Niko Kuokkanen

KRIITTISEN INFRASTRUKTUURIN SUOJAAMINEN SUOMESSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Kuokkanen, Niko
Kriittisen infrastruktuurin suojaaminen Suomessa
Jyväskylä: Jyväskylän yliopisto, 2020, 48 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Clements, Kati

Tämän kirjallisuuskatsauksena toteutetun kandidaatin tutkielman tavoitteena oli ottaa selvää suomalaisen kriittisen infrastruktuurin vastuista, kattavuudesta ja kyberturvallisuuden suojaustoimista. Tutkimuksen taustalla vallitsi epäselvyys suomalaisen kriittisen infrastruktuurin sektoreista ja niihin liittyvistä julkisen ja yksityisen sektorin vastuista. Kyberturvallisuuden näkökulma kriittiseen infrastruktuuriin perusteltiin sillä, että yhteiskunnan kriittiset palvelut ovat yhä yleistyvämmissä määrin yhteydessä yrityksen tai julkiseen verkkoon, mikä altistaa ne kyberhyökkäyksille. Tutkimuksen myötä selvisi yleisimmät kriittisen infrastruktuurin sektorit ja niihin liittyvät vastuut, suojattavat kohteet ja kyberturvallisuuden suojaustoimet. Tutkimuksessa selvinneet suojaustoimet voidaan luokitella ei-teknisiin poikkisektorillisiin suojaustoimiin, teollisuuden ohjausjärjestelmien suojaustoimiin sekä sektorikohtaisiin suojaustoimiin. Lisäksi saatuja tutkimustuloksia peilataan siihen, miten ne edesauttavat resilienssiä, pelotetta ja puolustusta, jotka ovat Euroopan komission asettamia kehitysalueita valtioiden kyberturvallisuudelle. Tutkimus tarjoaa varsin yleismaailmallisen kuvan siitä, mitä kriittinen infrastruktuuri pitää sisällään ja miten siihen liittyvät vastuut jakautuvat Suomessa, mutta nykyisen laajalle hajautuneen mallin tehokkuutta ja soveltuvuutta yhteistyötä ja avoimuutta korostavassa toimintaympäristössä voisi tutkia vielä tarkemmin.

Asiasanat: kriittinen infrastruktuuri, kriittisen infrastruktuurin suojaaminen, kyberturvallisuus, kyberturvallisuusstrategia, teollisuuden ohjausjärjestelmä

ABSTRACT

Kuokkanen, Niko
Critical infrastructure protection in Finland
Jyväskylä: University of Jyväskylä, 2020, 48p.
Information Systems, Bachelor's Thesis
Supervisor: Clements, Kati

The purpose of this bachelor's thesis, executed as a literature review, was to find out the responsibilities, coverage and cyber security practices of the Finnish critical infrastructure. The background to the study was the lack of clarity about the Finnish critical infrastructure sectors and both public and private sector responsibilities related to them. The cyber security perspective on critical infrastructure was justified by the fact that critical services of society are increasingly connected to a company or public network, which exposes them to cyber attacks. The study revealed the most common critical infrastructure sectors and their responsibilities, the objects to be protected and the practices to protect cyber security. The practices that have emerged in the study can be categorized as non-technical cross-sectoral practices, industrial control systems practices, and sector-specific practices. In addition, the results will be mirrored in their contribution to resilience, deterrence, and defence, which have been identified as a development area for European cyber security. The study provides a quite general picture of what the critical infrastructure contains and how responsibilities are distributed in Finland. Nevertheless, the effectiveness and suitability of the current widely dispersed model could be explored even further, as the environment values cooperation and openness in an increasing manner.

Keywords: critical infrastructure (CI), critical infrastructure protection (CIP), cyber security, cyber security strategy, industrial control system (ICS)

TAULUKOT

SISÄLLYS

1 JOHDANTO

Kyberturvallisuuden tärkeys kansallisen turvallisuuden osana on korostunut, sillä lähes kaikki yhteiskunnan perus- ja kriittiset toiminnot ovat nykyisin automatisoituja ja yhteydessä toisiinsa (Kuusisto & Kuusisto, 2015). Verkottumisen taustalla on näkemys siitä, että tietoyhteiskunnan kehittäminen nähdään avaimena tuottavuuteen ja kehitykseen, jonka erilaiset tieto- ja viestintäteknologiat mahdollistavat (Rantapelkonen & Jantunen, 2013). Tämä näkemys on ajanut myös julkisen sektorin toimijat liittämään palvelunsa osaksi verkostoa, mikä on johtanut kriittisen infrastruktuurin sisäisten ja ulkoisten kyberriippuvuuksien lisäksi myös siihen, että kriittisiä palveluita voi usein hallita etänä verkon ja erilaisten järjestelmien avulla. Esimerkiksi pitkälle automatisoiduilla teollisuuden ohjausjärjestelmillä on usein yhteys yritysverkkoon, joka on puolestaan yhteydessä Internetiin, minkä vuoksi kyberhyökkäykset infrastruktuuriin matojen, virusten ja tietovuotojen muodossa ovat mahdollisia. (Amoroso, 2012; Xiao-Juan & Li-Zhen 2010.) Ilman Internetiä ja verkkojen yhdistettävyyttä kyberturvallisuuden takaaminen olisi paljon helpompaa, mutta yhdistyneisyyden hyödyt ovat niin suuret, ettei niitä voi sivuuttaa (Geers, 2011). Toisin sanoen tietoyhteiskunta teknologioineen tarjoaa välineet niin tehokkaaseen ja tuottavaan toimintaan, että toiminnan harjoittaminen keskeytysten ja häiriöidenkin uhalla nähdään riskin ottamisen arvoiseksi.

Keskeytykset ja häiriöt johtuvat usein kyberhyökkäyksistä, jotka ovat yksi kasvavimmista uhista nyky-yhteiskunnan tullessa entistä riippuvaisemmaksi kybertoimintaympäristöstä, joten kyberturvallisuuden tarve on välttämätön, kun halutaan varmistaa informaation kulun ja hallinnoimisen, sekä yksilöiden, organisaatioiden ja kriittisen infrastruktuurin turvallisuus (Faysel & Haque, 2010). Valtiollisten ja liiketoiminnallisten toimijoiden lisäksi kyberturvallisuus koskee yhä yleistyvämmissä määrin tavallisia kansalaisia, joiden aktiivisuus kybertoimintaympäristössä on kasvanut merkittävästi teknologioiden, kuten älylaitteiden saatavuuden parantuessa. (Rantapelkonen & Salminen, 2013; Norri-Sederholm, Laitinen, Lehto & Kari, 2019). Kyberhyökkäyksiltä suojautumista vaikeuttaa kuitenkin se, ettei valtioilla tai yrityksillä ole suoraa kontrollia Internetiin tai muihin viestintäkanaviin (Rantapelkonen & Salminen, 2013), sillä

kyberavaruudella ei ole yhtä tiettyä kontrollipistettä tai viestintäkanavaa, minkä vuoksi sen keskitetty hallinta on mahdotonta (Rantapelkonen & Jantunen, 2013). Euroopan unionin kyberturvallisuusstrategiassa (2013) tunnistetaan Euroopan haavoittuvuus nykyisillä valmiuksilla ja Hanska (2013) ilmaisee huolensa liittyen pohjoismaihin kohdistuvaan kyberhyökkäykseen, sillä kehittyneet yhteiskuntamme ovat niin riippuvaisia Internet-yhteydestä ja tietojärjestelmistä, että pienikin häiriö niissä voi johtaa odottamattomiin seurauksiin. Kansainvälisen ja kansallisen turvallisuuden vastuullisilla on siis aito tarve valmistella kyberpuolustusta taktisella ja strategisella tasolla (Geers, 2011). Maanlaajuiset sähkökatkot, taivaalta putoavat lentokoneet, kaasuputkien räjähtely, myrkyllisten kaasujen vapautuminen sekä satelliittien suistuminen kiertoradoiltaan ovat muun muassa niitä katastrofaalisia ilmiöitä, joita kyberhyökkäysten pelätään pahimmillaan aiheuttavan (Clarke, 2009). Vaikkei nämä uhkakuvat ole vielä toteutuneet, niin kyberavaruuden tuhovoimaista potentiaalia niiden toteuttamisessa ei sovi aliarvioida.

Myös kyberuhkien aiheuttajien eli kyberhyökkääjien kirjo on laajentunut, sillä aiemmin hyökkäyksistä vastanneiden yksilöiden ja ryhmien rinnalle ovat tulleet yritykset, jotka saattavat havitella kilpailijoiden yrityssalaisuuksia, sekä kybersodankäynnin yksiköt ja ryhmittymät, jotka toimivat usein valtioiden kontrollissa. Hakkerit ovat silti edelleen vastuussa valtaosasta hyökkäyksistä, kun taas valtiolliset toimijat ovat selkeästi harvinaisempia hyökkäysten suorittajia. (Edwards, 2014.) Teknologioiden kehittyessä hyökkääjät pyrkivät usein adaptoimaan uutta teknologiaa hyökkäyksissään saavuttaakseen tavan kiertää puolustuksen, joka ei välttämättä ole ehtinyt kehittyä yhtä nopeasti kuin hyökkääjien keinot. Kyberuhilta suojautuminen edellyttääkin jatkuvaa muutosta valtioiden ja yritysten turvallisuussektoreilla, sillä luovuus, rohkeus ja jatkuva innovointi ovat tärkeitä ominaisuuksia kyberuhkien torjumisessa. Siksi kyberhyökkääjien muuntautumiskyky ja ajantasaisuus voidaan nähdä haastavina valtiollisille ja julkisille rakenteille, jotka mielletään usein verrattain raskaiksi ja jäykähköiksi. (Gheorghe, Tatar & Gokce, 2017.)

Uhkakuvien laajentuessa ja kyberhyökkäysten lisääntyessä useat valtiot ovat alkaneet suhtautua entistä valveutuneemmin kyberturvallisuuteen ja aloittaneet kehittämään yksilöllisiä linjauksia ja lähestymistapoja kriittisen infrastruktuurin suojaamisessa (Rantapelkonen & Salminen, 2013), sekä antaneet julkilausumia strategisista toimintatavoistaan kyberhyökkäysten torjumisessa (Gheorghe, Tatar & Gokce, 2017). Toisaalta, kun kyseessä on kansallinen turvallisuus, näiden julkilausumien tarkoituksena voi totuuden kertomisen sijaan olla jopa harhaanjohtaminen, jottei valtion terävintä kyberosaamista paljasteta ja tarjota hyökkääjille etulyöntiasemaa. Sen takia tieto- ja kyberturvallisuusstrategioiden tarkemmat yksityiskohdat jää usein kuvaamatta, jolloin ne jäävät usein hyvin yleismaailmallisiksi. Jo tämä seikka kielii aihealueeseen liittyvän tutkimuksen haasteista, kun totuudenmukaista tai konkreettista näyttöä käytännön toimintatavoista ei välttämättä ole saatavilla. (Robinson, Jones & Janicke, 2015.)

Kriittisen infrastruktuurin suojaamisessa tulee myös usein esiin julkisen ja yksityisen sektorin rooli, mikä on yksi tämän tutkielman keskeisistä teemoista.

Yksityinen osakeyhtiö saattaa olla vastuussa valtion kannalta kriittisestä palvelusta (Quigley, 2013), kuten sähkönjakelusta, jolloin herää kysymys, että kuka on vastuussa sähkönjakelun turvallisuusinvestoinneista ja sitä myötä kyberturvallisuuden kehittämisestä. Kriittisen infrastruktuurin digitaalisten riippuvuuksien takia sen suojaaminen sisällytetään usein osaksi kyberturvallisuusstrategiaa, jossa tarkemmat yksityiskohdat yhteistyökumppanien vastuista ja menettelytavoista jäävät usein turvallisuussyistä kuvaamatta. Lisäksi kyberturvallisuusstrategia on vielä varsin tuore käsite, sillä vasta vuonna 2013 Euroopan unioni julkaisi ensimmäisen vakavasti otettavan kyberturvallisuusstrategiansa, jossa se loi pohjan eurooppalaiselle kyberturvallisuudelle esimerkiksi velvoittamalla EU:n jäsenvaltioita perustamaan kyberturvallisuuden erikoisyksiköitä ja suosittelemalla laatimaan kansallisia strategioita kyberuhkien ehkäisemiseksi ja torjumiseksi (Euroopan unionin kyberturvallisuusstrategia, 2013). Vuonna 2017 Euroopan komissio päivitti kyberturvallisuusstrategiaansa painottamalla resilienssin, pelotteen ja puolustuksen merkitystä eurooppalaisessa kyberturvallisuudessa (Euroopan komissio, 2017).

Edellä käsiteltyjen teemojen pohjalta tämän tutkimuksen tarkoituksena on selvittää, että mitä kriittinen infrastruktuuri käsittää, ja millaisia kyberpohjaisia ominaisuuksia kriittiset sektorit pitävät sisällään. Esimerkiksi Suomen kyberturvallisuusstrategiassa (2013) ei määritellä tarkasti suomalaisen kriittisen infrastruktuurin kattavuutta, vaan keskitytään yhteiskunnan elintärkeisiin toimintoihin, joka on merkittävästi laajempi kokonaisuus yhteiskunnan toimintoja. Kun kriittisen infrastruktuurin sektorit ovat selvillä, pyritään selvittämään sektorien suojaamisesta vastuulliset toimijat Suomessa. Turvallisuusvastuullisten ollessa selvillä, pyritään löytämään niiden hyödyntämiä kyberturvallisuuden työkaluja kriittisen infrastruktuurin suojaamisessa. Tutkimuskysymys on asetettu seuraavasti:

- Millaisia kyberturvallisuustoimia kriittisen infrastruktuurin suojaamisessa hyödynnetään Suomessa ja kuka niistä on vastuussa?

Tutkimuskysymyksen avulla pyritään saamaan vastaus siihen, miten yleisesti kriittiseksi infrastruktuuriksi miellettävien sektoreiden vastuut ja suojaaminen hoidetaan Suomessa. Sektorien ja niistä vastuullisten ollessa selvillä, kartoitetaan kriittisen infrastruktuurin suojaamisessa hyödynnettäviä kyberturvallisuuden työkaluja ja sitä, että edistävätkö ne resilienssiä, puolustusta tai pelotetta. Mikäli suomalaisen kriittisen infrastruktuurin suojaamiseen liittyviä työkaluja tai keinoja ei löydy, pyritään ajantasaisia suojaustoimia selvittämään kirjallisuudesta.

Tutkimus toteutetaan kirjallisuuskatsauksen muodossa. Fink (2019) määrittelee metodin seuraavasti:

> Kirjallisuuskatsaus on systemaattinen, yksityiskohtainen ja toistettavissa oleva metodi, jonka avulla alan asiantuntijoiden aiemmin tuottamia tutkimuksia voidaan arvioida, tunnistaa ja yhdistää.

Kirjallisuuden tutkinnan tulee myös olla mahdollisimman läpinäkyvää ja avointa eritoten siinä, miten lähteet valiutuvat ja miten ne tukevat tutkimusta (Hart, 2018). Toisin sanoen kirjallisuuskatsauksen tarkoituksena on hyödyntää alan aiempaa kirjallisuutta ja mahdollistaa tutkimuksen toistaminen asettamalla selkeät tutkimuskysymykset ja perusteet tutkimukselle, sekä rajata tiedonhakuun liittyvät tekijät esimerkiksi hakusanoin ja lähteiden luotettavuuden perusteella. Tässä tutkimuksessa tiedonhaku keskittyy erityisesti sähköiseen lähdemateriaaliin, jonka etsimiseen käytetään JYKDOK ja Google Scholar -hakukoneita. Tutkimuksen tiedonhaku rajoittuu teoksiin, joihin on joko vapaa pääsy tai Jyväskylän yliopiston kautta saatu lukuoikeus. Tutkimusaiheen kannalta keskeisiä termejä, joita on käytetty myös lähdeaineiston hakusanoina, ovat "critical infrastructure", "critical infrastructure protection", "cyber security" "cyber security strategy" ja "industrial control system". Tutkimuksen kannalta on relevanttia keskittyä erityisesti kriittiseen infrastruktuuriin liittyvään kyberturvallisuuteen. Löydetyn lähdemateriaalin luotettavuus pyritään varmistamaan hyödyntämällä vertaisarvioituja tieteellisiä julkaisuja, kuten kirjoja, tutkimuksia tai artikkeleita, mutta tutkimusaiheen luonteen takia myös strategisia asiakirjoja ja virastojen verkkojulkaisuja hyödynnetään. Lähdeaineiston ajantasaisuuteen pyritään valitsemalla pääasiassa vuoden 2009 jälkeen julkaistua materiaalia, mutta muutamia vanhempiakin julkaisuja valiutui mukaan. Tieteellisen kirjallisuuden luotettavuus pyritään varmistamaan viittausten määrän ja JUFO-luokituksen perusteella, jonka tavoite on olla vähintään 1. Mahdollisten poikkeusten kohdalla tulee olla hyvät perusteet, kuten tutkimuksen loogisuus ja luotettavuus, tai tutkimuksen taustalla oleva uskottava lähdekirjallisuus. Loppujen lopuksi tutkielman lähdeaineisto koostuu 68 lähteestä.

Tutkielma on jaettu pääsisällöltään kolmeen osaan. Johdannon jälkeinen ensimmäinen osa keskittyy kyberturvallisuuden käsitteen määrittelyyn, historiaan ja strategiseen ulottuvuuteen. Toisessa osassa saadaan parempi ymmärrys kriittisestä infrastruktuurista käsitteenä, sekä siihen liittyvistä osa-alueista ja ongelmista. Näiden osien tavoitteena valmistaa lukijaa kolmanteen osaan, jossa kaksi käsiteltyä aihepiiriä yhdistyvät tulosten muodossa. Tuloksia käsittelevän luvun lopussa tuloksia peilataan asetettuun tutkimuskysymykseen, minkä jälkeen koostetaan vielä yhteenveto ja spekuloidaan tutkimuksen pohjalta kumpuavia jatkotutkimusaiheita.

2 KYBERTURVALLISUUS

Tässä luvussa lukijalle on tarkoitus koostaa käsitys yleinen käsitys kyberturvallisuudesta, kyberuhista ja kyberturvallisuuden strategisesta ulottuvuudesta. Luku on jaettu kolmeen alalukuun, joista ensimmäisessä määritellään tieto- ja kyberturvallisuus, jotta niiden eroavaisuudet ja samankaltaisuudet voidaan tunnistaa. Toisessa alaluvussa suoritetaan läpileikkaus verkkoympäristöä järkyttäneiden haittaohjelmien historiaan, jotta saadaan käsitys siitä, miltä yritetään suojautua. Kolmannessa alaluvussa käydään läpi kyberturvallisuuden kehittämiseen liittyviä toimia Euroopan unionin kyberturvallisuusstrategiasta poimittujen otteiden avulla, jotka asettavat yleiset vaatimukset eurooppalaiselle kyberturvallisuudelle.

2.1 Tieto- ja kyberturvallisuus

Vaikka kyberturvallisuus (engl. cyber security) on paljon esillä nykypäivän tutkimuksessa ja turvallisuuspolitiikassa, niin silti sen eroavaisuudet suhteessa tietoturvallisuuteen (engl. information security) jäävät usein määrittelemättä. Termit saatetaan helposti sekoittaa toisiinsa, koska on olemassa useita kyberturvallisuuden määritelmiä, jotka ovat rinnastettavissa tietoturvallisuuteen. (Von Solms & Van Niekerk, 2013.) Termien samankaltaisuudesta kielii esimerkiksi se, että erästä vuonna 2008 julkaistua Suomen hallituksen asiakirjaa muokattiin vuonna 2011 siten, että aikaisemmassa dokumentissa käytetty tietoturvallisuuden termi korvattiin kyberturvallisuuden termillä (Rantapelkonen & Jantunen, 2013).

2.1.1 Tietoturvallisuuden määrittely

Kyberturvallisuuden sanaston (2018) mukaan tietoturvallisuus käsittää

> ne järjestelyt, joilla varmistetaan tiedon saatavuus, eheys ja luottamuksellisuus. Saatavuus tarkoittaa, että tieto on hyödynnettävissä haluttuna aikana. Tiedon eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvan järjestelyjä ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö.

Lisäksi tiedon käsittelyyn, varastointiin ja siirtoon käytettävien laitteistojen ja ohjelmistojen suojaaminen ovat osa tietoturvallisuutta (Whitman & Mattord, 2012).

2.1.2 Kyberturvallisuuden määrittely

Kyberturvallisuudesta on kansainvälisesti useita määritelmiä ja universaalin määritelmän kehittäminen on ollut haastavaa, sillä määritelmät saattavat erota merkittävästi toisistaan (Craigen, Diakun-Thibault & Purse, 2014; Luiijf, Besseling & de Graaf, 2013). Määritelmiä ovat tehneet niin valtiot, virastot, kuin tieteenharjoittajatkin. Esimerkiksi Yhdysvaltain kotimaan turvallisuusvirasto (2014) määrittelee kyberturvallisuuden toiminnaksi, kyvykkyydeksi tai tilaksi, jonka avulla viestintä- ja tietojärjestelmiä suojataan vaurioilta, luvattomilta käytöiltä tai muutoksilta. Määritelmä vaikuttaa varsin samanlaiselta, kuin tietoturvallisuuden määritelmä, joka keskittyy erityisesti tiedon ja sitä käsittelevien laitteiden suojaamiseen. Sen sijaan kansainvälinen televiestintäliitto ITU (2009) keskittyy kyberturvallisuuden määritelmässään kokoelmaan toimenpiteitä, joista kyberturvallisuus muodostuu. Näitä ovat muun muassa erilaiset linjaukset, riskienhallinnan lähestymistavat, koulutukset, vakuutukset ja teknologiat, joita voidaan käyttää kybertoimintaympäristön, organisaation ja sen työntekijöiden suojeluun. ITU:n kanssa samoilla linjoilla ovat Von Solms & Van Niekerk (2013), joiden määritelmän mukaan kyberturvallisuus käsittää kyberavaruuden suojaamisen lisäksi myös siellä toimivien tahojen ja kyberavaruuden kautta saavutettavissa olevan omaisuuden suojaamisen. Esimerkki kyberavaruudessa toimivasta yksittäisestä tahosta voisi olla vaikka yksityinen yritys, joka on liittänyt yritystilojen turvajärjestelmän hallittavaksi Internetin välityksellä, jolloin turvajärjestelmään kohdistuva kyberhyökkäys voi aiheuttaa yrityksen työntekijöille hengenvaaran esimerkiksi murron tapahtuessa. Sähköisen omaisuuden suojelemisesta esimerkkinä voidaan käyttää musiikin ja elokuvien laitonta lataamista, jolloin niiden tuotannosta vastuussa olevat toimijat jäävät ilman tuottoja.

Myös Suomessa huomattiin tarve kyberturvallisuuden piiriin kuuluvien käsitteiden määrittelyyn, jotta aiheeseen liittyvä kehitys ja viestintä olisi mahdollisimman tehokasta. Vuonna 2017 käynnistettiin asiantuntijaryhmävetoinen projekti, jonka tarkoituksena oli selvittää keskeiset käsitteet kyber- ja tietoturvaan liittyen ja tarjota niille vastineet suomenkielisestä termistöstä. Projektin myötä syntyi Kyberturvallisuuden sanasto (2018), jossa kyberturvallisuus määritellään seuraavasti:

> Kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia.

Tässä tutkielmassa yhdistetään ITU:n (2009), Von Solmsin & Van Niekerkin (2013) sekä Kyberturvallisuuden sanaston (2018) määritelmät siten, että kyberturvallisuudella tarkoitetaan tavoitetilaa, jossa yhteiskunnan ja organisaatioiden toiminnot sekä yksilöiden hyvinvointi ja omaisuus on turvattu kyberavaruudesta käsin tapahtuvilta hyökkäyksiltä. Lisäksi kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. Sitomalla kyberturvallisuuden määritelmä

kybertoimintaympäristöön, organisaatioihin ja yksilöihin, sekä kyberturvallisuutta kehittäviin toimenpiteisiin, voidaan löytää helpommin yhteyksiä eri entiteettien, turvallisuustoimenpiteiden ja kriittisen infrastruktuurin välillä. Lisäksi kyberturvallisuustoimet on täten helpompi tunnistaa ja jaotella käyttäjiin, teknologiaan tai linjauksiin liittyviksi.

2.1.3 Tieto- ja kyberturvallisuuden yhteydet ja eroavaisuudet

Kyberturvallisuuden sanastossa (2018) tunnistetaan kyberturvallisuuden ja tietoturvallisuuden yhteys esimerkiksi siten, että kybertoimintaympäristön toiminnan häiriytyminen on usein seuraus ilmenneestä tietoturvauhkasta. Toisin sanoen tietoturva on keskeinen tekijä pyrittäessä kyberturvallisuuteen. Tietoturvallisuus keskittyy tiedon turvaamiseen, kun taas kyberturvallisuus on laajempi kokonaisuus, jonka yhtenä osana tiedon turvaaminen voidaan nähdä. Käsitteiden suurin ero on puolestaan siinä, että tietoturvan tarkoittaessa tiedon saatavuutta, eheyttä ja luottamuksellisuutta (Kyberturvallisuuden sanasto, 2018), kyberturvalla tarkoitetaan pääsääntöisesti yhteiskunnan tai organisaation toimintojen ja väestön hyvinvoinnin suojaamista kyberavaruudesta käsin tapahtuvilta hyökkäyksiltä (Högmander, 2012). Kyberturvallisuus ei siis ole synonyymi tietoturvallisuudelle, verkkoturvallisuudelle tai muille samankaltaisille turvallisuustermeille (Kyberturvallisuuden sanasto, 2018).

Siten selittyy ehkä myös tietoturvallisuuden termin korvaaminen kyberturvallisuudella hallituksen asiakirjassa, jos asiakirjan tavoitteena on turvallisen tiedonhallinnan lisäksi käsitellä kansalaisten, yritysten, virastojen ja muiden yhteiskunnan toimijoiden toiminnan turvaaminen kyberavaruudessa, jolloin kyberturvallisuus on tarkoituksenmukaisempi termi.

2.2 Haittaohjelmien historia

Ajatus niin kutsutuista itsemonistuvista ohjelmista, joita alettiin myöhemmin kutsua madoiksi, juontaa vuoteen 1949. Tuolloin John von Neumann, unkarilaissyntyinen matemaatikko, visioi tulevaisuuden tietokoneet ja tietokoneohjelmien kyvyn jäljentää itseään. Itsemonistuvien ohjelmien jalostuneita versioita alettiin kutsua madoiksi vuonna 1979 ja ensimmäinen tietokonevirus luotiin vuonna 1983. 1970- ja 1980-luvulla luodut haittaohjelmat olivat kuitenkin liki täysin kokeellisia, joten niitä ei vielä valjastettu käyttötarkoitukseensa. (Geers, 2011; Chen & Robert, 2004.)

Vasta Internetin ja sähköpostin käytön yleistyttyä 1990-luvulla haittaohjelmien määrä moninkertaistui ja samalla niiden laatu parani. Ajalle tyypillistä oli haittaohjelmien leviäminen sähköpostin kautta, hyödyntäen saastuneen viestin avanneen käyttäjän sähköpostiosoitetta ja sähköpostilistoja. Haittaohjelmat yleistyivät niin paljon, että järjestettiin tutkimus, jonka tarkoituksena oli jaotella haittaohjelmat hyökkääjien motivaation perusteella. Tutkimus ennusti, että

tulevaisuuden haittaohjelmilla olisi mahdollista vakoilla kansalaisia ja manipuloida kriittisen infrastruktuurin osia kybersodan merkeissä. (Geers, 2011.) 2000-luvun taitteessa haittaohjelmilla saattoi olla jo merkittäviä taloudellisia vaikutuksia kohteisiinsa. Virukset kuten ”I LOVE YOU”, ”Klez” ja ”Sobig” aiheuttivat kukin miljardiluokan vahinkoja, tyhjentämällä tärkeitä tiedostoja ja lähettämällä arkaluontoisia sähköpostiviestejä satunnaisille kontakteille (Fosnock, 2005).

2000-luvun alkuun mennessä haittaohjelmilla ei oikeastaan ollut yksilöityjä kohteita, vaan madot, virukset ja troijalaiset levisivät käytännössä sinne, minne ikinä pääsivätkään. 2000-luvun edetessä siihen tuli kuitenkin muutos. Vuonna 2001 15-vuotias opiskelija Montrealista suoritti palvelunestohyökkäyksiä joitakin maailman suurimpia yrityksiä kohtaan. Erona vuonna 1988 tapahtuneeseen ensimmäiseen palvelunestohyökkäykseen oli se, että hyökkäys oli kohdistettu satunnaisuuden sijaan tiettyjä yrityksiä kohtaan. "MafiaBoy"-nimimerkkiä käyttänyt opiskelija aiheutti hyökkäyksellään häiriöitä yritysten liiketoiminnassa, minkä myötä yritykset menettivät tuottoja yhteensä yli miljardin dollarin edestä. (Verton, 2002.)

Haittaohjelmat saavuttivat pian myös poliittisia ja maanpuolustuksellisia ulottuvuuksia. Vuonna 2007 Syyrian ilmapuolustuksen raportoitiin kokeneen lamauttavan kyberhyökkäyksen juuri ennen Israelin suorittamaa ilmaiskua, jonka kohteena oli kiistelty syyrialainen ydinvoimala (Makovsky, 2012). Viroon vuonna 2007 ja Georgiaan vuonna 2008 kohdistuneet kyberhyökkäykset olivat ensimmäisten joukossa olevia tapauksia, joissa kyberhyökkäyksillä pyrittiin vaikuttamaan vastapuoleen. Viroon kohdistuneet kyberhyökkäykset aiheuttivat häiriöitä joissakin kriittisiksi luokitelluissa palveluissa. Hyökkäyksellä oli tarkoitus vaikuttaa virolaisten päätöksentekijöiden ratkaisuihin koskien neuvostoaikaisen monumentin siirtämistä. Georgian sota puolestaan oli ensimmäinen sota, joka sai kyberavaruudellisia ulottuvuuksia. Palvelunestohyökkäykset ja hallinnollisten nettisivujen kaappaukset johtivat tilanteeseen, jossa Georgian hallinnolla oli vaikeuksia saada yhteys ulkomaailmaan ja valtion hallinnolliset nettisivut täytettiin propagandalla. Pankkipalvelut ja matkapuhelinyhteydet eivät myöskään toimineet. Vuonna 2009 Kirgisian valtio koki massiivisen palvelunestohyökkäyksen, jonka vuoksi suuri osa kansallisista tietoliikenneyhteyksistä kaatui. Hyökkäyksen taustalla oli näkemyserot Venäjän ja Yhdysvaltojen välillä, kun Kirgisia myönsi sotilaslentokentän käyttöoikeudet Yhdysvalloille sodankäynnissä Afganistania vastaan. Hyökkäyksen alkuperä jäljitettiin samoille venäläisille palvelimille, joita järjestäytynyt hakkeriryhmä oli hyödyntänyt Viroon ja Georgiaan kohdistuneissa kyberhyökkäyksissä. (Kozlowski, 2014.)

Tähänastiset kyberhyökkäykset, joilla oli pyritty vaikuttamaan valtioiden kriittisiin palveluihin, koostuivat enimmäkseen palvelunestohyökkäyksistä, mutta vuonna 2009 Stuxnet mullisti kyberturvallisuuden kenttää. Yhdysvaltojen ja Israelin kehittämä Stuxnet-mato tuli tunnetuksi, kun sen haittakoodi levisi saastuneen USB-tikun kautta Iranilaiseen ydinvoimalaan, jossa se aiheutti häiriöitä uraanin rikastamisprosessin kannalta keskeisissä sentrifugeissa. Se oli suunniteltu aktivoitumaan täsmälleen kyseisen ydinvoimalan ohjausjärjestelmässä, jossa se toimisi naamioituneena järjestelmän syövereihin. Lopulta koodi pääsi

kuitenkin leviämään vahingossa Internetiin, minkä myötä se paljastui koko maailmalle. Stuxnetin vaikutus verkkoympäristöön oli huomattava, sillä sen jälkeen teollisuuden valvomo-ohjelmistoihin kohdistuneiden kyberhyökkäysten määrä vuositasolla kasvoi 20-kertaisesti verrattuna edeltävien viiden vuoden keskiarvoon. Myös hyökkäysten motiivit ja kohteet muuttuivat. (Bologna, Fasani & Martellini, 2013.) Stuxnetin katsotaan olleen ensimmäinen valtiojohtoinen kyberhyökkäys, sillä aikaisemmista hyökkäyksistä vastuussa olivat joko hakkerit, aktivistit tai rikolliset. Aikaisemmin kohteiksi valikoituivat yksityiset henkilöt tai yritykset, joilta yritettiin kavaltaa tietoa tai omaisuutta, mutta Stuxnetin jälkeen yhä useammat hyökkäykset ovat alkaneet kohdistua valtion laitoksiin vahingonaiheutus tarkoituksessa (Bologna, Fasani & Martellini, 2013). Stuxnet voidaan nähdä muurinmurtajana haittaohjelmien saralla myös siksi, että sen uskotaan olleen ensimmäinen ase, joka sai aikaan aineellisia vahinkoja ilman fyysistä olomuotoa. (Kärkkäinen, 2013.)

Edellä mainitut esimerkit haittaohjelmien vaikutuksista merkittäviin yrityksiin, kriittiseen infrastruktuuriin ja puolustusjärjestelmiin ovat pakottaneet kansalliset ja kansainväliset turvallisuusviranomaiset huomioimaan kehittyneet haittaohjelmat ja kiinnittämään entistä enemmän huomiota kyberturvallisuuteen. Myös hyökkääjät toimivat kansainvälisemmin ja ammattimaisemmin kuin aikaisemmin. Vuosikymmen sitten tapahtunut radikaali murros kyberhyökkääjissä, motiiveissa ja kohteissa kertoo osaltaan siitä, miten teknologian kehitys on ajanut turvallisuuden ja lainsäädännön ohi, mahdollistaen verkkoympäristön väärinkäytökset ilman vakavia seurauksia ja rangaistuksia. Viimeistään tuolloin turvallisuusviranomaiset maailmanlaajuisesti heräsivät kehittämään teknologioita, lainsäädäntöä ja strategioita, joilla kyberuhkia voitaisiin tunnistaa, ehkäistä ja torjua.

2.3 Euroopan unionin kyberturvallisuusstrategia

Euroopan unionin kyberturvallisuusstrategiassa (2013) määritellään liittovaltion kattava visio siitä, miten verkon häiriöitä ja verkkohyökkäyksiä ehkäistään ja torjutaan. Tavallaan kyberturvallisuusstrategialla määritellään myös minimitaso, johon EU:n jäsenvaltioiden kyberturvallisuuden tulisi yltää. Strategian sisältämät linjaukset ja toimet keskittyvät eritoten

- kyberresilienssin saavuttamiseen,
- kyberrikollisuuden vähentämiseen,
- kyberpuolustuslinjausten ja -kyvykkyyksien kehittämiseen,
- teollisten ja teknologisten resurssien kyberturvallisuuden kehittämiseen, sekä
- yhtenäisten ja kansainvälisten verkkoympäristölinjausten laatimiseen.

Kyseinen strategia muun muassa valtuuttaa jokaista jäsenvaltiota perustamaan kansallisen CERT-ryhmän (Computer Emergency Response Team), jonka

tarkoitus on ennaltaehkäistä, tunnistaa ja ratkaista kyberuhkia. Tämä yleisen selvyyden vuoksi, sillä aikaisemmin valtioilla oli saattanut olla vaikeuksia päättää, mikä valtiollinen virasto tai laitos olisi vastuullinen elin merkittävän kyberhyökkäyksen tapahtuessa (Luiijf, Besseling & de Graaf, 2013). Kansallisten CERT-ryhmien perustamisella ja strategioiden laatimisella pyritään kansallisen turvallisuuden tehostamisen lisäksi helpottamaan kansainvälisen yhteistyön harjoittamista, kun valtiot ovat määritelleet kansalliseen verkkoturvallisuuteen liittyvät toimet ja vastuut. Strategiaan sisältyy myös kehittyvä lainsäädäntö, jonka osana esitellään verkko- ja tietoturvaan liittyvä NIS-direktiivi (Network and Information Security), joka astui voimaan vuonna 2016. Direktiivissä säädetään oikeudelliset toimenpiteet kyberturvallisuuden yleisen tason parantamiseksi EU:ssa, minkä sen seurauksena jokaisen jäsenvaltion tuli laatia kansallinen verkko- ja tietoturvastrategia ja määrittää siitä vastuussa olevat tahot. (Euroopan unionin kyberturvallisuusstrategia, 2013.) Näillä toimilla pyritään parempaan kyberresilienssiin, tietoliikenneverkon vakauteen ja tietoverkkorikollisuuden vähentämiseen.

Lisäksi strategiassa tunnistetaan julkisen ja yksityisen sektorin yhteistyön tärkeys, sillä suurin osa kriittisestä infrastruktuurista on yksityisyritysten omistamia ja hallitsemia. Tämän vuoksi yksityisten yritysten sitoutumista ja valmiutta tulisi kehittää. Strategian mukaan yritysten tulisi avoimesti raportoida havaitsemistaan potentiaalisista kyberuhista valtion CERT- tai NIS-toiminnoille ja toimia yhteistyössä niiden kanssa, jotta kyberuhat ehkäistään ja torjutaan jatkossakin. Vaikka yhteistyö valtiollisten yksiköiden kanssa saattaa lisätä byrokratiaa ja viedä aikaa, niin yksityisen sektorin näkökulmasta on tärkeää tiedostaa kyberuhkien riskit ja muodostaa riskinhallintakulttuuri, jotta toiminta kriittisen infrastruktuurin suojaamisessa olisi mahdollisimman riskisietoista.

Myös avoimuus ja yhteistyö näkyvät EU:n kyberturvallisuusstrategiassa kyberturvallisuusaiheisten kansainvälisten harjoitusten muodossa. EU on tähänkin mennessä järjestänyt vuosittaisia harjoituksia, joihin ovat ottaneet osaa niin jäsenvaltiot, yksityisyritykset kuin EU:n ulkopuolisetkin valtiot, mutta niiden määrää ja laatua on tarkoitus kehittää. Harjoituksissa saatetaan esimerkiksi simuloida kyberhyökkäys, ja häiriötilanteesta selvitäkseen osapuolten on harjoitettava yhteistoimintaa. Kriittisestä infrastruktuurista vastaavien tahojen harjoittamisen lisäksi komissio tunnistaa tarpeen kehittää kansalaisten tietoisuutta kyberturvallisuutta kohtaan. Esimerkiksi vuonna 2012 jotkin jäsenvaltiot lanseerasivat yhdessä Euroopan unionin verkko- ja tietoturvaviraston (ENISA) kanssa eurooppalaisen kyberturvallisuuskuukauden, jonka teemana oli kasvattaa kansalaisten tietoutta kybertoimintaympäristön uhista. (Euroopan unionin kyberturvallisuusstrategia, 2013.)

.

2.3.1 Kyberturvallisuus Virossa ja Norjassa

EU:n tapauksessa kyberturvallisuusstrategian ydin koostuu avoimuudesta, turvallisuudesta ja vakaudesta, joiden avulla se pyrkii ohjaamaan eurooppalaista

kyberturvallisuutta kohti koherenttia käsitystä ja toimintaa läpi valtionrajojen. Esimerkiksi toimeenpanemalla kansalliset CERT-toiminnot, pyritään yhtenäistämään valtioiden ja yritysten kyberturvallisuusraportoinnin prosessia, minkä pohjalta hyväksi todetut käytänteet voidaan jakaa ja toimintaa yhtenäistää, jolloin yhteistyötä on selkeämpää harjoittaa niin yritysten, julkisen sektorin, kuin valtioidenkin välillä.

Kyberturvallisuuden edelläkävijöistä muun muassa Viro ja Norja antavat hyvän esimerkin ydinarvojen ja erityisesti avoimuuden soveltamisesta pyrittäessä kohti parempaa kyberturvallisuutta. Esimerkiksi Viroon vuonna 2007 kohdistunut kyberhyökkäys sai virolaiset ymmärtämään, että heidän tulee kehittää kyberturvaansa kansallisen turvallisuuden takaamiseksi. Sen sijaan, että he olisivat salanneet haavoittuvuutensa, he tunnistivat kehitystarpeensa ja perustivat vapaaehtoisista koostuvan kyberturvaosaston, joka on verrattavissa kybertoimintaympäristössä toimivaan reserviläisarmeijaan (Kerigan-Kyro, 2014.) Virosta tuli myös yksi ensimmäisistä valtioista, joka kehitti ja julkaisi kyberturvallisuusstrategiansa. Strategia julkaistiin vuonna 2008, pian sen jälkeen, kun Viron hallinnolliset elimet altistuivat kyberhyökkäyksille.

Vaikkei Norja kuulu Euroopan unioniin, niin sen kansallinen CERT-ryhmä kuuluu EGC-yhteisöön (European Government CERTs), joka koostuu tiettyjen eurooppalaisten valtioiden kansallisista CERT-ryhmistä, jotka harjoittavat yhteistoimintaa ja kehittävät siten tehokkaampia kyberturvallisuuden linjauksia. Norjan kyberturvallisuuskeskus, NorCERT, auttoi estämään Statoil -energiayhtiöön kohdistuneen kyberhyökkäyksen. Statoilin työntekijät huomasivat vastaanottaneensa epäilyttäviä sähköposteja, joista raportoitiin NorCERT:lle. Sähköpostiviestit sisälsivät hyvin naamioituja viruksia, jotka olisivat voineet aiheuttaa häiriöitä energiantuotannossa, mutta varhaisen tunnistamisen ansiosta ongelmilta vältyttiin. Statoil ja Norja luottavat syyllistämättömään avoimeen kulttuuriin, kun taas monet valtiot saattavat edelleen nojata syyllistävään kulttuuriin. Avoin kulttuuri on avaintekijä kyberuhkien varhaisessa tunnistamisessa, sillä syyllistävässä kulttuurissa työntekijät saattavat jättää raportoimatta mahdollisesta kyberuhasta, koska he pelkäävät joutuvansa syytetyiksi ongelmasta (Kerigan-Kyro, 2014). Toisin sanoen Norja ja Viro näyttävät mallia miten kriittisen infrastruktuurin kyberturvallisuutta kehitetään jakamalla tietoa avoimesti ja tehokkaasti yksityisen ja julkisen sektorin välillä.

2.3.2 Resilienssi, pelote ja puolustus

Vuonna 2017 komissio tarkasteli vuoden 2013 strategiaa ja esitti painotettavia kehitysalueita, joiden turvallisuuden edistämiseen liittyvät toimet olisi määrä tulla voimaan vuonna 2019, tarkoituksena parantaa Euroopan unionin kyberturvallisuutta. Kehitysalueet koostuvat pääasiassa kolmesta osa-alueesta: resilienssi, pelote ja puolustus.

Ensimmäinen askel kohti parempaa kyberturvallisuutta on voimaanpanna NIS-direktiivi, joka on edellytys paremmalle resilienssille (engl. resilience). Direktiivi velvoittaa esimerkiksi digitaalisia palveluntarjoajia avoimuuteen ja

ilmoittamaan toimintaa häiritsevistä tekijöistä kyberviranomaisille, kuten NIS- ja CERT-toiminnoille. Euroopan komissio haluaa myös, että jokainen kantaa kortensa kekoon paremman kyberturvallisuuden kehittämiseksi (Euroopan komissio, 2017). Eurooppalaisen kyberturvallisuuskuukauden tavoin yhteiskunnallisen kybertietoisuuden lisäämiseksi on aikaisemminkin järjestetty erilaisia kampanjoita, mutta niiden toteutuksen ja osallistavuuden suhteen on havaittu parantamisen varaa (Luiijf, Besseling & de Graaf, 2013). Siksi Euroopan komissio suositteleekin kybervalistuksen sisällyttämistä osaksi akateemisia ja ammatillisia koulutuksia. Teollisuusalojen turvallisuusratkaisujen tapauksessa puolestaan suositellaan, että turvallisuus suunniteltaisiin osaksi teollisuuden ohjausjärjestelmiä, jolloin jälkikäteen suoritettavilta turvallisuusratkaisujen paikkauksilta vältyttäisiin. (Euroopan komissio, 2017.)

Pelotteella tai pelottelulla (engl. deterrence) Euroopan komissio (2017) tarkoittaa rikosten hallinnassa hyödynnettävää laillista uhkailua. Yleisesti sen voidaan sanoa tarkoittavan toimien torjumista tai tapahtumien estämistä aiheuttamalla vastapuolessa pelkoa tai epäilystä. Tässä tapauksessa tarkoitetaan siis toimia, joilla kyberhyökkäyksiä pyrittäisiin erinäisin pelottein ja seurauksin estämään ja torjumaan. Toistaiseksi kyberhyökkäysten potentiaaliset hyödyt ovat hyökkäyksistä koituvia haittoja suuremmat, minkä verrattain tehoton teknologia ja lainsäädäntö nykyisellään mahdollistavat (Kärkkäinen, 2013). Komission tahtotilana onkin tehostaa pelotetta eritoten teknologiaa ja lainsäädäntöä päivittämällä. Ensimmäisenä toimena on rohkaista IPv6:n (Internet Protocol version 6) käyttöönottoa, joka yleistyessään mahdollistaisi tehokkaamman tutkinnan kyberhyökkäysten alkuperän selvittämisessä. Kun hyökkääjät pystytään kehittyneemmän teknologian ansiosta paremmin identifioimaan, voidaan heidät myös saada vastuuseen toimistaan. (Euroopan komissio, 2017.) Tällöin puolestaan tehokkaan ja ajantasaisen lainsäädännön merkitys korostuu, sillä pelotteen luomiseksi haktivismia, kyberrikollisuutta, kybervakoilua ja kybersotaa koskevat rangaistukset tulisi olla yksiselitteisesti kirjattuna lainsäädäntöön. Jo näillä kahden osa-alueen kehittämisellä saataisiin aikaan tehokkaampi pelote, jonka ansiosta kyberhyökkäysten määrä voitaisiin saada laskuun.

Komissio haluaa hyödyntää myös valtioiden rajoista riippumatonta yhteistyötä kyberhyökkäysten ehkäisemisessä ja torjumisessa, minkä edistämiseksi EU:n ulkopuolisiakin valtiota halutaan mukaan yhteistyöhön, jotta globaali kyberturvallisuus kehittyisi. Lisäksi komissio ilmaisee valmiutensa valtiollisten ja yksityisten toimijoiden rankaisemiseen erilaisilla toimilla ja sanktioilla, mikäli ne jotenkin uhkaisivat Euroopan sisäistä kyberturvallisuutta. (Euroopan komissio, 2017.) Rajat ylittävä kybertoimintojen yhteenlinjaaminen tai kyberrikollisten jäljittäminen eivät tähän asti ole vaikuttaneet yltävän valtioiden prioriteettilistojen kärkeen, vaikka etenkin EU valtioiden tulisi harjoittaa ja edistää yhteistoimintaa. Yhteistyön ongelmina on nähty muun muassa näkemyserot valtioiden välillä liittyen kyberturvallisuuden kattavuuteen. Kaikki valtiot eivät välttämättä ole edes määritelleet kyberturvallisuuden käsitettä kansallisissa kyberturvallisuusstrategioissaan, minkä vuoksi niin ulkoinen, kuin sisäinenkin käsitys kansallisen

kyberturvallisuuden kattavuudesta ja tavoitetilasta voi olla ristiriitainen. (Luiijf, Besseling & de Graaf, 2013.)

Näihin Euroopan komission asettamiin kehitysalueisiin panostamalla valtiot voivat pyrkiä kohti kokonaisvaltaisempaa kyberturvallisuutta. Kohdealueiden kehittymistä ja toteutumista yhteiskunnallisella tasolla voidaan arvioida tarkastelemalla esimerkiksi valtion kriittistä infrastruktuuria, koska sen suojaamiseen liittyviä kyberturvallisuustoimia ja yhteistoimintaa voidaan peilata siihen, miten ne toteuttavat resilienssin, pelotteen ja puolustuksen osa-alueita yhteiskunnan tärkeimpien toimintojen suojaamisessa.

3 KRIITTINEN INFRASTRUKTUURI

Kun kyberturvallisuus ja Euroopan unionin tahtotila liittovaltion kattavan kyberturvallisuuden suhteen on määritelty, voidaan ymmärrettävämmin käsitellä kriittistä infrastruktuuria kyberpohjaisesta näkökulmasta. Luku on jaettu kolmeen alalukuun, joista ensimmäisessä ja toisessa määritellään kriittinen infrastruktuuri, kolmannessa käsitellään lyhyesti teollisuuden ohjausjärjestelmät, ja viimeisessä keskitytään kyberturvallisuuden ja kriittisen infrastruktuurin ongelmallisin liityntäkohtiin omistajuuden ja yhteistyön perspektiiveistä. Luvun tavoitteena on koostaa lukijalle käsitys kriittisestä infrastruktuurista sekä sen yhteyksistä kyberturvallisuuteen, minkä myötä on loogista siirtyä aihepiirit yhdistävään ja tuloksia käsittelevään lukuun.

3.1 Kriittisen infrastruktuurin määrittely

Toinen keskeinen termi tämän tutkimuksen kannalta on kriittinen infrastruktuuri (engl. critical infrastructure), jota on määritelty varsin laajalti. Käsitteen määritelmät itsessään eivät merkittävästi eroa toisistaan, mutta ne toiminnot ja järjestelmät, joita kriittinen infrastruktuuri pitää sisällään, vaihtelevat riippuen esimerkiksi yksittäisten valtioiden ja tieteen harjoittajien näkökulmista. Tässä alaluvussa keskitytään kriittisen infrastruktuurin yleispiirteisiin, kun taas seuraavassa alaluvussa käsitellään tarkemmin, mitä eri yhteiskunnan sektoreita kriittinen infrastruktuuri pitää sisällään.

Koska tutkimuksessa keskitytään erityisesti suomalaiseen menettelytapaan kriittisen infrastruktuurin suojaamisessa, voidaan käsitteen määrittelyssä lähteä liikkeelle eurooppalaisesta näkökulmasta, sillä Euroopan unionin lainsäädäntömuutokset vaikuttavat myös toimintaan Suomessa. Euroopan komission (2008) mukaan kriittisellä infrastruktuurilla tarkoitetaan omaisuutta, järjestelmää tai sen osaa, joka on välttämätön jäsenvaltioiden turvallisuuden ja hyvinvoinnin ylläpitämiseksi, ja jonka häiriintymisellä tai tuhoutumisella on merkittäviä vaikutuksia jäsenvaltion turvallisuuteen. Tutkimuksen näkökulmasta on tärkeää määritellä käsite myös suomalaisesta ja kyberturvallisuuden näkökulmista, jotka suomalaisten asiantuntijoiden laatimat Kyberturvallisuuden sanasto (2018) ja Kokonaisturvallisuuden sanasto (2017) tarjoavat. Sanastojen mukaan kriittinen infrastruktuuri käsittää perusrakenteet, palvelut ja niihin liittyvät toiminnot, jotka ovat välttämättömiä yhteiskunnan elintärkeiden toimintojen ylläpitämisessä. Lisäksi mainitaan kriittisen infrastruktuurin kyberfyysiset ominaisuudet, eli fyysisten laitosten ja rakenteiden lisäksi se pitää sisällään myös digitaalisia toimintoja ja palveluita. Näistä esimerkkeinä energiateollisuus, julkiset palvelut, talous- ja liikennejärjestelmät, tieto- ja viestintäliikenne, terveydenhuolto, sekä vedenjakelu. Eurooppalaisesta ja suomalaisesta määritelmästä voidaan todeta, että kriittinen infrastruktuuri muodostuu yhteiskunnalle elintärkeistä

palveluista, laitteista, välineistä ja tietojärjestelmistä, jotka voivat sisältää sekä fyysisiä että kyberpohjaisia ominaisuuksia.

Vaikka tässä tutkimuksessa käytetään termiä kriittinen infrastruktuuri, on joissakin tutkimuksissa ja asiakirjoissa korvaavana terminä saatettu käyttää kansallista infrastruktuuria (engl. national infrastructure). Esimerkiksi Amoroso (2012) puhuu kansallisesta infrastruktuurista, tarkoittaen niitä taustalla olevia jakelu- ja tukijärjestelmiä, jotka mahdollistavat valtiolle välttämättömien palveluiden toiminnan. Näiksi välttämättömiksi koetuiksi palveluiksi hän lukee muun muassa tiedonkeruujärjestelmät, lainvalvontatietokannat, sotilaalliset tukipalvelut ja tietoliikenneverkot. Kyberturvallisuusstrategioissa saatetaan usein myös mainita yhteiskunnan elintärkeät toiminnot (engl. vital societal functions), joita ei tule suoraan sekoittaa kriittiseen infrastruktuuriin. Esimerkiksi Suomen kyberturvallisuusstrategiassa (2013) elintärkeisiin yhteiskunnallisiin toimintoihin luokitellaan johtaminen, kansainvälinen aktiivisuus, puolustuskyky, sisäinen turvallisuus, talous ja infrastruktuuri, väestön toimintakyky sekä psykologinen sietokyky kriisien suhteen. Eli kriittinen infrastruktuuri voidaan laskea elintärkeiden toimintojen alalohkoksi, joka osaltaan mahdollistaa yhteiskunnan sujuvan toiminnan.

3.2 Kriittisen infrastruktuurin sektorit

Määriteltäessä kriittisen infrastruktuurin käsitettä, ei määritelmien välillä ilmene merkittäviä eroavaisuuksia. Eroavaisuuksia löytyy puolestaan siinä, että mitä eri yhteiskunnan sektoreita kukin valtio mieltää kriittiseksi. Koska suomalaisissa kyberturvallisuusstrategioissa ei ole määritelty kriittisen infrastruktuurin kattavuutta sen tarkemmin, koostetaan muiden valtioiden määritelmistä yleisimmät sektorit, joita voitaisiin Suomen tapauksessakin pitää kriittisinä. Yleisimpien kriittisten sektorien selvittämiseksi tutkitaan eri valtioiden kriittisen infrastruktuurin kattavuutta, minkä jälkeen eniten mainitut sektorit otetaan mukaan tutkimukseen. Taulukossa 1 on kuvattu eri valtioiden kriittiseksi luokittelemat sektorit.

Selvityksen perusteella ilmeni yhteensä 23 sektoria, joista vielä yhdistettiin pitkälti toisiinsa kietoutuvat osa-alueet. Esimerkiksi yksi EU:n kriittiseksi luokittelemista sektoreista on avaruus ja tutkimus, joten Espanjan erillisiksi kokonaisuuksiksi luokittelemat tutkimus- ja avaruussektorit yhdistettiin tässä tapauksessa. Yhdistelyn myötä sektoreita tunnistettiin yhteensä 18, joista seitsemän ilmeni selkeästi muita yleisimpinä, ja lisäksi hallinto ja lainsäädäntö erottui joukosta, kun kahdeksasta valtiosta seitsemän mielsi sen kriittiseksi. Täten taulukon avulla voidaan osittain vastata kysymykseen siitä, että mitä kriittinen infrastruktuuri pitää sisällään. Yleisimmät valtioiden kriittiseksi mieltämät sektorit on korostettu tummempana taulukossa.

Tutkimuksen näkökulmasta on edullista huomata, että jokaiselta yleisesti kriittiseksi luokitellulta sektorilta löytyy kyberpohjaisia ominaisuuksia, joita voidaan tarkastella Euroopan unionin kyberturvallisuusstrategian pohjalta.

Esimerkiksi hallinnon ja lainsäädännön tehokkuutta voidaan kyberturvallisuuden näkökulmasta tutkia siten, että millä keinoin kyberturvallisuutta kehitetään ja ylläpidetään lainsäädännön tai päätöksenteon avulla. Myös energiantuotannossa ja -jakelussa, kuljetuksessa ja liikenteessä, elintarviketeollisuudessa, sekä vedenjakelu- ja jätevesijärjestelmissä käytetään niiden prosessien hallintaan erikoistuneita järjestelmiä, joiden suojaamiseen Euroopan unionin kyberturvallisuusstrategiassa otetaan kantaa.

TAULUKKO 1 Kriittisen infrastruktuurin sektorit. Taulukon lähteet Australia (Australian hallitus, 2010), Espanja (CNPIC, 2010), EU (Euroopan komissio, 2005), Kanada (Kanadan hallitus, 2009), Ruotsi (Ruotsin turvallisuusvirasto, 2014), Saksa (Saksan liittovaltion sisäministeriö, 2009), USA (Yhdysvaltain kotimaan turvallisuusvirasto, 2017) ja Viro (Viron puolustusministeriö, 2008.

	Australia	Espanja	EU	Kanada	Ruotsi	Saksa	USA	Viro
Avaruus ja tutkimus		X	X					
Elintarviketeollisuus	X	X	X	X	X	X	X	X
Energiantuotanto- ja jakelu	X	X	X	X	X	X	X	X
Hallinto ja lainsäädäntö	X	X		X	X	X	X	X
Hätätilapalvelut						X	X	
Julkiset tilat							X	
Kemianteollisuus		X	X				X	X
Kriittinen perusteollisuus				X	X		X	
Liikenneinfrastruktuuri	X	X	X	X	X	X	X	X
Media ja maamerkit						X		
Padot							X	
Pankki- ja rahoitusala	X	X	X	X	X	X	X	X
Puolustus ja puolustusteollisuus				X	X		X	
Terveydenhuolto	X	X	X	X	X	X	X	X
Tieto- ja viestintäteknologia	X	X	X	X	X	X	X	X
Vakuutukset					X			
Vedenjakelu	X	X	X	X	X	X	X	X
Ydinvoima ja ydinjäte		X	X				X	X

3.3 Kriittisen infrastruktuurin ohjausjärjestelmät

Kriittisen infrastruktuurin osaksi voidaan katsoa valtion toiminnalle tärkeät teollisuuden alat ja yritykset, jotka tuottavat yhteiskunnan kannalta elintärkeitä palveluita. Näihin palveluihin lukeutuvat esimerkiksi luotettavasti toimiva sähköverkko, elintarvikkeiden jakeluketju ja vedenjakelu. Vedenjakelulla, energiateollisuudella ja elintarviketeollisuudella on yhteistä se, että niiden tarpeisiin

räätälöidyillä ohjausjärjestelmillä on suuri rooli kullekin ominaisten päivittäisten toimintojen sujuvuudessa.

Teollisuuden ohjausjärjestelmillä (engl. industrial control systems) tarkoitetaan laitetta tai laitteiden yhdistelmää, jonka avulla koneellisten prosessien valvonta, hallinta ja sääntely voidaan suorittaa koneellisesti (Wei & Ji, 2010). Yleensä niiden avulla pyritään saavuttamaan hallinta maantieteellisesti hajautuneista toiminnoista, kuten jakelujärjestelmistä, joita ovat esimerkiksi vedenjakelu- ja jätevesijärjestelmät, energianjakelujärjestelmät, tai raideliikenteen järjestelmät. Ohjausjärjestelmiä voidaan toisaalta käyttää myös tuotantoprosessien hallinnassa ja valvonnassa. Tuotanto- ja jakeluprosesseissa hyödynnettävät järjestelmät voivat olla toiminnoiltaan hyvin samanlaisia, mutta niiden suurin ero on toiminnan mittakaavassa. Tuotantoprosessien suorittaminen on usein mahdollista varsin paikallisesti, jolloin järjestelmän tiedonsiirto on mahdollista suorittaa lähiverkon (engl. LAN) kautta nopeasti ja luotettavasti. Jakelujärjestelmille ominaista on puolestaan laaja toiminta-alue, sillä esimerkiksi veden- ja sähkönjakelun tapauksessa etäisyys tuotantolaitoksen, keskitetyn hallinta-aseman, etähallinta-aseman ja loppuasiakkaan välillä voi olla hyvin pitkä, minkä vuoksi järjestelmät saattavat kattaa hyvin suuria alueita. Pitkien etäisyyksien vuoksi jakelujärjestelmät hyödyntävät laajaverkkoa (engl. WAN), jonka kautta tapahtuvassa tiedonsiirrossa voi etäisyyden vuoksi ilmetä viiveitä ja tiedon katoamista. (Stouffer, Falco & Scarfone, 2011.)

Esimerkkejä teollisuuden ohjausjärjestelmistä ovat muun muassa SCADA-järjestelmät (engl. Supervisory Control And Data Acquisition systems), hajautetut ohjausjärjestelmät (engl. Distributed Control Systems, DCS) ja PLC-logiikat (engl. Programmable Logic Controllers). SCADA-järjestelmiä hyödynnetään hajautuneiden toimintojen, kuten sähkönjakelu-, vedenjakelu- tai raideliikenteen järjestelmien hallinnassa, joissa keskitetty tiedonkeruu ja hallinta ovat tärkeitä. DCS:tä voidaan parhaiten hyödyntää paikallisten tuotanto- ja valmistusjärjestelmien hallinnassa, joista esimerkkeinä vesi- ja jätevesihuollossa tai sähkövoimalaitoksissa hyödynnettävät järjestelmät. SCADA- ja DCS-järjestelmiä hyödynnetään usein myös toisiinsa liittyneinä esimerkiksi sähkövoimalaitoksissa, joissa DCS:llä voidaan ohjata tuotantoa SCADA-järjestelmän tarjoamien siirto- ja jakeluvaatimusten avulla. PLC-logiikoita hyödynnetään DCS- ja SCADA-järjestelmissä ohjauskomponentteina prosessien paikallisen hallinnan tarjoamiseksi. PLC:tä voi käyttää myös ensisijaisena ohjaimena pienemmissä erillisten prosessien ohjausjärjestelmissä, kuten autojen kokoonpanolinjojen ja voimalaitosten noenpuhaltimen toiminnan ohjaamisessa. (Macaulay & Singer, 2016; Stouffer ym., 2011; Wei & Ji, 2010.)

Ohjausjärjestelmistä erityisesti SCADA-järjestelmät ovat yleensä varsin eristettyjä järjestelmiä, ja ne on räätälöity juuri niiden hallitsemaa ja valvomaa prosessia varten. Ne keräävät esimerkiksi jakelua koskevat tiedot keskitetylle hallinta-asemalle, jossa tiedon pohjalta toimintaa voidaan ohjata reaaliaikaisesti. Teollisuuden ohjausjärjestelmille on kuitenkin ominaista niiden pitkä ikäisyys, minkä vuoksi niiden turvallisuuden päivittäminen ja paikkaaminen on haasteellista, jolloin esimerkiksi järjestelmän virustorjunta ja palomuuri voivat olla

puutteellisia (Macaulay & Singer, 2016). Vanhoja teknologioita on alettu korvaamaan laajasti saatavilla olevilla ja edullisilla verkkoprotokollia tukevilla laitteilla, jolloin teollisuuden ohjausjärjestelmät mukailevat entistä enemmän tavallisia ja yhdistettäviä tietojärjestelmiä, vaarantaen siten eristyneisyytensä ja turvallisuutensa (Stouffer ym., 2011). Yhdistettävyyden myötä ohjausjärjestelmien etähallinta mahdollistuu, mutta yhteys yritysverkkoon voi puolestaan altistaa ne verkon kautta tapahtuville kyberhyökkäyksille. (Karabacak & Tatar, 2014.) Toisaalta Stuxnet osoitti, että nykyisin merkittävää vahinkoa voi saada aikaan ilman verkkoyhteyttäkin, hyödyntämällä esimerkiksi inhimillistä tekijää, jolla on suora pääsy järjestelmän tarkoin suojattuihin osiin. Stuxnet oli suunniteltu iskemään teollisuuden ohjausjärjestelmistä PLC-logiikoihin, jotka se asetti uudelleen siten, että ne lähettivät haitallisia komentoja sentrifugeja ohjaaville toimilaitteille (Bologna, Fasani & Martellini, 2013; Stouffer ym., 2011).

Teollisuuden ohjausjärjestelmien pettäessä seurauksena on lähes aina laajoja ja välittömiä fyysisiä seurauksia. Hyökkäykset näihin kriittisiin järjestelmiin voivat johtaa muun muassa virtapiikkeihin, veden- ja energianjakelun katkoksiin tai prosessin hallinnan menettämiseen. (Macaulay & Singer, 2016.) Elintarviketeollisuudessa hyökkäyksen seuraukset voivat ilmetä häiriöinä tuotanto-, varasto- ja kuljetusjärjestelmissä (Marten & Atalan-Helicke, 2015). Voidaan siis sanoa, että ohjausjärjestelmien merkitys kriittisten sektorien, kuten elintarvikealan, sähkön- ja vedenjakelun sekä liikenneinfrastruktuurin toimintojen suojaamisessa on huomattava, minkä vuoksi niiden suojaamiseen liittyvät vastuut tulisi olla yksiselitteisesti ja selkeästi määritelty. Siitä päästäänkin seuraavan alaluvun aiheeseen, joka käsittelee kriittisen infrastruktuurin omistajuutta, sekä julkisten ja liiketoiminnallisten toimijoiden yhteistyön haasteita sektorien suojaamisessa.

3.4 Kriittisen infrastruktuurin omistajuus

Useimmissa tapauksissa kyberfyysiset järjestelmät muodostavat perustan valtion kriittiselle infrastruktuurille, minkä vuoksi kyberjärjestelmiin kohdistuvilla hyökkäyksillä voi olla suuret vaikutukset yhteiskunnan fyysisiinkin rakenteisiin (Ten, Manimaran & Liu, 2010). Voisi luulla, että järjestelmien altistuminen niin fyysisille kuin kyberpohjaisille uhille motivoisi varmistamaan riittävän suojauksen, mutta nykypäivän kriittiset järjestelmät voivat olla turvattomia, kompleksisia ja verkottuneisuuden vuoksi toisistaan riippuvaisia (Lazari, 2014). Verkottuneisuuden ja riippuvuuksien vuoksi häiriöt yhdellä sektorilla voivat johtaa ketjureaktioon aiheuttaen häiriöitä myös muilla sektoreilla (Stouffer, Falco & Scarfone, 2011; Ten, Manimaran & Liu, 2010). Esimerkiksi tietoliikenneyhteydet koostuvat oikeastaan kokonaan tietoteknologioista, jotka nojaavat luotettavaan sähkönjakeluun. Sähkö on siitä ongelmallinen tuote, ettei sille ole korviketta, minkä takia sähkönjakelun ja -tuotannon turvallisuusratkaisuilla on suora vaikutus kansalliseen ja kansainväliseen turvallisuuteen. Kriittisen infrastruktuurin tärkeys ja verkottuneisuus tekee siitä houkuttelevan kohteen niin valtiollisille toimijoille, kuin yksittäisille toimijoille ja hakkeriryhmille. Kriittiseen

infrastruktuuriin kohdistuvien kyberhyökkäysten määrän kasvu onkin Foremanin (2017) mukaan väistämätöntä lähitulevaisuudessa ja puutteet valtioiden ja yritysten valmiudessa nykyisellään tulevat johtamaan merkittäviin yhteiskunnallisiin häiriöihin.

Oman haasteensa kriittisten infrastruktuurien suojaamiseen tuo se seikka, että suurin osa niistä on yksityisomistuksessa. Esimerkiksi Internet-palveluntarjoajat ja energiayhtiöt tarjoavat palveluitaan niin valtiollisille, kaupallisille, kuin yksittäisille toimijoille. (Geers, 2009.) Valtioiden, valtion yritysten ja yksityisyritysten välisten suhteiden merkitystä kriittisen infrastruktuurin suojaamisessa ei siis voida vähätellä. Julkisilla ja yksityisillä tahoilla saattaa kuitenkin olla vaikeuksia toistensa tarpeiden ymmärtämisessä. (Black, 2014.) Yritykset, jotka tarjoavat kriittisen infrastruktuurin kannalta välttämättömiä palveluita ovat usein pörssiyhtiöitä, joiden tavoitteena on olla vastuullisia, tuottavia ja sidosryhmiä hyödyttäviä. Tällöin merkittävät turvallisuusinvestoinnit saatetaan nähdä lähinnä lisätaakkana, joista ei välttämättä ole konkreettista hyötyä liiketoiminnassa. (Quigley, 2013; Euroopan unionin kyberturvallisuusstrategia, 2013.) Esimerkiksi teollisuuden ohjausjärjestelmissä havaittujen turvallisuuspuutteiden paikkaaminen jälkikäteen saatetaan nähdä yritysjohdossa vain kulueränä ilman liiketoiminnallista hyötyä. Valtiot puolestaan haluaisivat varmistaa kriittisen infrastruktuurinsa kannalta välttämättömän palvelunsaannin, joka on sekä tehokas, luotettava ja turvallinen (Black, 2014).

Blackin (2014) mukaan valtioiden ja virastojen tulisikin huomioida kriittisen infrastruktuurinsa suunnittelussa kansainvälisten yritysten resilienssi, eli kriisinsietokyky, jolla tarkoitetaan tässä tapauksessa yrityksen 1) kykyä säilyttää toimintakyky muuttuvissa olosuhteissa ja 2) valmiutta ja palautumiskykyä kohdatessaan häiriöitä ja kriisejä. Yritys voisi olla esimerkiksi energiayhtiö, jonka voimalaitokseen kohdistunut kyberhyökkäys voi lamauttaa alueellisen tai jopa valtiollisen sähkönjakelun kokonaan, mutta yritykselle se ei välttämättä ole suuri ongelma, koska sillä voi olla maailmanlaajuisesti niin paljon korvaavia resursseja, ettei yhden voimalaitoksen menettäminen vaikuta merkittävästi sen liiketoimintaan. Valtioiden ja virastojen tulisikin varmistaa, että kriittisen infrastruktuurin kannalta tärkeät yritykset ovat motivoituneita ja sitoutuneita ylläpitämään palveluidensa turvallisuutta ja jakelun luotettavuutta, jotta yhteiskunnan kannalta kriittiset toiminnot pysyvät toiminnassa. Joissain tapauksissa valtiollinen toimija voi tarjota yritykselle taloudellista tukea ja rahoitusta. (Black, 2014.) Yksityistä sektoria voitaisiin motivoida korkeatasoiseen kyberturvallisuuteen myös kannustimien avulla, kun kyberturvallisuudeltaan korkeatasoiset yritykset voisivat esimerkiksi käyttää korkeasta laadusta kieliviä kyberturvallisuusmerkintöjä tuotteissaan ja palveluissaan, saavuttaen siten kilpailuetua (Euroopan komissio, 2017; Euroopan unionin kyberturvallisuusstrategia, 2013). Julkisen sektorin osallistuminen kriittisestä infrastruktuurista vastaavien yritysten turvallisuuspolitiikkaan saattaa yksityisyritysten näkökulmasta hidastaa esimerkiksi kyberturvallisuuslinjausten luomisprosessia, sillä julkisen ja yksityisen toimijan toimintatavat usein eroavat toisistaan nopeuden ja joustavuuden osalta. Jotta julkisen ja yksityisen sektorin yhteistyö olisi saumatonta, tulisi valtiojohdolla ja virastoilla

olla parempi ymmärrys kansainvälisten yritysten toiminnasta ja liiketoimintamalleista. Siten kriittistä infrastruktuuria koskevat turvallisuusratkaisut voitaisiin linjata mahdollisimman tehokkaasti. (Black, 2014.) Toisin sanoen julkinen sektori laahaa usein kilpailukyvyltään ja organisaatiodynamiikaltaan perässä, joten kyseisten ominaisuuksien kehittäminen parantaisi tiedonvaihdon ja linjauksien toimeenpanon laatua ja nopeutta yksityisen sektorin kanssa (Quigley, 2013).

Kriittisen infrastruktuurin suojaaminen voi siis olla haastava, kallis ja aikaa vievä prosessi. Vaikka julkisen ja yksityisen sektorin yhteistyössä on saattanut olla vaikeuksia menneisyydessä, niin nykyisin niiden kumppanuus nähdään edellytyksenä kriittisen infrastruktuurin tehokkaassa suojaamisessa. Kansainvälisillä yrityksillä on yleensä huippuosaamista ja teknologiaa, joiden avulla kriittisiä palveluita tuotetaan, sekä turvallisuusuhkia tunnistetaan ja torjutaan. Yhdistämällä yksityissektorin tietotaidon, liiketoimintamallit ja ketteryyden julkissektorin tietoon, rahoitukseen ja asiantuntijuuteen saadaan yhdistelmä, josta molemmat osapuolet hyötyvät. Valtio saa alan huippuosaamista kriittisen infrastruktuurin ympärille, kun taas yritys kehittää toimintansa turvallisuutta ja säästää kustannuksissa julkishallinnollisen kumppanuuden ansiosta.

4 Kyberturvallisuusvastuut ja -toimet kriittisen infrastruktuurin suojaamisessa

Tämä luku käsittelee tutkimustuloksia, jotka on selkeyden vuoksi jaettu kolmeen alalukuun. Ensimmäinen alaluku käsittelee ei-teknisiä kyberturvallisuustoimia, joita voidaan soveltaa kriittisen infrastruktuurin suojaamisessa sektorista riippumatta. Toinen alaluku keskittyy teollisuuden ohjausjärjestelmien kyberturvallisuuteen. Kolmannessa alaluvussa käsitellään puolestaan kriittisen infrastruktuurin sektoreita ja niiden suojaamiseen liittyviä sektorikohtaisia vastuita, suojattavia kohteita ja suojaustoimia. Luvun tavoitteena on vastata asetettuun tutkimuskysymykseen ja koostaa lukijalle yleiskuva suomalaisesta kriittisen infrastruktuurin suojaamisesta.

4.1 Useilla sektoreilla sovellettavat kyberturvallisuustoimet

Tutkittaessa suomalaisen kriittisen infrastruktuurin suojaamisessa hyödynnettäviä kyberturvallisuuden keinoja, selvisi useita poikkisektorillisia kyberturvallisuustoimia, joita niin Euroopan unionin kyberturvallisuusstrategia, kuin tieteellinen kirjallisuus suosittelevat hyödynnettäviksi. Koska näille keinoille on yhteistä se, että ne ovat ei-teknisiä vastatoimia, joiden ytimessä ovat yhteistyö, tietoisuus ja turvallisuuslinjaukset, niin niitä voidaan yhtä lailla käyttää muun muassa teollisuuden ohjausjärjestelmien, pankki- ja rahoitusalan tai terveydenhuollon kyberturvallisuuden kehittämiseen.

Kyberturvallisuuteen liittyvien linjausten ja toimintatapojen suhteen Euroopan unionin kyberturvallisuusstrategia (2013), Luiijf ym. (2013) ja Weiss (2013) ohjeistavat sekä organisaatioita että valtioita toteuttamaan strategiatasolla suoritettavan riskianalyysien ja kyberturvallisuuslinjausten päivittämisen. Uhkien muovautuessa teknologian kehityksen tahtiin, ajantasaisilla ja sopeutuvilla linjauksilla ja riskianalyyseilla on tärkeä osa kyberuhkien tunnistamisessa ja ehkäisyssä. Kyberturvallisuuslinjausten päivittämisessä voidaan hyödyntää muun muassa optimaalista määrää selkeästi muotoiltuja sääntöjä, jotka auttavat minimoimaan inhimillisen tekijän aiheuttamaa riskiä ja maksimoimaan kyberjärjestelmien resilienssiä. Inhimillinen tekijä voidaankin usein nähdä suurimpana uhkana turvallisuudelle, mutta ihmisen aiheuttamaa organisaation haavoittuvuutta voidaan vähentää lisäämällä työntekijöiden tietoisuutta turvallisuuteen liittyvistä tekijöistä. Jos organisaatio haluaa olla turvallinen, se ei voi rajata turvallisuuskoulutusta ainoastaan tietokoneen ääressä työskenteleville, vaan kaikki organisaation jäsenet tulee ottaa mukaan. (Karabacak & Tatar, 2014.) Liian tiukka tai löysä sääntely voi toisaalta johtaa järjestelmän haavoittuvuuteen ja siten pienempään resilienssiin. Esimerkiksi turvallisuutta koskevan sääntelyn ollessa liian laaja kokonaisuus työntekijöiden sisäistettäväksi hetkessä, sen kouluttamiseen kuluva aika on pois työajasta, jolloin töiden suorittaminen lyhyemmässä

ajassa voi stressin kautta johtaa tehokkuuden laskuun ja virhealttiuden kasvuun. Gisladottir, Ganin, Keisler, Kepner & Linkov (2017) ovat kehittäneet viitekehyksen, jonka avulla sääntely voidaan optimoida tasolle, jossa riskien minimointi ja resilienssin maksimointi kohtaavat. Epäselvyyksien välttämiseksi myös sisäisen kyberturvallisuusstrategian kytkökset olemassa oleviin turvallisuusstrategioihin ja -linjauksiin tulisi määritellä (Luiijf ym., 2013).

Jokaisen organisaation, oli kyseessä valtio tai yritys, tulisi määritellä mitä sisäinen kyberturvallisuus kattaa, jotta yhteistyökumppaneilla olisi kuva eroavaisuuksista ja yhteneväisyyksistä organisaatioiden yhteisen kyberturvallisuuden harjoittamiseksi. Paras mahdollinen tilanne olisi, että organisaatioilla olisi harmoninen käsitys kyberturvallisuudesta, mutta organisaatioiden yksilöityjen käsitysten muodostumiseen vaikuttaa muun muassa niiden vallitseva toimintaympäristö ja kulttuuri. (Luiijf, ym., 2013.) Lisäksi yhteistyö valtioiden, yritysten ja kansalaisten kanssa nähdään korvaamattomana vastatoimena taistelussa kyberuhkia vastaan. Ennen kaikkea yhteistyö kriittisen infrastruktuurin omistajien kanssa on valtiolle välttämätöntä, ja riippuen kyberuhkan tyypistä, organisaatioiden tulisi harjoittaa yhteistoimintaa eri osapuolten kanssa. Esimerkiksi yhteistyö Internet-palveluntarjoajien ja CERT-ryhmien kanssa on merkittävä vastatoimi haktivismia kohtaan, kun taas kyberrikollisuutta vastaan taisteleminen edellyttää yhteistyötä lainvalvonnan ja lainsäädännön kanssa. Kybersodankäynnillisten toimien torjumiseksi tulisi puolestaan liittoutua CERT-ryhmien ja toisten valtioiden kanssa, ja kybervakoilua voitaisiin torjua yhteistyössä kansalaisten, työntekijöiden ja huipputeknologioiden valmistajien kanssa. (Karabacak & Tatar, 2014.) Varsinkin Internet-palveluntarjoajia halutaan tuoda suuremmaksi osaksi yhteistyötä, jotta ne voisivat tarjota kuluttajille ja yrityksille ajantasaisia kyberturvallisuuden työkaluja, kuten erilaisia salaus-, tunnistus- ja suojausohjelmia. Internet-palveluntarjoajien ja kriittisen infrastruktuurin omistajien olisi hyvä harjoittaa avointa matalan kynnyksen viestintää, jonka avulla voitaisiin esimerkiksi pitää osapuolten tilannekuvaa yllä verkkoliikennöinnin piikkien suhteen. (Luiijf ym., 2013; Karabacak & Tatar, 2014.)

Suomen elintärkeitä toimintoja ja niiden suojaamisessa hyödynnettäviä toimintamalleja käsittelevässä Yhteiskunnan turvallisuusstrategiassa (2017) korostetaan muun muassa kansallisen, kansainvälisen, sekä pohjoismaisen yhteistyön merkitystä. Oikeastaan jokaisen kriittisen infrastruktuurin sektorin suojaamiseen liittyvissä toimenpiteissä mainitaan yhteistyö vastuuministeriöiden, julkisen sektorin, valtion yritysten tai yksityisyritysten välillä. Tämä myötäilee myös Euroopan unionin kyberturvallisuusstrategiaa, joka korostaa viestinnän avoimuutta yhteistyöosapuolten välillä ja raportoinnin merkitystä kyberviranomaisille. Lisäksi Yhteiskunnan turvallisuusstrategiassa mainitaan yhteistoiminnan ja kyberturvallisuusharjoitusten merkityksestä kyberuhilta suojautumisessa, jota myös EU:n kyberturvallisuusstrategia ajaa kansallisilla ja kansainvälisillä kyberturvallisuutta testaavilla harjoituksilla. (Euroopan unionin kyberturvallisuusstrategia, 2013; Yhteiskunnan turvallisuusstrategia, 2017.)

Edellä mainituilla ei-teknisillä vastatoimilla valtio, yritykset kuin kansalaisetkin voivat ottaa vastuun uskottavan resilienssin, pelotteen ja puolustuksen

luomisessa. Oikeastaan kaikkia tässä luvussa käsiteltyjä ei-teknisiä toimia voidaan hyödyntää kriittisen infrastruktuurin suojaamisessa sektorista riippumatta. Kyberturvallisuuteen liittyvien vastuiden määrittelyllä, toimenpiteillä ja linjauksilla on positiivinen vaikutus tilannetietoisuuteen ja valmiuteen, joilla on resilienssiä vahvistava vaikutus. Myös yhteiskunnan toimijoiden tietoisuuden lisääminen kehittää valveutuneisuutta kyberturvallisuuden uhkia ja suojautumiskeinoja kohtaan, jolloin yhteiskunnan kriisinsietoisuus kasvaa. Tietoisuuden lisäämisellä kehitetään tavallaan myös pelotetta, sillä yritysten ja kansalaisten tullessa tietoisemmiksi suojautumiskeinoista ja turvallisista teknologioista, niitä todennäköisemmin myös hyödynnetään enemmän. Toisin sanoen motivaatiota kyberhyökkäysten suorittamiseen on mahdollista laskea turvallisten teknologioiden ansiosta, niiden mahdollistaessa hyökkäysten torjunnan ja hyökkääjien jäljittämisen. Puolustusta voidaan puolestaan kehittää kansallisen ja kansainvälisen yhteistyön voimin, jonka ytimessä nähdään yhteisymmärrys kyberturvallisuuden laajuudesta. Kansallinen yhteistyö rakentuu kattavasta vastuuministeriöiden, julkisen sektorin, viranomaisten ja yksityisyritysten yhteistyöstä ja -toiminnasta. Kansainvälistä yhteistyötä voidaan harjoittaa erilaisin yhteistoimintaharjoituksin, joissa sekä julkiset kuin yksityisetkin osapuolet voivat olla osallisina.

4.2 Teollisuuden ohjausjärjestelmien kyberturvallisuus

Tarkasteltaessa kriittisten sektorien suojattavia kohteita voidaan huomata, että kahdeksasta sektorista neljä, eli puolet, hyödyntävät jollain tavalla teollisuuden ohjausjärjestelmiä prosessiensa valvonnassa, hallinnassa tai sääntelyssä. Nämä neljä sektoria ovat elintarvikeala, energiantuotanto ja -jakelu, liikenneinfrastruktuuri, sekä vedenjakelu- ja jätevesijärjestelmät. Alat hyödyntävät omien tarpeidensa mukaan joko tuotanto- tai jakelujärjestelmiä, tai niiden yhdistelmiä, mutta kaikkiin niihin voidaan soveltaa pitkälti samoja suojaustoimia.

Alun perin teollisuuden ohjausjärjestelmien suunnittelussa on turvallisuuden sijaan keskitytty toimivuuteen ja luotettavuuteen, mutta niiden turvallisuutta vaarantavat kyberuhat, inhimilliset tekijät ja monimutkaisten verkkojen epävarmuustekijät ovat asettaneet ohjausjärjestelmien suunnittelulle uusia vaatimuksia (Rieger, Gertman & McQueen, 2009). Useiden lähteiden mukaan kriittisten järjestelmien tapauksessa turvallisuus tulisi suunnitella sisällytettäväksi järjestelmiin jo valmistusvaiheessa, jolloin ainakin suurimmilta jälkikäteen suoritettavilta turvallisuusratkaisujen toteutuksilta ja järjestelmien käyttökatkoksilta vältyttäisiin. (Bloomfield, Bendele, Bishop, Stroud & Tonks, 2016; Karabacak & Tatar, 2014; Euroopan unionin kyberturvallisuusstrategia, 2013; Amoroso, 2012). Esimerkkejä sisäänrakennettavista turvallisuusmekanismeista ovat muun muassa palomuurit, tunkeutumisen havaitsemisjärjestelmät ja salaukset, jotka muodostavat osan kriisinsietoista teollisuuden ohjausjärjestelmää (Wei & Ji, 2010). Kriisinsietoinen, eli resilientti teollisuuden ohjausjärjestelmä on sellainen, jonka suunnittelulla ja käytöllä pyritään:

- minimoimaan kyberturvallisuuspoikkeamien esiintyvyyttä
- lievittämään toteutuneita kyberturvallisuuspoikkeamia
- minimoimaan häiriötilanteista koituvia seurauksia
- palautumaan häiriötilanteista nopeasti

Kyberturvallisuuspoikkeamien esiintyvyyttä voidaan minimoida käyttämällä omia viestintälinjoja, eristämällä automaatioverkko yritysverkosta tai hyödyntämällä salausta. Minimoimalla poikkeamien esiintyvyyttä pystytään vähentämään järjestelmään kohdistuvaa painetta, joka tarkoittaa myös toteutuneiden kyberturvallisuuspoikkeamien vähentymistä. Silti toteutuneitakin poikkeamia voidaan vielä lievittää muun muassa hyvin sijoitetuilla palomuureilla. Esimerkiksi sähköverkon automaatioverkon ollessa yhteydessä yritysverkkoon syntyy kyberuhka, mutta uhkaa voidaan lievittää suojaamalla verkkoja yhdistävä tiedonsiirtoportti palomuurilla, joka tunnistaa tunkeilijat ja suodattaa haitalliset datapaketit. Myös sopivilla turvallisuuskäytänteillä, kuten pääsynhallinnalla ja tunkeutumisen havaitsemisprofiililla voidaan lieventää suurinta osaa kyberhyökkäyksistä. Kyberturvallisuuspoikkeamien aiheuttamien häiriötilanteiden vaikutuksia voidaan minimoida suunnittelemalla esimerkiksi sähköverkon ohjausjärjestelmän tunnistamaan sen osiin kohdistuvat hyökkäykset, jolloin esimerkiksi hyökkäyksen kohteena olevan sähköverkon sivuaseman sähkövirta voidaan ohjata muille sivuasemille (Wei & Ji, 2010). Mikäli tunkeutumisen havaitsemisjärjestelmiä hyödynnetään, niin niiden keräämä data häiriötilanteista voidaan puolestaan lähettää valvoville kyberviranomaisille, jolloin häiriötilanteen aiheuttajat on mahdollista jäljittää ja asettaa vastuuseen toimistaan. Jäljittäminen ja tutkinta on kuitenkin tähän asti ollut haastavaa yhä laajalti hyödynnettävän IPv4 protokollan vuoksi, joka mahdollistaa tuhansien käyttäjien sijoittamisen saman IP-soitteen taakse (Euroopan komissio, 2017). Tehdäkseen muutoksen tilanteeseen, Euroopan komissio (2017) rohkaisee IPv6:n yleistyvää käyttöönottoa, minkä myötä yksi IP-osoite voitaisiin osoittaa kullekin käyttäjälle, helpottaen siten lainvalvontaa ja kyberturvallisuustutkintaa. Tällöin tulee kuitenkin varmistua siitä, että kriittiset ohjausjärjestelmissä käytetään sekä IPv4 että IPv6 liikennettä tukevia ja tunnistavia teknologioita, kuten palomuureja, kytkimiä ja reitittimiä (Macaulay & Singer, 2016). Viimeinen ohjausjärjestelmien kriisinsietoisuuden osa-alue liittyy häiriötilanteista palautumiseen, jota voidaan nopeuttaa suunnittelemalla ohjausjärjestelmän tunnistamaan ja paikallistamaan hyökkäykset, jolloin hyökkäykset voidaan lyhyessä ajassa eristää tai uudelleenohjata muualle, minkä jälkeen suorituskyky voi palata normaaliksi. (Wei & Ji, 2010.) Resilientti ohjausjärjestelmä on siis sellainen, joka on säilyttää tilannetietoisuuden ja määrätyn toimintatason odottamattomista ja haitallisista häiriöistä huolimatta.

Teollisuuden ohjausjärjestelmistä SCADA-järjestelmien kyberturvallisuutta voidaan arvioida käyttämällä erilaisia haavoittuvuusanalyysi-, simulaatio- ja mallintamistekniikoita. Haavoittuvuusanalyysi toteutetaan ohjausjärjestelmään kohdistuvilla toistuvilla hyökkäyksillä. Haavoittuvuuksien paljastamisen lisäksi haavoittuvuusanalyysiä voidaan hyödyntää myös järjestelmän virheilmoitusten määrittämisessä, minkä ansiosta järjestelmää on mahdollista

ymmärtää paremmin ja tarjota siten sen haavoittuvuuksien paikkaamiseen tarvittavat toimet. Tunkeutumistestaukset ja haavoittuvuusanalyysit voidaan nähdä tehokkaina tekniikoina SCADA-järjestelmän kyberhaavoittuvuuksien ja -turvallisuuden arvioinnissa. (Ten, Liu & Manimaran, 2010.) Toisaalta liian kovaotteisilla testeillä on havaittu olevan haitallisia vaikutuksia teollisuuden ohjausjärjestelmien toimivuuteen, joten sopivien tekniikoiden valintaan tulee kiinnittää huomiota. Esimerkiksi Duggan, Berg, Dillinger & Stamp (2005) ovat selvittäneet niin sanottuja pehmeitä tekniikoita, joita voi hyödyntää tunkeutumistestauksissa ja haavoittuvuusanalyyseissä ilman järjestelmän vaurioitumista.

Edellä mainitut kyberturvallisuustoimet tarjoavat hyvän perustan kaikkien teollisuuden ohjausjärjestelmien jatkuvan toimivuuden ja luotettavuuden varmistamiseksi. Ehkäisemällä uhkien syntymistä ja lievittämällä syntyneitä uhkia, sekä minimoimalla seurauksia ja palautumalla nopeasti häiriötilanteista luodaan parempaa kriisinsietoisuutta. Haavoittuvuuden testaustekniikoilla voidaan puolestaan tunnistaa aukot suojauksessa omilla ehdoilla ja paikata ne ennen kuin niitä hyödynnetään kyberhyökkäysten läpäisypisteinä. Osiltaan resilienssin parantamiseen osallistuvat myös kehittyneet teknologiat, kuten tunkeutumisen havaitsemisjärjestelmät ja IPv6, joiden avulla häiriötilanteiden aiheuttajat on mahdollista tunnistaa ja jäljittää. Tunnistaminen ja jäljittäminen puolestaan mahdollistavat paremman kyberturvallisuustutkinnan, joka tuottaa siten tehokkaamman pelotteen kybertoimintaympäristön väärinkäytösten vähentämiseksi.

4.3 Sektorikohtaiset kyberturvallisuusvastuut ja -toimet

Tutkimuksessa selvisi useita sektorikohtaisia suojaustoimia, jotka on selvyyden vuoksi jaoteltu omiin alalukuihinsa. Taulukoihin 2-9 on tiivistetty keskeisimmät tiedot koskien sektorikohtaisia vastuita, suojauskohteita ja suojaustoimia. Sektorit, joiden yleisesti katsotaan kuuluvan kriittiseen infrastruktuuriin löytyvät kunkin taulukon riveiltä, kun taas pitkälti tutkimuskysymystä täydentävät kysymykset löytyvät sarakkeista. Taulukoiden soluista saadaan siten tiedot kunkin kriittisen sektorin vastuista, suojauskohteista ja suojaustoimista. Suomalaisen kriittisen infrastruktuurin vastuulliset ja suojauskohteet on pitkälti selvitetty hyödyntämällä Yhteiskunnan turvallisuusstrategiaa (2017) ja Kyberturvallisuuskeskuksen (2019a) vastuuviranomaiskartoitusta, joissa pääpiirteiset vastuut ja toimintamallit yhteiskunnan elintärkeiden toimintojen suojaamiseksi on kuvailtu. Riippuen sektorista, suojaustoimet saattavat yhteiskunnan turvallisuusstrategiassa lueteltujen toimien lisäksi sisältää kirjallisuudesta löydettyjä täydennyksiä ja ehdotuksia.

4.3.1 Elintarvikeala

TAULUKKO 2 Elintarvikeala

	Kuka vastaa? (Yhteiskunnan turvallisuusstrategia, 2017; Kyberturvallisuuskeskus, 2019a)	**Mitä suojataan?** (Yhteiskunnan turvallisuusstrategia, 2017)	**Miten suojataan?**
Elintarvikeala	**Julkinen:** Metsä- ja maatalousministeriö, viestintä- ja liikenneministeriö, sekä energiavirasto **Yksityinen:** Tuotannosta, prosessoinnista ja jälleenmyynnistä vastaavat yritykset	-Tärkein ruoantuotanto ja -jakelu -Toimitusketjun turvallisuus ja luotettavuus -Yritysverkko ja teollisuuden ohjausjärjestelmät	- Pilvi- ja sumupohjainen kyberfyysinen järjestelmä (Davcev ym., 2018; Chen, 2017) - Lohkoketjuteknologia (Davcec ym., 2018) - Salaus, palomuurit, tunkeutumisen havaitsemisjärjestelmät (Wei & Ji, 2010) - IPv4/v6 teknologiat (Macaulay & Singer, 2016) - Haavoittuvuusanalyysi-, simulaatio- ja mallintamistekniikat (Ten, Liu & Manimaran, 2010)

Valtioneuvoston elimistä viestintä- ja liikenneministeriö vastaa elintarvikealan kyberturvallisuuden ja jakelun toimivuudesta, kun taas metsä- ja maatalousministeriön tehtävänä on varmistaa tärkein ruoantuotanto (Yhteiskunnan turvallisuusstrategia, 2017). Lisäksi energiavirasto toimii valvovana viranomaisena (Kyberturvallisuuskeskus, 2019a). Elintarvikkeiden tuotannosta, prosessoinnista ja jälleenmyynnistä vastaavien yritysten vastuulla on varmistua siitä, että prosessien suorittamisessa ja valvonnassa hyödynnettävät järjestelmät ovat asianmukaisesti suojattu (Yhteiskunnan turvallisuusstrategia, 2017). Vielä vuonna 2019 kyberturvallisuuskeskuksen teettämässä teollisuuden ohjausjärjestelmien turvallisuutta koskevassa kartoituksessa havaittiin elintarviketeollisuuden yritykselle kuulunutta suojaamatonta PLC-logiikkaa (Kyberturvallisuuskeskus, 2019b). Yksinkertaiset elintarviketeollisuuden ohjausjärjestelmien kyberturvallisuusratkaisut voitaisiin toteuttaa esimerkiksi implementoimallaIPv4 ja v6 liikennettä tukevia ja tunnistavia palomuureja, reitittimiä ja kytkimiä osaksi järjestelmiä (Macaulay & Singer, 2016). Myös tilaus- ja toimitusketjun fyysisen ja digitaalisen toimivuuden varmistaminen on keskeinen osa yritysten vastuuta, minkä vuoksi yhteistyö yritysten välillä on merkittävässä roolissa, sillä toimijoiden välisellä tiedonkululla ja yhteistyöllä on suuri merkitys tilannekuvan ylläpidossa. Turvallisuuslinjauksiin ja teollisuuden ohjausjärjestelmiin liittyvien

suojaustoimien lisäksi konkreettisia esimerkkejä koskien elintarvikealaa ei juurikaan löytynyt virallisista asiakirjoista, mutta yritysten resurssisuunnittelun järjestelmien perustuessa reaaliaikaiseen informaatioon, voitaisiin tilaus- ja toimitusketjun tilannekuvan ylläpito ja läpinäkyvyys mahdollistaa sumulaskenta-pohjaisella kyberfyysisellä järjestelmällä (Davcev, Kocarev, Carbone, Stankovski & Mitresk, 2018; Chen, 2017). Lisäksi Davcev ym. (2018) ehdottavat hyödynnettäväksi lohkoketjuteknologiaa, joka läpinäkyvän ja turvallisen toimitusketjun lisäksi tarjoaisi varmuuden ruuan alkuperästä sekä sen tuotantoon, kuljettamiseen ja jakeluun liittyvistä prosesseista. Pilvi- ja sumuteknologiaan ja lohkoketjuteknologiaan pohjautuva järjestelmä mahdollistaisi siis tuottajan, prosessoijan, jälleenmyyjän ja jopa asiakkaan välillä reaaliaikaisen, luotettavan ja turvallisen tiedonkulun.

4.3.2 Energiantuotanto ja -jakelu

TAULUKKO 3 Energiantuotanto ja -jakelu

	Kuka vastaa? (Yhteiskunnan turvallisuusstrategia, 2017; Kyberturvallisuuskeskus, 2019a)	**Mitä suojataan?** (Yhteiskunnan turvallisuusstrategia, 2017)	**Miten suojataan?**
Energiantuotanto- ja jakelu	**Julkinen:** Työ- ja elinkeinoministeriö **Yksityinen:** Fingrid Oyj ja energiayhtiöt	- Voimalaitokset ja jänniteverkko - Yritysverkko ja teollisuuden ohjausjärjestelmät	- Verkon automatisointi ja maanalainen kaapelointi (Yhteiskunnan turvallisuusstrategia, 2017) - Salaus, palomuurit, tunkeutumisen havaitsemisjärjestelmät (Wei & Ji, 2010) - IPv4/v6 teknologiat (Macaulay & Singer, 2016) - Haavoittuvuusanalyysi-, simulaatio- ja mallintamistekniikat (Ten, Liu & Manimaran, 2010)

Energiantuotannon ja -jakelun turvaamisen lisätoimista vastaa työ- ja elinkeinoministeriö. Yrityksistä Fingrid Oyj vastaa kantaverkon käytön suunnittelusta ja valvonnasta, sekä verkon ylläpidosta ja kehittämisestä. Lisäksi energiayhtiöillä on vastuussa käytännön toimenpiteistä energianjakelun turvaamiseksi, joille myös lainsäädäntö luo linjat ja vaatimukset. (Yhteiskunnan turvallisuusstrategia, 2017.) Jänniteverkkoa pyritään suojaamaan maanalaisella kaapeloinnilla ja verkon automatisoinnilla (Yhteiskunnan turvallisuusstrategia, 2017), mutta voimalaitosten, yritysverkon ja teollisuuden ohjausjärjestelmien suojaamiseen

liittyvistä yksityiskohtaisemmista toimista ei mainita julkisissa asiakirjoissa sen tarkemmin. Edeltävässä alaluvussa käsitellyt teollisuuden ohjausjärjestelmiin liittyvät kyberturvallisuuden suojaustoimet sopivat kuitenkin sähköntuotannon ja -jakelun tarpeisiin täydellisesti. Esimerkiksi suunnittelemalla sähköverkon ohjausjärjestelmän tunnistamaan sen osiin kohdistuvat kyberhyökkäykset, voidaan hyökkäyksen kohteena olevan sivuaseman sähkövirta ohjata muille sivuasemille (Wei & Ji, 2010).

4.3.3 Hallinto ja lainsäädäntö

TAULUKKO 4 Hallinto ja lainsäädäntö

	Kuka vastaa? (Yhteiskunnan turvallisuusstrategia, 2017; Kyberturvallisuuskeskus, 2019a)	**Mitä suojataan?** (Yhteiskunnan turvallisuusstrategia, 2017)	**Miten suojataan?**
Hallinto ja lainsäädäntö	**Julkinen:** Valtioneuvosto, talousministeriö, valtiovarainministeriö ja Traficomin kyberturvallisuuskeskus **Yksityinen: J**ulkishallinnolle palveluita tuottavat palvelukeskukset ja yritykset	- Julkisen hallinnon ICT-infrastruktuuri ja digitaaliset palvelut - Julkisen hallinnon turvallisuusverkko ja sen palvelut	- Kyberrikollisuuden torjunta aktiivisella lainsäädännön ja oikeuden kehittämisellä (Yhteiskunnan turvallisuusstrategia, 2017)

Valtioneuvoston kanslian vastuulla on varmistaa valtiojohdon ja ministeriöiden käyttämien tietojen ja digitaalisten palveluiden turvallisuus, kun taas julkisen hallinnon ICT-infrastruktuurin ja digitaalisten palveluiden turvaamisesta vastaa talousministeriö. Valtiovarainministeriö vastaa julkisen hallinnon tietoturvallisuuden yleisestä kehittämisestä ja valtionhallinnon tietoturvallisuuden ohjauksesta, sekä ohjaa tietohallinnon kehitystä valtion- ja kunnallishallinnossa. (Yhteiskunnan turvallisuusstrategia, 2017.) Digitaalisten palveluiden valvovana viranomaisena toimii Traficomin kyberturvallisuuskeskus (Kyberturvallisuuskeskus, 2019a), kun puolestaan julkishallinnolle palveluita tuottavat palvelukeskukset ja yritykset ovat vastuussa käytännön toteutuksista (Yhteiskunnan turvallisuusstrategia, 2017). Sektorin suojaamiseen liittyviä toimia ei suoranaisesti löytynyt, lukuun ottamatta Yhteiskunnan turvallisuusstrategiassa (2017) mainittua osallistumista kyberrikollisuuden torjuntaan kehittämällä kansainvälistä lainsäädäntöä ja oikeutta EU:n puitteissa. Toisaalta tieto- ja viestintäteknologian sektori sisältää varsin samanlaisia aihepiirejä verrattuna hallinnon ja lainsäädännön vastuisiin, joten tieto- ja viestintäteknologioiden suojaustoimia saattaisi olla mahdollista soveltaa osittain tässä tapauksessa.

4.3.4 Tieto- ja viestintäteknologiat

TAULUKKO 5 Tieto- ja viestintäteknologiat

	Kuka vastaa? (Yhteiskunnan turvallisuusstrategia, 2017; Kyberturvallisuuskeskus, 2019a)	**Mitä suojataan?** (Yhteiskunnan turvallisuusstrategia, 2017)	**Miten suojataan?**
Tieto- ja viestintäteknologia	**Julkinen:** Talousministeriö, liikenne- ja viestintäministeriö, viestintävirasto Traficomin kyberturvallisuuskeskus **Yksityinen: Tietoliikenneyritykset ja energiayhtiöt**	- Liikenteen ohjausjärjestelmä, terveydenhuollon järjestelmät, sähköiset verkot, maksujärjestelmät ja julkisen hallinnon turvallisuusverkko	- Laissa säädetyt turvallisuusvaatimukset ja niiden noudattaminen - Julkishallinnollisen ICT-arkkitehtuurin ja tietoturvan yleisten periaatteiden laatiminen - yhteistyö ja säännöllinen testaus (Yhteiskunnan turvallisuusstrategia, 2017.)

Tieto- ja viestintäteknologioiden alueella talousministeriö vastaa kriittisten ICT- ja digipalveluiden tieto- ja kyberturvallisuuteen liittyvistä seikoista. Liikenne- ja viestintäministeriö vastaa sähköisen viestintäverkon toimivuudesta. (Yhteiskunnan turvallisuusstrategia, 2017.) Viestintävirasto vastaa, että Suomessa on monipuoliset ja turvalliset viestintäyhteydet, kun taas liikenne- ja viestintävirasto Traficomin kyberturvallisuuskeskus toimii valvovana viranomaisena (Kyberturvallisuuskeskus, 2019a). Lisäksi tietoliikenneyrityksillä on vastuu omista turvallisuus- ja valmiusjärjestelyistä, joita myös lainsäädäntö ohjaa. Myös energiayhtiöillä on roolinsa palveluiden jatkuvuudessa, koska tieto- ja viestintäteknologiat ovat sähköstä riippuvaisia. (Yhteiskunnan turvallisuusstrategia, 2017.) Palveluiden digitalisoituessa tieto- ja viestintäteknologioilla on merkittävä rooli tietoyhteiskunnassa, ja niiden turvallisuusratkaisuilla on suora vaikutus liikenteen ohjausjärjestelmien, terveydenhuollon järjestelmien sähköverkkojen, maksujärjestelmien ja julkisen hallinnon turvallisuusverkon toimintaan. Sektorin vastuisiin kuuluu muun muassa julkishallinnollisen ICT-arkkitehtuurin ja tietoturvan yleisten periaatteiden laatiminen. Esimerkiksi kriittisille ICT- ja digipalveluille on laadittu turvallisuusvaatimukset, joihin niiden tulee yltää turvallisuuden ja jatkuvuuden alueilla. Näistä esimerkkinä ICT:n laatuvaatimukset tietoturvalaissa. Turvallisen toiminnan takaamiseksi tulisi myös harjoittaa niin kansallista, kuin kansainvälistä yhteistyötä, sekä säännöllistä toiminnan testausta. (Yhteiskunnan turvallisuusstrategia, 2017).

4.3.5 Liikenneinfrastruktuuri

TAULUKKO 6 Liikenneinfrastruktuuri

	Kuka vastaa? (Yhteiskunnan turvallisuusstrategia, 2017; Kyberturvallisuuskeskus, 2019a)	**Mitä suojataan?** (Yhteiskunnan turvallisuusstrategia, 2017)	**Miten suojataan?**
Liikenneinfrastruktuuri	**Julkinen:** Liikenne- ja viestintäministeriö ja tarvittaessa puolustus- ja sisäministeriö **Yksityinen:** Finavia Oyj ja muut liikennealan yritykset	- Satamat, terminaalit, lentokentät, raideliikenne ja maantieliikenne, sekä niiden tietojärjestelmät	- Varajärjestelmät sekä tiivis yhteistyö energia- ja tietoliikenneyritysten kanssa (Yhteiskunnan turvallisuusstrategia, 2017) - Salaus, palomuurit, tunkeutumisen havaitsemisjärjestelmät (Wei & Ji, 2010) - IPv4/v6 teknologiat (Macaulay & Singer, 2016) - Haavoittuvuusanalyysi-, simulaatio- ja mallintamistekniikat (Ten, Liu & Manimaran, 2010)

Liikenne- ja viestintäministeriön tehtävänä on varmistaa liikenneverkoston turvallisuus ja toimivuus. Poikkeustilanteissa myös puolustus- ja sisäministeriöllä on vastuu fyysisen liikenneverkoston turvallisuuden varmistamisessa. Liikenneverkosto koostuu satamista, terminaaleista, lentokentistä, raideliikenteestä ja maantieliikenteestä, joiden toiminnan sujuvoittamiseksi käytetään erilaisia ohjaus- ja liikennejärjestelmiä. Esimerkiksi Finavia Oyj on vastuussa lentokenttien turvallisuudesta ja toimivuudesta, mutta poikkeustilanteissa muillakin liikennealan yrityksillä on roolinsa. Yksi liikenneverkon hallinnassa hyödynnettävistä järjestelmistä on esimerkiksi automaattinen junaliikenteen ja metron hallinta- ja viestintäjärjestelmä, jota voidaan verrata SCADA-järjestelmään. Tällaisten hajautuneidein järjestelmien suojaamisessa voidaan hyödyntää esimerkiksi Wein & Lin (2010) listaamia resilientin ohjausjärjestelmän suojaustoimia, kuten salausta, palomuureja ja tunkeutumisen havaitsemisjärjestelmiä. Lisäksi liikenneinfrastruktuurin suojaamisessa hyödynnetään testattuja varajärjestelmiä ja tiivistä yhteistyötä energia- ja tietoliikenneyritysten kanssa (Yhteiskunnan turvallisuusstrategia, 2017).

4.3.6 Pankki- ja rahoitusala

TAULUKKO 7 Pankki- ja rahoitusala

	Kuka vastaa? (Yhteiskunnan turvallisuusstrategia, 2017; Kyberturvallisuuskeskus, 2019a)	**Mitä suojataan?** (Yhteiskunnan turvallisuusstrategia, 2017)	**Miten suojataan?**
Pankki- ja rahoitusala	**Julkinen:** Talousministeriö **Yksityinen:** Rahoitusmarkkinapalveluita tarjoavat yritykset	- Rahoitusmarkkinoiden ja niitä koskevien palveluiden toiminta - Internet-yhteydet ja -palvelut, sekä pankkijärjestelmät	- Luotettavat ja testatut pää- ja varajärjestelmät -Tiivis yhteistyö ICT- ja kyberturvallisuustoimijoiden kanssa - lainsäädännön ennakointi ja noudattamainen (Yhteiskunnan turvallisuusstrategia, 2017)

Pankki- ja rahoitusalalla on talousministeriön vastuulla varmistaa, että taloudellinen järjestelmä toimii tarkoituksenmukaisesti. Rahoitusmarkkinapalveluita tarjoavat yritykset ovat vastuussa järjestelmiensä turvallisuudesta, toimivuudesta ja laillisuudesta. Euroopan unioni säätelee rahapolitiikkaa koskevia lakeja ja sen piirissä olevien yritysten toimintavaatimuksia. Suojattaviin kohteisiin kuuluvat rahoitusmarkkinoiden ja niitä koskevien palveluiden toiminta. Lisäksi pankkipalveluiden Internet-yhteydet ja -palvelut, sekä järjestelmät ovat tärkeimpiä suojattavia kokonaisuuksia. (Yhteiskunnan turvallisuusstrategia, 2017.) Yhteiskunnan turvallisuusstrategian (2017) mukaan luotettavat ja testatut varajärjestelmät ovat talousalan yritysten turvallisen toiminnan edellytys. Internet-yhteyksien ja palveluiden, sekä pankkijärjestelmien turvallisuus pyritään takaamaan tiiviillä yhteistyöllä ICT- ja kyberturvallisuustoimijoiden kanssa. Myös turvallisuutta koskevan lainsäädännön ennakointi ja noudattaminen parantaa ja varmistaa osaltaan toiminnan turvallisuutta.

4.3.7 Terveydenhuolto ja hyvinvointi

TAULUKKO 8 Terveydenhuolto ja hyvinvointi

	Kuka vastaa? (Yhteiskunnan turvallisuusstrategia, 2017; Kyberturvallisuuskeskus, 2019a)	**Mitä suojataan?** (Yhteiskunnan turvallisuusstrategia, 2017)	**Miten suojataan?**
Terveydenhuolto ja hyvinvointi	**Julkinen:** Sosiaali- ja terveysministeriö, työ- ja elinkeinoministeriö, Valvira ja Kansaneläkelaitos **Yksityinen:** Sosiaali- ja terveyspalveluita tuottavat yritykset ja sote-tietojärjestelmien valmistajat	- Kansallinen sosiaali- ja terveydenhuollon tietolähde - Potilas- ja asiakastietojärjestelmät - Kriittisten järjestelmien sähkönsyöttö	- Varajärjestelmät - Tietojen säilyttäminen Suomessa - Yhteistyön lisääminen (Yhteiskunnan turvallisuusstrategia, 2017) - Kyber-terveys -hanke (Huoltovarmuuskeskus, 2019b)

Terveydenhuollon ja hyvinvoinnin vastuullisia julkisia toimijoita ovat sosiaali- ja terveysministeriö sekä työ- ja elinkeinoministeriö. Terveydenhuolto- ja hyvinvointialan valvovana viranomaisena toimii sosiaali- ja terveysalan lupa- ja valvontavirasto Valvira. Yksi suojattavista kohteista on esimerkiksi kansallinen sosiaali- ja terveydenhuollon tietolähde, jonka ylläpitämisestä Kansaneläkelaitos vastaa. Sosiaali- ja terveyspalvelut vastaavat puolestaan omista tietojärjestelmistään, ja sosiaali- ja terveystietojärjestelmien valmistajilta odotetaan palveluiden kriittisyydelle ominaista luotettavuutta ja työnlaatua. Myös luotettava veden- ja sähkönsyöttö on turvallisen toiminnan edellytys, ja niiden resilientti toimivuus pyritäänkin varmistamaan yhteistyössä vesi- ja sähköyhtiöiden kanssa. Esimerkiksi tehohoidossa akuilla on varmennettu ainakin ne laitteet, joita tarvitaan potilasta siirrettäessä. Tiedon oikeellisuudesta pyritään varmistumaan säilyttämällä tiedot Suomessa, jotta ylimääräistä tiedonsiirroilta ja -prosessoinneilta vältytään. Myös riskinarvioinnin pohjalta laadittavat varajärjestelmät ovat tärkeitä potilastietojen säilyttämisessä. (Yhteiskunnan turvallisuusstrategia, 2017.) Vaikka tiedot säilytetäänkin Suomessa, niin Yhteiskunnan turvallisuusstrategiassa (2017) mainitaan, että pohjoismaista yhteistyötä ja harjoittelua tulisi lisätä. Sen hyötyinä voidaan nähdä turvallisuuteen ja toimintaan liittyvien hyvien käytänteiden leviäminen ja mahdollisimman saumaton rajat ylittävä yhteistyö poikkeustilanteissa. Vuonna 2017 käynnistettiin myös suomalaista terveydenhuoltoalan kyberturvallisuutta edistävä Kyber-terveys -hanke, jonka kehitysvaihe tuli päätökseensä vuoden 2019 loppupuolella. Hanke keskittyi neljään kehittämisalueeseen, joista ensimmäinen oli henkilöstön kouluttaminen ja tietoisuuden lisääminen. Toinen osa-alue puolestaan keskittyi prosessien ja työkalujen kehittämiseen siten, että tietoturvavalvomojen ja niiden tiedonhallintajärjestelmien nopea reagointikyky varmistettaisiin. Kolmas kehittämisalue liittyi kyberturvallisuuden vaatimusten huomiontiin hankintojen kilpailuttamisessa. Neljäs

kehittämiskohde piti sisällään kriittisyysluokitukset järjestelmille ja niiden sisältämille tiedoille. Hankkeeseen osallistui yliopistosairaaloita ylläpitävien sairaanhoitopiirien lisäksi Keski-Suomen sairaanhoitopiiri ICT-palveluntarjoajineen, mutta hankkeen päätyttyä saadut tulokset on tarkoitus jakaa ja ottaa käyttöön laajemmin. (Huoltovarmuuskeskus, 2019b.)

4.3.8 Vedenjakelu ja jätevesijärjestelmät

TAULUKKO 9 Vedenjakelu ja jätevesijärjestelmät

	Kuka vastaa? (Yhteiskunnan turvallisuusstrategia, 2017; Kyberturvallisuuskeskus, 2019a)	**Mitä suojataan?** (Yhteiskunnan turvallisuusstrategia, 2017)	**Miten suojataan?**
Vedenjakelu- ja jätevesijärjestelmät	**Julkinen:** Maa- ja metsätalousministeriö, ELY-keskukset, ympäristöministeriö, sosiaali- ja terveysministeriö, THL, sekä Valvira. Kunnat, paikalliset vesilaitokset ja osuuskunnat.	- Vedenjakeluketju - Yritysverkko ja teollisuuden ohjausjärjestelmät	- Salaus, palomuurit ja tunkeutumisen havaitsemisjärjestelmät (Wei & Ji, 2010) - IPv4/v6 teknologiat (Macaulay & Singer, 2016) - Haavoittuvuusanalyysi-, simulaatio- ja mallintamistekniikat (Ten, Liu & Manimaran, 2010) - Kyber-vesi -hanke (Huoltovarmuuskeskus, 2019a)

Vedenjakelun operatiivisesta toiminnasta ja turvallisuudesta vastaa kunnat, paikalliset vesilaitokset ja asiakkaiden omistamat osuuskunnat. Vastuualueisiin kuuluu koko vedenjakeluketjun suojaaminen, aina vedenlähteistä jätevedenpuhdistukseen. Hallintoelimistä vedenjakelun valvonnasta vastaa maa- ja metsätalousministeriö sekä ELY-keskukset, kun taas jätevedenkäsittelystä vastaa ympäristöministeriö. Juomaveden laadusta vastaa puolestaan sosiaali- ja terveysministeriö, terveyden ja hyvinvoinnin laitos THL, sekä Valvira. (Yhteiskunnan turvallisuusstrategia, 2017.) Lisäksi tulee suojata vedenjakeluun liittyvät teollisuuden ohjausjärjestelmät ja niiden taustalla oleva yritysverkko. Syksyllä 2018 päätökseen tulleessa Kyber-vesi -hankkeessa kartoitettiin vesihuoltolaitosten tietoturvallisuuden tilaa, selvittämällä tieto- ja automaatiojärjestelmien fyysisen ja teknisen tietoturvan ominaisuuksia. Selvityksen pohjalta saatiin yleiskuva, jonka pohjalta pystytiin laatimaan ohjeistuksia ja arviointityökaluja laitosten oman toiminnan ja ostopalvelujen kyberturvallisuuden arviointiin. (Huoltovarmuuskeskus, 2019a.) Sen tarkemmin kyberturvallisuuden työkaluista ei kerrota, mutta kirjallisuudesta löydettyjä SCADA-järjestelmien turvaamiseen hyödynnettäviä

suojaustoimia, kuten Ten & Manimaranin (2016) määrittelemiä järjestelmähaavoittuvuuksien testaustekniikoita voitaisiin tässä tapauksessa soveltaa.

4.3.9 Sektorikohtaisten tulosten tulkinta

Tulosten pohjalta voidaan todeta, että kaikilla kriittisen infrastruktuurin sektoreilla pääpiirteiset vastuut julkisen ja yksityisen sektorin välillä on määritelty, mutta kuten ennakoitiin, niin yksityiskohtaisempia vastuita ja suojaustoimia ei ole turvallisuussyistä kuvailtu julkisissa asiakirjoissa sen tarkemmin. Tarkempien suojaustoimien tunnistamista, etsimistä ja kohdentamista kuitenkin helpottaa se, että Yhteiskunnan turvallisuusstrategiassa (2017) käsitellään varsin kattavasti sektorien vastuita ja suojattavia kohteita. Tutkittaessa sektorien turvaamiseen hyödynnettävien suojaustoimien yhteyksiä Euroopan komission asettamiin kehitysalueisiin voidaan huomata, että kullakin sektorilla oli vähintään yksi suojaustoimi, joka jollakin tavalla edistää resilienssiä, pelotetta tai puolustusta. Kriittisen infrastruktuurin kriisinsietoisuutta parannetaan esimerkiksi Kyber-terveys -hankkeen ansiosta lisääntyvän kyberturvallisuustietoisuuden ja turvallisempien järjestelmähankintojen avulla. Kyberhyökkäysten ja -rikosten ehkäisemisessä auttavat puolestaan hallinnon ja lainsäädännön aktiivinen osallistuminen kansainvälisen oikeuden kehittämiseen, sekä tietojärjestelmiin asennettavat tunkeutumisen havaitsemisjärjestelmät. Lopulta vielä yhteiskunnan kokonaisvaltainen puolustuskyky paranee, kun linkittyneiden sidosryhmien harjoittaman yhteistyön lisäksi yhteistoimintaa halutaan kasvavissa määrin harjoittaa eri toimijoiden kanssa niin kansallisella, kuin kansainvälisellä tasolla.

5 YHTEENVETO JA JATKOTUTKIMUSAIHEET

Tämän kirjallisuuskatsauksena toteutetun kandidaatin tutkielman lähtökohtina olivat epäselvyydet kriittisen infrastruktuurin laajuudesta ja vastuista, sekä sen suojaamiseen hyödynnettävistä keinoista. Koska ongelmaa päätettiin lähestyä kotimaisesta näkökulmasta, niin heti aluksi huomattiin, ettei suomalaista kriittisen infrastruktuurin sektoreita ja kattavuutta ole kansallisissa kyberturvallisuusstrategioissa sen tarkemmin määritelty. Ensiksi käsiteltiin tutkimuksen kannalta keskeisimmät käsitteet: kyberturvallisuus ja kriittinen infrastruktuuri. Kyberturvallisuuden ja tietoturvallisuuden eroavaisuudet ja yhteneväisyydet määriteltiin, minkä jälkeen suoritettiin lyhyt katsaus haittaohjelmien historiaan. Luvun lopuksi perehdyttiin vielä kyberturvallisuuden strategiseen ulottuvuuteen hyödyntämällä Euroopan kyberturvallisuusstrategiaa, joka asettaa päälinjat myös Suomen kyberturvallisuusstrategialle. Tämän jälkeen määriteltiin kriittinen infrastruktuurin käsite, sekä sen sisältämät sektorit. Kriittisten sektorien kokonaiskuvan koostamiseksi tutkittiin muiden valtioiden yleisesti kriittiseksi mieltämiä sektoreita, minkä pohjalta pystyttiin tunnistamaan selkeästi yleisimmät kriittisen infrastruktuurin sektorit. Sektorien ollessa selvillä, pyrittiin selvittämään niiden sisältämiä kyberturvallisuuteen liittyviä ominaisuuksia, sekä suojaamiseen hyödynnettäviä toimia. Pohjana toimi pitkälti kansallinen Yhteiskunnan turvallisuusstrategia (2017), jossa kriittisen infrastruktuurin vastuut, suojattavat kohteet ja tietyissä määrin myös suojaustoimet oli kuvailtu. Strategiassa mainittujen suojattavien kohteiden avulla niiden suojaamiseen pystyttiin kirjallisuudesta ammentamaan olemassa tai kehitteillä olevia kyberturvallisuuden suojaustoimet. Löydetyt suojaustoimet pystyttiin jaottelemaan ei-teknisiin poikkisektorillisiin suojaustoimiin, teollisuuden ohjausjärjestelmien suojaustoimiin, ja sektorikohtaisiin suojaustoimiin. Riippuen kriittisestä sektorista, suojaustoimia löytyi varsin vaihdellen, mutta kuitenkin siten, että kullekin sektorille pystyttiin kohdistamaan joitakin toimia. Oli myös hienoa huomata, että löydetyistä toimista kukin tavallaan edistivät Euroopan komission (2017) asettamia resilienssin, pelotteen ja puolustuksen kehitysalueita.

Tutkimukseen liittyy toisaalta myös kritiikkiä, sillä tutkimuksen kattaessa koko kriittisen infrastruktuurin vastuut, suojattavat kohteet ja suojaustoimet, tutkimustulokset jäävät laajuuden vuoksi varsin yleismaailmallisiksi. Rajaamalla tutkimuksen tarkemmin yhteen tai muutamaan sektoriin, saataisiin varmasti paljon yksityiskohtaisempia tuloksia. Esimerkiksi teollisuuden ohjausjärjestelmiin ja niihin liittyviin sektoreihin keskityttiin tässä tapauksessa paljon enemmän, kuin rahoitus- ja pankkialan tai hallinnon ja lainsäädännön kyberturvallisuusratkaisuihin. Myös tieto- ja viestintäteknologian alueeseen olisi mahdollisesti voinut käyttää enemmän resursseja sen sisältämän kyberpotentiaalin takia. Kaiken kaikkiaan tutkimus tarjoaa kuitenkin varsin tiiviissä muodossa kokonaiskuvan suomalaisesta kriittisestä infrastruktuurista ja siihen liittyvistä vastuista, suojattavista kohteista ja suojaustoimista.

Jatkotutkimusaiheita pohdittaessa nousee esiin kysymys liittyen kriittisen infrastruktuurin vastuiden laajuuteen nykyisessä rakenteessa. Tutkimustuloksista pystyy huomaamaan, kuinka kriittisen infrastruktuurin ja kyberturvallisuudenkin parissa toimii todella monta hallinnollista ja virastollista toimijaa, mikä laittaa pohtimaan nykyisen mallin tehokkuutta, kun yhteistyön, avoimuuden ja läpinäkyvyyden merkitystä turvallisuuden tehostamiseksi korostetaan enenevissä määrin. Olisiko kriittisen infrastruktuurin ja sen kyberturvallisuuden hallintaan olemassa kenties jokin parempi malli, kun nykyisellään roolit ja vastuut ovat varsin hajallaan. Eräs mielenkiintoinen tutkimusaihe voisi myös olla 5G:n vaikutus yleisiin ja kriittisiin tietojärjestelmiin sekä teollisuuden ohjausjärjestelmiin kohdistuvien kyberhyökkäysten määrään, vai toimiiko Euroopassa vuonna 2019 käyttöön otettu kybervalvonnan viitekehys riittävänä pelotteena kyberrikollisuuden vähentämisessä, kun Euroopan neuvoston on mahdollista määrätä kyberrikoksiin ja -väärinkäytöksiin liittyviä rangaistuksia. Lisäksi tässä tutkimuksessa vähemmälle huomiolle jääneen pankki- ja rahoitusalan kyberturvallisuusratkaisuja ja ratkaisumalleja voisi vielä tutkia enemmän. Jatkotutkimuksessa voitaisiin kartoittaa esimerkiksi lohkoketjuteknologian potentiaalisia hyötyjä ja soveltuvuuksia pankkitoiminnassa, sillä pankkitoiminnan luotettavuuden ja turvallisuuden perusedellytyksenä nähdään läpinäkyvyys, joka on myös yksi lohkoketjuteknologioiden kulmakivistä.

LÄHTEET

Amoroso, E. (2012). *Cyber attacks: protecting national infrastructure*. Elsevier.

Australian hallitus. (2010). Critical Infrastructure Resilience. Australian Government. Haettu 1.10.2019 osoitteesta https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/critical-infrastructure-resilience

Black, P. (2014). Issues Facing Businesses in the Implementation of Critical Infrastructure Protection. Teoksessa: Edwards, M. & IOS Press. *Critical Infrastructure Protection*. Amsterdam: IOS Press.

Bloomfield, R., Bendele, M., Bishop, P., Stroud, R. & Tonks, S. (2016). The risk assessment of ERTMS-based railway systems from a cyber security perspective: Methodology and lessons learned. *International Conference on Reliability, Safety, and Security of Railway Systems*, 3-19. Springer, Cham.

Bologna, S., Fasani, A. & Martellini, M. (2013). Cyber security and resilience of industrial control systems and critical infrastructures. Teoksessa: *Cyber Security* (s. 57-72). Springer, Cham.

Chen, R. Y. (2017). An intelligent value stream-based approach to collaboration of food traceability cyber physical system by fog computing. *Food Control*, *71*, 124-136.

Chen, T. M. & Robert, J. M. (2004). The evolution of viruses and worms. *Statistical methods in computer security*, *1*, 1-16.

Clarke, R. (2009). War From Cyberspace. *The National Interest,* (104), 31-36.

CNPIC. (2010). What is a critical infrastructure? National Center of Infrastructure Protection and Cyber Security. Haettu 1.10.2019 osoitteesta http://www.cnpic.es/en/Preguntas_Frecuentes/Que_es_una_Infraestructura_Critica/index.html

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Davcev, D., Kocarev, L., Carbone, A., Stankovski, V. & Mitresk, K. (2018). Blockchain-based Distributed Cloud/Fog Platform for IoT Supply Chain Management. In *Eighth international conference on advances in computing, electronics and electrical technology (CEET)* (pp. 51-58).

Duggan, D., Berg, M., Dillinger, J. & Stamp, J. (2005). Penetration testing of industrial control systems. *Sandia national laboratories*.

Edwards, M. & IOS Press. (2014). An analysis of a cyberattack on a nuclear plant: The stuxnet worm. *Critical Infrastructure Protection*, *116*, 59. Amsterdam: IOS Press.

Euroopan komissio. (2005). The European Programme for Critical Infrastructure Protection (EPCIP). Haettu osoitteesta https://europa.eu/rapid/press-release_MEMO-06-477_en.htm

Euroopan komissio. (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Haettu osoitteesta https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2008.345.01.0075.01.ENG

Euroopan komissio. (2017). Euroopan komissio, Yhteinen tiedonanto Euroopan parlamentille ja neuvostolle: Resilienssi, pelote ja puolustus: vahvan kyberturvallisuuden rakentaminen EU:lle, JOIN(2017) 450 lopullinen, 13.9.2017. Haettu osoitteesta https://op.europa.eu/fi/publication-detail/-/publication/794f8627-985b-11e7-b92d-01aa75ed71a1

Euroopan unionin kyberturvallisuusstrategia. (2013). Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa verkkoympäristö, JOIN(2013) 1 lopullinen, 7.2.2013. Haettu osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=JOIN:2013:0001:FIN

Faysel, M. A. & Haque, S. S. (2010). Towards cyber defense: research in intrusion detection and intrusion prevention systems. *IJCSNS International Journal of Computer Science and Network Security*, *10*(7), 316-325.

Fink, A. (2019). *Conducting research literature reviews: From the Internet to paper* (5th ed.). Thousand Oaks, CA: SAGE Publications.

Foreman, J.C. (2017). Architecture for Community-Scale CI Coordination for Security and Resilience. Teoksessa: Gheorghe, A. V., Tatar, Ü. & Gokce, Y. *Strategic Cyber Defense : A Multidisciplinary Perspective*. Amsterdam, Netherlands: IOS Press.

Fosnock, C. (2005). Computer worms: past, present, and future. *East Carolina University*, *8*. Haettu osoitteesta https://pdfs.semanticscholar.org/c6a3/a4fcba55f36572be99e37dd155a7d0347b3d.pdf

Geers, K. (2009). The Cyber Threat to National Critical Infrastructures: Beyond Theory. *Information Security Journal: A Global Perspective*, *18*(1), 1–7.

Geers, K. (2011). *Strategic cyber security*. CCD COE Publications.

Gheorghe, A. V., Tatar, U. & Gokce, Y. (2017). *Strategic Cyber Defense : A Multidisciplinary Perspective*. Amsterdam, Netherlands: IOS Press.

Gisladottir, V., Ganin, A.A., Keisler, J.M., Kepner, J. & Linkov, I. (2017). Resilience of Cyber Cystems with Over- and Underregulation. *Risk analysis: an official publication of the Society for Risk Analysis*, *37*(9), 1644-1651.

Hanska, J. (2013) The Emperor's Digital Clothes: Cyberwar and the Application of Classical Theories of War. Teoksessa: Rantapelkonen, J. & Salminen, M. (2013). The fog of cyber defence. *Julkaisusarja 2. Artikkelikokoelma n: o 10*.

Hart, C. (2018). *Doing a literature review: Releasing the research imagination* (2nd edition.). Thousand Oaks, CA: SAGE Publications.

Högmander, J. (2012). iKyber: Kyberturvallisuuden johtamisjärjestelmä. Teoksessa: Ingalsuo, T. & Paunu, P. Kyberturvallisuus, hyökkäys ja puolustus, 13-18. Tampereen yliopiston informaatiotieteiden yksikkö.

Huoltovarmuuskeskus. (2019a). Kyberturvallisuutta vesilaitoksille. 21.1.2020. Haettu 9.1.2020 osoitteesta https://www.varmuudenvuoksi.fi/aihe/kriittinen_infrastruktuuri/399/kyberturvallisuutta_vesilaitoksille

Huoltovarmuuskeskus. (2019b). Kyber-terveys -hanke valmistuu. 21.1.2020. Haettu 9.1.2020 osoitteesta https://www.varmuudenvuoksi.fi/aihe/kyber/416/kyber-terveys_-hanke_valmistuu

ITU. (2009). Overview of Cybersecurity. *Recommendation ITU-T X.1205.* Geneva: International Telecommunication Union (ITU). Haettu 3.6.2019 osoitteesta https://www.itu.int/rec/T-REC-X.1205-200804-I/en

Kanadan hallitus. (2009). National Strategy for Critical Infrastructure. Public Safety Canada.Haettu 1.10.2019 osoitteesta https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx

Karabacak, B. & Tatar, Ü. (2014). Strategies to counter cyber attacks. Teoksessa: Edwards, M. Critical Infrastructure Protection. IOS Press.

Kärkkäinen, A. (2013). The Origins and the Future of Cyber Security in the Finnish Defence Forces. Teoksessa Rantapelkonen, J. & Salminen, M. The Fog of Cyber Defence. *Julkaisusarja 2. Artikkelikokoelma n: o 10*.

Kerigan-Kyro, D. (2014). NATO and Critical Infrastructure Resilience. Teoksessa: Edwards, M. & IOS Press. *Critical Infrastructure Protection*. Amsterdam: IOS Press.

Kokonaisturvallisuuden sanasto. (2017). Sanastokeskus TSK 50. Sanastokeskus TSK ry. Helsinki. Haettu 28.4.2019 osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Kokonaisturvallisuuden_sanasto.pdf

Kozlowski, A. (2014). Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. *European Scientific Journal, ESJ*, *10*(7).

Kuusisto T. & Kuusisto R. (2015). Cyberworld as a Social System. Teoksessa: Lehto, M. & Neittaanmäki, P. *Cyber security: Analytics, technology and automation*, 78, 31-44. Springer, Switzerland.

Kyberturvallisuuden sanasto. (2018). Sanastokeskus TSK ry, Huoltovarmuuskeskus ja Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Haettu 28.4.2019 osoitteesta https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

Kyberturvallisuuskeskus. (2019a). NIS-koordinointi ja viranomaisyhteistyö. 24.10.2019. Liikenne ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Haettu 9.1.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/nis-koordinointi-ja-viranomaisyhteistyo

Kyberturvallisuuskeskus. (2019b). Suojaamattomia automaatiojärjestelmiä suomalaisissa verkoissa. Liikenne ja viestintävirasto Traficomin Kyberturvallisuuskeskus. Haettu 9.1.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Suojaamattomia_automaatioj%C3%A4rjestelmi%C3%A4_suomalaisissa_verkoissa_2019.pdf

Lazari, A. (2014). *European critical infrastructure protection*. Springer International Publishing.

Luiijf, E., Besseling, K. & de Graaf, P. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures, 9*(1), 3-31. January 2013.

Macaulay, T. & Singer, B. L. (2016). *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS*. CRC Press.

Makovsky, D. (2012). The Silent Strike. *New Yorker*, *17*, 34-40. Haettu 5.9.2019 osoitteesta https://www.washingtoninstitute.org/uploads/Documents/opeds/Makovsky20120917-NewYorker.pdf

Marten, G. G. & Atalan-Helicke, N. (2015). Introduction to the symposium on American food resilience. *Journal of Environmental Studies and Sciences*, *5*(3), 308-320.

Norri-Sederholm, T., Laitinen, T., Lehto, M. & Kari, M. J. (2019). Terveydenhuolto ja kyberuhkat. *Finnish Journal of eHealth and eWelfare*, *11*(1-2), 86-99.

Quigley, K. (2013). Canada's Strategy for Protecting Critical Infrastructure. *Can Public Admin*, *56*: 142-164.

Rantapelkonen, J. & Jantunen, S. (2013). Cyberspace, the Role of State, and Goal of Digital Finland. Teoksessa Rantapelkonen, J. & Salminen, M. The Fog of Cyber Defence. *Julkaisusarja 2. Artikkelikokoelma n: o 10*.

Rantapelkonen, J. & Salminen, M. (2013). The Fog of Cyber Defence. *Julkaisusarja 2. Artikkelikokoelma n: o 10*.

Rieger, C. G., Gertman, D. I. & McQueen, M. A. (2009). Resilient control systems: Next generation design research. In *Conference on Human System Interactions, 2,* 632-636. IEEE.

Robinson, M., Jones, K. & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & security*, *49*, 70-94.

Ruotsin turvallisuusvirasto. (2014). Action Plan for the Protection of Vital Societal Funtions and Critical Infrastructure. Swedish Civil Contingencies Agency (MSB). Haettu 1.10.2019 osoitteesta https://www.msb.se/RibData/Filer/pdf/27412.pdf

Saksan liittovaltion sisäministeriö. (2009). National Strategy for Critical Infrastructure Protection (CIP Strategy). Federal Ministry of the Interior. Haettu 1.10.2019 osoitteesta https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.html;jsessionid=9B2CD8F888A2685A52AAA080EA563F1F.1_cid287

Sanger, D. E. (2012). Obama order sped up wave of cyberattacks against Iran. *The New York Times*, *1*(06), 2012.

Stouffer, K., Falco, J. & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST special publication*, *800*(82), 16-16.

Suomen Kyberturvallisuusstrategia. (2013). Finland's Cyber Security Strategy. Government Resolution, 24 Jan 2013. Haettu 6.9.2019 osoitteesta https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/FinlandsCyberSecurityStrategy.pdf

Ten, C., Manimaran, G. & Liu, C. (2010). Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 40, no. 4, pp. 853-865.

Verton, D. (2002). *The hacker diaries*. McGraw-Hill, Inc.

Viron puolustusministeriö. (2008). Cyber Security Strategy. Cyber Security Strategy Committee & Ministry of Defence. Tallinn, Estonia. Haettu 1.10.2019 osoitteesta https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwi01dSrsafnAhUEpIsKHTjrDE0QFjAAegQIAxAB&url=https%3A%2F%2Fwww.enisa.europa.eu%2Ftopics%2Fnational-cyber-security-strategies%2Fncss-map%2Fnational-cyber-security-strategies-interactive-map%2Fstrategies%2Fcyber-security-strategy%2F%40%40download_version%2F993354831bfc4d689c20492459f8a086%2Ffile_en&usg=AOvVaw2T0xjRQUD86YR9hP4CxlmV

Von Solms, R. & Van Niekerk, J. (2013). From information security to cyber security. *Computers & security*, *38*, 97-102.

Wei, D. & Ji, K. (2010). Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights. *International Symposium on Resilient Control Systems*, *3*, 15-22. Idaho Falls.

Weiss, J. (2013). Industrial Control System (ICS) Cyber Security for Water and Wastewater Systems. Teoksessa: Clark, R. M. & Hakim, S. *Securing Water and Wastewater Systems: Global Experiences*, *2*, 87.

Whitman, M. E. & Mattord, H. J. (2012). *Principles of information security*. Cengage Learning.

Xiao-Juan, L. & Li-Zhen, H. (2010). Vulnerability and interdependency of critical infrastructure: A review. *Next generation infrastructure systems for eco-cities*, pp. 1-5. Shenzhen.

Yhdysvaltain kotimaan turvallisuusvirasto. (2014). A Glossary of Common Cybersecurity Terminology. National Initiative for Cybersecurity Careers and Studies: Department of Homeland Security. Haettu 1.6.2019 osoitteesta http://niccs.us-cert.gov/glossary#letter_c

Yhdysvaltain kotimaan turvallisuusvirasto. (2017). Critical infrastructure sectors. Department of Homeland Security. Haettu 1.10.2019 osoitteesta https://www.dhs.gov/cisa/critical-infrastructure-sectors

Yhteiskunnan turvallisuusstrategia. (2017). Turvallisuuskomitea. Haettu 29.9.2019 osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf