Kalle Palho

TOIMITUSKETJUN KYBERTURVALLISUUSRISKIEN HALLINTA JA MINIMOINTI

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2021

TIIVISTELMÄ

Palho, Kalle Joonas
Toimitusketjun kyberturvallisuusriskien hallinta ja minimointi
Jyväskylä: Jyväskylän yliopisto, 2021, 24 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja(t): Räisänen, Jaana

Toimitusketjun kyberturvallisuusriskien hallinta ja minimointi on globaalisti niin kaupallisia kuin ei-kaupallisia osapuolia vahvasti koskettava aihe nyt ja tulevaisuudessa. Tässä kandidaatintutkielmassa perehdytään toimitusketjun kyberturvallisuuden- hallintaan sekä lisäämiseen. Tämä kandidaatintutkielma on muodoltaan narratiivinen, kuvaileva kirjallisuuskatsaus, jonka tarkoitus on antaa laaja kuva käsiteltävästä aiheesta helppolukuisessa muodossa. Tutkielman keskeisimmät löydöt ovat mikä on toimitusketjujen kyberturvallisuuden nykytila ja kuinka sitä hallitaan sekä miten toimitusketjujen kyberturvallisuustasoa voidaan parantaa. Tutkimuksessa havaitaan myös, että yhtä yhtenäistä mallia toimitusketjun kyberturvallisuuden hallintaan ei ole ja jatkotutkimusta tältä osin tarvitaan.

Asiasanat: toimitusketju, kyberturvallisuus, tietoturva

ABSTRACT

Palho, Kalle Joonas
Supply chain cybersecurity risks management and minimization.
Jyväskylä: University of Jyväskylä, 2021, 24 s.
Information Systems Science, Bachelor's Thesis
Supervisor(s): Räisänen, Jaana

Managing and minimizing cybersecurity risks in supply chains is a topic of strong concern to both commercial and non-commercial parties globally now and in the future. This bachelor's thesis focuses on supply chain cyber security management and enhancement. Thesis is in the form of a narrative, descriptive literature review designed to provide a broad picture of the topic at hand in an easy-to-read format. The main findings of this thesis is that what is the current state of cybersecurity in supply chains and how it is managed, and how the level of cyber security in supply chains can be improved. The thesis also finds that there is no cohesive model for supply chain cyber security management and further research is needed in this regard.

Keywords: supply chain, cybersecurity, information security

KUVIOT

KUVIO 1 tyypillinen toimitusketju 8
KUVIO 2 Toimitusketjun kyberturvallisuus elinkaari 15
KUVIO 3 Graafinen luettelo kyberomaisuudesta 16
KUVIO 4 Esimerkki RFID:tä ja sensoreita käyttävästä ruokapakkauksesta poimitun tiedon kulusta 18

TAULUKOT

TAULUKKO 1 taulukko hyökkäyskanavista 17

SISÄLLYS

1 JOHDANTO 6
1.1 Toimitusketju 8
1.2 COVID-19 vaikutukset toimitusketjujen kyberturvallisuuteen 9

2 TOIMITUSKETJUN KYBERTURVALLISUUDEN HALLINTA 10
2.1 Strategioita kyberuhkien hallintaan 10
2.2 Kyberfyysisten toimitusketjujen riskinhallinta 13

3 KÄYTÄNTEET KYBERTURVALLISUUDEN LISÄÄMISEKSI 15

4 JOHTOPÄÄTÖKSET 20

1 JOHDANTO

Jokaisen kuluttajan tuotteen takana on toimitusketju. Toimitusketju on organisaatioiden verkosto, joka yhteistyössä kehittää materiaaleja tai palveluita (Logistiikan maailma, 2021). Toimitusketjun kyberturvallisuuden hallinta, on yksi nykypäivän isoja kysymyksiä, joka vaatii vastausta pikaisesti. Covid-19 pandemian seurauksena ihmiset ovat siirtyneet enenevissä määrin etätöihin. Allianz riskibarometrissa (2021) digitalisaation kiihtyminen nähdään suurimpana pandemian aiheuttavana muutoksena liiketoimintaan. Digitalisaation kiihtymisen jälkeen suurin vaikutus on lisääntynyt etätyöskentely (Allianz Risk Barometer, 2021). Tämä aiheuttaa uusia riskejä kyberturvallisuuteen toimitusketjuissa. Toimitusketjujen kyberturvallisuutta on pyritty hallitsemaan erilaisin strategioin. Erästä tälläista strategiaa käydään läpi Cyber Security Risks and Challenges in Supply Chain (2017) tutkimuksessa. Kyberturvallisuus on aihe johon ei ole olemassa yhtä oikeaa vastausta, vaan optimaalinen turvallisuustaso on jatkuvaa puntarointia käytettävyyden, tehokkuuden ja tietoturvan kanssa. Lohkoketjuteknologioita on pyritty ottamaan käyttöön toimitusketjuissa parantamaan datan eheyttä, ja tutkimustulokset ovat olleet lupaavia sen osalta. Useat globaalit toimitusketjut ovat hyvin dynaamisia, ja toimitusketju kulkee eri mantereiden ja maiden kautta. Tämä aiheuttaa osaltaan omat haasteensa, kuinka toimitusketjujen kyberturvallisuus tulisi järjestää.

Tutkimuskysymykset ovat:

- Miten toimitusketjun kyberturvallisuusriskejä voidaan hallita?
- Millä toimilla toimitusketjun kyberturvallisuustasoa voidaan parantaa?
- Onko mahdollista luoda yhtenäistä mallia toimitusketjun kyberturvallisuuden hallintaan?

Kandidaatintutkielma on kuvaileva kirjallisuuskatsaus, joka on muodoltaan narratiivinen (Salminen, 2011). Kirjallisuuskatsauksen tavoitteena on antaa laaja kuva käsiteltävästä aiheesta helppolukuisessa muodossa.
Lähdeaineistoa tähän kandidaatintutkielmaan on haettu pääasiassa IEEE Xplore Digital Library sekä ProQuest Information and Learning Company tietokannoista, JYKDOK tietokantaa apuna käyttäen. Kandidaatintutkielman lähdeai-

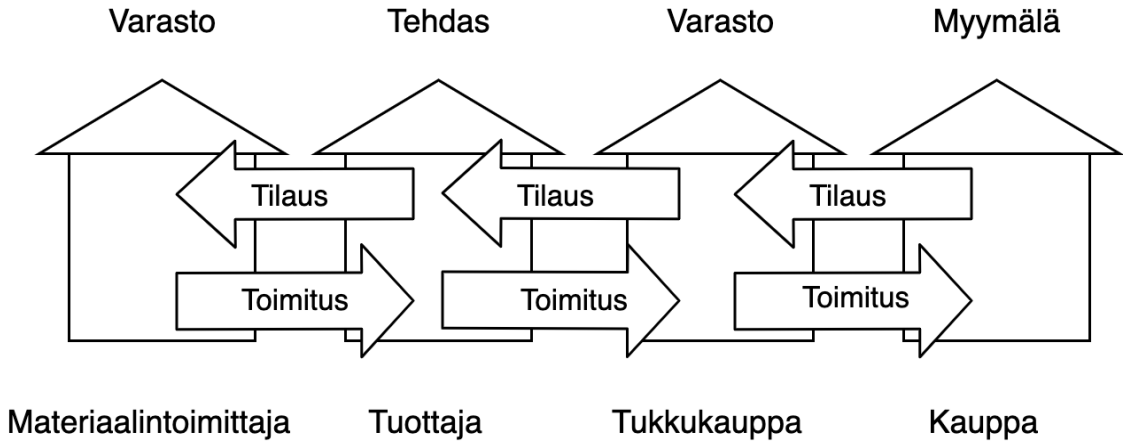
neiston hakusanoina käytettiin suurimmalta osin AND lausekkeen erottamana ”supply chain” ja ”cyber security” hakusanoja. Haku kohdistettiin tutkimusten tiivistelmään.

Lähdeaineisto koostuu suurimmalta osin tieteellisistä artikkeleista sekä konferenssijulkaisuista. Lähteiden luotettavuutta on arvioitu Julkaisuforumin JUFO luokituksen avulla. Muuta lähdeaineistoa, jolle ei ole ollut mahdollista saada JUFO luokitusta, on pyritty arvioimaan sen mukaan kuinka luotettava lähdeorganisaatio on.

Tutkielman teoriaosan ensimmäinen luku käsittelee toimitusketjun kyberturvallisuuden hallintaa. Tässä luvussa käydään läpi lähdeaineistosta ilmenneitä tapoja hallita toimitusketjun kyberturvallisuutta sekä toimitusketjun kyberturvallisuustasoon vaikuttavia muuttujia. Toinen sisältöluku keskittyy konkreettisiin toimiin toimitusketjun kyberturvallisuustason parantamisen näkökulmasta.

1.1 Toimitusketju

Toimitusketjulla tarkoitetaan eri organisaatioiden verkostoa, jotka yhteistyössä kehittävät materiaaleja- tai palveluita. Kullakin toimitusketjun osallisella on oma roolinsa verkostossa. Toimitusketjun rakenne riippuu tuotteesta ja asiakkaista. Alla havainnollistava kuva tyypillisestä toimitusketjusta.



KUVIO 1 tyypillinen toimitusketju (Logistiikanmaailma, 2021)

Toimitusketju voi olla hyvinkin dynaaminen johtuen nykyisistä globaaleista organisaatioverkostoista. Tämä tarkoittaa sitä, että tavaran kulkeminen materiaalintoimittajalta tuottajalle voi kulkea usean mantereen läpi kohdaten useita toimitusketjun jäseniä, jotka käsittelevät tilausta (Schauer, Polemi, & Mouratidis, 2019). Toimitusketjun suunnittelu koordinoi resursseja optimoidakseen tavaroiden, palvelujen ja tietojen toimittamisen toimittajalta asiakkaalle tasapainottaen kysyntää ja tarjontaa (Blanchard, 2010). Toimitusketjun organisaatioympäristön kyberturvallisuudesta on tullut suuri haaste eri sidosryhmäjärjestelmien ja integraatioiden keskinäisten suhteiden vuoksi, joilla tavoitellaan organisaation tavoitteita (Yeboah-Ofori & Islam, 2019).

1.2 COVID-19 vaikutukset toimitusketjujen kyberturvallisuuteen

Modernit yritysinfrastruktuurit ovat enenevissä määrin riippuvaisia monimutkaisista informaatioteknologiaan perustuvista toimitusketjuista. Covid-19 on vaikuttanut omalta osaltaan myös huomattavasti toimitusketjujen digitalisoitumiseen. Allianz vakuutusyhtiön 2021 riskibarometrin mukaan vastaajien mielestä suurin liiketoimintaa kohtaava pandemiasta johtuva muutos on digitalisaation kiihtyminen ja etätyöskentelyn lisääntyminen. Etätyössä jokainen altistuu normaalien kyberturvallisuusriskien lisäksi myös etäverkossa oleville kyberturvallisuusriskeille. Riskibarometrin mukaan kyberselkkaus on kolmanneksi suurin globaalia liiketoimintaa kohtaava riski. (Allianz 2021) Kyberselkkauksella tarkoitetaan sellaista selkkausta, joka tapahtuu informaatioverkostossa. Kyberturvallisuudella tarkoitetaan tilaa, jossa kybertoimintaympäristöstä koituvat riskit ja uhat ovat hallinnassa, ja kyberytoimintaympäristöllä maailmanlaajuista informaatioverkostoa. (Johdatus kyberturvallisuuteen, 2021) Allianz (2021) riskibarometrin mukaan kyberuhat ovat toistuvasti sijoittuneet barometrissä kolmen kärkeen yrityksiä kohtaaviin vaaroihin. Kyberuhalla tarkoitetaan sellaista uhkaa, joka toteutuessaan vaarantaa yhteiskunnan elintärkeän toiminnon tai muun kyberympäristöstä riippuvaisen toiminnon (Johdatus kyberturvallisuuteen, 2021). Maailma on muuttunut paljon viimeisen vuosikymmenen aikana, joka on johtanut uudenlaiseen puntarointiin liiketoimintaa koskevista riskitekijöistä. Monet riskit ovat muuttuneet informaatioteknologiaan liittyviksi. (Allianz 2021)

2 TOIMITUSKETJUN KYBERTURVALLISUUDEN HALLINTA

Toimitusketjut ovat jatkuvan kyberuhan alla. Tavanomaiset menetelmät kyberturvallisuuden takaamiseksi menettävät merkitystään toimitusketjuissa, joissa jokainen verkostossa toimiva organisaatio voi olla kyberturvallisuustapaturman syynä. Toimitusketjun kyberturvallisuudella tarkoitetaan tilaa, jossa toimitusketjun kybertoimintaympäristön uhkat ja riskit ovat hallinnassa. Schauer ym. (2019) ovat tutkimuksessaan sitä mieltä, että toimitusketjujen kyberturvallisuus vaatii toimitusketjun hallintaa, laadunvarmistusstandardeja sekä IT ulottuvuuden hallintaa. Suuri osa toimitusketjuista on dynaamisia toimitusketjuja, jotka sisältävät meriteitse kulkevia, moniporttisia reittejä. (Schauer ym., 2019) Tästä voisi päätellä, että toimitusketjujen kyberturvallisuus ja sen hallinta tulisi nähdä moniulotteisena ongelmana.

2.1 Strategioita kyberuhkien hallintaan

Markkinavoimien hyvä kyberturvallisuuden hallinta korreloi positiivisesti kaupallisen toimijan liiketoiminnan kanssa. Toimitusketjun kyberturvallisuuden hallintaan on mahdollista soveltaa useita eri strategioita. Tutkimuksessaan Pal ym. (2017) esittää, että tuottaja päässä yritykset käyttävät kyselyä turvallisuusstandardien arvioimiseen toimitusketjun eri osa-alueilla, jotta saavat kuvaa siitä minkälainen tietoturvan taso toimitusketjussa on. Kysymyksiä on mm.
1) Onko suunnittelu prosessi dokumentoitu?
2) Onko ohjelmiston tai laitteiston suunnitteluprosessi toistettavissa?
3) Kuinka myyjä käsittelee olemassa olevat ja ilmaantuvat haavoittuvuudet ja kuinka kyvykäs myyjä on osoittamaan näitä haavoittuvuuksia?
4) Millaiset standardit myyjällä on käytössä valmistuksen hallintaa, monitorointia, kokoamista ja testausta koskevia prosesseja kohtaan?
5) Miten koodin laatu testataan?

6) Mitä tekniikoita, menettelyitä ja lähestymistapoja käytetään haittaohjelmilta suojautumiseen ja niiden havaitsemiseen?
7) Kuinka tuotteen ”peukaloinnin esto” on toteutettu? Mitkä ovat metodit takaovien sulkemiseen?
8) Onko kaikki prosessit dokumentoitu oikein ja onko kokeet suoritettu standardien mukaan?
9) Minkä laatuista kulunvalvontaa harjoitetaan?
10) Kuinka asiakkaan data on suojattu?
11) Mitkä ovat salausmekanismit?
12) Kuinka pitkä on datan säilytysaika?
13) Mikä on käytäntö datan tuhoamisesta kun kumppanuus raukeaa?
14) Tehdäänkö työntekijöille taustatarkistus? Jos tehdään niin kuinka usein?
15) Minkälaisia turvallisuuskäytäntöjä noudatetaan?
16) Onko olemassa asianmukainen kyberturvallisuustarkastuslista toimitusketjun alku- että loppupäässä? Kuinka sitoutuneita tarkastuslistaa kohtaan ollaan?
17) Tehdäänkö asianmukaisia turvallisuustarkastuksia jakeluprosessiin?
18) Mitkä ovat jakelukanavien valintakriteerit?
19) Mikä mekanismi poistaa väärennetyn komponentin?
20) Miten myyjä varmistaa prosessin turvallisuuden, tuotteen, palvelun ym. tuotteen elinkaaren ajan? (Pal ym., 2017)

Edellä esitellystä kyselystä voi havaita kuinka moniulotteinen kysymys kyberturvallisuus on. Jokaisella kysymyksellä on vaikutusta siihen minkä tasoinen koko toimitusketjun kyberturvallisuus on. Tämä on tärkeää tietoa niin tilaajalle kuin toimittajalle. Tilaajan täytyy tietää, minkälaiseen tietoturvaympäristöön hän laittaa tuotteensa valmistukseen, jotta voi varmistua siitä että tuotteen koko toimitusketju on turvallinen asiakkaalle saakka. Myös toimittajan tulee tietää, minkä tasoiseen turvallisuusympäristöön organisaation on sitouduttava, jotta täytetään tilaajan laatimat laatustandardit.

Toimitusketju kehittyy aina, kun tekniikat, valmistusprosessit, kuljetusmenetelmät ja kuluttajien tarpeet muuttuvat (Barron, Cho, Hua, Norcross, Voigt & Haimes 2016). Toimitusketjujen globalisoituessa, monet toimitusketjut kulkevat esimerkiksi meriteitse ympäri maapalloa, samalla osallistuen useaan eri kyberympäristöön. Schauer ym. (2019) mukaan moderneissa toimitusketjuissa toimitusketjun infrastruktuuri on suurissa määrin riippuvainen monimutkaisista ICT ratkaisuista. Toimitusketjuissa on ollut pyrkimys lisätä joustavuutta, mutta se on tullut sillä kustannuksella, että toimitusketjun jäsenillä on hyvin epäyhtenäiset ICT ratkaisut. (Schauer ym., 2019) Viime vuosina kyberiskujen määrä on noussut joka puolella maapalloa. Vakuutusyhtiö Allianzin riskibarometrissa kyberuhkat ovat kolmanneksi suurin uhka liiketoiminnalle (Allianz, 2021). Schauer ym. (2019) tutkimuksessa tutkittiin dynaamisten toimitusketjujen kyberturvallisuutta ja sen hallintaa. Kuten tutkimuksessa todettiin, strukturoidusta ja integroidusta hallintaprosessista on tullut keskeinen osa liiketoimintaa eri sektoreilla. Useat nykyiset riskienhallintamekanismit kuten standardit ja viitekehykset on suunniteltu organisaation sisällä toimiviksi. Tarvetta on kuitenkin koko toimitusketjun kattavalle standardoinnille sekä viitekehykselle.

Standardit ISO 28000 (2007) ja ISO 28001 tarkentavat koko toimitusketjun riskinhallintaa ja ohjeistusta. ISO 28000 tarkentaa hallintasysteemiä, joka on logistiikkateollisuuden suunnittelema sekä esittelemä, ja ISO 28001 laajentaa ISO 28000:aa keskittyen enemmän käytännön implementointiin kuten hallintajärjestelmiin. Molempien standardien tavoitteena on avustaa organisaatioita saavuttamaan kohtuullinen turvallisuustaso sekä parempi riskiperusteinen päätöksentekokyky toimitusketjun turvallisuuden takaamiseksi. Kumpikaan edellä mainituista ei koske erityisesti kyberturvallisuutta, jonka vuoksi näiden käyttäminen kyberturvallisuusongelmien ratkaisemiseen ei ole kovin käytännöllistä. Tähän tarkoitukseen on luotu ISO/IEC 27001 (2013) ja ISO/IEC 27002 (2013). ISO/IEC 27001 tarkentaa tietoturvan hallintajärjestelmien vaatimuksia. ISO/IEC 27002 miten tietoturvan hallintajärjestelmiä tulee implementoida organisaatioiden sisällä. Vaikka edellä mainittua standardointia on tehty ja sitä kautta ollut yritystä luoda parempaa kyberturvallisuutta dynaamisten toimitusketjujen hallintaan, tutkimuksessa nähdään, että edelleen on pulaa selkeistä menetelmistä millä tarvittava kyberturvallisuuden taso voitaisiin saavuttaa käytännöllisesti. Tutkimuksessa ehdotettiin uutta näyttöön perustuvaa MITIGATE riskinarviointimenetelmää, jotta voidaan analysoida koko merenkulun toimitusketjun riskitaso. MITIGATE-menetelmän päätavoitteena on tukea satamaviranomaisia sekä kaikkien liikekumppaneiden riskivirkailijoita. (Schauer ym, 2019)

On olemassa toimitusketjuja joissa standardit ei ole riittävä tietoturvan tae. Joissain kaupallisissa tai ei-kaupallisissa toimitusketjuissa käsitellään tietoturvallista dataa. Sobb ja Turnbull (2020) käsittelevät tutkimuksessaan sotilaallisten toimitusketjujen vaatimuksia. Arkaluontoinen data vaatii erilaista kyberturvallisuustasoa toimitusketjussa kuin vähemmän arkaluontoinen data. Tutkimuksessaan Sobb ja Turnbull (2020), ehdottivat uutta mallia nimeltä Military Supply Chain Cyber Implications Model (M-SCCIM) jonka tehtävänä on auttaa armeijan päätöksentekijöitä ymmärtämään potentiaaliset kyberturvallisuusvaikutukset uusien teknologioiden implementoinnissa toimitusketjuun. Kyberturvallisuuskentän ja teknologioiden kehittyessä jatkuvasti, riskiarviointi on vahvasti painottunut uusien teknologioiden implementoinnin riskien, sekä sen missä määrin implementoinnilla voi olla seurauksia kyberturvallisuuden ymmärtämiseen. Sotilaallisilla tahoilla ja kaupallisilla toimitusketjuilla on useasti hyvin erilaiset päämäärät toimitusketjuilleen sekä seuraukset toimitusketjun kyberturvallisuusriskien pettäessä. Sotilaallisten tahojen toimitusketjut ovat enemmän keskittyneet turvallisuuteen kuin tuoton maksimointiin, kun taas kaupalliset toimitusketjut ovat enemmän keskittyneet tuoton maksimointiin. Jos sotilaallisessa toimitusketjussa tapahtuu esimerkiksi tietovuoto tai jokin muu vastaava kyberturvallisuuteen liittyvän riskin realisoituminen, sillä voi olla suoranaisia vaikutuksia kansalliseen turvallisuuteen.

M-SCCIM on konseptimalli, joka sisältää kolme vaihetta: 1) alustava vaihe (the Preliminary Phase) 2) pilotti vaihe (the Pilot Phase) ja 3) implementointivaihe (the Implementation Phase). 1) Alustava vaihe puntaroi lähdettä, teknologian kypsyyttä, esimerkki implementointeja sekä kyberturvallisuutta. Lähteen pohtimisessa on tarkoitus selvittää mm. missä teknologian rajat menevät, ja

kuinka syvälle se tunkeutuu toimitusketjuun. Kypsyyden arvioinnissa pyritään ymmärtämään teknologian nykytila. Kypsyyttä arvioidaan arvioimalla neljää tekijää: a) yhteisöä, b) korjaustiedostoja ja versioita d) vakautta e) hype-sykliä. 2) Pilottivaiheessa tehdään päätös, onko pilotin implementointi tutkimisen arvoinen vai tulisiko siitä luopua. 3) Implementointivaiheessa uusi teknologia implementoidaan kokonaisuudessaan osaksi toimitusketjua. (Sobb & Turnbull, 2020)

Toimitusketjujen kyberturvallisuus moniulotteisena ongelmana vaatinee moniulotteisia ratkaisuja sen hallitsemiseen. Johnson (2015) havaitsee tutkimuksessaan, että hallitukset ympäri Eurooppaa ja Pohjois-Amerikkaa luottavat jossain määrin markkinavoimiin, sääntelytoimiin, verkkovakuutuksiin ja vahingonkorvauksiin, kyberturvallisuustason määrittämisessä toimitusketjuissa (Johnson, 2015). Kyberturvallisuuteen liittyy usein julkisen ja yksityisen sektorin etujen yhdenmukaistaminen (Kosseff, 2018). Täydellisillä markkinoilla edellä mainitut toimet riittävät, eikä olisi tarvetta suuremmalle määrälle sääntelyä. On kuitenkin havaittu, että kuluttajat eivät aina ole niin valveutuneita, että osaisivat tehdä oikean päätöksen sen suhteen mitä toimitusketjua tulisi suosia. (Johnson, 2015) Tästä voisi päätellä, että kuluttajakaupassa kuluttajalla ei ole aina riittävää ymmärrystä ostamansa tuotteen toimitusketjusta, saati sen nauttimasta kyberturvallisuuden tasosta. Johnson (2015) toteaa tutkimuksessaan, että markkinoilla on jatkuva paine pienentää kuluja, ja potentiaalisilla asiakkailla voi olla rajallinen tietämys kyberturvallisuudesta sekä rajallinen motivaatio sen tason selvittämiseen. Myös organisaatioiden oma tietämyksen taso aihetta koskien voi olla puuttellista. Tästä johtuen monet organisaatiot kamppailevat kysymyksen edessä, onko kannattavaa palkata pätevää työvoimaa kyberturvallisuuden saralle (Johnson, 2015). Tästä voisi päätellä, että sääntelyssä on pyrkimys antaa markkinoille mahdollisimman vapaat kädet kyberturvallisuustason määrittämisessä. Voisi kysyä miksi ei kaikkeen toimitusketjuun vain sovellettaisi korkeinta mahdollista kyberturvallisuuden tasoa. Syitä on useita, mutta usein korkeampi kyberturvallisuus maksaa käytettävyydessä ja tehokkuudessa. Kuten Sobb ja Turnbull (2020) tutkimuksesta ilmeni, erilaisissa toimitusketjuissa painotus voi olla enemmän turvallisuudessa, joka johtaa siihen, että toimitusketjun joustavuudesta voidaan tinkiä turvallisuus perusteisesti.

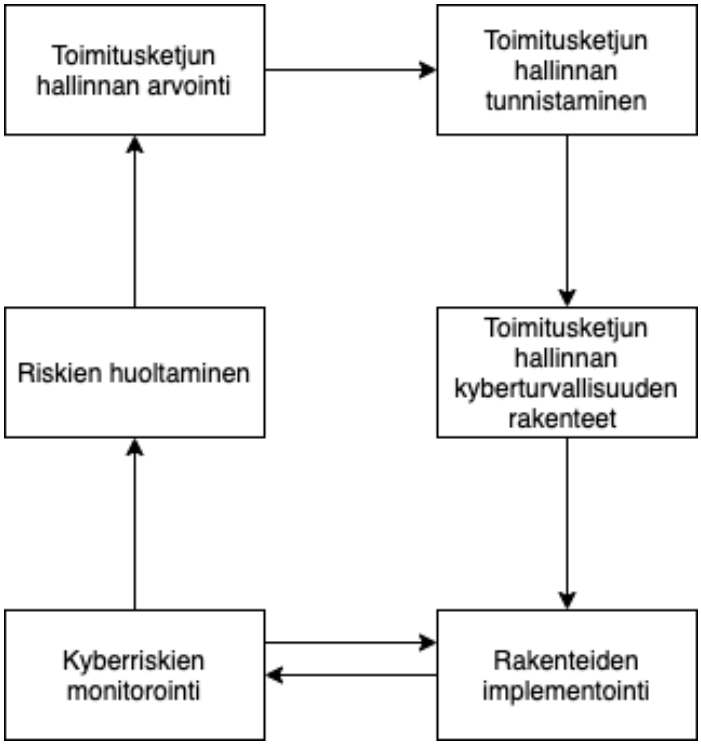
2.2 Kyberfyysisten toimitusketjujen riskinhallinta

Kyberfyysiset järjestelmät tarkoittavat integraatioita, joissa on laskentaa fyysisten prosessien lisäksi (Cyber-Physical Systems (CPS)) (Lee, 2006). Teollisuuden ohjausjärjestelmät ovat tietynlaisia kyberfyysisiä järjestelmiä, joita käytetään usein kriittisten infrastruktuurien hallintaan (Hou, Such & Rashid, 2019). Yeboah-Ofori ja Opoku-Akyea (2019) tutkimuksen mukaan, merkittävä osa kyberhyökkäyksistä käyttää “island hopping” menetelmää kyberhyökkäysten toimittamiseksi. Tämä tarkoittaa sitä, että hyökkääjä käyttää pienempien organisaatioiden heikompia tietoturvakäytäntöjä hyväkseen, hyökätessään isom-

paan organisaatioon. Tutkimuksessa omaksuttiin kybertoimitusketjun riskinhallintaprosessiksi viisiosainen prosessi, jolla voi määrittää miten vastata erilaisiin kyberhyökkäyksiin. Prosessin vaiheet ovat
A) Riskivaste (Risk Response) jossa päätetään miten käsitellä riskiä ja kuka on vastuussa.
B) Riskinhallintatoimenpiteet (Risk mitigation) eli toimet uhkaan sen perusteella mitä tietoa on kerätty. Riskinhallintatoimenpiteet jakautuvat viiteen osaan 1) Riskin siirtäminen 2) Riskin välttäminen 3) Riskin jakaminen 4) riskin vähentäminen ja 5) riskin hyväksyminen. 1) Riskin siirtämisellä tarkoitetaan esimerkiksi vakuutusyhtiön kanssa riskin jakamista, 2) riskien välttämisellä toimenpiteitä joilla saavutetaan riittävä turvallisuustaso riskin välttämiseksi 3) riskin jakamisella riskin jakamista 4) riskin vähentämisellä kouluttamista ja käyttäjien tietoisuuden lisäämistä mm. asiantuntijoiden palkkaamisella ja kommunikointimekanismeilla ja 5) riskin hyväksymisellä jolla tarkoitetaan sellaisiin riskeihin varautumista joiden tapahtuminen on välttämätöntä kuten maanjäristys.
C) Riskin monitorointi ja kontrollointi (Risk Monitoring & Control), joka tarkoittaa prosessia, jossa monitoroidaan ja kategorisoidaan riski, riskirekisteriin.
D) Riskikommunikointi (Risk Communication) sisältää harjoitusten ja töiden organisoinnin sitä kohti, että mahdollisesti vallalla olevat riskit tunnistetaan.
E) Tulosten vertailu muiden teosten kanssa. (Comparing Results with Other Works) Kyberfyysisten järjestelmien ja kybertoimitusketjujen riskienhallintaan on olemassa olevia teoksia. (Yeboah-Ofori & Opoku-Akyea, 2019).

3 KÄYTÄNTEET KYBERTURVALLISUUDEN LISÄÄMISEKSI

Tässä luvussa kootaan käytänteitä, joita toimitusketju voi ottaa käyttöön, lisätäkseen toimitusketjun kyberturvallisuuden tasoa. Pal ym. (2017) tutkimuksessa todetaan, että kyberturvallisuusriskien minimoimiseksi vaaditaan riskivapaa ja tehokas tuotteen elinkaari. Tietoturvajärjestelmät pelkästään eivät ole riittäviä kriittisen tiedon suojaamiseen koko toimitusketjun kattavasti, ellei koko toimitusketju käytä kyberturvallisuuskäytäntöjä ja -standardeja.

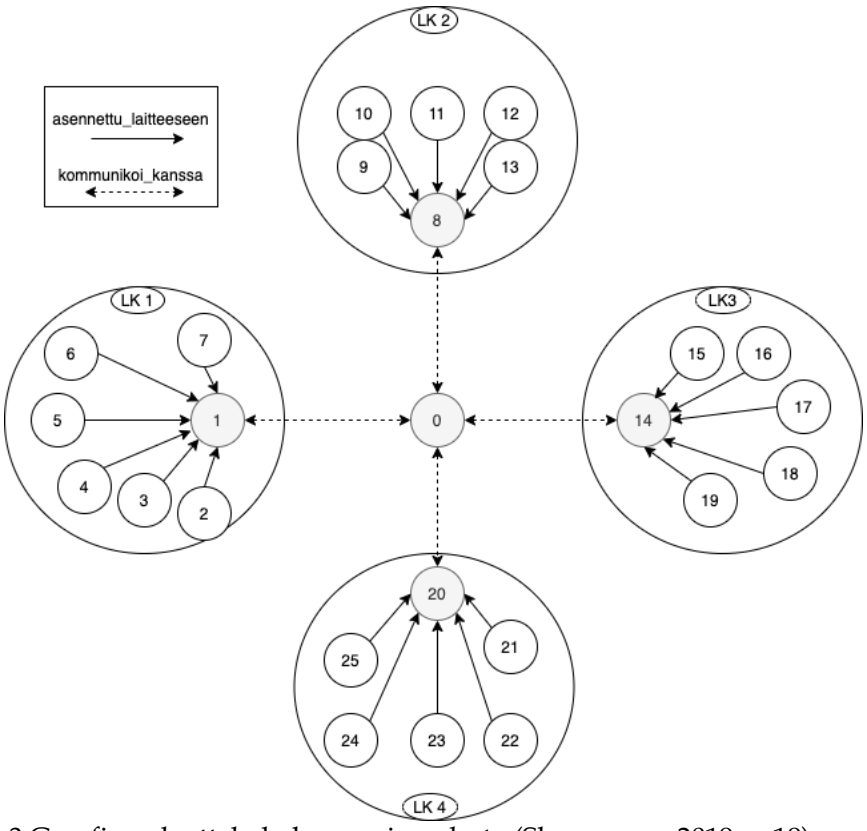


KUVIO 2 Toimitusketjun kyberturvallisuus elinkaari (Pal ym., 2017, s.664)

Pal ym. (2017) esittävät tutkimuksessaan edellä olevaa mallia toimitusketjun kyberturvallisuuden elinkaareksi. Edellä esitelty mallin noudattaminen voi tutkimuksen mukaan osoittautua tärkeäksi. Huolellisella vaiheiden seuraamisella voidaan saavuttaa riskivapaa toimitusketjunhallinnan elinkaari.

Shauer ym (2019) tutkimuksessaan esittelemä näyttöön perustuva ”MITIGATE” menetelmä pyrkii arvioimaan koko merenkulun toimitusketjun riskitason. Menetelmän tärkein anti on

1) graafinen luettelo kaikesta kyberomaisuudesta (LK = liikekumppani kuvio 4)
2) luettelo kaikista mahdollisista hyökkäyskanavista (taulukko 1)
3) arvio nollapäivän hyödynnettävistä haavoittuvuuksista
4) arvio yksittäisistä, kumulatiivisista ja lisääntyneistä haavoittuvuuksista sekä kaikkien omaisuuksien vaikutuksista ja riskeistä
5) optimaalinen lieventämisstrategia, joka perustuu annettuihin mahdollisiin puolustustoimenpiteisiin.



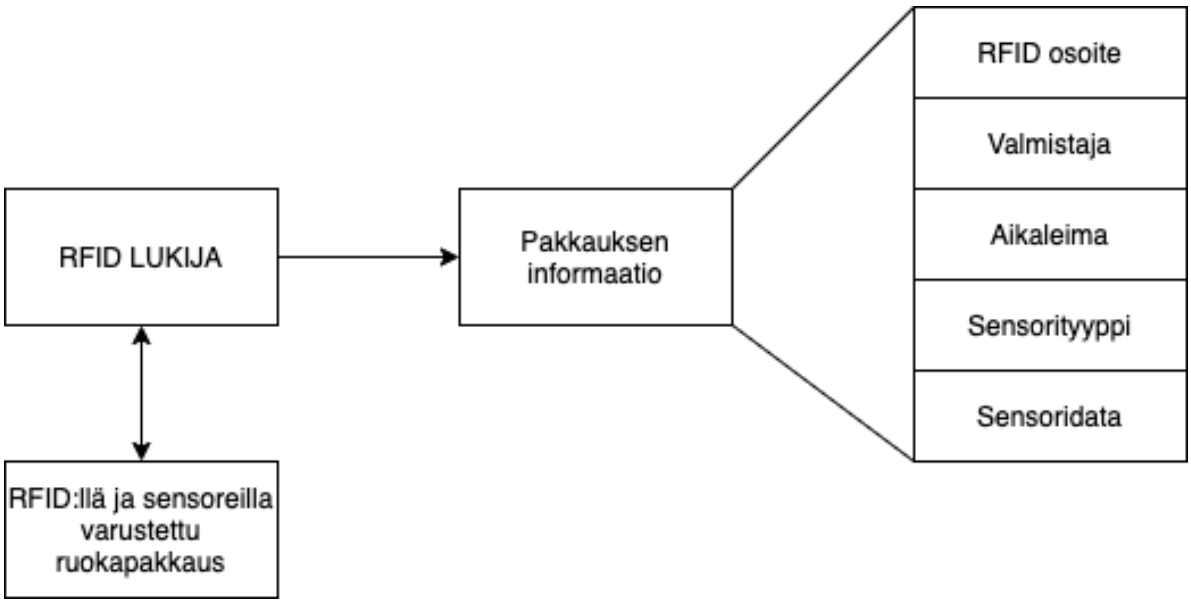
KUVIO 3 Graafinen luettelo kyberomaisuudesta (Shauer ym., 2019, s. 19)

TAULUKKO 1 taulukko hyökkäyskanavista

Uhka ID	**Uhkan kuvaus**	**Liittyvät omaisuudet**
U1	Tietojenkalastelu	10, 16, 22
U2	Identiteettivarkaus	1-25
U3	Tietovuoto	1-25
U4	Kiristyshaittaohjelma	1-25
U5	Datan eheyden menetys	1-7, 14-19
U6	Palvelunestohyökkäys	1-7
U7	Tietojen menetys	1-25
U8	Viestintäverkon katkos	0

Vaikka edellä mainittuja toimenpiteitä voi käyttää lisäämään toimitusketjun kyberturvallisuuden tasoa, Pal ym. (2017) näkevät tutkimuksessaan, että nykyiset käytännöt kyberturvallisuusriskien torjumiseksi eivät ole riittäviä toimitusketjuissa (Pal ym., 2017).

Lohkoketjuteknologia auttaa pyrkimyksissä varmistamaan datan eheyttä läpi toimitusketjun. Ruokahävikkiä tapahtuu ruoan toimitusketjun eri vaiheissa, heti tuotannossa, jalostuksessa, pakkaamisessa, kuljetuksessa, tukkumarkkinoilla, jälleenmyynnissä ja kulutuksen aikana (Parvin, Gawanmeh & Venkatraman 2018). Mondal, Wijewardena, Karuppuswami, Kriti, Kumar ja Chahal esittävät vuonna 2019 julkaisemassa tutkimuksessaan, että lohkoketjuteknologia tarjoaa mahdollisuuden hajautettuun järjestelmään pitää kirjaa transaktioista ja tapahtumista, joita ei pysty väärentämään. Uskotaan että lohkoketju kykenee ratkaisemaan suurimman osan myös esineiden internetin eheyskysymyksistä (Makhdoom, Abolhasan, Lipman, Liu & Ni, 2019). Lohkoketjuun integroidut älykkäät sopimukset voivat auttaa automaattisessa suorituksessa suojatulla todennuksella (Gupta, Tiwari, Bukkapatnam & Karri 2020). Älykkäät sopimukset ovat koodin palasia, joista tulee osa lohkoketjua ja niitä voidaan käyttää ohjelmointimallin ominaisuuksien toteuttamiseen (Paavolainen, Elo & Nikander, 2018). Lohkoketjuteknologiaa voidaan käyttää ruoan toimitusketjuissa parantamaan datan eheyttä (Mondal ym, 2019). Käytännössä tämä tarkoittaa sitä, että voidaan paremmin olla selvillä siitä mitä tapahtumia missäkin toimitusketjun vaiheessa on. Lohkoketju on joukko lohkoja, joissa jokainen lohko sisältää hajautusarvon (hash) edellisestä lohkosta ja näin luo ketjun lohkoista. Mylrea ja Gourisetti (2018) mukaan yksi lohkoketjujen haaste on, että lohkoketjuille on olemassa monia erilaisia määritelmiä. Tämä luo haasteita lohkoketjuteknologian sääntelyviranomaisille ja päättäjille, jotka yrittävät luoda sovellutuksia ja hallintoa lohkoketjuteknologialle (Mylrea & Gourisetti, 2018). Mondal ym. (2019) tutkimuksessa tehtiin turvallisuusanalyysi RFID (radio frequency identification) pohjaisen informaatioarkkitehtuurin käytöstä lohkoketjuympäristössä. (Mondal ym., 2019) RFID on datankeräystekniikka, joka välittää informaatiota radioaalloilla vastaanottavalle yksikölle (Blachard, 2010).



KUVIO 4 Esimerkki RFID:tä ja sensoreita käyttävästä ruokapakkauksesta poimitun tiedon kulusta (Mondal ym., 2019, s.2)

Mondal ym. (2019) esittää tutkimuksessaan, että datan eheyttä koskevia merkittäviä haavoittuvuuksia ovat:

1) datan peukalointi,
2) roskaposti,
3) yksityisyyden varastaminen,
4) fyysisen kerroksen hyökkäys ja
5) erityiskohtelu

Tutkimuksessa käytiin haavoittuvuuksia läpi seuraavista näkökulmista: peukalointi tarkoittaa tässä yhteydessä luvattomien lohkojen lisäämistä lohkoketjuun, roskapostilla roskapostihyökkäystä jonka vaikutukset vertautuvat palvelunestohyökkäykseen, yksityisyyden varastamisella tilanteita joissa saastunut pääte varastaa informaatiota esiintyen alkuperäisenä päätteenä, fyysisen kerroksen hyökkäyksellä kaikkia fyysisellä tasolla tapahtuvia hyökkäyksiä ja erityiskohtelulla joidenkin transaktioiden mahdollisuutta tulla suosituksi suhteessa toiseen transaktioon puolueellisessa päätteiden verkossa.

Turvallisuusanalyysissä tultiin lopputulemaan että olemassa oleva data on datan peukaloinnilta suojassa salauksen turvin, kuitenkin ei-halutun lohkon validointi voi tapahtua tilanteessa, jossa vilpillinen pääte lähettää valheellisen transaktion, ja samalla transaktioon liittyy useita vilpillisiä solmuja (node) jotka lähettävät takaisin kuittauksen. Roskapostihyökkäykset voivat olla ongelma hajautetussa arkkitehtuurissa, jos esimerkiksi vilpillinen pääte rekisteröi vilpil-

lisen sensorID:n verkossa. Tästä voi aiheutua se että oikeita sensorID:tä ei enää rekisteröidä, mutta muistia varataan. Tämä voidaan ratkaista sertifikaattipohjaisella todennuksella, toisin sanoen fyysisen kerroksen tunnisteet tulisi suojata. Fyysisen kerroksen informaatio kuten sensorID:n RFID osoite ja skannaus solmun ip-osoite ovat tärkeätä informaatiota, mikä pitäisi suojata. Riippuen siitä kuinka hyvin fyysisen kerroksen suojausmekanismit on järjestetty, voidaan päätellä mitä kaikkea fyysisen kerroksen hyökkäyksellä voidaan saada aikaan, ja miten näiltä tulisi suojautua. Erityiskohtelu voi tulla kysymykseen, mutta tutkimuksessa se nähtiin vähiten todennäköisenä tapahtumana, sillä suurin osa transaktioinformaatiosta kommunikoidaan salattuna. (Mondal ym., 2019)

4 JOHTOPÄÄTÖKSET

Kun rahtilaiva liikkuu satamasta toiseen toimittaen toimitusketjun yläjuoksulta materiaaleja tai palveluita kohti toimitusketjun alajuoksua, tulee jatkuvasti olla tietoinen kyberympäristön mahdollisista riskeistä ja kuinka näihin tulisi olla varautunut. Aiempana esitellystä voisi olettaa, että tavanomaiset menetelmät kyberturvallisuuden takaamiseksi eivät ole riittäviä toimitusketjuissa, joissa jokainen toimitusketjussa toimiva organisaatio voi olla kyberturvallisuustapaturman syynä. Kun kyberhyökkäysmenetelmänä on esimerkiksi ”island hopping”, toimitusketjun kyberturvallisuuden voisi nähdä yhtä vahvana kuin sen heikoin lenkki. Tämän kirjallisuuskatsauksen lähdeaineiston perusteella, voisi olettaa, että tarvitaan erilaisia viitekehyksiä, malleja ja kyselyitä, jotta voidaan saavuttaa kyberturvallisuuden taso, joka on liiketoiminnan vaatimusten kannalta tyydyttävä. Onneksi tällä saralla tutkimusta tehdään ja toivottavasti tulevaisuudessa olisi saatavilla lähes yhtenäinen viitekehys tai malli, jolla toimitusketjun kyberturvallisuutta voisi ohjata.

Toimitusketjujen kyberturvallisuuden voi lähdeaineiston perusteella olettaa olevan moniulotteinen ongelma. Schauer ym. (2019) tutkimuksesta voi saada kuvan, että toimitusketjun kyberturvallisuus vaatii toimitusketjun hallintaa, laadunvarmistusstandardeja sekä IT ulottuvuuden hallintaa. Suuri osa toimitusketjuista on dynaamisia toimitusketjuja, jotka sisältävät meriteitse kulkevia monien satamien läpi kulkevia reittejä. (Schauer ym., 2019) Näillä reiteillä altistutaan jatkuvasti kyberuhille. Standardointi on osaltaan hyvä ratkaisu kyberturvallisuuden tason laadun varmistamisessa, mutta siitä huolimatta tämän kirjallisuuskatsauksen lähdemateriaalin perusteella voisi olettaa, että on olemassa tarve selkeille menetelmille, joilla voidaan saavuttaa tyydyttävä kyberturvallisuuden taso. Olisiko tarpeeksi kattava standardointi ratkaisu toimitusketjun kattavaksi kyberturvallisuuden takaajaksi, vai tarvitaanko yhtenäinen viitekehys kaikille toimijoille. Toimitusketjut ovat niin monimutkaisia laitteiston ja sitä koskevan kyberturvallisuuden osalta, että sitä koskien on hyvin hankala tehdä yhtenäistä mallia, jolla haluttu kyberturvallisuustaso saavutettaisiin.

Voisi nähdä, että lähes kaikessa tässä kirjallisuuskatsauksessa käsitellyssä lähdekirjallisuudessa toistuu sama ongelma, yhtä yhtenäistä mallia

toimitusketjun kyberturvallisuuden hallintaan ei ole. Kirjallisuuskatsauksen perusteella vaikuttaa, että yhdelle yhtenäiselle toimitusketjujen kyberturvallisuutta luokittelevalle järjestelmälle olisi kysyntää. Se helpottaisi myös kuluttajaa olemaan tietoisempi siitä, minkälaisen kyberuhan alle hän tietonsa altistaa. Miten yhtenäistä mallia sitten tulisi lähteä kehittämään? Aihe vaatinee jatkotutkimusta tältä osin.

LÄHTEET

Allianz. (2021). Allianz risk barometer 2021 identifying the major business risks for 2021. Haettu osoitteesta https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2021.pdf

Barron S., Cho Y. M., Hua A., Norcross W., Voigt J. & Haimes Y. (2016). Systems-based cyber security in the supply chain. *2016 IEEE Systems and Information Engineering Design Symposium (SIEDS)*, (20-25).Charlottesville, Va, USA. 29-29 April, 2016

Blanchard, D., (2010). Supply Chain Management Best Practices. Wiley Best Practices, 2nd ed. Haettu osoitteesta https://eds-a-ebscohost-com.ezproxy.jyu.fi/eds/ebookviewer/ebook/bmxlYmtfXzMxOTUwOF9fQU41?sid=23d2ea6e-c245-45dd-bb05-b5ddcfcb7f6a@sessionmgr4006&vid=1&format=EB

Gupta, N., Tiwari, S. T. S., Bukkapatnam & Karri, R. (2020). Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks. *IEEE Access, 8,* 47322-47333

Hou Y., Such J. & Rashid A. (2019). Understanding Security Requirements for Industrial Control System Supply Chains. *2019 IEEE/ACM 5th International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS)*, (50-53), Montreal, QC, Canada, 28-28 May 2019

Johdatus kyberturvallisuuteen. (2021). Kyberuhat ja niiden aiheuttajat. Haettu 10.5.2021 osoitteesta https://peda.net/jyu/it/do/kkv/4kjna

Johnson, C. W., (2015). The role of cyber-insurance, market forces, tort and regulation in the cyber-security of safety-critical industries. *10th IET System Safety and Cyber-Security Conference 2015*, (1-7). Bristol, UK, 21-22 Oct. 2015

Kosseff J. (2018). Developing collaborative and cohesive cybersecurity legal principles. *10th International Conference on Cyber Conflict (CyCon)*, Tallinn, Estonia, 29 May-1 June 2018

Lee, E. A., (2006). Cyber-Physical Systems - Are Computing Foundations Adequate? Haettu osoitteesta https://ptolemy.berkeley.edu/publications/papers/06/CPSPositionPaper/Lee_CPS_PositionPaper.pdf

Logistiikan maailma. (2021). Logistiikka ja toimitusketju. Haettu 27.4.2021 osoitteesta https://www.logistiikanmaailma.fi/logistiikka/logistiikka-ja-toimitusketju/

Makhdoom I., Abolhasan M., Lipman J., Liu R. P. & Ni W. (2019). Anatomy of Threats to the Internet of Things. *IEEE Communications Surveys & Tutorials,* 21 (2), 1636-1675

Mondal, S., Wijewardena, K. P., Karuppuswami, S., Kriti, N., Kumar, D. & Chahal, P. (2019). Blockchain Inspired RFID-Based Information Architecture for Food Supply Chain. *IEEE Internet of Things Journal, 6(3),* 5803-5813.

Mylrea M. & Gourisetti S. N. G. (2018). Blockchain for Supply Chain Cybersecurity, Optimization and Compliance. *Resilience Week (RWS)*, (70-76). Denver, CO, USA, 20-23 Aug. 2018

Paavolainen, S., Elo, T. & Nikander, P. (2018). Risks from Spam Attacks on Blockchains for Intemet-of-Things Devices. *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2018, (314-320),* Vancouver, BC, Canada: 1-3 Nov. 2018

Pal, O., Srivastava, V., & Alam, B. (2017). Cyber security risks and challenges in supply chain. *International Journal of Advanced Research in Computer Science, 8(5),* 662-666

Parvin S., Gawanmeh A. & Venkatraman S. (2018). Optimised Sensor Based Smart System for Efficient Monitoring of Grain Storage. *2018 IEEE International Conference on Communications Workshops (ICC Workshops),* (1-6), Kansas City, MO, USA, 20-24 May 2018

Salminen A. (2011). *Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin.* Vaasan yliopiston julkaisusarja, opetusjulkaisuja 62, Julkisjohtaminen 4.

Schauer, S., Polemi, N., & Mouratidis, H. (2019). MITIGATE: A dynamic supply chain cyber risk assessment methodology. *Journal of Transportation Security, 12(1-2)*

Sobb, T. M., and Turnbull, B. (2020). Assessment of Cyber Security Implications of New Technology Integrations into Military Supply Chains. Teoksessa 2020 IEEE Security and Privacy Workshops (SPW), (128-135). San Francisco, CA, USA, 21-21 May 2020.

Yeboah-Ofori, A. & Opoku-Akyea, D. (2019). Mitigating Cyber Supply Chain Risks in Cyber Physical Systems Organizational Landscape. 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), Accra, Ghana, 29-31 May 2019

Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. Future Internet, 11(3), 63.