Alex Virtanen

KRIITTISEN INFRASTRUKTUURIN OHJAUSJÄRJESTELMIEN KYBERTURVALLISUUS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Virtanen, Alex
Kriittisen infrastruktuurin ohjausjärjestelmien kyberturvallisuus
Jyväskylä: Jyväskylän yliopisto, 2018, 33 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja(t): Kollanus, Sami

Tämä tutkielma käsittelee kriittisen infrastruktuurin tuotanto- ja jakeluprosessien SCADA-järjestelmien toimintavarmuutta sekä resilienssiä kyberturvallisuuden näkökulmasta. Tutkielman tarkoituksena on selvittää, kuinka erilaiset parhaat käytänteet ja viitekehykset neuvovat kriittisen infrastruktuurin organisaatioita vahvistamaan omaa toimintavarmuuttaan jatkuvasti muuttuvan kyberulottuvuuden toimintahäiriöiden varalta. Tutkielma pyrkii etsimään näistä viitekehyksistä yhteneväisyyksiä sekä eroavaisuuksia ja vertailemaan näitä luvussa neljä esitellyn toimintavarmuustaulukon avulla. Tutkimus toteutettiin kirjallisuuskatsauksena, jossa hyödynnettiin aikaisempia vertaisarvioituja tieteellisiä julkaisuja, artikkeleita, kirjallisuutta ja viitekehyksiä. Tutkimuksen tuloksia tarkastellessa huomattiin, että oikeanlainen suunnittelu ja sen suunnitelman toteutus toimintahäiriön varalle ovat avaintekijöitä organisaation toimintavarmuuden palauttamiseen ja resilienssin vahvistamiseen.

Asiasanat: kriittinen infrastruktuuri, kyberturvallisuus, ohjausjärjestelmä, SCADA, toimintavarmuus, resilienssi

ABSTRACT

Virtanen, Alex
Cyber Security of Critical Infrastructure's Industrial Control Systems
Jyväskylä: University of Jyväskylä, 2018, 33 pp.
Information Systems, Bachelor's Thesis)
Supervisor(s): Kollanus, Sami

This Bachelor's Thesis addresses the reliability of critical infrastructure's SCADA systems from a resilience and cyber security perspective. This thesis is meant to define how different best practices and frameworks advise critical infrastructure organizations to strengthen their own operational reliability in the event of ever-changing cyber-disruptions. The thesis aims to find similarities and differences between these frameworks and compare them with the operational reliability table presented in Chapter 4. The research was done by using systematic literature review methods where data that was used were from peer-reviewed academic papers, articles, literature, and frameworks. The study found that proper planning and implementation for possible operational cyber-malfunctions are key factors in restoring the operational reliability of the organization and strengthening resilience.

Keywords: critical infrastructure, cyber security, ICS, SCADA, reliability, resilience

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Yhteiskunnan kriittinen infrastruktuuri ylläpitää sen tärkeimpiä toiminnallisuuksia. Käsitteelle on tapauskohtaisesti erilaisia määritelmiä, mutta pääasiassa kriittiseen infrastruktuuriin voidaan lukea esimerkiksi finanssiala, liikenne ja jakeluketjut, energiantuotanto, yleishyödylliset laitokset, terveydenhuollon palvelut, elintarvikehuolto sekä viestintäpalvelut. Kokonaisuuteen kuuluu fyysisiä laitoksia sekä rakenteita ja sähköisiä palveluja. (Huoltovarmuuskeskus, 2018; Työ- ja elinkeinoministeriö, 2018) Sana ”infrastruktuuri” tarkoittaa yhteiskuntajärjestelmän perustoiminnallisuuksia, jotka ovat kriittisiä yhteiskunnan toiminnan kannalta, ja ne voidaan jakaa sosiaalisiin ja teknisiin infrastruktuureihin. Sosiaalisilla infrastruktuurit käsittävät julkiset sekä yksityiset palvelut ja tekninen infrastruktuuri taas esimerkiksi liikenneverkot, energia-, vesi- ja jätteenhuoltoverkot sekä tietoliikenneverkot (Finto.fi, 2018).

Kriittinen infrastruktuuri nojautuu nykyaikana yhä enemmän informaatioteknologiaan ja sen tuottamiin liiketoimintahyötyihin. Lisääntynyt verkostoituminen ja datavirran määrä kasvattavat kyberhyökkäysten potentiaalia erilaisten hyökkäysrajapintojen määrän kasvaessa. (Dupont, 2013; Lee & Lim, 2016) Näiden ilmiöiden myötä myös kriittisen infrastruktuuriin kohdistuvat kyberhyökkäykset ovat kasvaneet eksponentiaalisesti viime vuosien aikana ja monet valtiot ja suuret kansainväliset organisaatiot ovat alkaneet vastatoimiin kyberturvallisuusuhkien varalle (Lee & Lim, 2016). Tutkimuskysymys, johon tutkimus pyrkii vastaamaan on: Mitkä tekivät vaikuttavat kriittisen infrastruktuurin tuotantoprosessien toimintavarmuuteen sekä resilienssiin kyberturvallisuuden kannalta ja minkälaisilla keinoilla sitä voi vahvistaa?

Tässä tutkimuksessa tutkitaan systemaattisen kirjallisuuskatsauksen menetelmin (Okoli & Schabram, 2010) kriittisen infrastruktuurin tuotanto- ja jakeluprosessien rakennetta sekä järjestelmiä, niiden toimintavarmuutta sekä resilienssiä ja kyberturvallisuusstrategioita sekä viitekehyksiä, joilla kriittisen infrastruktuurin toimijat voivat vahvistaa omaa kyberturvallisuuttaan. Tutkimus toteutettiin hakemalla eri tietokannoista, kuten Google Scholar, Scopus ja IEEE Xplore, aihealueeseen liittyviä artikkeleita ja teoksia. Näistä teoksista valittiin osuvimmat tulokset, joissa käsiteltiin kriittisen infrastruktuurin informaa-

tioulottuvuuden rakennetta, kyberturvallisuutta ja kyberturvallisuusstrategioita, kyberturvallisuusviitekehyksiä ja tuotantojärjestelmien resilienssiä. Nämä käsitellyt aiheet toimivat tietokantahaussa hakusanoina niin suomeksi kuin englanniksi. Käytettyjä hakusanoja olivat muun muassa: critical infrastructure, resilience, SCADA, ICS, cyber security strategy, cyber security framework sekä näistä muodostettuja yhdistelmiä ja muunnelmia. Tutkielman tiedonhakuvaiheessa pyrittiin hyödyntämään useita eri julkaisukanavia ja kriittisesti arvioimaan näiden luotettavuutta lähdekirjallisuutena. Julkaisukanavien laatua tarkasteltiin esimerkiksi julkaisufoorumi.fi -verkkosivun luokittelutasojen mukaan, joissa arvosteluasteikko on 0-3. (Julkaisufoorumi.fi, 2018)

Tutkielman rakenne on seuraavanlainen: Toisessa luvussa käsitteellään kriittistä infrastruktuuria käsitteenä sekä sen rakennetta länsimaisessa valtiossa. Luvussa kuvataan lisäksi kriittisen infrastruktuurin ohjausjärjestelmiä kokonaisarkkitehtuurisesta sekä tietoteknisestä näkökulmasta. Tutkielman kolmannessa luvussa esitellään kriittisen infrastruktuurin kyberturvallisuusympäristöä, erilaisia uhkia, riskejä ja haavoittuvuuksia sekä lähdekirjallisuuden parhaita käytänteitä. Neljännessä luvussa näitä parhaita käytänteitä vertaillaan tietoteknisten ja ei-tietoteknisten ominaisuuksien perusteella. Luvussa kuvaillaan resilienssin ja toimintavarmuuden varmistamiseen liittyviä toimia kyberturvallisuuden sekä organisaation riskienhallinnan näkökulmista. Viimeisessä pääluvussa tutkielmasta tehdään yhteenveto ja esitellään muun muassa jatkotutkimusaiheita tulevaisuuden tutkimuksille.

2 KRIITTINEN INFRASTRUKTUURI

Moderneissa länsimaissa yhteiskunnan toimintavarmuus perustuu useiden eri kriittisen infrastruktuurin toimijan yhteistoiminnasta. Näiden toimijoiden toimintavarmuus nojautuu yhä enemmän digitaalisten laitteiden toimintakykyyn jokaisessa tilanteessa. Tässä luvussa keskitytään kriittisen infrastruktuurin käsitteen määrittelyyn ja sen rakenteen selvittämiseen. Ensimmäisenä esitellään modernin länsimaisen valtion kriittisen infrastruktuurin rakennetta sekä merkitystä yhteiskunnalle ja lopuksi käsitellään tuotanto- ja jakelujärjestelmiä, joilla kriittisen infrastruktuurin toimijat pystyvät tuottamaan palveluita ja tuotteita yhteiskunnan käyttöön.

2.1 Kriittisen infrastruktuurin rakenne

Kriittinen infrastruktuuri muodostuu eri aloista ja toiminnoista sekä fyysisestä että digitaalisesta toimintaympäristöstä. Näitä osia kuitenkin yhdistää NATO:n ja Huoltovarmuuskeskuksen määritelmä, jossa kriittisen infrastruktuuri koostuu välineistä, laitteista, palveluista sekä tietojärjestelmistä, jotka ovat kriittisiä yhteiskunnan turvallisuuden, kansantalouden, terveyden sekä valtiohallinnon toiminnalle. (Huoltovarmuuskeskus, 2018; NATO, 2018) Nämä toimijat tuottavat palveluita, kuten terveydenhuoltoa, sekä tuotanto- ja jakeluprosesseja, joiden lopputuotteena on yhteiskunnalle tärkeitä palveluita ja hyödykkeitä, kuten sähköä, öljyä ja vettä.

Yksi tärkeimpiä toimijoita digitaalisen yhteiskunnan toiminnan kannalta ovatkin sähkövoimalaitokset sekä sähkönjakeluverkot, joiden myötä sähkön hyödyntäminen liiketoiminnassa on mahdollista ja jopa itsestään selvää modernissa yhteiskunnassa. Häiriötekijät sähkötuotannossa voivat tarkoittaa muiden toimijoiden toiminnan lamaantumisen, sillä sähkön hyödyntäminen on monen kriittisen infrastruktuurin toimijan elinehto eivätkä esimerkiksi varageneraattorit pysty tuottamaan sähköä kuin muutamiksi tunneiksi. (Simonoff, Restrepo, Zimmerman, & Naphtali, 2008). Sähkön käyttäminen prosesseissa mahdollistaa

myös näiden prosessien digitalisoitumisen, joka tarkoittaa sitä, että tuotanto- ja jakeluprosesseja ohjataan tietokonelaitteistoilla ja -ohjelmistoilla. Ohjelmistot sekä teknologiat kehittyvät ja trendi onkin laitteiston, jopa kokonaisten tuotantolaitosten, verkostoituminen. Näin voidaan todeta, että kriittinen infrastruktuuri on sidoksissa ja riippuvainen kyberympäristön dynaamisesta ulottuvuudesta. (Lehto, Limnéll, Kokkomäki, Pöyhönen & Salminen, 2018)

2.2 Kriittisen infrastruktuurin järjestelmät

Kriittisen infrastruktuurin tuotanto-, jakelu- ja kuljetusprosessit tukeutuvat ohjelmistoihin, joilla on erilaisia käyttötarkoituksia. Vaikka lopputuote tai tarjottava palvelu eroaisikin toisistaan, kuten esimerkiksi vedenpuhdistamon prosessit sähkövoimalaitoksen prosesseista, niiden järjestelmillä on yksi yhteinen päämäärä: kriittisen infrastruktuurin palveluiden ja tuotannon luotettavuuden ja turvallisuuden takaaminen reaaliaikaisesti tiettyjen standardien mukaisesti (Roe & Schulman, 2018).

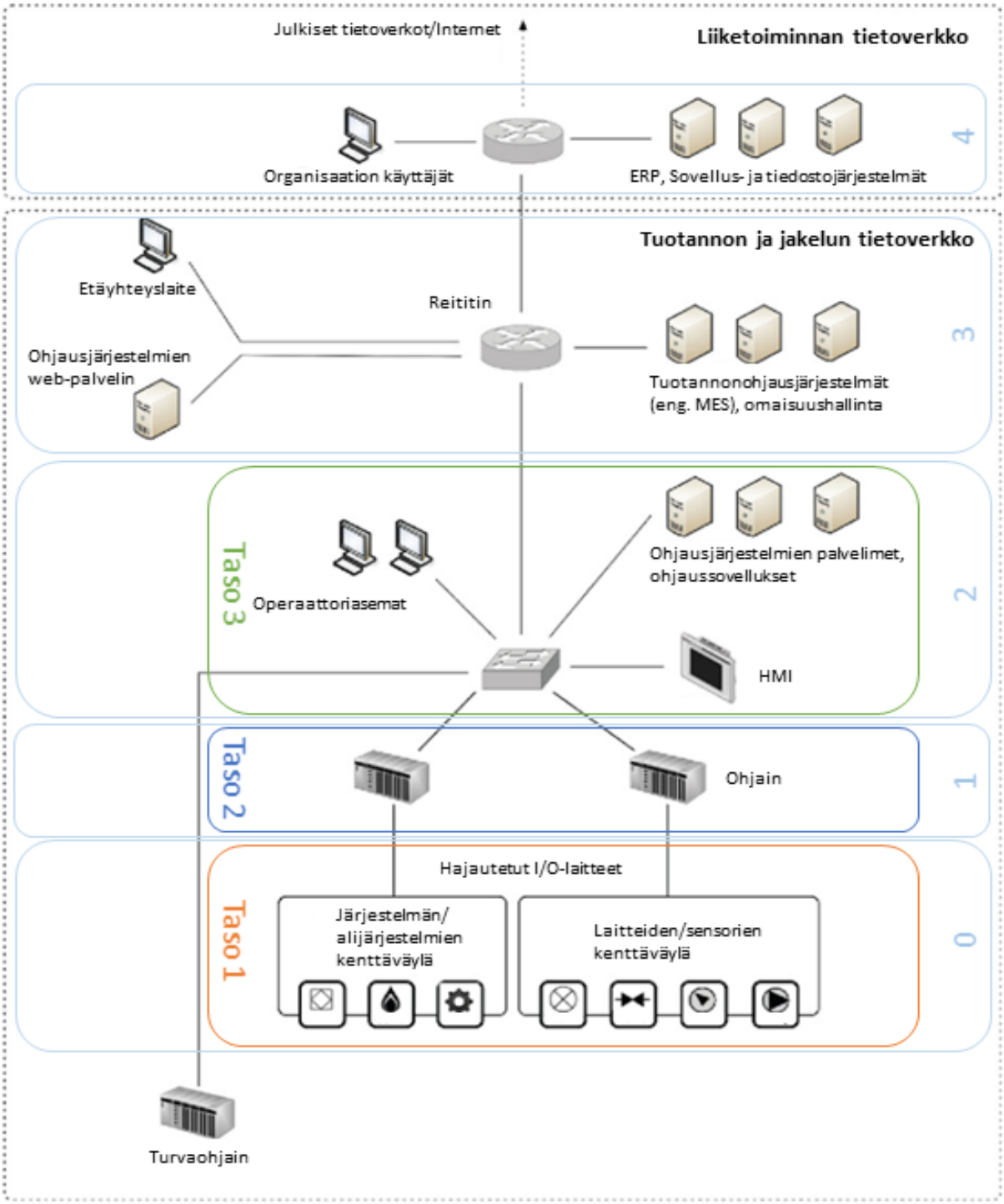
Tuotanto- ja jakeluprosessien toimintaan ja niiden valvontaan liittyvät järjestelmät ovat luokiteltu **ohjausjärjestelmiks**i (engl. *Industrial Control Systems,* ICS), joka on yleisnimitys kaikille teollisten prosessien ohjaamiseen tarvittaville ohjelmistoille ja laitteille. Nämä järjestelmät ovat kyberfyysisiä kokonaisuuksia, jossa järjestelmän tuottamaa sekä käsittelemää informaatiota hyödynnetään synkronoidusti fyysisessä ja digitaalisessa ympäristössä (Lee, Bagheri & Kao, 2015). Järjestelmäkokonaisuudet koostuvat valvontalaitteista, ohjaimista sekä sähköisistä, pneumaattisista, mekaanisista tai hydraulisista ohjainkomponenteista, joiden avulla prosessin tavoite, esimerkiksi sähkön jakaminen, saavutetaan. Ohjausjärjestelmien toimintalogiikka voidaan luokitella kolmeen ohjainsilmukka-malliin: avoimeen silmukkaan (engl. *open loop*), suljettuun silmukkaan (engl. *closed loop*) ja manuaaliseen tilaan. Näiden toimintamallien eroavaisuudet perustuvat toimintalogiikkaan, jossa ohjausjärjestelmän tuottama informaatio eli tuloste, esimerkiksi mitattu lämpötila, käsitellään eri tavoilla. Avoimen silmukan toimintamallissa tuloste käsitellään vakiintunein ohjein, jotka on ohjelmoitu laitteiston ohjelmalogiikkaan. Suljetun silmukan toimintamallin tuloste vaikuttaa syötteeseen, mutta kuitenkin niin, että haluttu tavoite säilyy prosessissa koko ajan. Suljetun silmukan järjestelmä saakin näin muuttaa prosessin toimintaa ennalta määrätyin parametrien rajoissa. Manuaalinen toimintamalli perustuu ihmisten tekemiin päätöksiin ja on täysin ihmisten monitoroimaa sekä ohjaama. Usein ohjausjärjestelmä koostuu useista ohjainsilmukasta, ihmisen ja laitteen välisestä rajapinnasta (engl. *Human-Machine-Interface*, HMI) ja työkaluista, joilla järjestelmää voidaan diagnosoida ja huoltaa. (mm. Boyer, 2009; National Institute of Standards and Technologies, 2014)

Sähkövoimalaitoksissa, jakeluverkostoissa ja tehtaissa ohjelmisto- sekä laitearkkitehtuuri on usein monitasoista, jolloin näiden kaikkien ohjelmien automaation valvontaan tarvitaan tuotantoprosessien ohjausjärjestelmä. Näistä **SCADA-järjestelmä** (engl. *Supervisory Control And Data Acquisition*) on yksi

tunnetuimmista saatavilla olevista ohjaus- ja valvontaohjelmistoista (Poletykin, 2018). SCADA-järjestelmä tunnetaan suomalaisessa kontekstissa valvomo-ohjelmistona, jonka tarkoitus on monitoroida ja hallita tuotantoprosessien dataa etäyhteyden avulla niin, että tuotantoprosessin hallinta ei tarvitse fyysistä läsnäoloa työntekijöiltä. (mm. Boyer, 2009; Kumar, Gaur & Kumar, 2018) SCADA-järjestelmät kuuluvat osaksi tuotantolaitoksen paikallista verkkoa (engl. *Local Arean Network*, LAN) tai laajaverkkoa (engl. *Wide Area Network*, WAN), jossa jokainen ohjausjärjestelmä toimii osana segmentoituja tuotanto- tai jakeluprosesseja. Suurin ero näiden kahden tietoverkkoteknologian välillä on tuotanto- tai jakeluprosessin monitorointipisteen ja mittauspisteen välimatka toisiinsa. LAN-ratkaisu on hyödyllinen silloin, kun monitoroidaan lähialueen, esimerkiksi voimalaitoksen sisäisiä sensoreita ja WAN-ratkaisu taas silloin, kun monitoroitava mittauspiste on kauempana monitorointipisteeltä, esimerkiksi jakeluverkoissa.

SCADA-järjestelmillä on aina kolme toimintatasoa (Kuvio 1): kenttä- tai laitostaso (taso1 1) (engl. *Field/Plant Level*) on toimintataso, jossa syötesignaali käsitellään. Tämän toimintatason laitteistoon kuuluvat muun muassa lämpö- ja virtaussensorit, tasoindikaattorit sekä ohjauslaitteistot, kuten erilaiset venttiilit. Suoraan ohjaustasoon (taso 2) (engl. *Direct Control Level*) kuuluu järjestelmän ohjelmoitavat logiikkaohjaimet (engl. *Programming Logic Controller*, PLC) ja etäterminaaliyksiköt (engl. *Remote Terminal Unit*, RTU). Nämä ohjaimet ja yksiköt pitävät sisällään ohjelmoidun toimintalogiikan, jolla järjestelmän komponentteja voidaan ohjata sekä valvoa. Tämä taso sisältää myös parametrit esimerkiksi suljetun silmukan järjestelmissä. Kolmas taso on valvonta- ja ohjaustaso (taso 3) (engl. *Supervisor Control Level*), joka on SCADA-järjestelmälle tärkein toimintataso. Tällä toimintatasolla käsitellään kaikki kenttätason monitorointi- ja ohjaustehtävät sekä tapahtumakäsittelyt.

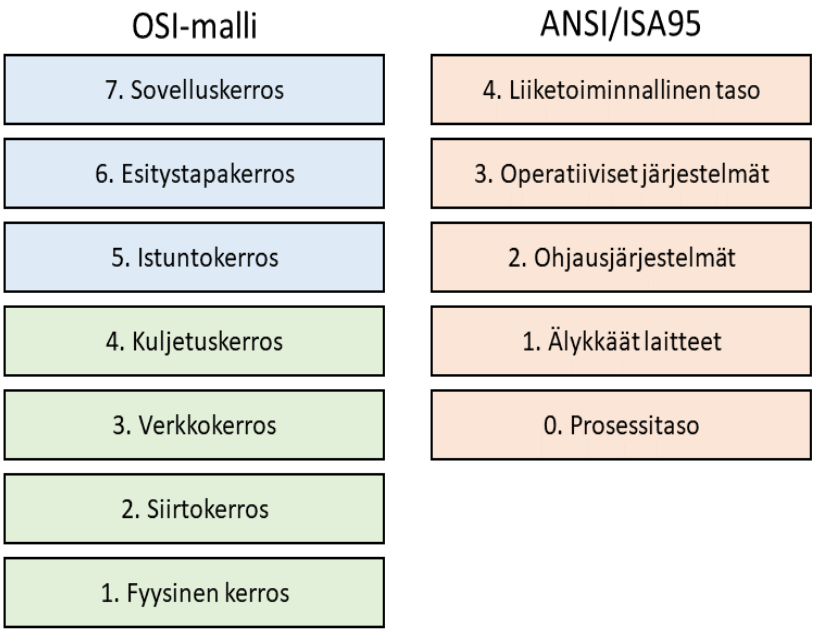
SCADA-järjestelmän toiminta perustuu sensoridataan, jossa tuotantoprosessin fyysistä toimintaa, kuten painetta, lämpötilaa, virtausta tai jännitettä, voidaan monitoroida tai ohjata. Nämä sensorit on yhdistetty fyysiseen tuotantolaitteen, kuten esimerkiksi vesipumpun ohjelmointilogiikkaohjaimeen tai etäterminaaliyksikköön. Näiden komponenttien avulla järjestelmä pystyy etäohjaamaan fyysistä tuotantolaitetta lähettämällä ensin syötesignaalin, joka muutetaan tuotantolaitteessa digitaaliseksi dataksi. Vastaanotettua dataa verrataan laitteen mikroprosessorin ohjelmointilogiikkaan, joka johtaa päätöksentekoon. Tämän jälkeen tapahtumasta lähetetään data järjestelmän valvonta- ja ohjaustasolle samaa tekniikkaa hyödyntäen monitorointia ja analysointia varten. (Boyer, 2009; National Institute of Standards and Technologies, 2014; Kumar, Gaur & Kumar, 2018)



KUVIO 1 Kriittisen infrastruktuurin toimijan tietoverkkojen ja järjestelmien jakautuminen (mukaillen Knapp & Langill, 2014)

Kriittisen infrastruktuurin järjestelmiä voidaan tarkastella järjestelmän tietoliikenteen toimintaperiaatteen sekä kokonaisarkkitehtuurin näkökulmasta (Kuvio 2). Tietoliikenteen toimintaperiaatetta tarkasteltaessa järjestelmät voidaan luokitella OSI-mallin (engl. *Open Systems Interconnection Reference Model*) mukaan seitsemään kerrokseen. OSI-mallin fyysinen kerros kuvaa fyysisiä tiedonsiirtolaitteita, siirtoyhteyskerros kuvaa tietoliikennepakettien kehystystasoa, verkkokerros kuvaa kahden laitteen välistä kommunikaatiota, kuljetuskerros vastaa tietoliikennepakettien toimituksesta sekä niiden järjestelystä, istuntokerros vastaa useiden yhteyksien multipleksoinnista, esitystapakerros vastaa merkistökoodaustapojen yhteensovittamisesta ja sovelluskerros vastaa sovelluksien viestinnästä käyttäjälle.

Kokonaisarkkitehtuurin näkökulmasta tarkasteltaessa voidaan käyttää organisaation tuotannon kokonaishallintaan kehitettyä ANSI/ISA-95 -standardin Purdue -mallia, jonka mukaan organisaation sovellukset jaetaan viiteen tasoon (Kuvio 1 & 2). Purdue -mallissa tasot määräytyvät seuraavasti: Ensimmäinen taso, mallin mukaan taso 0, on fyysisten prosessien taso, jossa kaikki fyysisiä instrumentteja käyttävät prosessit tapahtuvat. Taso 1 on älykkäiden laitteiden taso, joka tunnistaa ja manipuloi fyysisen tason prosesseja, esimerkiksi sensorit. Taso 2 on ohjausjärjestelmätaso, joka monitoroi sekä ohjaa fyysisiä prosesseja esimerkiksi SCADA-järjestelmän avulla. Taso 3 pitää sisällään tuotannon operatiiviset järjestelmät, joiden avulla tuotetaan haluttu lopputuote tai palvelu. Taso 4 on liiketoiminnallisen logistiikan taso, jossa esimerkiksi toiminnanohjausjärjestelmien avulla pystytään hallinnoimaan liiketoiminnan aktiviteetteja sekä tuotantoprosesseja ylimmillä tasoilla, kuten kokonaisen tuotantolaitoksen tasolla. (Knapp & Langill, 2014)



KUVIO 2 OSI-malli ja ANSI/ISA95 Purdue-malli

3 KRIITTINEN INFRASTRUKTUURIN KYBERTURVALLISUUS

Tässä luvussa käsitellään kriittisen infrastruktuurin toimijoiden kyberturvallisuutta. Kappaleessa esitellään ensimmäisenä tunnetuimpia kirjallisuudesta löydettyjä kyberturvallisuusuhkia sekä -riskejä. Sen jälkeen käsitellään yleisimpiä kyberturvallisuusstrategioita sekä erilaisia viitekehyksiä, joilla kriittisen infrastruktuurin organisaatiot voivat parantaa sekä vahvistaa omaa toimintaansa kyberturvallisuusympäristössä.

3.1 Kyberturvallisuusuhkat ja -riskit

Oxford-sanakirja määrittelee kyberturvallisuus -termin tilaksi, jossa puolustaudutaan ei-auktorisoituja tai laittomia elektronista dataa hyödyntäviä toimia vastaan tai niitä toimia, joilla tämän tilan voi saavuttaa (Oxford Dictionary, 2018). Kybertoimintaympäristön jatkuva kehittyminen auttaa liiketoimintamahdollisuuksissa, mutta samanaikaisesti se kasvattaa uhkafaktoreiden määrää kyberhyökkäyksille. Kybertoimintaympäristössä ilmeneviä uhkia, eli kyberuhkia, voidaan luokitella karkeasti kahteen luokkaan: tahallisiksi ja tahattomiksi (Limnéll, Majewski & Salminen, 2014). Oxford-sanakirjassa kyberuhka määritellään tietoverkkojen ja järjestelmien vahingoittamisen sekä häirinnän mahdollisuudeksi. Uhka on siis todellinen, jos on olemassa mahdollisuudet sen toteutumiseen. (Oxford Dictionary, 2018) Suomen kyberturvallisuusstrategiassa (2013) kyberuhka linjataan samankaltaiseksi kuin edeltävissä lähteissä. Kyberuhkat määritellään kybertoimintaympäristön uhkafaktoreiksi, joilla on vakavia negatiivisia vaikutuksia Suomen valtion julkisiin palveluihin, talouteen sekä hallintoon.
Kyberturvallisuusstrategian taustamuistiossa tarkennetaan, että kyberhyökkäys esimerkiksi kriittistä infrastruktuuria kohtaan voi lamauttaa valtion elintärkeiden toimijoiden toiminnan aikaansaaden huomattavia haittoja. (Valtioneuvosto, 2013). Kyberturvallisuusriskit ovat riskejä, joiden aiheuttajina järjestelmien haavoittuvuudet ja niitä hyväksikäyttävät kyberuhkat (Refsdal, Solhaug & Stølen, 2015). Nämä kyberriskit ja niiden vakavuus perustuu kriittisen infrastruktuurin

toimijoiden kohdalla mahdolliseen liiketoiminnan häiriintymiseen tai äkilliseen keskeytymiseen.

ISO 27002 -standardissa esitellään laajassa käytössä olevaa CIA-analysointimallia, jolla tieto- ja kyberturvallisuuden osa-alueita voidaan havainnollistaa. Mallissa kirjaimet tarkoittavat eri osa-alueita: luottamuksellisuutta (engl. *Confidentality*), eheyttä (engl. *Integrity*) ja saatavuutta (engl. Availability). Tässä kontekstissa luottamuksellisuudella tarkoitetaan sitä, että käsiteltävä tieto on vain oikeutettujen henkilöiden käytössä. Eheys tarkoittaa, että tiedon käsittelymenetelmät ovat olleet oikeellisia ja tieto on pysynyt täydellisenä sekä muokkaamattomana. Saatavuus on osa-alueena se ominaisuus, jonka avulla tieto on aina tarvittaessa saatavilla. (ISO 27002 -standardi) Näihin osa-alueisiin liitetään usein myös muita ominaisuuksia, kuten kiistämättömyys, jolla tietoon liittyvä tapahtuma voidaan todistaa muille, ja todentaminen, jolla tiedon käyttämiseen vaaditaan auktorisoitu käyttäjä. Näitä osa-alueita tarkastellaan seuraavissa kappaleissa riskienhallinnan ja uhkamallinnuksen näkökulmasta.

3.1.1 Ei-tietotekniset uhkat ja riskit

Ei-tietotekniset uhat voidaan nähdä koskevan kaikkea mikä ei ole suoranaisesti yhteydessä järjestelmän laitteistoon tai ohjelmistoon. Näitä ovat esimerkiksi heikko fyysinen turvallisuus, kuten avoin pääsy kriittisestä prosessista vastaavaan tilaan, luonnonkatastrofit, epäsymmetrinen toimintaympäristö sekä ihmisen tahallinen tai tahaton toiminta.

Eling ja Wirfsin (2019) tuoreessa tutkimuksessa tutkittiin kyberriskien ja ei-kyberriskien aikaansaamia taloudellisia tappioita organisaatioille, jossa kokonaisriskien määrästä (N=1579) yli 75 % tapauksista olivat ihmisten tuottamia. Tämä sisältää hakkeroinnit, fyysisen tietovarkauden, inhimillinen virhe tai laiminlyönti sekä kaikki sellaiset tapaukset, jossa dataa manipuloidaan tahallisesti tai tahattomasti organisaatioiden työntekijöiden toimesta. (Eling & Wirfs, 2019) Tutkimustulokset vahvistavat käsityksen siitä, että ihmisten tuottamat häiriöt ovat yleisin syy kyberriskien syntymiselle (mm. Evans, Maglaras, He, & Janicke, 2016).

Kriittisen infrastruktuurin yleisiin heikkouksiin ja haavoittuvuuksiin kuuluu toimintakentän ominaisuuksia. Kriittisen infrastruktuurin toimijoiden välinen riippuvuus, sektoreiden sidosteisuus, fyysinen laajuus sekä epäselvät hallintosuhteet nähdään toimintakentän vakavimpina uhkina (Lewis, 2014). Yhteiskunnan sektoreiden sidosteisuus näkyy useiden länsimaiden kriittisestä infrastruktuurista, jossa voimalaitoksista, veden- ja sähkönjakeluverkoista, terveydenhuollosta, logistiikasta 80-90% on yksityisten toimijoiden omistuksessa (Limnéll, 2018). Julkisen ja yksityisen sektorin yhteistyö yhteiskunnan kokonaisturvallisuuden takaamiseksi vaatii jaettua vastuuta kaikilta toimijoilta, jotta resilienssiä kyber- ja hybridiuhkille voidaan kasvattaa. (Limnéll, 2018). Toimijoiden välinen riippuvuus perustuu yleishyödyllisille yhteisille resursseille, kuten vedelle ja sähkölle, joita poikkeuksetta jokainen kriittisen infrastruktuurin toimija tarvitsee toimiakseen. Useat valtiot ovat myös riippuvaisia muiden val-

tioiden tarjoamista tuotteista ja palveluista, joka näkyy energiapoliittisena asymmetriana valtioiden välillä. (Lewis, 2014)

Enescu, Bizon ja Moraru (2019) listaavat tutkimuksessaan kriittisen infrastruktuurin tulevaisuuden kannalta varteenotettavimpia uhkia. Kuten valtiollisella tasolla niin myös organisaatiotasolla on nähtävissä tietynlaista asymmetriaa toimijoiden välillä - Isot IT-organisaatiot pyrkivät yhä isompaan markkinaosuuteen sekä ylivaltaan saatavilla olevista resursseista. Kansainvälisesti toimivat isot yritykset, kuten Googlesta, Amazonista, Facebookista, Applesta ja Microsoftista koostuva ”The Internet Big Five” (Battelle, 2011), pyrkivät kasvattamaan osuuttaan esimerkiksi datakeskuksilla maailmanlaajuisesti. Tarkastellessa tätä ilmiötä valtakunnallisesti tietyt suuret palveluntarjoajat, kuten operaattorit, hankkivat kattavuutta tietoliikenneverkoista, joka on yksi tärkeimpiä digitalisoituneen yhteiskunnan kriittisen infrastruktuurin osa-alueita. Tämän lisäksi tulevaisuuden uhkiksi tutkimuksessa todetaan hakkeroinnit ja kyberrikollisuus kaikkine lieveilmiöineen sekä uudet teknologiat, jotka epäkäytännöllisyydellä ja vallankumouksellisuudella aiheuttavat lisää hyökkäysrajapintaa kohteisiin. (Enescu, Bizon & Moraru, 2019).

3.1.2 Tietotekniset uhkat ja riskit

Johtuen digitalisoituneesta sekä verkostoituneesta toimintakentästä laite-, järjestelmä- ja tietoverkkokohtaiset haavoittuvuudet ovat myös todella varteenotettavia uhkia kriittiselle infrastruktuurille. SCADA-järjestelmiä on käytetty tuotanto- ja jakeluprosessien ohjauksessa jo useamman vuosikymmenen ajan ja sen myötä erilaiset vanhentuneet järjestelmät (engl. *legacy systems*) ovat usein säilyneet yhdistettynä avoimeen internettiin. Yhteys internettiin ei kuitenkaan korreloi suoraan potentiaaliseen haavoittuvuuteen, mutta se kasvattaa uhkan mahdollisuutta hyökkäyspinta-alan laajuuden myötä. Johtuen vanhentuneesta teknologiasta, turvallisuusominaisuuksien puutteesta ja järjestelmän päivittämättömyydestä vanhemmat SCADA-järjestelmät ovat todennäköisemmin haavoittuvaisempia kyberriskeille kuin tämän hetkiset järjestelmät. Vaikka kyber- ja tietoturvallisuuden näkökulmasta turvalliseen järjestelmään kuuluu oikeanlaiset päivityskäytänteet, ohjausjärjestelmien kohdalla asiat voivat poiketa muista järjestelmistä. Säännöllisillä laitteisto- ja ohjelmistopäivityksillä saadaan järjestelmän sisäisiä haavoittuvuuksia karsittua minimiin, mutta SCADA-järjestelmien kohdalla päivitykset voivat tuottaa suuriakin ongelmia. Tuotanto- ja jakeluprosesseissa järjestelmän sammuttaminen päivitystä varten voi pahimmillaan tarkoittaa, että prosessi joudetaan keskeyttämään pitkäksikin ajaksi sekä mahdollisesti jopa kuukausien etukäteistä suunnittelua. Lisäksi tietyt päivitykset saattavat aiheuttaa ristiriitoja turvallisuussertifioinnin kannalta tai lisätä haavoittuvuuspinta-alaa. (Cárdenas, Amin, Lin, Huang, Huang & Sastry, 2011). Suurin turvallisuusongelma vanhoissa SCADA-järjestelmissä on järjestelmien kytkeytyminen toisiinsa ja eri ikäisten järjestelmien tietoturvastandardien erot. Vanhentuneet järjestelmät voivat toimia eräänlaisena porttina, jonka kautta hyökkääjä pystyy mahdollisesti etenemään vertikaalisesti sekä horison-

taalisesti esimerkiksi sisäverkon sisäisesti muihin järjestelmiin. (Campbell, 2016; Cárdenas ym., 2011; Knapp & Langill, 2014). Esimerkki tästä haavoittuvuudesta on 2010-luvun alussa käytetty Stuxnet-haittaohjelma, joka onnistui leviämään Iranin ydinlaitoksien uraanirikastamoiden Windows-päätelaitteisiin. Tämä oli mahdollista fyysisen laitteen, tässä tapauksessa muistitikun, kytkemisellä rikastamon laitteeseen, joka oli kytkettynä muihin laitoksen järjestelmiin. Tämä yksi laite toimi porttina haittaohjelmalle edetä muihin laitteisiin vakoilemaan sekä uudelleenohjelmoimaan teollisuuskoneiden lähdekoodia aiheuttaen fyysistä vahinkoa ja Iranin ydinaseohjelman hetkellistä keskeytymistä. (Chen & Abu-Nimeh, 2011; Langner, 2011) Ralston, Graham ja Hieb (2007) tuovat artikkelissaan esiin SCADA-järjestelmiä koskevan potentiaalisen laitteistokohtaisen riskitekijän: kaupalliseen käyttöön tarkoitetut tuotteet (engl. Commercial of-the-Shelf, COTS) sisältävät usein omat kaupalliset käyttöjärjestelmät, joita ei ole suunniteltu suoraan esimerkiksi tuotantolaitoksen tarpeisiin. Laitteistot ja niiden dokumentaatiot ovat kaupallisesti saatavilla, joten niiden laitteisto- ja järjestelmähaavoittuvuudet ovat todennäköisemmin potentiaalisen hyökkääjän käytössä. COTS käsitteen alle voidaan lukea kaikki tuotteet mikropiireistä ohjelmistoihin (ENISA CIS, 2011; Department of Homeland Security, 2009; Ralston, Graham & Hieb, 2007)

3.2 Kyberturvallisuuden parhaat käytänteet

ICS-järjestelmien kyberturvallisuuden vahvistamiseen on tarjolla monenlaisia regulaatioita, standardeja ja ohjesääntöjä. Keinovalikoima sisältää strategioita, viitekehyksiä ja yleisiä ohjeistuksia kyberturvallisuuden näkökulmasta. Tässä alaluvussa esitellään tunnetuimpia keinoja, jotka on tarkoitettu kriittisen infrastruktuurin kyberturvallisuuden vahvistamiseen.

Strategialla tarkoitetaan kaiken toiminnan yhtenäistämistä liiketoiminnan ja vision tavoitteiden saavuttamiseksi. **Kyberturvallisuusstrategia** on esimerkiksi valtion tai organisaation strateginen suunnitelma turvalliseen kyberulottuvuudessa toimimiseen. (Luiijf & Besseling, 2013) **Tietoturvastrategia** taas ottaa kantaa organisaation informaation suojaamiseen ja keskittyykin näin ollen informaation luottamuksellisuuden, eheyden sekä saatavuuden takaamiseen. Baskervillen ja Dhillonin (2008) mukaan tietoturvastrategia on kokonaisvaltainen suunnitelma organisaation tietoturvan kehittämiseen ja hallintaan. Artikkelissaan Baskerville ja Dhillon kuvailevat prosessinäkökulmaa, jonka mukaan tietoturvastrategiaan sisältyy yksi tai useampi strategian laadintaprosessi. Nämä prosessit vaativat tavoitteidenmäärittelyn organisaation tietoturvan kannalta, esimerkiksi valtiollisten ja kansainvälisten standardien, regulaatioiden sekä parhaaksi nähtyjen toimintatapojen puitteissa. Strategien laadintaprosessille kirjoittajat kertovat kaksi organisointitapaa: tuotekriteerien ja prosessikriteerien mukainen tapa. Tuotekriteerisessä tavassa strategian laadintaprosessi toteutetaan lajittelemalla aktiviteetit prosessin lopputuotteen mukaan. Tällä tavalla toteutettuun strategiaan sisältyy visio, ydinarvot, ja strategiset suunnitelmat, ku-

ten organisaation turvallisuusrakenne, turvallisuusoperaatiot ja turvallisuusbudjetointistrategia. Prosessikriteerisessä tavassa strategian laadintaprosessi tapahtuu lajittelemalla aktiviteetit tärkeiden komponenttien mukaan. Näitä komponentteja ovat turvallisuus- ja organisaatiostrategian yhteensovittaminen, operatiivisten strategioiden suunnittelu ja organisaation turvallisuussuunnittelu. (Baskerville & Dhillon, 2008).

Kyberturvallisuusviitekehyksien tarkoituksena on luoda organisaatiolle mahdollisuudet toimia, torjua ja palautua kyberturvallisuusriskien varalta. Viitekehyksiä tähän tarkoitukseen löytyy useista eri lähteistä ja niiden rakenne vaihtelee valtio- ja organisaatiokohtaisesti. Tässä kappaleessa esitellään kyberturvallisuusviitekehyksien yhtenäisiä piirteitä ja malleja sekä vertaillaan niiden ominaisuuksia. Paté-Cornell, Kuypers, Smith ja Keller kirjoittavat artikkelissaan (2018) kyberturvallisuusriskien analyysimallista ja kolmesta case-tutkimuksesta, joissa kyberturvallisuusviitekehyksiä käsitellään riskienhallinnan näkökulmasta. Artikkelin mukaan usein kyberturvallisuusriskien hallinta nähdään ylhäältä alas eteneväksi prosessiksi (engl. *top-down management*), jossa painotetaan ohjelmistokehittäjien sekä ohjelmien käyttäjien hyväksi havaittuja käytänteitä ohjelmistosuunnittelussa ja itse ohjelman käyttämisessä ottamatta huomioon järjestelmän omaa rakennetta. Tällä kirjoittajat tarkoittavat sitä, että kyberturvallisuus huomioidaan suunnittelun ja käytön osalta, mutta tarkkoja ohjeita tai strategioita ei ole saatavilla. (Paté-Cornell, Kuypers, Smith & Keller, 2018) Useilla valtioilla on erilaisia suunnitelmia valtiollisen kyberturvallisuuden kehittämistä varten. Yhdysvallat ovat kehittäneet kyberturvallisuusviitekehyksiään ja järjestäneet uudelleen kyberturvallisuusjärjestelmää kriittisen infrastruktuurin näkökulmasta. Iso-Britannia on perustanut ”kyberturvallisuushubin” tarkoituksena tehokas viestintä sekä yhteistoimintaharjoitusten järjestäminen kriittisen infrastruktuurin toimijoiden kanssa. (Lee & Lim, 2016).

4 VERTAILUA

Tässä luvussa keskitytään vertailemaan aikaisemmin käsiteltyjen tieto- ja kyberturvallisuusriskien vastatoimia. Vertailu toteutetaan soveltamalla lähdekirjallisuuden erilaisia viitekehyksiä, jotka tarjoavat joko tietoteknisiä tai strategisia kyberturvallisuusratkaisuja. Lopuksi esitellään kriittisen infrastruktuurin toimintavarmuustaulukko (Taulukko 2), jossa eri vastatoimet asetetaan neljään toimintavarmuuden luokkaan. Kappaleen lopussa tutkitaan näiden yhtäläisyyksiä ja eroavaisuuksia sekä analysoidaan niiden menetelmiä toimintavarmuuden ja resilienssin parantamiseksi kriittisen infrastruktuurin näkökulmasta.

Tietoteknisten ratkaisujen vertailussa (Taulukko 1) käytetään hieman toisistaan eroavia viitekehyksiä. Vertailuun otettiin mukaan pääasiassa SCADA-järjestelmiä tai yleisesti tuotanto- ja jakeluprosessien automaatiojärjestelmiä koskevia viitekehyksiä. Yhdysvaltain kotimaan turvallisuusministeriön (2009) viitekehys, "Cyber Security Procurement Language for Control Systems", on valituista viitekehyksistä selvästi spesifein ja siinä kuvaa erittäin tarkasti kaikki siihen kuuluvat toimenpiteet. ISO/IEC 27002 -standardi (2013) painottaa toimenpiteitään kolmeen pääluokkaan: fyysiseen ja ympäristöturvallisuuteen, henkilöstöturvallisuuteen sekä käyttö- ja pääsyoikeuksien hallintaan. National Institute of Standards and Technologyn kolmessa viitekehyksissä (2011; 2014; 2014) toimenpiteiden spesifiys vaihtelee, mutta johtuen ohjeiden ristiviittauksista, nämä kolme viitekehystä voidaan laskea teoreettisesti yhdeksi kokonaisuudeksi. Kokonaisuudessa otetaan kantaa tarkempiin toimenpiteisiin, kuten tietoverkkojen ja laitteiden suojaamiseen, mutta kokonaisuuden "Cyber Security Framework for Critical Infrastructure" -viitekehyksessä (2014) keskitytään lähinnä strategiseen toimintaan ja riskienhallintaan. Vertailun vanhin viitekehys on Yhdysvaltojen Energiaministeriön laatima 21 askeleen ohjesääntö (2002) SCADA-järjestelmien suojaamiseksi. Ohjesääntö ottaa kantaa ensimmäisissä vaiheissa yleisellä tasolla muun muassa turvallisuusjärjestelmien käyttöönottoon sekä turvallisen tietoverkkoarkkitehtuurin suosituksiin. Viimeiset vaiheet käsittelevät ohjausjärjestelmien suojaamisen strategisia toimia, kuten palautumis- ja jatkuvuussuunnitelmien laatimista.

4.1 Kyberturvallisuuden takaaminen

Tässä aliluvussa tutkitaan kyberturvallisuusstrategioiden ja viitekehyksien tietoteknisiä toimenpiteitä organisaation kyberturvallisuuden parantamiseksi. Kyberturvallisuustoimenpiteillä tarkoitetaan lähdekirjallisuudessa esiteltyjä ratkaisuja, joilla kriittisen infrastruktuurin toimijat voivat kehittää sekä vahvistaa ohjausjärjestelmien kyberturvallisuutta. Taulukko 2 esittelee tutkielman lähdekirjallisuudesta löydettyjä yleisimpiä kyberturvallisuuden vahvistamiseen liittyviä toimenpiteitä. Taulakossa kuvataan sitä, mitkä viitekehykset ottavat kantaa toimenpiteeseen ohjeissaan sekä mihin OSI- ja Purdue-mallien mukaiseen tasoon tai kerrokseen toimenpide vaikuttaa, jotta SCADA-järjestelmän eri toimintatasojen kriittisyys voidaan havainnollistaa.

Taulukosta (Taulukko 1) voidaan todeta, että viitekehyksien välillä on suuria yhtäläisyyksiä sekä muutamia poikkeavuuksia. Vahvimmat yhtäläisyydet löytyivät tietoverkkojen, salasanapolitiikan, autentikoinnin, fyysisen suojaamisen sekä auditointien osalta. Ohjesäännöissä kuvattiin, että johtuen SCADA-järjestelmien komponenttien etäisyyksistä toisiinsa, prosessien kriittisyydestä sekä yleisistä parhaaksi katsotuista käytänteistä tietoverkon kyberturvallisuuteen kiinnitetään eniten huomiota. Hyvin toteutetulla tietoverkkoarkkitehtuurilla ja palomuuriratkaisuilla voidaan estää haittaohjelmien, kuten ohjelmistotroijalaisten, viruksien, matojen sekä vakoiluohjelmien leviämistä mahdollisen haavoittuvuuden esiintyessä. Eristetyillä ja hajautetuilla tietoverkoilla pystytään myös pienentämään palvelunestohyökkäyksien mahdollisuutta, sekä rajaamaan tietoliikennettä tietoverkon laitteiden välillä, esimerkiksi portti- ja sovellussuodattamisella sekä palomuurisäännöillä. Myös modernit teknologiat, kuten esineiden internet (engl. Internet of Things, IoT) ja pilvilaskenta mahdollistavat SCADA-järjestelmien siirtymisen uuteen aikakauteen. Tällä siirtymällä on kuitenkin haasteensa muun muassa tiedon saatavuuteen, luottamuksellisuuteen, salaukseen sekä riskienhallintaan liittyen (Sajid, Abbas & Saleem, 2016). Lisäksi kaikki viitekehykset käsittelivät ohjeissaan oikeanlaista autentikointia. Autentikoinnin tärkeys korostuu etäohjattavissa, pitkille maantieteellisille etäisyyksille hajautetuissa tuotanto- ja jakeluprosesseissa. Autentikointiin liittyviä hyväksi nähtyjä toimenpiteitä olivat myös muun muassa kaikki käyttäjätunnuksiin ja salasanoihin liittyvät säännökset sekä hallinnointitoimet, kuten vahvojen salasanojen käyttäminen sekä mahdolliset kaksivaiheiset autentikointimenetelmät.

Taulukon muista kohdista poikkeava tietoteknisen suojaamisen osa-alue, fyysisten laitteiden suojaaminen, nousu esille kaikissa viitekehyksissä. Tämä voidaan nähdä suhteellisen itsestään selvänä, sillä ei-haluttu fyysinen pääsy kriittisten prosessien tiloihin saattaa olla yksi suurimmista uhka- sekä riskitekijöistä mitä tämän kaltaisille prosesseille. Tahallinen haitallinen toiminta järjestelmän fyysisten laitteiden tilassa mahdollistaa prosessien yhteyksien salakuuntelun, laitteistoon liittymisen esimerkiksi avointen fyysisten terminaali- ja konsolirajapintojen kautta sekä yksittäisten kriittisten prosessien (engl. *Single point*

of failure) häirintää, joka saattaa lamauttaa kaikki muut tuotantoprosessit. (mm. Department of Energy, 2002; Department of Homeland Security, 2009; International Organization for Standardization, 2013; National Institute of Standards and Technology, 2014; 2011; 2011).

Taulukosta voidaan tehdä myös johtopäätös siitä, että viitekehyksien kehittäjät luottavat usein myös toistensa ratkaisuihin. NIST:n kaikkia kolmea viitekehystä tarkastellessa pystyi dokumentaatiosta huomaamaan, että toimintaperiaatteita oli lainattu niin organisaation omista versioista, kuin myös esimerkiksi CIS CSC, COBIT 5, ISA 62334 ja ISO/EIC 27002 viitekehyksistä. Tämä vahvistaa käsitystä, että kriittisen infrastruktuurin järjestelmien suojaamisen periaatteet perustuvat aina parhaimmiksi nähtyihin käytänteisiin.

TAULUKKO 1 Yleisempiä kyberturvallisuuden tietoteknisiä suojaustoimenpiteitä

	Homeland Security*	ISO/IEC 27002:2013**	NIST***	Department of Energy****	OSI-mallin taso	Purdue-mallin taso
Järjestelmien rajaaminen	X		X		1-3	0-4
Järjestelmien eristäminen	X		X		1-3	0-4
Tietoverkkojen eristäminen	X	X	X	X	1-3	0-4
Tietoverkkojen yhteyksienhallinta	X	X	X	X	1-3	0-4
Tietoverkkoarkkitehtuurin hallinta	X	X	X	X	1-3	0-4
Tietoverkkojen reitityksenhallinta	X	X	X	X	3	2-4
Tietoverkkojen monitorointi	X	X	X	X	1-3	0-4
Tietoverkkojen käyttöoikeuksien hallinta	X			X	3	2-4
Protokollien hallinta	X		X	X	1-3	0-4
Ulkoisten yhteyksien autentikointi ja hallinta	X	X	X	X	3	2-4
Salasanavaatimukset	X	X	X	X	1-3	2-4
Salasanojen hallinta	X	X	X		1-3	0-4
Uniikit käyttäjätilit	X		X		1-3	0-4
Käyttäjien rekisteröinti		X	X		1-3	2-4
Käyttäjien autentikointi	X	X	X	X	3	1-4
Turvallisuusohjelmistot (IDS- ja IPS-järjestelmät)	X		X	X	1-3	0-4
Fyysisten laitteiden suojaaminen	X	X	X	X	1-3	0-4
Portti- ja sovellussuodatus	X	X	X		1-3	0-4
Penetraatiotestaus-auditointi			X	X	1-3	0-4
Järjestelmien ja verkkojen auditointi	X	X	X	X	1-3	0-4

* (Department of Homeland Security, 2009)
** (ISO/IEC 27002:2013 -standardi, 2013)
*** (National Institute of Standards and Technology, 2014; 2011; 2011)
**** (Department of Energy, 2002).

4.2 Toimintavarmuuden ja resilienssin takaaminen

Resilienssillä tarkoitetaan järjestelmäajattelussa kykyä jatkaa toimintaansa häiriötilanteesta huolimatta ja palautua vikatilanteista nopeasti. Resilientti järjestelmä pystyy adaptoitumaan odotettuun tai yllätyksellisesti muuttuvaan tilanteeseen, jatkamaan liiketoimintaansa jatkuvasta häiriöstä huolimatta sekä palautumaan häiriötilanteista. (Hilton, Wright & Kiparoglou, 2012; Wright, Kiparoglou, Williams & Hilton, 2012). Jotta organisaatiosta saataisiin mahdollisimman resilientti, organisaation kyvykkyyksiin tulee lukeutua useita keinoja. Wrightin, Kiparogloun, Williamsin ja Hiltonin (2012) mukaan organisaation tulee osata ennakoida, estää sekä lievittää häiriötekijöitä minimoidakseen niiden laajuutta, kestoa sekä niistä aiheutuvia kustannuksia (Wright, Kiparoglou, Williams & Hilton, 2012). Kyberresilienssi voidaankin nähdä koko organisaation ja liiketoiminnan rakenteiden läpimenevänä kokonaisuutena, jolla organisaatio pystyy vastaamaan ja palautumaan kyberulottuvuuden häiriötekijöistä (Campbell, 2016).

Tässä tutkielmassa sovelletaan Roe ja Schulman (2018) kriittisen infrastruktuurin toimintavarmuustaulukkoa (Taulukko 2), joka esittää kriittisen infrastruktuurin toimijoiden toimintavarmuutta riskien ja uhkien ilmaantuessa. Ensimmäisessä sarakkeessa nimetään neljä toimintavarmuuden tyyppiä: estetyt, vältetyt, väistämättömät ja korvattavissa olevat toimintahäiriöt. Estetyt toimintahäiriöt ovat niitä tapahtumia, joiden ilmaantuminen pystytään estämään täysin. Vältetyt toimintahäiriöt tarkoittavat häiriöitä, jotka on onnistuttu välttämään omalla toiminnalla. Väistämättömät häiriöt ovat nimensä mukaisesti väistämättömiä ja niiden ilmaantumisen todennäköisyyteen ei voida vaikuttaa. Korvattavat toimintahäiriöt ovat tapahtumia, jotka ovat ilmaantuneet ja vaikuttaneet jollain tavalla toimijan liiketoimintaan, mutta niiden myötä toimijat pystyvät korvaamaan tapahtunutta kehittämällä omaa toimintaansa. Taulukon toinen sarake kuvastaa toimintavarmuuden sen hetkistä tilaa, joka voi olla normaalia toimintaa, häiriötilaa tai palautumista sekä näiden yhdistelmiä. Kolmas sarake on toimintavarmuuden standardi, joka tarkoittaa tässä tapauksessa toimintavarmuuden hyväksyttyjä toimintaperiaatteita tietyssä hetkessä. Sarakkeen tarkoituksena on kuvata yleistä ja organisaation sisäistä suhtautumista toimintahäiriöihin ja niiden tapahtumiseen. Viimeinen sarake kertoo toimintavarmuuden strategiat, joilla tarkoitetaan toimia erilaisiin, muuttuviin tilanteisiin.

Taulukon ensimmäinen rivi kuvastaa estettyjen toimintahäiriöiden vaikutusta kriittisen infrastruktuurin toimijan toimintavarmuuteen. Tässä tapauksessa estetyt tapahtumat mahdollistavat prosessien ja toimintojen normaalin toiminnan ilman minkäänlaista haittavaikutusta. Standardina pidetään sitä, että sosiaalisesti hyväksymättömiä tapauksia ei saa tapahtua missään tilanteessa. Tämä toimintavarmuuden tila saavutetaan strategialla, joka perustuu tekniseen suunnitteluun, analyyttiseen operointiin ja edeltävään resilienssiin. Taulukon toinen sarake kuvastaa vältettyjen toimintahäiriöiden vaikutusta prosessien

toimintavarmuuteen. Toimintahäiriöltä vältytään oman toiminnan ansioista, joten mahdollistaen normaalin toiminnan sekä mahdollisen riskin tai häiriötekijän korjaamisen. Tässä tapauksessa standardina on, että organisaation sisäisesti hyväksymättömiä tapauksia ei saa tapahtua. Strategia taas perustuu hyöty-riski-suhteeseen ja tietynlaiseen harkittuun riskien vaihtokauppaan, jolla pyritään saamaan hyötyä potentiaalisen riskin ilmaantumisen todennäköisyydellä. Kolmas sarake on väistämättömien toimintahäiriöiden tila, johon organisaatio ei voi vaikuttaa millään tavalla. Väistämättömät tapahtumat aiheuttavat väistämättä toimintahäiriön ja mahdollisesti järjestelmän pettämisen. Standardina on, että odottamattomille sekä väistämättömille asioille ei voida mitään ja ne katsotaan hyväksytyiksi sosiaalisesti. Strategiana väistämättömille sekä odottamattomille tapahtumille on vakuutukset, häiriötilannetiimit, korjausmahdollisuudet ja vahva palautumisen resilienssi. Viimeisen sarakkeen tapahtumat ovat jo ilmaantuneita ja tapahtuneita tapahtumia, joista palaudutaan normaalisti muodostaen uuden normaalin tilan toiminnalle. Häiriötilanteista opitaan tulevaisuuden kannalta uudet toimenpiteet ja näiden pohjalta jatketaan toimintaa. Strategiana näille tapahtumille on ajan tasalla olevat teknologiat, proseduureihin perustuvat uudistukset ja mahdolliset uudelleen organisoinnit esimerkiksi organisaation riskienhallintastrategian priorisoinnissa. (Roe & Schulman, 2018)

TAULUKKO 2 Toimintavarmuustaulukko (Roe & Schulman, 2018)

Toimintavarmuuden tyyppi	**Infrastruktuurin tila**	**Toimintavarmuuden standardi**	**Toimintavarmuusstrategia**
Estetyt	Normaalit toiminnot	Sosiaalisesti hyväksymättömiä asioita ei saa tapahtua	Tekninen suunnittelu, analyyttinen operointi, edeltävä resilienssi
Vältetyt	Normaali, häiriön korjaaminen	Sisäisesti hyväksymättömiä asioita ei saa tapahtua	Riski-hyöty-analyysi ja harkittu riskien vaihtokauppa
Väistämättömät	Häiriö, järjestelmän pettäminen	Sosiaalinen hyväksyntä odottamattomille ja väistämättömille häiriöille	Vakuutus, häiriötilannetiimi, korjaaminen, palautumisen resilienssi
Korvattavat	Palautuminen, uuden normaalin muodostaminen	Epäonnistumiset annetaan anteeksi ja niistä opitut asiat asetetaan uudeksi normaaliksi	Teknologioiden päivittämiset, proseduurimainen uudistus, uudelleenorganisointi

4.2.1 Estetyt tapahtumat

Lähdekirjallisuuden eri strategioissa ja viitekehyksissä on esitelty useita eri tapoja, joilla kriittisen infrastruktuurin organisaatio voi estää toimintahäiriöiden tapahtumista. Toimintatavoissa on tietoteknisten ratkaisujen lisäksi myös ohjeita organisaation toimintavarmuuden kannalta.

National Institute of Standards and Technology (NIST) kriittisen infrastruktuurin kyberturvallisuusviitekehys (2014) kuvailee estettyjä tapahtumia suojaustoimien avulla, jotka ovat konkreettisia toimia kriittisen infrastruktuurin järjestelmien suojaamiseksi. Toiminnossa painotetaan identiteetin, autentikoinnin sekä käyttö- ja pääsyoikeuksien hallintaa, tietoisuuden levittämistä ja henkilöstön kouluttamista. Tapahtumien estäminen vaatii toimia myös datan turvaamisen, informaation suojaamisprosessien ja -käytänteiden, huoltotoimenpiteiden sekä suojausteknologiaratkaisujen käytön osalta. NIST:n lisäksi myös Yhdysvaltojen Energiaministeriö korostaa ohjesäännössään tietoteknisiä ratkaisuja, kuten tietoverkkojen ja järjestelmien hajauttamista sekä eristämistä, turvallisuusohjelmistojen käyttöönottoa sekä oikeanlaista pääsy- ja käyttöoikeuksien hallintaa. (NIST, 2014)

Department of Homeland Security: n ohjeistus "Cyber Security Procurement Language for Control Systems" (2009) ei anna itse tekstissä ohjeita tiettyihin tapahtumiin, mutta ohjeen toiminnot voidaan sijoittaa vertailun neljään toimintavarmuuden tyyppiin. Ohjesäännössä epäedullisten tapahtumisen estäminen onnistuu proaktiivisilla toimilla, kuten tunkeutumisen havaitsemiseen, estämiseen sekä monitorointiin liittyvillä turvallisuustoimilla. Hyvä järjestelmäsuunnittelu sekä implementoidut turvallisuustoimet luovat mahdollisuudet estää mahdolliset häiriöt ja niiden aiheuttajat. Ohjesääntö painottaa toiminnan tärkeyttä ja siirtääkin suunnitelman useissa kohdissa kolmannen osapuolen vastuulle, joten ohjesäännöstä ei löydy yksiselitteisiä ohjeita toimintavarmuuden säilyttämiseksi. (Department of Homeland Security, 2009)

ISO 27002:2013-standardi (2013) sisältää samankaltaisia ohjeita toimintahäiriötapahtumien estämiselle, kuten edellä mainitut ohjeet ja viitekehykset. Standardi painottaa oikeanlaista suunnittelua yli muiden toimien, kun aiheena on toimintahäiriöiden estäminen. Oikeanlainen suunnittelu mahdollistaa heikkouksien sekä haavoittuvuuksien kartoituksen ja optimaalisen riskienhallintaprosessin, jolla organisaatio pystyy keskittämään toimintaansa varteenotettaviin uhkiin. Kun resurssit optimoidaan tiettyihin osa-alueisiin, ne eivät todennäköisesti aiheuta toimintahäiriöitä. (ISO, 2013)

Yhdysvaltain energiaministeriön ohjeistus (2002) ohjausjärjestelmien suojaamiselle on kuten edellä oleva ohjesääntö: ohjeistus keskittyy spesifeihin toimiin, jotka sitten heijastuvat organisaation toimintavarmuuden tilaan. Kuten muissakin ohjeissa ja viitekehyksissä, toiminnot ovat ennaltaehkäiseviä ja estäviä, joilla organisaatio eliminoi mahdolliset riskit tietyistä järjestelmien osa-alueista. (Department of Energy, 2002)

4.2.2 Vältetyt tapahtumat

Vertailtavissa strategioissa ja viitekehyksissä toimintahäiriötilanteiden välttämiselle on havaittavissa monia yhtäläisyyksiä.

NIST:n viitekehykset (2011, 2014) perustavat tällaisten tapahtumien välttämisen sen tunnistustoimien kolmeen riskienhallintakategoriaan. Näissä kategorioissa painotetaan organisaation voimavarojen haavoittuvuuksien sekä ulkoisten ja sisäisten uhkien tunnistamista. Tämän lisäksi organisaation tulee priorisoida kaikki riskien vastaamistoimet ja päättää organisaation sisäisesti riskitoleranssista. Jos organisaatiolla on tavarantoimittajia tai kolmannen osapuolen yhteistyökumppaneita, myös näiden toimijoiden tietojärjestelmät, komponentit ja palvelut tulee tunnistaa, priorisoida ja arvioida. (NIST, 2011; 2014)

Department of Homeland Security: n ohjesäännössä (2009) toimintahäiriöt voidaan välttää, kuten aikaisemman toimintatilan tyypin kohdalla, oikeanlaisella proaktiivisella suojaamistoiminnalla. Häiriötilanteen sattuessa tilanne pyritään rajaamaan häiriöalueelle, esimerkiksi järjestelmän verkon tiettyyn segmenttiin, jolloin sen leviäminen ja vaikutus järjestelmän muihin osiin voidaan minimoida. Tällaisessa tilanteessa painottuu myös järjestelmän suunnittelu sekä toteutus, jotka toimivat järjestelmän sekä verkkoyhteyksien rajauksien sekä kovantamisen myötä tietynlaisina esteinä häiriötilanteiden leviämisen varalta. (Department of Homeland Security, 2009)

ISO27002:2013-standardissa (2013) toimintahäiriöt voidaan välttää kuten myös tehtiin estämisen suhteen. Välttäminen tarkoittaa standardissa enemmän tapahtumien välttämistä omalla toiminnalla, joka sisältää ennalta suunniteltuja toimia. Nämä toiminnot varmistavat, että organisaation toiminta on turvallista ja mahdolliset häiriöt järjestelmässä pystytään välttämään. Esimerkkinä tästä on toimintasuunnitelma häiriötilanteessa, jonka myötä koko tuotanto ei pysähdy yhden prosessin pettäessä. (ISO, 2013)

Yhdysvaltain energiaministeriön ohjeistus (2002) toimintahäiriöt voidaan välttää, kuten aikaisemmassa aliluvussa kuvailtiin: toiminta pitää keskittää omiin heikkouksiin sekä mahdollisiin haavoittuvuuksiin. Hyökkäyspinta-ala pyritään pitämään mahdollisimman pienenä ja mahdolliset aukot turvallisuudessa paikataan omalla toiminnalla. Ohje mainitsee myös prosessien rakenteeseen kantaaottavan määritelmän, jossa prosessien ei tulisi missään vaiheessa nojautua yksittäisiin prosesseihin tai niiden osiin. Nämä yksittäiset prosessit ovat kriittisiä yksittäisiä pisteitä (engl. *Single point of failure*), joiden häiriintymisen myötä kaikki prosessit voivat lamaantua. (Department of Energy, 2002)

4.2.3 Väistämättömät tapahtumat

Väistämättömiin tapahtumiin turvaudutaan kaikissa lähdekirjallisuuden kriittisen infrastruktuurin kyberturvallisuusviitekehyksessä vastatoimenpiteillä.

NIST:n viitekehyksessä (2011, 2014) toimintahäiriöt, jotka ovat väistämättömiä sekä odottamattomia, käsitellään vastatoimenpiteillä, joita ovat toimintahäiriöön vastaamisen suunnitelman luominen sekä käyttö tapahtuman aikana tai sen jälkeen. Viestintä on tärkeässä roolissa toimintahäiriö kohdalla, sillä koordinoidulla viestinnällä organisaation sisällä, että myös ulkopuolella voidaan toimintahäiriön haittavaikutuksia vähentää huomattavasti. Toimintahäiriön ilmaantuessa tulee noudattaa analyyttisiä toimenpiteitä, joilla toimintahäiriön aiheuttaja sekä vaikutusaste saadaan selville mahdollisimman nopeasti. Lieventäviin toimenpiteisin kuuluu toimintahäiriön rajaaminen mahdollisimman pienelle pinta-alalle. Väistämättömistä tapahtumien vastatoimenpiteisiin lukeutuu myös virheistä ja epäonnistumisista oppiminen ja tulevaisuuden vastatoimenpiteiden strategian päivittäminen. (NIST, 2011; 2014)

Väistämättömien tapahtumien kohdalla Department of Homeland Security: n ohjesääntö (2009) sisältää ristiviittauksen NIST:n julkaisusarjan julkaisuun 800-61 (2012), joka on ohjeistus häiriötilannetoimintaan digitaalisessa ympäristössä. Itse ohjesääntö ei siis ota kantaa väistämättömien tapahtumien hoitamiseen ja toiminnan jatkuvuuden säilyttämiseen, vaan siirtää vastuun kolmannen osapuolen, tässä tapauksessa National Institute of Standards and Technology: n, vastuulle. Ohjeessa painotetaan, että väistämättömät tilanteet ovat luonteeltaan sen mukaisia, että niiden esiintyessä toiminta pitää kohdistaa häiriön minimoimiseen. Väistämättömän tai odottamattoman tilanteen ilmentyessä sen vakavuutta tai vaikutusta on vaikea arvioida, joten toiminta sen poistamiseksi tehokkaasti tulee aloittaa mahdollisimman pian. Jos tapahtumaa ei voida poistaa, tulee se rajata niin, että se ei voi vaikuttaa ympärillä oleviin liiketoiminnan komponentteihin, kuten prosesseihin tai laitteisiin. (NIST, 2012)

Kuten edellä, myös ISO:n ISO 27002:2013-standardissa painotetaan vastatoimenpiteitä ja onnistunutta vastaamis- sekä jatkuvuussuunnitelman toteuttamista. Standardin mukaan odottamattomat sekä väistämättömät toimintahäiriöt vaativat hyvät kommunikointi- ja raportointikyvykkyydet, joiden avulla organisaatio pystyy viestimään toimintahäiriöstä tehokkaasti. Tämän lisäksi olennaisena osana ISO:n vastaamis- ja jatkuvuussuunnitelmaa on tapahtumasta oppiminen, joka mahdollistaa luonnollisesti tulevaisuudessa samankaltaisten tapahtumien välttämisen tai estämisen. (ISO, 2013)

Yhdysvaltain Energiaministeriön SCADA-järjestelmien suojaukseen tarkoitetun ohjesäännön (2002) mukaan väistämättömiin toimintahäiriöihin tulee vastata myös oikeanlaisen suunnitelman toteuttamisella. Suunnitelmat ovat väistämättömissä tilanteissa tarpeen, sillä toimintasuunnitelma sellaisen tapahtuman ilmetessä on tarpeen, jotta organisaatio pystyy takaamaan toimintansa jatkuvuuden. Suunnitelmat väistämättömiin tilanteisiin sisältävät riskienhallinta- sekä palautumistoiminnot, joilla väistämättömän häiriötilanteen vaikutusta

pyritään minimoimaan ja toimintaa jatkamaan mahdollisimman tehokkaasti. (Department of Energy, 2002)

4.2.4 Korvattavat tapahtumat

Vertailtavien strategioiden ja viitekehyksien korvattaviin tapahtumiin liittyy kaikkien kohdalla toimintavarmuuden palauttaminen takaisin normaaliin tilaan. Toimintahäiriö on tässä vaiheessa joko aktiivinen tai juuri päättynyt.

Jokaisen viitekehyksen mukaan toimintavarmuus palautetaan noudattamalla ennalta suunniteltua palautumissuunnitelmaa. Palautumissuunnitelma sulautetaan tapahtumasta oppimiseen ja näin organisaation palautumisstrategia toimintahäiriöiden varalle voidaan päivittää ajan tasalle. Toimintahäiriö nähdään ensimmäisenä askeleena kohti uudelleenorganisoitua strategiaa, jolla kriittisen infrastruktuurin organisaatio pystyy vastaamaan tulevaisuuden tapahtumiin. Toiminta tapahtuman jälkeen tarkoittaa järjestelmän uudelleenkartoittamista riskien, uhkien sekä haavoittuvuuksien kohdalla sekä arviointia organisaation tarpeista välttää sekä estää samankaltaiset häiriötilanteet. (Department of Energy, 2002; Department of Homeland Security, 2009; NIST, 2011, 2012, 2014; ISO, 2013)

5 YHTEENVETO JA POHDINTA

Tutkielman tarkoitus on käsitellä kriittisen infrastruktuurin tuotanto- ja jakeluprosessien ohjausjärjestelmien kyberturvallisuutta, toimintavarmuutta sekä resilienssiä. Tutkimuksessa esiteltiin kriittisen infrastruktuurin rakennetta, sen eri järjestelmiä, kyberulottuvuuden uhkia ja riskejä. Tarkoituksena oli luoda tutkielmalle vahva käsitys siitä, minkälaisia ominaisuuksia kriittisen infrastruktuurin toimijoilla kybertoimintaympäristössä toimiessa täytyy olla.

Tutkimuksen pääkysymyksenä oli, mitkä tekijät vaikuttavat kriittisen infrastruktuurin tuotanto- ja jakeluprosessien järjestelmien toimintavarmuuteen ja resilienssiin. Vastaus kysymykseen on varsin yksiselitteinen: Tietotekniset ratkaisut, kuten tietoliikenneverkkojen sekä järjestelmien vahvistaminen eri keinoin kyberriskien varalta ovat tärkeitä kriittisen infrastruktuurin toiminnan kannalta, mutta tärkeimmät tekijät löytyvät organisaation strategisista suunnitelmista. Viitekehyksiä sekä ohjeita vertailtaessa huomattiin, että oikeanlainen suunnittelu ja sen suunnitelman toteutus toimintahäiriön varalle ovat avaintekijöitä organisaation toimintavarmuuden palauttamiseen ja resilienssin vahvistamiseen. Suunnitelmille käytettiin lähdekirjallisuudessa monia eri nimiä, kuten jatkuvuussuunnitelma, vastaussuunnitelma ja palautumissuunnitelma. Näitä kaikkia suunnitelmia yhdistää organisaation kyvykkyys ymmärtää sen resurssien potentiaalisia haavoittuvuuksia sekä priorisoida omaa toimintaansa toimintahäiriön tapahtuessa. Jatkuvuutta edistävät oikeanlainen tilannetiedon muodostaminen, ylläpitäminen ja saatuihin tietoihin perustuvat päätöksentekoprosessit. Varsinkin kriisi- ja konfliktitilanteissa, onnistunut tiedolla johtaminen pienentää yhteiskunnallisia heijastevaikutuksia. Kyberturvallisuuden kannalta kriittisen infrastruktuurin eri toimijoiden ja osa-alueiden toimintavarmuus ja -kyvykkyys tulee rakentaa niin, että näiden entiteettien proaktiivisuus ja muutosjoustavuus säilyvät. Näin varmistutaan siitä, että sietokyky mahdollisille haavoittuvuuksille ja uhkille on suuri. Tutkielman viitekehyksien ja ohjeiden vertailussa ohjausjärjestelmien uniikit vaatimukset suorituskyvyn ja jatkuvuuden takaamiseksi tulivat esille vahvoina toimintoina. Näillä toiminnoilla pyritään estämään, välttämään, korvaamaan toimintahäiriöt ja toimimaan väistämättömissä sekä odottamattomissa tilanteissa. Jokaisen vertailukohdan koh-

dalla otettiin kantaa tutkielmaan valitun toimintavarmuustaulukon (Taulukko 2) osa-alueisiin melko yhtenäisellä tavalla ja retoriikalla. Vaikka lähdeteoksessa sanavalinnat eivät aina olleet samankaltaisia, teoksista pystyi joka tapauksessa löytämään paljon yhtäläisyyksiä. Tämä johtuukin siitä, että ohjeistukset täydentävät useissa tapauksissa toisiaan ja ristiin viittaavat eri lähteitä. Yhteenvetona jokaisen lähdeteoksen kohdalla voidaan todeta, että kriittisen infrastruktuurin toimijat pyrkivät säilyttämään oman toimintansa jatkuvuuden proaktiivisilla sekä preventiivisillä toimilla, jotka pitävät sisällään useita tietoteknisiä ja strategisia päätöksiä. Toiminnan häiriöt pyritään minimoimaan, mutta toimintahäiriön ilmaantuessa organisaation tulee olla valmis muuttumaan: Häiriö liiketoiminnassa tarkoittaa uudelleensuunnittelua lähes jokaisella organisaation osa-alueella, jotta tulevaisuuden kannalta jatkuvuus voidaan taata entistä paremmin.

Muuttunut toimintaympäristö on vaikuttanut kriittisen infrastruktuurin rooliin kyberulottuvuuden toimijana. Verkottunut yhteiskunta asettaa uudenlaisia haasteita valtiollisille organisaatioille, jotka pyrkivät tarjoamaan katkeamatonta palvelua yhteiskunnalle. Aiheesta on löydettävissä kiitettävä määrä erilaisia tutkimuksia eri näkökulmista, mutta tutkimusalue kaipaisi lisää yhteen vetävää vertailua yhteiskunnallisella tasolla. Käypänä jatkotutkimusaiheena voidaankin mainita esimerkiksi eri valtioiden kriittisen infrastruktuurin kyberturvallisuusstrategioita vertaileva tutkimus. Näin tieteenalalla pystytään tarkastelemaan tehokkaasti ilmiön nykytilaa sekä arvioimaan tulevaisuutta.

Kriittinen infrastruktuuri on sidoksissa oman kyberulottuvuutensa toimintavarmuuteen ja resilienssiin. Erilaiset palvelut, kuten sähkö- ja tietoverkot, voimalaitokset, jakeluverkot, logistiikka, liikenne ja terveydenhuollon järjestelmät vaativat eheitä tiedonsiirto- ja tiedonsäilytysmenetelmiä toimiakseen. Modernit kriittisen infrastruktuurin osat vaativat toimiakseen tiedonsiirron ja erilaisten järjestelmien toimintakyvyn jatkuvuuden turvaamisen sekä nopean ja reaktiivisen toiminnan häiriötilanteissa. Kriittisen infrastruktuurin keskinäisriippuvuudesta, haavoittuvuuksista sekä odottamattomista häiriöistä johtuen häiriösietokykyä tulee suunnitella, harjoitella ja testata yhdessä valtiollisella ja kansainvälisellä tasolla – Tarve laajapohjaiselle tarkastelulle ja toiminalle on olemassa (Lehto ym., 2018).

LÄHTEET

Baskerville, R., and Dhillon, G. (2008). Information Systems Security Strategy: A Process View. Teoksessa: Information Security: Policy, Processes, and Practices. Advances in Management Information Systems, D.W. Straub, S.E. Goodman and R. Baskerville (toim.). Armonk, NY: M. E. Sharpe., s. 15-45.

Boyer, S. (2009). Scada: Supervisory Control and Data Acquisition (4. painos). International Society of Automation, USA.

Campbell, R. J. (2016). Cybersecurity issues for the bulk power system. National critical infrastructure policy: Background and select cybersecurity issues, s. 59-93.

Cárdenas, A., Amin, S., Lin, Z., Huang, Y., Huang, C. & Sastry, S. (2011). Attacks against process control systems: Risk assessment, detection, and response. Proceedings of the 6th International Symposium on Information, Computer and Communications Security, ASIACCS 2011, s. 355-366.

Chen, T. & Abu-Nimeh, S. (2011). Lessons from Stuxnet. Computer, 44(4), s. 91-93.

Department of Energy. (2002). 21 Steps to Improve Cyber Security of SCADA networks. President's Critical Infrastructure Protection Board, Yhdysvallat. Haettu osoitteesta: https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/21_Steps_-_SCADA.pdf

Department of Homeland Security. (2009) Cyber Security Procurement Language for Control Systems, Homeland Security, Yhdysvallat. Haettu osoitteesta: https://ics-cert.us-cert.gov/sites/default/files/documents/Procurement_Language_Rev4_100809_S508C.pdf

Dupont, B. (2013). Cybersecurity Futures: How Can We Regulate Emergent Risks? Technology Innovation Management Review, 3(7), 6-11.

Enescu, F., Bizon, N. & Moraru, C. (2019). Issues in securing critical infrastructure networks for smart grid based on SCADA, other industrial control and communication systems. Teoksesta: Power Systems. 2019, s. 289-324. Spinger.

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. Security and Communication Networks, 9(17), s. 4667-4679.

Hilton, J., Wright, C. and Kiparoglou, V. (2012). Building resilience into systems. 2012 IEEE International Systems Conference SysCon 2012.

Knapp, E. & Langill, J. (2014). Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Syngress.

Kumar, S., Gaur, N., & Kumar, A. (2018). Developing a Secure Cyber Ecosystem for SCADA Architecture. Proceedings of the 2nd International Conference on Computing Methodologies and Communication, ICCMC 2018, s. 559-562. doi:10.1109/ICCMC.2018.8487713.

Langner, R. (2011). Stuxnet: Dissecting a Cyberwarfare Weapon. IEEE Security & Privacy 9(3), s. 49-51.

Lee, J., Bagheri, B., Kao, H-A. (2015). A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems, Manufacturing Letters 3, s. 18-23.

Lee, K. & Lim, L. (2016). The Reality and Response of Cyber Threats to Critical Infrastructure: A Case Study of the Cyber-terror Attack on the Korea Hydro & Nuclear Power Co., Ltd. KSII Transactions on Internet and Information Systems 10(2), s. 857-880.

Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J. & Salminen M. (2018). Kyberturvallisuuden strateginen johtaminen Suomessa. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 28/2018.

Lewis, T. (2014). Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation. John Wiley & Sons Inc. New Jersey, Yhdysvallat.

Limnéll, J. (2018). Countering Hybrid Threats: Role of Private Sector Increasingly Important – Shared Responsibility Needed. Julkaisussa Strategic Analysis March 2018. European Centre of Excellence for Countering Hybrid Threats.

Limnéll, J., Majewski, K. & Salminen, M. (2014). Kyberturvallisuus. Jyväskylä: Docendo Oy

Luiijf, E. & Besseling, K. (2013). Nineteen national cyber security strategies. International Journal of Critical Infrastructure Protection, 9(1/2).

National Institute of Standard and Technology. (2012). Computer SecurityIncident Handling Guide. 800-61, Versio 2.

National Institute of Standards and Technology. (2014). Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0

National Institute of Standards and Technology. (2014). Guidelines for Smart Grid Cyber security. Volume 1 - Smart Grid Cyber security Strategy, Architecture, and High-Level Requirements.

National Institute of Standards and Technology. (2011). NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security.

Okoli, C. & Schabram, K. (2010). A Guide to Conducting a Systematic Literature Review of Information Systems Research. Sprouts : Working Papers on Information Systems.

Oxford Dictionary. (2018) Määritelmä sanalle ”cyber security”. Haettu osoitteesta: https://en.oxforddictionaries.com/definition/cybersecurity 22.11.2018

Oxford Dictionary. (2018) Määritelmä sanalle ”cyberthreat”. Haettu osoitteesta: https://en.oxforddictionaries.com/definition/cyberthreat 22.11.2018

Poletykin, A. (2018). Cyber Security Risk Sssessment Method for Scada of Industrial Control Systems. 2018 International Russian Automation Conference, RusAutoCon 2018, doi:10.1109/RUSAUTOCON.2018.8501811

Pöyhönen, J., Noujua, V., Lehto, M. & Rajamäki, J. (2018). Application of Cyber Resilience Review to an Electricity Company. Proceedings of the 17th European Conference on Cyber Warfare and Security.

Ralston, P., Graham, J., & Hieb, J. (2007). Cyber security risk assessment for SCADA and DCS networks. ISA Transactions, 46(4), s. 583-594.

Roe, E., & Schulman, P. R. (2018). A reliability & risk framework for the assessment and management of system risks in critical infrastructures with central control rooms. Safety Science, 110, s. 80-88.

Sajid, A., Abbas, H., & Saleem, K. (2016). Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. IEEE Access, 4, s. 1375-1384.

Simonoff, J., Restrepo, C., Zimmerman, R. & Naphtali, Z. (2008). Analysis of Electrical Power and Oil and Gas Pipeline Failures. Teoksesta Critical Infrastructure Protection. (Goetz, E. & Shanoi, S.) s. 381-394

Työ- ja elinkeinoministeriö. (2018). Valtioneuvoston päätös huoltovarmuuden tavoitteista. Valtioneuvoston yleisistunto 5.12.2018, Helsinki.

Wright, C., Kiparoglou, V., Williams, M., and Hilton, J. (2012). A framework for resilience thinking, New challenges in Systems Engineering and Architecture. Conference on Systems Engineering Research 2012.