se tulisi tuottaa tilaustutkimuksena esimerkiksi valtionhallinnon toimijan toimesta.

LÄHTEET

Aleksiev, A., Oberschelp de Meneses, A. & Young, M. (2023). New EU Cyber Law "NIS2" Enters Into Force. Inside Privacy. Haettu 2.11.2023. https://www.insideprivacy.com/cybersecurity-2/new-eu-cyber-law-nis2-enters-into-force/

Alshathry, S. (2017). Cyber Attack on Saudi Aramco. King Saud University. International Journalof Managementand Information Technology. ISSN 2278 – 5612. Haettu 23.12.2023 osoitteesta: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiGwsKQgqaDAxUoIjQIHekABesQFnoECAwQAQ&url=https%3A%2F%2Frajpub.com%2Findex.php%2Fijmit%2Farticle%2Fview%2F5613%2Fpdf&usg=AOvVaw0j1b7p_YAHLMJqHLEpj2J5&opi=89978449

Asevelvollisuuslaki 28.12.2007/1438. https://www.finlex.fi/fi/laki/ajantasa/2007/20071438

Atkins, S. (2021). Creating Restraint in Cyberspace, Forward Cyber Operations and Theories of Restrain. Royal United Services Institute for Defence and Security Studies. Haettu 28.10.2023 osoitteesta: https://cesmar.it/wp-content/uploads/2023/04/202104-Cyberspace.pdf

Beecroft, N. & Gilmore, T. (2023). The Advantages of "Hunt Forward" Extend Beyond the Hunt. Digital Intelligence. BAE Systems. Haettu 12.11.2023 osoitteesta: https://www.baesystems.com/en-media/uploadFile/20230622095544/1573692584787.pdf

Bergvall-Kåreborn, B, Mirijamdotter, A., & Basden, A. (2004). Basic principles of SSM modeling: An examination of CATWOE from a soft perspective. Systemic Practice and Action Research. 17. 55-73. 10.1023/B:SPAA.0000018903.18767.18.

Bodeau, D., Graubart, R. & Heinbockel, W. (2013). Mapping the Cyber Terrain: Enabling Cyber Defensibility Claims and Hypotheses to Be Stated and Evaluated with Greater Rigor and Utility (MTR130433). Haettu 12.11.2023 osoitteesta: http://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13- 4175.pdf.

Bonnie, K. & Joseph, M. (2005). Qualitative Research Methods for Evaluating Computer Information Systems. 10.1007/0-387-30329-4_2.

Burge, S. (2015). An Overview of the Soft Systems Methodology. Haettu 28.12.2023 osoitteesta https://www.burgehugheswalsh.co.uk/Uploaded/1/Documents/Soft-Systems-Methodology.pdf

Caton, J. (2020). Examining the Roles of Army Reserve Component Forces in Military Cyberspace Operations (US Army War College Press, 2019), https://press.armywarcollege.edu/monographs/384

Cavelty, D. (2010). The Reality and Future of Cyberwar, Parliamentary, 2010

CERT-UA, The Computer Emergency Response Team of Ukraine. (2022). Попередження щодо можливих кібератак. the State Service of Special Communication and Information Protection of Ukraine. Haettu 18.11.2023 osoitteesta: https://cert.gov.ua/article/37211

Cerulus, L. (2022). EU to mobilize cyber team to help Ukraine fight Russian cyberattacks. Politico. Haettu 18.11.2023 osoitteesta: https://www.politico.eu/article/ukraine-russia-eu-cyber-attack-security-help/

CISA, Cybersecurity and Infrastructure Security Agency. (2021). Cyber-Attack Against Ukrainian Critical Infrastructure https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

CISA, Cybersecurity and Infrastructure Security Agency. (2022). Iranian State Actors Conduct Cyber Operations Against the Government of Albania. CYBERSECURITY ADVISORY. Haettu 4.11.2023 osoitteesta: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a

CNMF, Cyber National Mission Force, A. (2022). Before the Invasion: Hunt Forward Operations in Ukraine. Haettu 10.1.2024 osoitteesta https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://nsarchive.gwu.edu/sites/default/files/documents/rmsj3h-751x3/2022-11-28-CNMF-Before-the-Invasion-Hunt-Forward-Operations-in-Ukraine.pdf&ved=2ahUKEwjbg-29w56FAxVpJBAIHUM_BVUQFnoECA0QAw&usg=AOvVaw2n5hSxGhu3-GNrA9cSZUue

CNMF, U.S. Cyber National Mission Force, B. (2022). Partnership in Action: Croatian, U.S. Cyber Defenders Hunting for Malicious Actors. The Department of the Navy Information Technology Magazine. Haettu 2.11.2023 osoitteesta: https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=15814

CRRT, Cyber Rapid Response Team. (2023). Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRTs). Haettu 13.11.2023 osoitteesta: https://crrts.eu/

CRS, Congressional Research Service. (2021). Colonial Pipeline: The DarkSide Strikes. Haettu 23.12.2023 osoitteesta https://crsreports.congress.gov/product/pdf/IN/IN11667

CYBER4DE. (Ei pvm). Cyber Rapid Response Toolbox for Defence Use. Haettu 12.11.2023 osoitteesta: https://www.cyber4de.eu/about

De Falco, M. (2012). Stuxnet Facts Report. A Technical and Strategic Analysis. NATO Cooperative Cyber Defence Center of Excellence. Tallinna, Viro.

DOA, Department of the Army. (2021). FM 3-12. Cyberspace Operations and Electromagnetic Warfare. No. 3-12. Washington, D.C. Haettu 29.10.2023 osoitteesta https://irp.fas.org/doddir/army/fm3-12.pdf

DOD, U.S. Department of Defence. (2023). 2023 Cyber Strategy of The Department of Defense. Haettu 2.11.2023 osoitteesta https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

DOD, U.S. Department of Defense. (2014). Mission Analysis for Cyber Operations of Department of Defense. Haettu 30.10.2023 osoitteesta https://info.publicintelligence.net/DoD-CyberMissionAnalysis.pdf

Ebrahimi, A., Leithner, A., Lowham, A. & Tiscareño, S. (2020). National Guard Cyber Protection Teams as a Response to Cybersecurity Threats. Haettu 6,11,2923 osoitteesta: https://cci.calpoly.edu/sites/default/files/2021-05/NGCPT_6.30.20.pdf

Edgar, T. & Manz, D. (2017). Research Methods for Cyber Security. Syngress. ISBN 9780128053492. Haettu 13.11.2023 osoitteesta https://doi.org/10.1016/B978-0-12-805349-2.00030-3.

Ekstorm, B. (2022) s. 27. Defining, measuring, and analyzingdefensibility in the defensive cyberoperations context. Naval Postgraduate School. Montere, California.

Energiateollisuus. (2022). Vihreällä siirtymällä irti venäläisestä energiasta. Haettu 14.11.2023 osoitteesta https://energia.fi/energiapolitiikka/ukrainan_sota/vihrealla_siirtymalla_irti_venaja-riippuvuudesta

ENISA, The European Union Agency for Cybersecurity. (2017). Threat Landscape Report 2016, 15 Top Cyber-Threats and Trends. Haettu 25.11.2023 osoitteesta: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016

Euroopan parlamentin ja neuvoston direktiivi 2022/2557. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32022L2557

Fingrid, A. (Ei pvm.). Suomen sähköjärjestelmä. Haettu 20.12.2023 osoitteesta https://www.fingrid.fi/kantaverkko/kehittaminen/suomen-sahkojarjestelma/

Fingrid, B. (Ei pvm.). Voimalaitokset. Haettu 20.12.2023 osoitteesta https://www.fingrid.fi/sahkomarkkinainformaatio/alkuperatakuun-tapahtumat/voimalaitokset/

Fingrid. (2022). Fingrid Oyj:n sähkönsiirtoverkko. Haettu 12.12.2023 osoitteesta https://www.fingrid.fi/globalassets/dokumentit/fi/kantaverkko/sahkonsiirto/a3_kartta_selite_22.pdf

Forescout Research. (2024). Clearing the Fog of War. A Critical Analysis of Recent Energy Sector Attacks in Denmark and Ukraine. Vedere Labs. Noudettu 31.2.2024 osoitteesta https://www.forescout.com/resources/clearing-the-fog-of-war/

Galinec, D., Steingartner, W. & Zebić, V. (2019). Cyber Rapid Response Team: An Option within Hybrid Threats," 2019 IEEE 15th International Scientific Conference on Informatics, Poprad, Slovakia

Gasgrid. (Ei pvm.). Gas transmission network. Haettu 22.3.2024 osoitteesta: https://gasgrid.fi/en/gas-network/gas-transmission-network/

Hagelstam, A. (2005). CIP – kriittisen infrastruktuurin turvaaminen: Käsiteanalyysi ja kansainvälinen vertailu. Huoltovarmuuskeskus. Julkaisuja 1/2005. Haettu 10.12.2023 osoitteesta: https://www.huoltovarmuuskeskus.fi/files/019d67575f48fdb84212fd8bd9164b8ac8829ccd/cip-raportti_final.pdf

Hakoniemi, J. (2021). Case Vastaamo. Karhunpainia tietoturvan kanssa – Mediaseuranta tapahtuneesta. Poliisiammattikorkeakoulun opinnäytetyö.

Hallintolaki 434/2003. https://www.finlex.fi/fi/laki/alkup/2003/20030434

Hartman, W. (2022). Cyber Command sent a 'hunt forward' team to help Lithuania harden its systems. Kirjoittanut Martin Matishak. The Recorded Future News. Haettu 3.11.2023 osoitteesta https://therecord.media/cyber-command-sent-a-hunt-forward-team-to-help-lithuania-harden-its-systems

HE 137/2011. Hallituksen esitys Eduskunnalle laeiksi valtioneuvostosta annetun lain ja eräiden siihen liittyvien lakien muuttamisesta. https://www.finlex.fi/sv/esitykset/he/2011/20110137

HE 152/2013. Hallituksen esitys eduskunnalle laiksi yhteistoiminnasta valtion virastoissa ja laitoksissa sekä eräiksi siihen liittyviksi laeiksi. https://finlex.fi/fi/esitykset/he/2013/20130152

Heinäaro, K. (2014). Electric Power as Critical Infrastructure. Kirjoitus osana Jouko Vankkan toimittamaa Critical Infrastructure Protection Against Cyber Threats. Maanpuolustuskorkeakoulu. Helsinki. ISBN 978-951-25-2600-0.

Herbert, S. (1996). The Sciences of the Artificial. MIT Press. ISBN 9780262193740. Massachusetts Institute of Technology

Hevner, A., Salvatore, M., Jinsoo, P. & Sudha, R. (2004). Design Science in Information Systems Research. Management Information Systems Quarterly.

Hillebrand, G. D. & Ault, B. (2018). Strategic Cyberspace Operations Guide. United States Army War College. Center for Strategic Leadership. Haettu 29.10.2023 osoitteesta

https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). Tutki ja kirjoita. (15. uud. painos). Helsinki: Tammi

Hutchins, E., Cloppert, M. & Amin, R (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. In: The Proceedings of the 6th International Conference on Information Warfare and Security, Washington, D.C., 17-18. maaliskuuta 2011. Yhdysvallat.

HVK, Huoltovarmuuskeskus, A. (2023). Ajankohtaisia kysymyksiä ja vastauksia kriittisestä infrastruktuurista ja varautumisesta. Verkkojulkaisu. Haettu 10.12.2023 osoitteesta: https://www.huoltovarmuuskeskus.fi/a/ajankohtaisia-kysymyksia-ja-vastauksia-kriittisesta-infrastruktuurista-ja-varautumisesta

HVK, Huoltovarmuuskeskus, B. (Ei pvm). Huoltovarmuusorganisaatio. Haettu 12.12.2023 osoitteesta: https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio

HVK, Huoltovarmuuskeskus, C. (2023). HVK on kehottanut kriittisen infrastruktuurin yrityksiä nostamaan varautumistasoa. Noudettu 20.3.2024 osoitteesta https://www.huoltovarmuuskeskus.fi/a/hvk-on-kehottanut-kriittisen-infrastruktuurin-yrityksia-nostamaan-varautumistasoa

HVK, Huoltovarmuuskeskus, D (2023). Kaasun toimitusvarmuuden ennaltaehkäisy- ja hätäsuunnitelma päivittyi. Haettu 20.3.2024 osoitteesta: https://www.huoltovarmuuskeskus.fi/a/kaasun-toimitusvarmuuden-ennaltaehkaisy-ja-hatasuunnitelma-paivittyi

HVK, Huoltovarmuuskeskus. (2008). Huoltovarmuusorganisaation työjärjestys. Haettu 21.12.2023 osoitteesta: https://www.huoltovarmuuskeskus.fi/files/deba4f01f0797cfc1ae4551ef13c85ba36a09cfe/hvotj_180908.pdf

HVK, Huoltovarmuuskeskus. (2022). Toimialojen kyberkypsyyden selvitys 2022. Kansallinen koosteraportti. ISBN: 978-952-7470-23-7. Haettu 21.12.2023 osoitteesta: https://www.huoltovarmuuskeskus.fi/files/29b11d0af56a115126ad490af444f1c4fd7885af/hvk-toimialojen-kyberkypsyyden-selvitys-2022.pdf

HVK, Huoltovarmuuskeskus. (2023). Huoltovarmuusorganisaatio. Haettu 14.11.2023 osoitteesta: https://www.huoltovarmuuskeskus.fi/huoltovarmuusorganisaatio

HVK, Huoltovarmuuskeskus. (2023). Toimialojen kyberkypsyyden selvitys 2022. ISBN: 978-952-7470-23-7. Kansallinen koosteraportti. Helsinki.

Jiawei, L., Zhang, R., Jianyi, L. & Gongshen L. (2019). Security and Communication NetworksLogKernel: A Threat Hunting Approach Based on BehaviourProvenance Graph and Graph Kernel Clustering.

Johnson, B., Caban, D., Krotofil, M., Scali, D., Brubaker, N. & Glyer, C. (2023). Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure.

Kadettikunta. (Ei pvm). NATO Enhanced Forward Presence. Turvallisuuspolitiikan Tietopankki. Haettu 3.11.2023 osoitteesta https://turpopankki.fi/suomen-lahialueet/baltian-maat/naton-lasnaolo-baltian-maissa/nato-enhanced-forward-presence/#toggle-id-1

Kapelanski, P., (2023). 177th Cyber Protection Team "Shadow Vikings" Organization & Capabilities Brief. Haettu 23.3.2024 osoitteesta https://www.lcc.mn.gov/lccs/Meetings/20230911/177-CPT-Capabilities-Brief-v6

Kasanen, E., Lukka, K. & Siitonen, A. (1993). The Constructive Approach in Management Accounting Research. Journal of Management Accounting Research.

Keränen J., Molarius R., Heikkilä A., Poussa L. & Partanen J. (2016). Varautumisen kehitystarpeet turvallisessa yhteiskunnassa. Valtioneuvoston selvitys-ja tutkimustoiminnanjulkaisusarja 12/2016. Haettu 22.12.2023 osoitteesta: https://tietokayttoon.fi/documents/10616/2009122/12_Varautumisen+kehitystarpeet+turvallisessa+yhteiskunnassa.pdf/bb4b6c20-173a-451e-8cfa-73c657fc2b70?version=1.0

Kiviharju, M., Huttunen, M. & Kantola, H. (2021). Kybertaktiikasta: taistelun elementit ja yleiset taktiset periaatteet kybertilassa. Puolustustutkimuksen Vuosikirja 2021. Puolustusvoimat. Riihimäki.

Kruszka, L., Klósak, M., Muzolf, P. (2019). Critical Infrastructure Protection. published under the NATO Science for Peace and Security series. ISBN 978-1-61499-964-5

KTK, Kyberturvallisuuskeskus. (2023). ISAC-tiedonvaihtoryhmät. Haettu 7.11.2023 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/isac-tiedonvaihtoryhmat

KTK, Kyberturvallisuuskeskus. (Ei pvm.). Ilmoita tietoturvapoikkeamasta (NIS-ilmoitusvelvollisuus). Haettu 26.12.2023 osoitteesta: https://www.kyberturvallisuuskeskus.fi/fi/asioi-kanssamme/ilmoita-tietoturvapoikkeamasta-nis-ilmoitusvelvollisuus?toggle=Energia

Kukkola, J. (2024). Suvereenit hiekkamadot : Venäjän kybertoiminta osana valtioiden välistä kamppailua 2000-luvulla. Maanpuolustuskorkeakoulu. Sotataidon laitos. Maanpuolustuskorkeakoulu. ISBN:978-951-25-3437-1

Kuokkanen, N. (2020). Kriittisen infrastruktuurin suojaaminen Suomessa. Informaatioteknologian tiedekunta. Jyväskylän yliopisto.

Laari, T., Flyktman, J., Härmä, K., Timonen J. & Tuovinen, J. (2019). #kyberpuolustus: kyberkäsikirja Puolustusvoimien henkilöstölle. Maanpuolustuskorkeakoulu. Sotataidon laitos. Helsinki. ISBN 978-951-25-3120-2

Laki kansainvälistä apua, yhteistoimintaa tai muuta kansainvälistä toimintaa koskevasta päätöksenteosta 28.6.2017/418. https://www.finlex.fi/fi/laki/ajantasa/2017/20170418

Laki Puolustusvoimien virka-avusta poliisille 20.5.2022/342. https://www.finlex.fi/fi/laki/ajantasa/2022/20220342

Laki Puolustusvoimista 11.5.2007/551. https://www.finlex.fi/fi/laki/ajantasa/2007/20070551

Laki sotilastiedustelusta 26.4.2019/590. https://www.finlex.fi/fi/laki/ajantasa/2019/20190590

Laki vapaaehtoisesta maanpuolustuksesta 556/2007. https://www.finlex.fi/fi/laki/alkup/2007/20070556

Laki vapaaehtoisesta maanpuolustuksesta annetun lain 23 §:n muuttamisesta 346/2022. https://www.finlex.fi/fi/laki/alkup/2022/20220346

Lappalainen, E. & Jormakka, J. (2004). Tekniset tutkimusmenetelmät Maanpuolustuskorkeakoulussa. MPKK Tekniikan laitos.

Lehto, M. (2022). Cyber-Attacks Against Critical Infrastructure In M. Lehto, & P. Neitaanmäki (Eds.), Cyber Security : Critical Infrastructure Protection (pp. 3-42). Springer. Computational Methods in Applied Sciences, 56. https://doi.org/10.1007/978-3-030-91293-2_1

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T. & Salminen, M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. Helsinki. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017. ISBN 978-952-287-368-2.

Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J. & Salminen, M. (2018). Kyberturvallisuuden strateginen johtaminen Suomessa. Helsinki. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018. ISBN 978-952-287-532-7.

Lewis, T. (2015). Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. Second Edition. Wiley. ISBN: 9780471786283

Libicki, M. (2009). Cyberdeterrence and Cyberwar. RAND Corporation. Santa Monica, CA.

Lieber, K. (2016). The Offense–Defense Balance and Cyber Warfare. Monterey, California, Naval Postgraduate School. Haettu 11.12.2023 osoitteesta https://core.ac.uk/download/pdf/36732393.pdf#page=109

Liesinen, K., Karinen, R. & Lahtinen, K. (2017). Puolustusvoimien antaman virka-avun nykytila ja kehittäminen. Puolustusministeriö. ISBN: 978-951-25-2926-1

Lipsanen, T. (2019). SCADA-järjestelmien kyberturvallisuuden erityispiirteet ja parantaminen SCADA-järjestelmien kyberturvallisuuden erityispiirteet ja parantaminen. Informaatioteknologian tiedekunta. Jyväskylän yliopisto.

Luckenbaugh, J. (2023). NATO Ponders Using Article Five for Cyber Attacks. National Defense News. Haettu 14.2.2024 osoitteesta: https://www.nationaldefensemagazine.org/articles/2023/8/31/nato-ponders-using-article-five-for-cyber-attacks

Lukka, K. (2003). The Constructive Research Approach. Publications of the Turku School of Economics and Business Administration.

Maavoimien esikunta. (2008). Komppanian taisteluohje. Ohjesääntönumero 456 ISBN 978–951–25–1909–5. Edita Prima Oy, Helsinki.

Mandiant. (2013). APT1: Exposing One of China's Cyber Espionage Units. Haettu 22.12.2023 osoitteesta: https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf

Martin, A. (2023). German spy chief warns of cyberattacks targeting liquefied natural gas terminals. Recorded Future News. Haettu 28.10.2023 osoitteesta: https://therecord.media/german-intelligence-warning-lng-terminals-cyberattacks

Martin, A. (2023). NATO allies' new cyber pledges to remain classified — but here's what we know. The Record Media. Haettu 14.2.2024 osoitteesta https://therecord.media/nato-new-cyber-pledges-remain-classified-here-is-what-we-know

Matishak, M. (2023). US, Canada sent cyber experts to Latvia to bolster digital defenses. Recorded Future News. Haettu 3.11.2023 osoitteesta https://therecord.media/latvia-hunt-forward-cyber-command-canada

McCroskey, E. & Mock, C. (2017). Operational Graphics for Cyberspace. Joint Force Quarterly 85. National Defense University Press. Haettu 25.11.2023 osoitteesta: https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-85 jfq-85_42-49_McCroskey-Mock.pdf

Miller, M. (2022). Albania weighed invoking NATO's Article 5 over Iranian cyberattack. Politico. Haettu 4.11.2023 osoitteesta https://www.politico.com/news/2022/10/05/why-albania-chose-not-to-pull-the-nato-trigger-after-cyberattack-00060347

Ministry of National Defence of Lithuania. (2019). Protection of critical information infrastructure trained at cybersecurity exercise of the Lithuanian Armed Forces Amber Mist 2019. Haettu 18.11.2023 osoitteesta https://kam.lt/en/protection-of-critical-information-infrastructure-trained-at-cybersecurity-exercise-of-the-lithuanian-armed-forces-amber-mist-2019/?__cf_chl_tk=creVKSHab5BAfEI5MoEKHhCLNSnqWPrt68YS9P0WnYA-1700299151-0-gaNycGzNDCU

Mitre Corporation. (Ei pvm). ATT&CK Framework. ICS Matrix. Haettu 11.12.2023 osoitteesta: https://attack.mitre.org/matrices/ics/

Molle, D. (2016). Defending Critical Infrastructure as Cyber Key Terrain. Air Command And Staff College. Air University. Maxwell Air Force Base, Alabama.

Monk, A. & Howard, S. (1998). The Rich Picture: A Tool for Reasoning About Work Context. Haettu 20.12.2023 osoitteesta https://www-users.york.ac.uk/~am1/RichPicture.pdf

Monte, M. (2015). Network Attacks and Exploitation: A Framework. Wiley, ISBN 1119183448

Muller, L., Gjesvik, L. & Friis, K. (2018). Cyber-weapons inInternational Politics. 3 / 2018NUPI ReportPossible sabotage against the Norwegianpetroleum sector. Norwegian Institute of International Affairs. Oslo, Norway. ISSN 1894-650X

Mustonen, L. (2021). Kyberturvallisuuden hallintorakenteen toiminnan analyysi : tapaus kriittisen infrastruktuurin organisaatiossa. Informaatioteknologian tiedekunta. Jyväskylän yliopisto.

Muttilainen, M. (2015). Harjoitusmallin kehittäminen valtiohallinnon Häiriöhallintaryhmälle. Laurea ammattikorkeakoulu. Leppävaara.

Nakasone, P. & Sulmeyer, M. (2020). How to Compete in Cyberspace Cyber? Command's New Approach. Forreign Affairs. Haettu 2.11.2023 osoitteesta: https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity

Nakasone, P. (2023). NPC Headliner Luncheon: Gen. Paul Nakasone. National Press Club Live. Haettu 2.11.2023 osoitteesta https://www.youtube.com/watch?v=tJnMlPydBak

Nato, The North Atlantic Treaty Organization, A. (2023). Collective defence and Article 5. Haettu 14.2.2024 osoitteesta: https://www.nato.int/cps/en/natohq/topics_110496.htm

Nato, The North Atlantic Treaty Organization, B. (2023). Cyber defence. Haettu 14.2.2024 osoitteesta: https://www.nato.int/cps/en/natohq/topics_78170.htm

Nato, The North Atlantic Treaty Organization. (2011). APP-6(C). Joint Military Symbology. NATO UNCLASSIFIED. Nato Standardization Agency. Haettu 25.11.2023 osoitteesta https://www.cimic-coe.org/resources/external-publications/app-6-c.pdf

Nato, The North Atlantic Treaty Organization. (2023). Collective defence and Article 5. Haettu 4.11.2023 osoitteesta: https://www.nato.int/cps/en/natohq/topics_110496.htm

Neitaanmäki, P., Lehto, M. & Savonen, M. (2021). Yhteiskunnan digimurros. Jyväskylän yliopisto. ISBN 978-951-39-8647-6

NGB, National Guard Bureau. (2015). National Guard cyber protection teams announced. Haettu 27.3.2024 osoitteesta https://www.nationalguard.mil/News/Article/577375/national-guard-cyber-protection-teams-announced/

NIC, National Intelligence Council. (2017). Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution. ICA 2017-01D. Haettu 3.11.2023 osoitteesta https://www.dni.gov/files/documents/ICA_2017_01.pdf

NIST, National Institute of Standards and Technology, A (Ei pvm.). Operational Technology. Haettu 21.12.2023 osoitteesta: https://csrc.nist.gov/glossary/term/operational_technology

NIST, National Institute of Standards and Technology, B. (Ei pvm.). Industrial Control System. Haettu 21.12.2023 osoitteesta https://csrc.nist.gov/glossary/term/industrial_control_system

NIST, National Institute of Standards and Technology, C, (Ei pvm.). Supervisory Control and Data Acquisition. Haettu 21.12.2023 osoitteesta: https://csrc.nist.gov/glossary/term/supervisory_control_and_data_acquisition

NIST, National Institute of Standards and Technology, D. (Ei pvm.). Distributed Control System. Haettu 21.12.2023 osoitteesta: https://csrc.nist.gov/glossary/term/distributed_control_system

NSA, National Security Agency. (Ei pvm.). NSA/CSS Leadership. Haettu 29.10.2023 osoitteesta: https://www.nsa.gov/About/Leadership/

ODNI, Office of The Director of National Intelligence. (2023). Annual Threat Assessment of the U.S. Intelligence Community. Haettu 28.10.2023 osoitteesta https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf

Oksala E., Heikkinen M., Vulli J. & Lehtinen, T. (2023). Tietoverkkotiedustelu ja verkkovakolu osana Kiinan suorittamia kyberoperaatioita. Kirjoitus osana Isokangas, J. toimittamaa Tiedustelun maailma: Kiina Tiedusteluanalyysi I

-kurssin raportteja. Informaatioteknologian tiedekunnan julkaisuja No. 99/2023. Jyväskylän yliopisto. ISBN 978-951-39-9604-8.

Pande, J. & Prasad, A. (2016). Digital Forensics. Post-Graduate Diploma in Cyber SecurityDigital Forensics. ISBN: 978-93-84813-94-9. Uttarakhand Open University.

Pearce, A. (2017). SD National Guard activates new cyber protection team. Defense Visual Information Distribution Service. Haettu 27.3.2024 osoitteesta https://www.dvidshub.net/news/238343/sd-national-guard-activates-new-cyber-protection-team

Peffers, K., Tuunanen, T., Rothenberger, M. & Chatterjee, S. (2007). A design science research methodology for information systems research. Journal of Management Information Systems. 24. 45-77.

Piirainen, K. & Gonzalez, R. (2013). Seeking Constructive Synergy: Design Science and the Constructive Research Approach. 7939. 59-72. 10.1007/978-3-642-38827-9_5.f

Pozzi, C. (2022). The EU Deploys a Cyber Defence Team to Support Ukraine. European Army Interoperability Centre. Haettu 18.11.2023 osoitteesta: https://finabel.org/wp-content/uploads/2022/04/IF-30.03.pdf

Proska, K., Wolfram, J., Wilson, J., Black, D., Lunden K., Kapellmann D., Brubaker N., Mclellan T. & Sistrunk C. (2023). Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology. Mandiant. Haettu 23.12.2023 osoitteesta: https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology

Puuska, S. (2021). Command and Control: Monitoring, defending and exploiting critical infrastructure. Jyväskylän yliopisto. ISBN 978-951-39-8755-8

Pöyhönen, J. (2020). Kyberturvallisuuden johtaminen ja kehittäminen osana kriittisen infrastruktuurin organisaation toimintaa – Systeemiajattelu. Jyväskylän yliopisto. Informaatioteknologian tiedekunta. ISBN A978-951-39-8258-4.

Pöyhönen, J., & Lehto, M. (2017). Cyber security creation as part of the management of an energy company. University College Dublin. 16th European Conference on Cyber Warfare and Security ECCWS2017. Ireland.

Pöyhönen, J., Rajamäki, J., Ruoslahti, H. & Lehto, M. (2020). Cyber Situational Awareness in Critical Infrastructure Protection" Disaster Risk Sciences, 3 no. 1

Raymond, D., Conti G., Cross, T. & Nowatkowski, M. (2016). Key Terrain in Cyberspace: Seeking the High Ground. 2014 6th International Conference on Cyber Conflict. NATO CCD COE Publications, Tallinn. Haettu

30.10.2023 osoitteesta https://ccdcoe.org/uploads/2018/10/d2r1s8_raymondcross.pdf

Remus, U. & Wiener, M. (2008) "A Multi-method, holistic strategy for researching critical success factors in IT projects", Information Systems Journal, Vol. 20, Issue 1.

Rikoslaki 39/1889. https://www.finlex.fi/fi/laki/alkup/1889/18890039001

Rogers, M. (2017). Statement before the House Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities. Haettu 30.10.2023 osoitteesta https://nsarchive.gwu.edu/media/15298/ocr

Roles, J. (2023). Cyber Shield Hones Skills, Builds Partnerships. Haettu 23.3.2024 osoitteesta: https://www.nationalguard.mil/News/Article/3432843/cyber-shield-hones-skills-builds-partnerships/

Rollins, S. (2023). Defensive Cyber Warfare Lessons from Inside Ukraine. U.S: Naval Institute. Haettu 27.3.2024 osoitteesta https://www.usni.org/magazines/proceedings/2023/june/defensive-cyber-warfare-lessons-inside-ukraine

Roussi, A. & Bordelon, B. (2023). NATO allies have eyes on cyber-defense in Vilnius. Politico. Haettu 14.2.2024 osoitteesta https://www.politico.eu/newsletter/digital-bridge/nato-allies-have-eyes-on-cyber-defense-in-vilnius/

Saaranen-Kauppinen, A. & Puusniekka, A., A (2006). KvaliMOTV - Menetelmäopetuksen tietovaranto 3.3.2 Reliabiliteetti. Tampere: Yhteiskuntatieteellinen tietoarkisto. Haettu 2.12.2023 osoitteesta https://www.fsd.tuni.fi/menetelmaopetus/kvali/L3_3_2.html

Saaranen-Kauppinen, A. & Puusniekka, A., B (2006). KvaliMOTV - Menetelmäopetuksen tietovaranto 3.3.1 Validiteetti. Tampere: Yhteiskuntatieteellinen tietoarkisto. Haettu 2.12.2023 osoitteesta https://www.fsd.tuni.fi/menetelmaopetus/kvali/L3_3_1.html

Securicon. (2019). What's the difference between OT, ICS, SCADA and DCS?. Securicon, Alexandria, VA. https://www.securicon.com/whats-the-difference-between-ot- ics-scada-and-dcs/

SektorCERT. (2023). The attack against Danish Critical Infrastructure. Haettu 23.12.2023 osoitteesta: https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

Seldin, J. (2023). US Cyber Teams Are on the Hunt in Lithuania. VoaNews. Haettu 3.11.2023 osoitteesta: https://www.voanews.com/a/us-cyber-teams-are-on-the-hunt-in-lithuania-/7265185.html

Sisäministeriö. (2023). Kansallinen riskiarvio 2023. ISBN 978-952-324-602-7 Sisäministeriön julkaisuja 2023:4. Helsinki.

Sisäministeriö. (2024). Lausuntopyyntö hallituksen esityksestä laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi. Luonnos hallituksen esitykseksi eduskunnalle. Haettu 21.3.2024 osoitteesta https://www.lausuntopalvelu.fi/FI/Proposal/DownloadProposalAttachment?proposalId=67962948-2e20-43d7-a9e5-e43c99b60a8c&attachmentId=21666

Sisäministeriö. (Ei pvm). Nato-jäsenyys ja Suomen kriisinkestävyys. Haettu 15.12.2023 osoitteesta: https://intermin.fi/ajankohtaista/suomi-ja-nato

Slayton, R. (2016). What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment. International Security, 41(3), 72–109. https://www.jstor.org/stable/26777791

Slowik, J. (2019). CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack. Dragos INC. Haettu 23.12.2023 osoitteesta https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf

Smalley, S. (2023). FBI warns energy sector of likely increase in targeting by Chinese, Russian hackers. Recorded Future News. Haettu 28.10.2023 osoitteesta: https://therecord.media/fbi-warning-energy-sector-increased-hacking-china-russia

STK, Säteilyturvakeskus. (Ei pvm). Sähköverkot synnyttävät sähkö- ja magneettikenttiä. Haettu 11.12.2023 osoitteesta: https://stuk.fi/sahkoverkot-ja-voimajohdot

Supo, Suojelupoliisi. (2022). Suomen energiasektorin huoltovarmuus toimi hyvin poikkeusvuonna. Vuosikirja 2022. Haettu 20.12.2023 osoitteesta: https://vuosikirja.supo.fi/energiasektorin-huoltovarmuus-poikkeusvuonna

Supo, Suojelupoliisi. (2023). Kansallisen turvallisuuden katsaus. Haettu 28.10.2023 osoitteesta: https://supo.fi/kansallisen-turvallisuuden-katsaus

Tams, R. (2020). SCADA-järjestelmään kohdistuvat kyberhyökkäykset ja niiltä suojautuminen. Informaatioteknologian tiedekunta. Jyväskylän yliopisto.

Terho, S. (2009). Strategian jäljillä. Maanpuolustuskorkeakoulu. Johtamisen ja sotilaspedagogiikan laitos. Helsinki. Edita Prima Oy. ISBN 978–951–25–1973–6.

Thales. (2023). Threat Landscape Report 2023. S21 Cyber Solutions by Thales. Haettu 2.12.2023 osoitteesta: https://www.s21sec.com/wp-content/uploads/2023/07/S21sec_Thales_ThreatLandscapeReport_2023_EN.pdf

The White House. (2022). Statement by NSC Spokesperson Adrienne Watson on Iran's Cyberattack against Albania. Briefing Room. Statements And Releases. Haettu 4.11.2023 osoitteesta:

https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/07/statement-by-nsc-spokesperson-adrienne-watson-on-irans-cyberattack-against-albania/

Tilastokeskus, B. (2023). Energian hankinta ja kulutus. Haettu 14.11.2023 osoitteesta: https://stat.fi/tilasto/ehk#graphs

Tilastokeskus., A. (2023). Sähkön tuotanto tuulivoimalla ja ydinvoimalla nousivat vuonna 2022. Haettu 14.11.2023 osoitteesta: https://www.stat.fi/julkaisu/cl8mo29omxf8t0dukky5aa8i1

Топалов, М. (2023). Наступна зима буде не менш складною, ніж попередня. До чого готуватися? Ukrainska Pravda. Haettu 27.10.2023 osoitteesta https://www.epravda.com.ua/publications/2023/07/13/702170/

Trent, S., Hoffman, R. & Beltz, B. (2016). An Empirical Assessment of Cyberspace Network Mapping Capabilities. Topic 7: Methodological Development, Experimentation, Analysis, Assessment and Metrics. 21st International Command and Control Research and Technology Symposium. Haettu 1.11.2023 osoitteesta https://static1.squarespace.com/static/53bad224e4b013a11d687e40/t/57d696e1893fc0cb7a12d519/1473681122707/paper_10.pdf

Trent, S., Hoffman, R., Merritt, D. & Smith, S. (2019). Modelling the Cognitive Work of Cyber Protection Teams. Spring. The Cyber Defense Review. Haettu 31.10.2023 osoitteesta: https://cyberdefensereview.army.mil/Portals/6/10_Trent_CDR_V4N1.pdf?ver=2019-04-30-105204-733

Tuomi, J. & Sarajärvi, A. (2018). Laadullinen tutkimus ja sisällönanalyysi. Helsinki. Kustannusosakeyhtiö Tammi

Tuomi, J. & Sarajärvi, A. (2018). Laadullinen tutkimus ja sisällönanalyysi. Kustannusosakeyhtiö Tammi. Helsinki. ISBN 978-952-04-0011-8

Turvallisuuskomitea. (2017). Yhteiskunnan turvallisuusstrategia. ISBN 978-951-25-2959-9. Valtioneuvoston periaatepäätös 2.11.2017. Helsinki.

Turvallisuuskomitea. (2019). Suomen kyberturvallisuusstrategia. ISBN: 978-951-663-051-2. Valtioneuvoston periaatepäätös 3.10.2019. Helsinki.

Turvallisuuskomitea. (2019). Suomen kyberturvallisuusstrategia. ISBN: 978-951-663-051-2. Valtioneuvoston periaatepäätös 3.10.2019. Helsinki.

Turvallisuuskomitean sihteeristö. (2013). Suomen kyberturvallisuusstrategia. ISBN: 978-951-25-2434-1. Valtioneuvoston periaatepäätös 24.1.2013. Helsinki

Turvallisuuskomitean sihteeristö. (2013). Suomen kyberturvallisuusstrategia. ISBN: 978-951-25-2434-1. Valtioneuvoston periaatepäätös 24.1.2013. Helsinki.

Ulkoministeriö. (Ei pvm). Kyberturvallisuus ja kybertoimintaympäristö. Haettu 27.10.2023 osoitteesta https://um.fi/kyberturvallisuus-ja-kybertoimintaymparisto

UPI, Ulkopoliittinen instituutti. (2018). Strategisen pelotteen paluu: Ydinaseet ja Euroopan turvallisuus. Haettu 28.10.2023 osoitteesta: https://www.fiia.fi/wp-content/uploads/2019/09/strategisen-pelotteen-paluu-tiivistelma.pdf

USCYBERCOM. (2022). CYBER 101: Hunt Forward Operations. Haettu 27.10.2023 osoitteesta: https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/

USCYBERCOM, A. (2022). CYBER 101 – Cyber Mission Force. Haettu 29.10.2023 osoitteesta: https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission-force/

USCYBERCOM, A. (2023). Shared threats, shared understanding: U.S., Canada and Latvia conclude defensive Hunt Operations. Haettu 2.11.2023 osoitteesta: https://www.cybercom.mil/Media/News/Article/3390470/shared-threats-shared-understanding-us-canada-and-latvia-conclude-defensive-hun/

USCYBERCOM, A. (2023). U.S. returns from second defensive Hunt Operation in Lithuania. Haettu 27.10.2023 osoitteesta: https://www.cybercom.mil/Media/News/Article/3522801/building-resilience-us-returns-from-second-defensive-hunt-operation-in-lithuania/

USCYBERCOM, B. (2022). CYBER 101: Hunt Forward Operations. Haettu 2.11.2023 osoitteesta https://www.cybercom.mil/Media/News/Article/3218642/cyber-101-hunt-forward-operations/

USCYBERCOM, B. (2023). Building Resilience: U.S. returns from second defensive Hunt Operation in Lithuania. Haettu 2.11.2023 osoitteesta https://www.cybercom.mil/Media/News/Article/3522801/building-resilience-us-returns-from-second-defensive-hunt-operation-in-lithuania/

USCYBERCOM, B. (2023). Shared threats, shared understanding: U.S., Canada and Latvia conclude defensive Hunt Operations. Haettu 27.10.2023 osoitteesta: https://www.cybercom.mil/Media/News/Article/3390470/shared-threats-shared-understanding-us-canada-and-latvia-conclude-defensive-hun/

USCYBERCOM, C. (2022). U.S. conducts first Hunt Forward Operation in Lithuania. Haettu 2.11.2023 osoitteesta: https://www.cybercom.mil/Media/News/Article/3505610/us-conducts-first-hunt-forward-operation-in-lithuania/

USCYBERCOM, C. (2023). Committed Partners in Cyberspace: Following cyberattack, US conducts first defensive Hunt Operation in Albania. Haettu 2.11.2023 osoitteesta: https://www.cybercom.mil/Media/News/Article/3337717/committed-partners-in-cyberspace-following-cyberattack-us-conducts-first-defens/

USCYBERCOM, D. (2022). Before the Invasion: Hunt Forward Operations in Ukraine. Haettu 2.11.2023 osoitteesta https://www.cybercom.mil/Media/News/Article/3229136/before-the-invasion-hunt-forward-operations-in-ukraine/

USCYBERCOM. (2018). Achieve and Maintain Cyberspace Superiority Command Vision for US Cyber Command. Haettu 29.10.2023 osoitteesta https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010

USCYBERCOM. (2020). Hunt Forward Estonia: Estonia, US strengthen partnership in cyber domain with joint operation. Haettu 2.11.2023 osoitteesta: https://www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/

USCYBERCOM. (Ei pvm.). Components. Our Service Cyber Partners. Haettu 29.10.2023 osoitteesta: https://www.cybercom.mil/Components.aspx

Vainio, K. (2018). Verkkoturva vinossa. Ulkopolitiikka. Haettu 18.11.2023 osoitteesta: https://ulkopolitiikka.fi/lehti/3-2018/verkkoturva-vinossa/

Valtioneuvosto, A. (2023). Valtioneuvoston U-kirjelmä U 20/2023. Liikenne- ja viestintäministeriö 6.7.2023 EU/688/2023 Helsinki. Haettu 18.11.2023 osoitteesta: https://www.eduskunta.fi/FI/vaski/Kirjelma/Sivut/U_20+2023.aspx

Valtioneuvosto. (2022). Valtioneuvoston huoltovarmuusselonteko. Valtioneuvoston julkaisuja 2022:59. Helsinki. ISBN 978-952-383-803-1. Haettu 14.11.2023 osoitteesta: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164329/VN_2022_59.pdf

Valtiovarainministeriö. (2020). Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. Tiedonhallintalautakunta, Valtiovarainministeriön julkaisuja. Helsinki. ISBN : 978-952-367-292-5. Haettu 12.12.2023 osoitteesta https://www.fsd.tuni.fi/fi/tietoarkisto/julkaisut/kvalimotv.pdf

Vankka J., Eronen, J., Häyhtiö M., Pöyhönen J. & Zaerens, K. (2023). Critical Infrastructure Protection. Sotatekniikan laitos. Maanpuolustuskorkeakoulu. Julkaisusarja 2: Tutkimusselosteita NRO 5. ISBN 978-951-25-3381-7

Vankka, J., Ahvenainen, S., Lantto, H., Hakkarainen, P., Vestama, T., Heinäaro, K., Timonen, J. & Zaerens, K. (2014). Critical Infrastructure Protection

Against Cyber Threats. Maanpuolustuskorkeakoulu. Helsinki. ISBN 978-951-25-2600-0.

Varga, M., Winkelholz C. & Träber-Burdin, S. (2019) An Exploration of Cyber Symbology. IEEE Symposium on Visualization for Cyber Security (VizSec), Vancouver, BC, Canada, 2019, pp. 1-5, doi: 10.1109/VizSec48167.2019.9161577

Vasiliauskaitė, E. & Šakūnas, T. (2018). Cyber Rapid Response Teams and Mutual Assistance in Cyber Security. Memo for Mutual Assistance in Cyber Security. Key Roles and Procedures for the CRRTs' Operations. Lessons Learnt from the Cyber Shield/ Amber Mist 2018 Exercise. Haettu 19.11.2023 osoitteesta https://kam.lt/wp-content/uploads/2022/03/CRRT-2018.pdf?__cf_chl_rt_tk=eL8mVpF9Qe4NCTYSbMmhPl86lTuhzKIMKm9Q10dGBu4-1700393065-0-gaNycGzNDHs

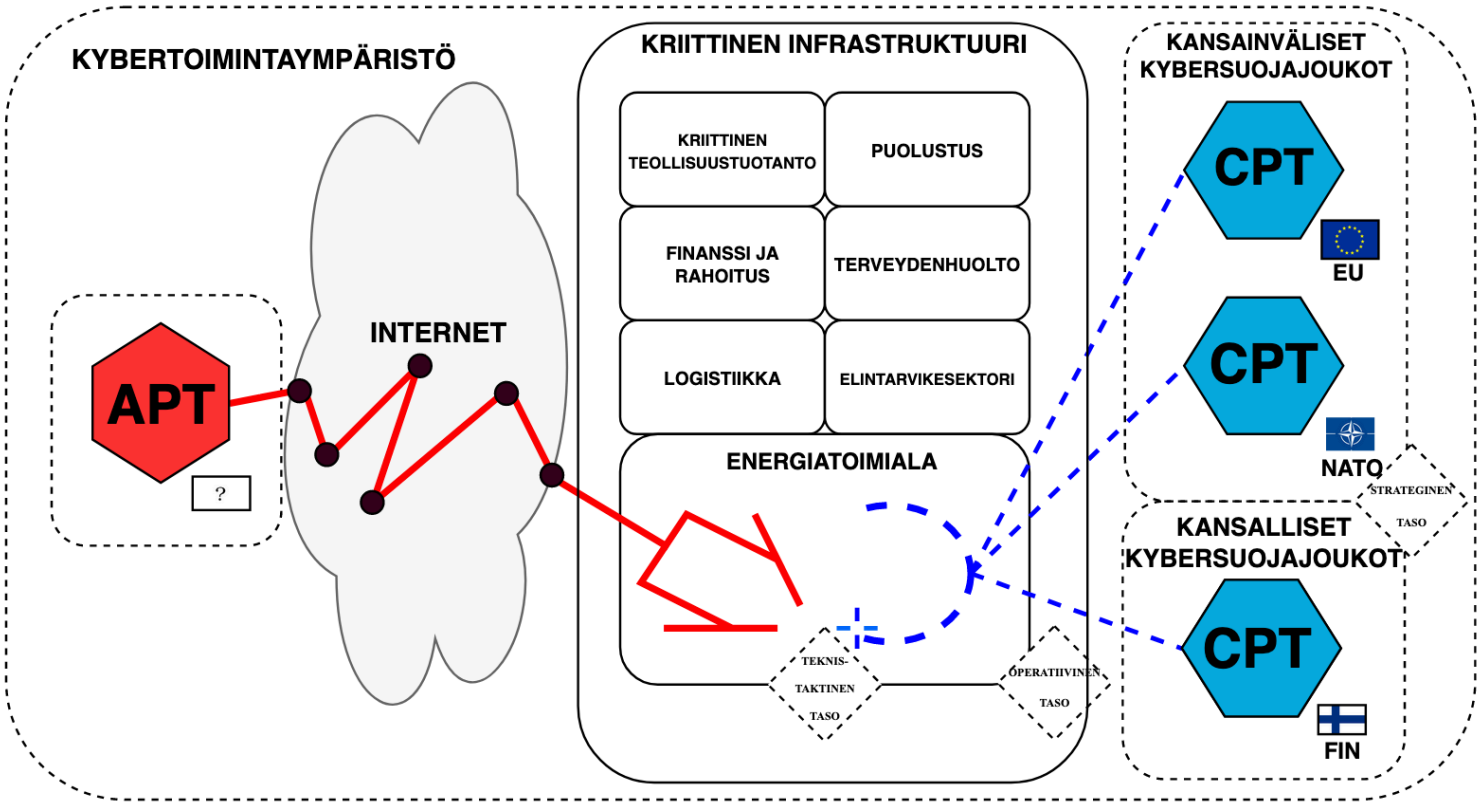
Vavra, S. (2022). Cyber Command deployed personnel to Estonia to protect elections against Russian threat. CyberScoop. Haettu 3.11.2023 osoitteesta https://cyberscoop.com/cyber-command-deployed-estonia-russia-2020-elections-hunt-forward/

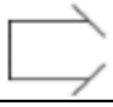
Vehkalahti, K. (2014). Kyselytutkimuksen mittarit ja menetelmät. Finn Lectura. https://doi.org/10.31885/9789515149817

Virtanen, A. (2019). Kriittisen infrastruktuurin ohjausjärjestelmien kyberturvallisuus. Informaatioteknologian tiedekunta. Jyväskylän yliopisto.

Xing, K., Li, A., Jiang, R., Jia, Y. (2021). Detection and Defense Methods of Cyber Attacks. Lecture Notes in Computer Science LNISA,volume 12647.

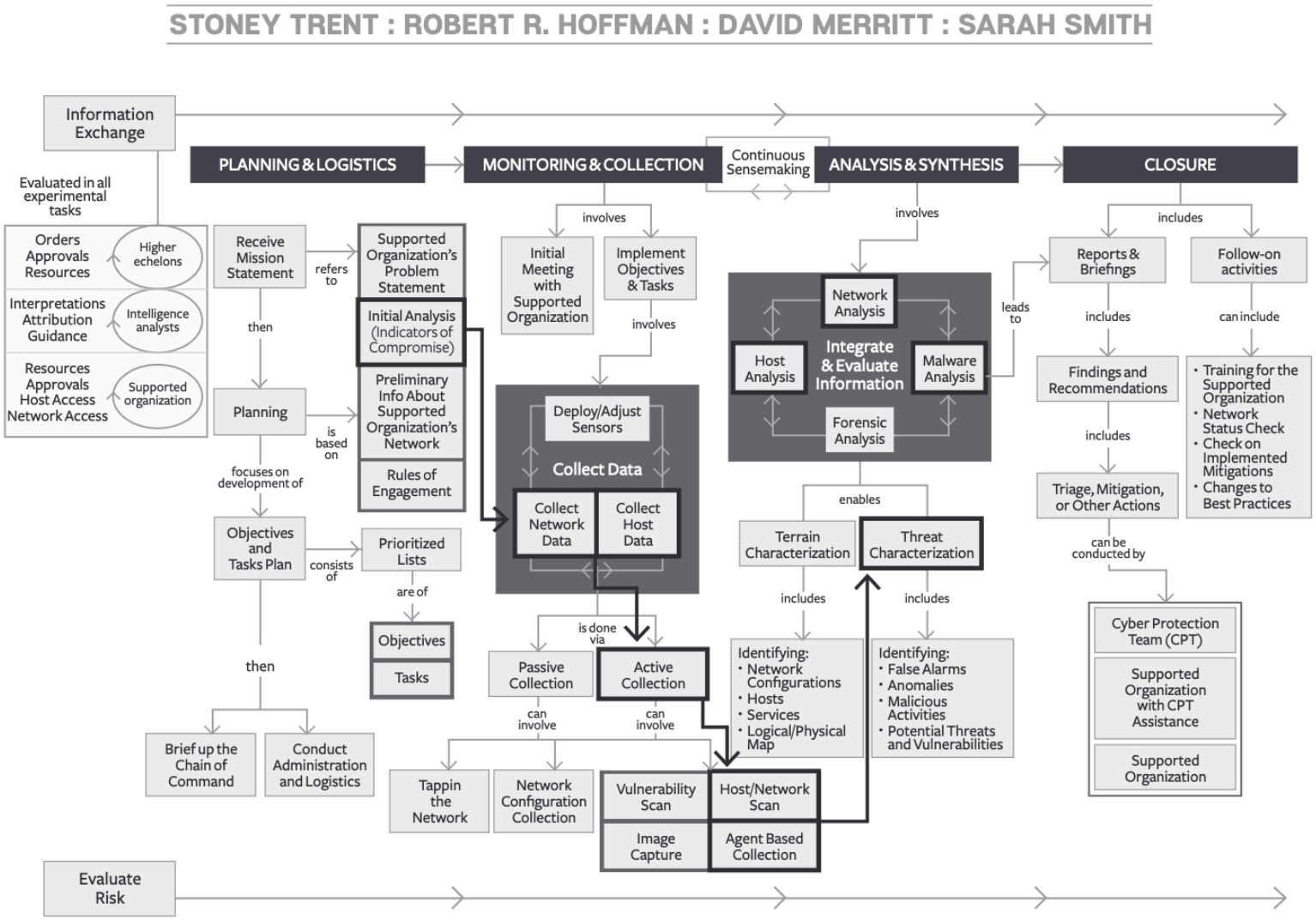
LIITE 1 PERUSANALYYSIN MUKAINEN PERUSKUVA TUTKIMUKSEN TOIMINTAYMPÄRISTÖSTÄ



KUVAUS	SELITE
	Valtuuttamaton pääsy kohdejärjestelmään (tunkeutuminen teknisen suojauksen läpi; haavoittuvuuden hyväksikäyttö)
	Puolustuksellinen suojaustoimi (DCO-IDM)
CPT	Ystävällismielinen (Friendly) kybersuojajoukko
APT	Vihamielinen (Hostile) APT-uhkatoimija
CPT	Cyber Protection Team, Kybersuojajoukko
APT	Advanced Persistent Threat, Edistynyt jatkuva uhka

LIITE 2 CPT:N TOIMINTAPERIAATTEITA JA TEHTÄVÄN RAKENNETTA KUVAAVA VIRTAUSKAAVIO

Tutkimuksen teknis-taktisen tason toimintatapamalli perustui Trent ym. (2019) tuottamaan CPT:n toimintaperiaatteita ja tehtävän rakennetta kuvaavan virtauskaavion (Trentin ym., 2019, s. 130).



LIITE 3 PESCO CRRT INCIDENT REPORT

CRRT:n neuvoston puheenjohtajalle esitettävä tukipyyntö (Vasiliauskaitė & Šakūnas, 2018, s. 31)

Requesting Entity	**Country**	Lithuania
	Organisation	National Cyber Security Centre (NCSC) under the Ministry of National Defence
Date of Request	**11-10-2018**	
Primary Mission Point of Contact	**Name and Surname**	
	Position	
	Organisation	NCSC under the Ministry of National Defence
	Telephone number	
	Email Address NU/NS/Internet	
Alternative Mission Point of Contact	**Name and Surname**	
	Position	
	Organisation	NCSC under the Ministry of National Defence
	Telephone number	
	Email Address NU/NS/Internet	
Incident evaluation	**Affected entities**	LTU transport, BT Energy, BT Ministry of Transport and Communications
	Affected sectors	Transportation, Energy, Government
	Incident duration	08-10-2018/Ongoing
	Incident source	Possibly the endpoint device in "LTU transport"
	Characteristics	"LTU transport" administration network has been encrypted as well as some parts of the OT network. Incident has affected other entities, such as BT Energy, BT Ministry of Transport and Communications. NCSC has been informed about other ongoing cyber-attacks (DDoS, defacement, and data exfiltration) in BT Energy, BT Ministry of Transport and Communications and other critical entities.
	Possible outcomes (nationally and internationally)	Disruption of critical services: unable to deliver cargo, power blockouts in some parts of Lithuania and Latvia.
	Possible scale (nationally and internationally)	Considering cargo delivery – Baltic Sea region; Considering power provision – Baltic States and (possibly) Crimsonia.
Expectations of RRT Assistance (from the point of view of the Requesting Entity):	**Mission Objectives (high-level)**	Investigate ransomware source, stop its spreading, restore critical services within transport, energy, government sectors.
	Desired Assistance (area of focus, priorities for each area)	Forensic investigation (LTU transport, BT Energy), network analysis and critical services backup (LTU transport, BT Energy ICS network).
	Criteria for Success or Termination	Restored critical services.
	Anticipated Duration of the Mission	2 days.
Requestor Details	**Name**	
	Position	
	Organisation	NCSC under the Ministry of National Defence
	Telephone number	
	Email Address NU/NS/Internet	
Requestor Authority	NCSC under the Ministry of National Defence of Republic of Lithuania	

LIITE 4 TIEDOTE TUTKIMUKSESTA

TIEDOTE TUTKIMUKSESTA

Aihe

Kybersuojajoukkojen puolustukselliset kyberoperaatiot kriittisen infrastruktuurin kohdearkkitehtuurissa

Tutkimus

Pyydän Teitä osallistumaan Pro Gradu -tutkielmaani, joka käsittelee kybersuojajoukkojen (engl. Cyber Protection Team ja Cyber Rapid Response Team) käyttöönoton toimintaperiaatteita osana kriittisen infrastruktuurin toimijoiden kohdearkkitehtuurissa toteutettuja uhkanmetsästysoperaatioita (engl. Threat Hunting). Tämä tiedote kuvaa tutkimusta ja Teidän mahdollista osuuttanne siinä. Jos päätätte osallistua tutkimukseen, teiltä pyydetään suostumus tutkimukseen osallistumisesta. Teille järjestetään myös halutessanne mahdollisuus esittää kysymyksiä tutkimuksesta joko ennen haastattelulle esitettyä ajankohtaa, tai haastattelun ajankohdan aikana. Vaihtoehtoisesti voitte esittää mahdolliset kirjalliset kysymykset suoraan sähköpostitse ennen haastattelun toimeenpanoa.

Tutkimuksen tarkoitus

Tutkimuksen tarkoitus on kartoittaa ns. kybersuojajoukkojen käyttöönottoa osana energiatoimialan organisaatioiden kohdearkkitehtuureissa toteutettua puolustuksellista kyberoperaatiota. Kybersuojajoukot ovat siviili- tai sotilasyksiköitä, jotka keskittyvät ns. kyberavainkohteiden (engl. Key Cyber Terrain) hallintaan ja suojaamiseen, operointivarmuuden takaamiseen (engl. Mission Assurance), uhkatietojen jakamiseen viranomaisten ja kriittisten toimijoiden kesken, sekä tunnistamaan ja torjumaan kyberuhkia erityisesti kriittisessä infrastruktuurissa. Tutkimusongelmana on pyrkiä luomaan kokonaisvaltainen operatiivisen ja teknis-taktisen tason toimintatapamalli kybersuojajoukkojen toteuttamien uhkanmetsästysoperaatioiden suunnittelun ja toimeenpanon mahdollistamiseksi osana kriittisen infrastruktuurin toimijoiden kohdearkkitehtuureissa toteutettua uhkanmetsästysoperaatiota. Osana tutkimusta haastatellaan asiantuntijoita ja alan toimijoita, joiden kautta pyritään muodostamaan ymmärrys muun muassa kybersuojajoukkojen toteuttamien operaatioiden toimeenpanon avaintoimijoista, prosesseista, toimintaympäristöstä ja operaatioiden mahdollisista mahdollisuuksista, uhkista ja rajoituksista.

Tutkimuksen toteuttaja

Tutkimuksen toteuttajana toimii Eero Oksala, joka tuottaa tutkimuksen osana Jyväskylän yliopiston kyberturvallisuuden maisteriohjelman opintokokonaisuutta. Tutkielmaa ohjaa Jyväskylän yliopiston lehtori Panu Moilanen.

Vapaaehtoisuus

Osallistuminen tähän tutkimukseen on täysin vapaaehtoista. Voitte kieltäytyä osallistumisesta tai peruuttaa suostumuksenne syytä ilmoittamatta milloin tahansa ilman siitä koituvaa haittaa. Voitte myös peruuttaa antamanne suostumuksen milloin tahansa tutkimuksenaikana ilman perusteluita ilmoittamalla siitä tutkimushenkilökunnalle. Suostumuksen peruuttamisesta ei koidu teille mitään haittaa. Jos päätätte peruuttaa suostumuksenne, tai osallistumisenne tutkimukseen keskeytyy jostain muusta syystä, siihen mennessä kerättyjä tietojanne voidaan edelleen käyttää tässä tutkimuksessa, mikäli tutkimuksen toteuttaminen sitä vaatii.

Tutkimuksen kulku

Tutkimus suoritetaan puolistrukturoituina teemahaastatteluina. Yhden haastattelun kesto on noin 60 – 90 minuuttia ja toteutetaan etäyhteydellä. Haastatteluja on tarkoitus pitää yksi haastattelu yhtä haastateltavaa kohden, mutta mikäli on tarpeellista tutkimuksen kannalta, voidaan haastattelutilaisuuksia järjestää useampia. Suunniteltu haastattelurunko ja käsiteltävät aihealueet on esitetty Liitteessä 2.

Tutkimuksesta mahdollisesti aiheutuvat riskit, haitat ja epämukavuudet sekä niihin varautuminen

Tutkimuksen arvioidaan tarjoavan arvokasta tietoa kybersuojajoukkojentoimintatavoista ja käyttöperiaatteista osana kriittisen infrastruktuurinproaktiivista suojaamista. Lisäksi tutkimuksen tulokset voivat mahdollisestiauttaa ymmärtämään paremmin kybersuojajoukkojen roolia ja merkitystäkansallisen turvallisuuden turvaamisessa ja sen varmistamisessa, lisätentietoisuutta strategisen, operatiivisen ja taktis-teknisen tason toimijoidenymmärrystä toimintaperiaatteista, prosesseista, sekä toimintaympäristöstäosana kybersuojajoukkojen käyttöönottoa ja toteutettaviauhkanmetsästysoperaatioita.

Hyödyt:

1) Luo käsityksen kybersuojajoukkojen operatiivisista ja teknis-taktisista toimintatavoista, parantaen mahdollisesti valmiuksia proaktiiviseen kyberpuolustukseen ja -turvallisuuteen.
2) Luo käsityksen kybersuojajoukkojen käyttöön liittyvistä prosesseista, sekä käyttöönoton suunnitteluun ja toteutukseen liittyvistä käytännöistä, vaiheista ja tarpeista.
3) Luo mahdollisuuden käyttää tutkimustietoa ymmärryksen levittämisessä osana toimintamahdollisuuksien kartoitusta ja käyttösuositusten laatimista.

Haitat:

1) Tutkimuksen tulokset voivat paljastaa puutteita tai haavoittuvuuksia osallistuvien organisaatioiden ja toimijoiden ymmärryksessä kyberpuolustuksen ja kansallisen tai kansainvälisen tuen vastaanottamisen suhteen
    a. Tutkimuksessa kaikki mahdollisesti havaitut puutteet ja haavoittuvuudet luottamuksellisesti, eikä niistä raportoida julkisesti ilman erillistä lupaa. Lisäksi kaikki tiedot anonymisoidaan ennen niiden julkaisemista.
2) Tutkimustiedon väärinkäyttö tai väärin tulkinta voi johtaa virheellisiin päätelmiin ja toimenpiteisiin, jotka luovat väärän kuvan toimintaympäristöstä, toimijoista tai suoritettavista prosesseista ja vaiheista.
    a. Tutkimuksessa selitetään tutkimustulokset ja niiden konteksti selkeästi ja yksityiskohtaisesti. Lisäksi tutkimuksessa käytetään luotettavia ja arvostettuja akateemisia tai ammattimaisia lähteitä. Tämä sisältää myös viranomaisten ja alan asiantuntijoiden julkaisemia raportteja sekä akateemisia kirjoja ja tutkimuksia. Lisäksi tutkimuksessa esitetyt väitteet, tiedot ja toimintatapamallit viitataan selkeästi, jotta lukijat voivat tarkistaa alkuperäisen lähteen.

Henkilötietojen käsittely ja tietojen luottamuksellisuus

Tutkimuksen aikana henkilötietoja kerätään vain niiltä osin, kuin on tarpeellista tutkimuksen kannalta. Tutkimuksen kannalta tarpeellisia henkilötietoja ovat tutkimukseen osallistuvan nimi, tehtävänimike ja edustettava organisaatio. Haastatteluihin osallistuvat henkilöt ja heidän edustamat organisaatiot jäävät vain tutkimuksen toteuttamiseen osallistuvien henkilöiden tietoon, ellei asiasta sovita

erikseen. Haastatteluiden tuloksena tuotettu tieto anonymisoidaan kaikkien haastatteluihin osallistuneiden osalta.

Mikäli haastatteluissa kerättyä muuta tietoa jaetaan tutkimusyhteisön ulkopuolelle, ne anonymisoidaan tai yleistetään siten, että yksittäisten henkilöiden tai organisaatioiden tunnistaminen ei ole mahdollista. Kaikilta tutkimukseen osallistujilta vaaditaan kirjallinen suostumus heidän tietojensa käsittelyyn. Suostumus pyydetään viimeistään haastatteluiden alussa, mutta sen voi halutessaan toimittaa etukäteen tutkijalle. Haastattelussa allekirjoitettava suostumus tutkimukseen osallistumisesta on esitetty Liitteessä 1.

Tutkimuksen kustannukset ja taloudelliset selvitykset

Tutkimukseen osallistumisesta ei makseta palkkiota.

Tutkijalle ja muulle henkilökunnalle ei makseta erillistä korvausta tutkimuksen tekemisestä.

Tutkimustuloksista tiedottaminen

Tutkimuksesta valmistuu yksi pro gradu -tutkielma, joka julkaistaan Jyväskylänyliopiston julkaisuarkistossa: https://jyx.jyu.fi/. Tutkimuksesta voidaan myös julkaista tutkimusartikkeleita. Aiheesta voidaan pitää myös esityksiä ja antaa opetusta.

Tutkimukseen osallistuneita ei voida tunnistaa tutkimustuloksista tai tutkimukseen liittyvistä julkaisuista.

Tutkittavien vakuutusturva

Jyväskylän yliopiston henkilökunta ja toiminta on vakuutettu. Vakuutukset korvaavat etänä suoritettavissa tutkimuksissa ainoastaan sellaiset vahingot, jotka liittyvät suoraan annettuun tutkimustehtävään ja jotka ovat sattuneet varsinaisen ohjeistetun tutkimustehtävän aikana.

Lisätietojen antajan yhteystiedot

Lisätietoja tutkimuksesta antaa:
Eero Oksala
Opiskelija | Jyväskylän yliopisto | Kyberturvallisuuden maisteriohjelma
eaoksala@student.jyu.fi

Liitteet

Liite 1: Haastattelussa allekirjoitettava suostumus tutkimukseen osallistumisesta
Liite 2: Haastattelurunko ja käsiteltävät aiheet ja apukysymykset

Kiitos mahdollisuudesta!

Suostumus haastatteluun osallistumisesta

Aihe

Kybersuojajoukkojen puolustukselliset kyberoperaatiot kriittisen infrastruktuurin kohdearkkitehtuurissa

Tutkimus

Minua on pyydetty osallistumaan yllä mainittuun tieteelliseen tutkimukseen. Olen lukenut ja ymmärtänyt saamani tutkimustiedotteen. Olen saanut riittävän selvityksen tutkimuksesta ja sen yhteydessä suoritettavasta henkilötietojeni keräämisestä, käsittelystä ja luovuttamisesta. Tutkimuksen sisältö on kerrottu minulle myös suullisesti ja olen saanut riittävän vastauksen kaikkiin tutkimusta koskeviin kysymyksiini. Tiedot on antanut minulle Eero Oksala.

Henkilötietojen käsittely ja tietojen luottamuksellisuus

Olen saanut riittävät tiedot oikeuksistani tutkittavana, tutkimuksen tarkoituksesta ja sen toteutuksesta sekä tutkimuksen hyödyistä ja riskeistä. Minulla on ollut riittävästi aikaa harkita osallistumistani tutkimukseen.

Vapaaehtoisuus

Ymmärrän, että tähän tutkimukseen osallistuminen on vapaaehtoista. Minulla on oikeus kieltäytyä siitä sekä peruttaa tutkimukseen antamani suostumus milloin tahansa tutkimuksen aikana ilman perusteluita ilmoittamalla siitä tutkimushenkilökunnalle.

Tutkimuksesta kieltäytymisestä tai suostumuksen peruuttamista ei aiheudu minulle. Olen tietoinen siitä, että mikäli peruutan suostumukseni tai osallistumiseni tutkimukseen keskeytyy muusta syystä, siihen mennessä kerättyjä tietojani voidaan edelleen käsitellä tässä tutkimuksessa, mikäli tutkimuksen toteuttaminen sitä vaatii ja lainsäädäntö sallii sen.

Allekirjoituksellani vahvistan osallistumiseni tähän tutkimukseen ja suostun vapaaehtoisesti tutkittavaksi sekä ymmärrän, että henkilötietojani käsitellään osana tätä tutkimusta.

__.__20__ [redacted]

Suostun osallistumaan tutkimukseen: Suostumuksen vastaanottaja:

Haastateltavan allekirjoitus Tutkijan allekirjoitus

_____ [redacted]

LIITE 5 KEHITETYN TOIMINTATAPAMALLIN VIIMEINEN KOMMENTOINTIVAIHE (MEMBER CHECKING)

Arvoisa vastaanottaja,

Olette osallistuneet vuoden 2024 aikana Pro Gradu -tutkimukseni asiantuntijahaastatteluun. Täten ilmoitan tutkimukseni puolistrukturoitujen teemahaastatteluiden tulleen päätökseen, jonka johdosta lähestyn Teitä tutkimukseni viimeisen vaiheen *(Member checking)* suhteen.

Olen päivittänyt tutkimukseni mukaista toimintapamallia haastattelujen havaintojen, huomioiden ja korjausehdotusten pohjalta. Tutkimukseni viimeisen vaiheen mukaisesti haluaisinkin esitellä Teille haastatteluiden pohjalta päivitetyn toimintatapamallin, sekä sen mukaisen kuvauksen.

Välitän Teille liitteenä kuvauksen haastatteluiden tuloksista, jossa toimintatapamallin eri vaiheita ja haastatteluiden huomioita on kuvattu tarkemmin *(CPT_Pro_Gradu_JYU.pdf)*. Lisäksi välitän Teille liitteenä toimintatapamallin kokonaisversion HTML-tiedostona, jonka kautta sen yksityiskohtainen tarkastelu on tehokkaampaa *(CPT_Pro_Gradu_JYU.html)*.

Pyytäisin Teitä mahdollisuuksienne mukaan tarkastelemaan päivitettyä toimintatapamallia ja saattamaan tietooni mahdolliset havaintonne tai eroavat näkemyksenne sen suhteen. **Pyytäisin esittämään mahdolliset havaintonne perjantaihin 5.4.2024 mennessä,** jonka jälkeen toimeenpanen vielä toimintatapamallin viimeisen version mahdollisten havaintojen pohjalta. Halutessanne voitte erillisellä ilmoituksella ilmoittaa halusta esittää korjausehdotuksia vielä määräajan jälkeen. Pyytäisin ilmoittamaan tästä kuitenkin ennen ilmoitettua määräaikaa.

Pyytäisin Teitä mahdollisuuksien mukaan ilmoittamaan hyväksyntänne toimintatapamallille, vaikka ette tunnistaisi siinä muutostarpeita. Näin voin varmistua yhteisymmärryksestä ja kasvattaa tutkimukseni luotettavuutta.

Välitän Teille myös liitteenä erillisen suostumuksen haastatteluun osallistumisesta, jonka pyytäisin vielä täyttämään, mikäli sitä ei haastatteluiden yhteydessä täytetty. Kyseisessä pohjassa on asetettu allekirjoitukseni päivämääräksi 25.3.2024, mutta halutessanne voin muokata siihen haastattelumme päivämäärän.

Lopuksi, **suuret kiitokset Teille haastatteluun ja tutkimukseeni osallistumisesta!** Tukenne on ollut ensisijaisen tärkeää, ja asiantuntijuutenne on luonut vankan pohjan tutkimukseni luotettavuudelle! Koen kaikkien haastattelujen kasvattaneen huomattavasti myös omaa osaamistani, minkä lisäksi olen tunnistanut useita jatkotutkimuksen aiheita, jotka tulen huomioimaan tutkimuksessani!

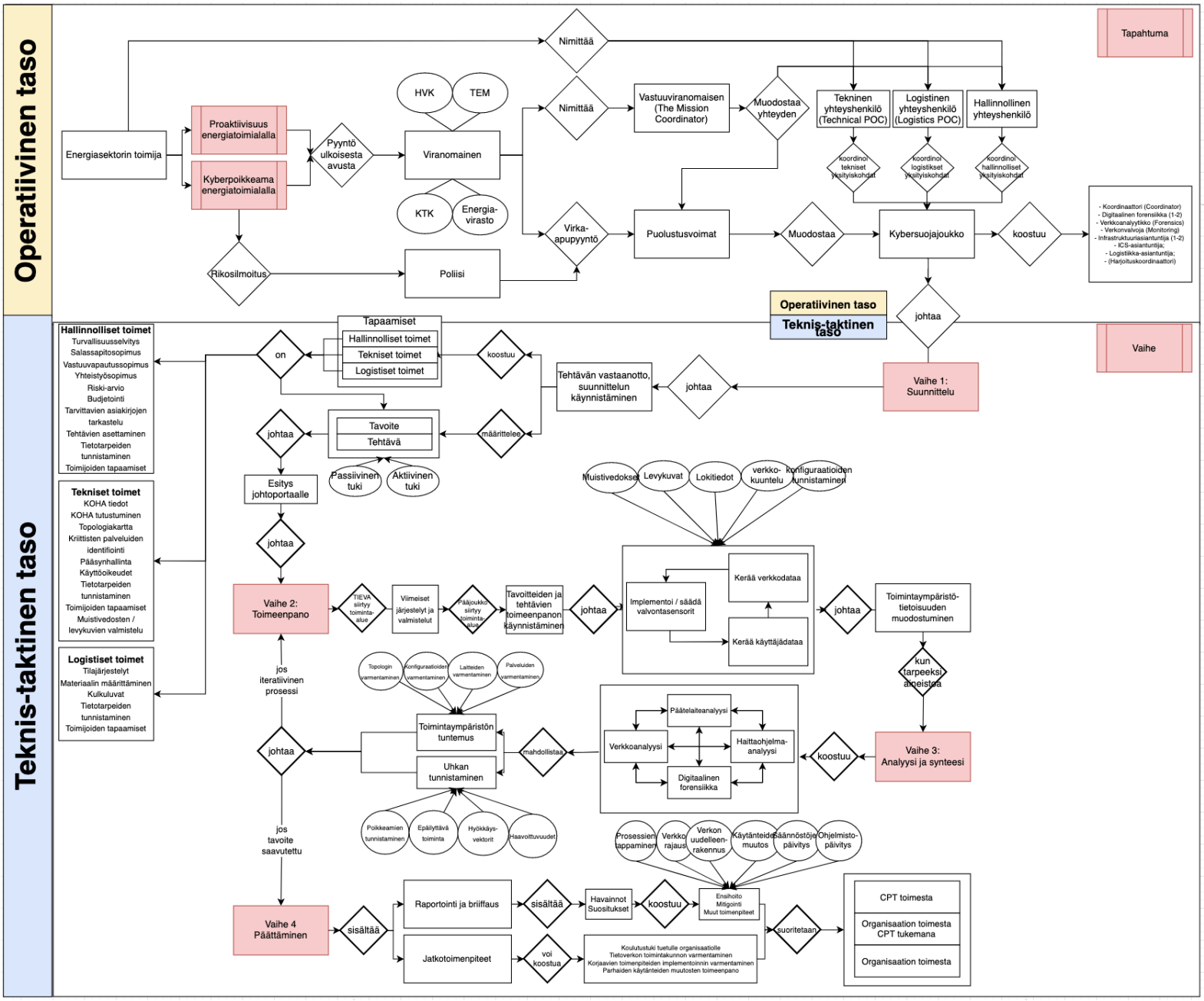
Kiitos!

LIITE 6 HAASTATTELURUNGON OSAKOKONAISUUDET JA APUKYSYMYKSET.

CATWOE - osakokonaisuudet	Kuvaus	Kysymys
Asiakas (Customer)	Prosessin vastaanottaja ja toimintaan vaikuttava taho.	1) Mitä tarpeita ja odotuksia asiakkaalla on prosessin käynnistämisen ja toimeenpanon suhteen? Miten tarpeet ja odotukset otetaan huomioon prosessin vaiheissa? 2) Millä tavoin prosessi voisi asiakkaan näkökulmasta olla entistä tehokkaampi tai tyydyttävämpi strategisella, operatiivisella tai teknis-taktisella tasolla?
Toimijat (Actors)	Prosessin käynnistävät ja toimeenpanevat toimijat	1) Keitä ovat keskeiset toimijat prosessin käynnistämisessä ja toimeenpanossa strategisella, operatiivisella ja teknis-taktisella tasolla, ja millaiset roolit ja vastuut heillä on? 2) Onko osapuolet vakiinnutettu, ja kyetäänkö hyödyntämään jotakin olemassa olevaa tiedonvaihto- tai johtamismallia? 3) Miten toimijoiden yhteistyö ja kommunikaatio prosessin aikana on tai voisi olla järjestetty, ja miten se voisi olla entistä sujuvampaa?
Muutosprosessi (Transformation Process)	Toiminnot, jotka muuttavat prosessin syötteet tuotokseksi	1) Mitä näkemyksiä, huomioita ja kehitysehdotuksia muodostuu esitettävän toimintatapamallin mukaisten kokonaisuuksien suhteen? 2) Mitkä arvioisitte toimintapamallin kriittisimmäksi vaiheeksi, tai sen vahvuuksiksi ja heikkouksiksi? 3) Mitä uhkia tunnistatte prosessin käynnistämisen ja kybersuojajoukkojen käyttöönoton ja niiden mukaisten operaatioiden toimeenpa-

		non suhteen? 4) Miten kybersuojajoukkojen käyttöönoton prosessin selkeys ja toimivuus voitaisiin varmistaa?
Maailmankuva (World View)	Näkökulmat, jotka ohjaavat muutosprosessin käynnistämiseen ja vaikuttavat loppuasetelman mukaiseen tahtotilaan	1) Minkä arvioisitte olevan kannustin sille, että huoltovarmuuskriittinen organisaatio esittää toimeenpantavaksi proaktiiviset suojaustoimenpiteet ja kybersuojajoukkojen mukaisen puolustuksellisen kyberoperaation? 2) Miten organisaation tahtotila operaation toimeenpanosta heijastuu laajemman hyödyn näkökulmasta
Omistaja (Owner)	Toimijatahot, jotka vastaavat prosessin toiminnasta, tuloksesta ja prosessin kehittämisestä.	1) Kenet näkisitte olevan kybersuojajoukkojen käyttöönoton ja toimeenpanoprosessin pääomistajat ja miten he vaikuttavat sen kulkuun? 2) Miten näkisitte omistajien osallistuvan prosessin kehittämiseen ja tulosten arviointiin?
Toimintaympäristö (Environmental Constrains)	Toimintaympäristö ja sen asettamat ulkoiset ja sisäiset rajoitukset	1) Millaisia ulkoisia ja sisäisiä rajoitteita toimintaympäristö asettaa prosessille? 2) Miten nämä rajoitteet vaikuttavat kybersuojajoukkojen käyttöönottoon ja toiminnan joustavuuteen?

LIITE 7 TUTKIMUKSEN TOIMINTATAPAMALLIN LUONNOS



LIITE 8 TUTKIMUSTULOKSEN TOIMINTATAPAMALLI