TURUN YLIOPISTO
Kauppakorkeakoulu

Digitaalisen toimitusketjun kyberturvallisuuden tehostaminen uusien teknologioiden avulla

Toimitusketjujen johtamisen kandidaatintutkielma

Laatija:
Kasimir Hälvä

Ohjaaja:
KTT Sini Laari

15.12.2024
Turku

Kandidaatintutkielma

Oppiaine: Toimitusketjujen johtaminen
Tekijä: Kasimir Hälvä
Otsikko: Digitaalisen toimitusketjun kyberturvallisuuden tehostaminen uusien teknologioiden avulla
Ohjaaja: KTT Sini Laari
Sivumäärä: 37 sivua
Päivämäärä: 15.12.2024

Tämä tutkielma käsittelee digitaalisten toimitusketjujen kyberturvallisuutta ja sen tehostamista Industry 4.0 teknologioiden avulla. Digitalisaation nopea eteneminen on alkanut muuttamaan toimitusketjuja monimutkaisiksi, integroiduiksi ja digitaalisiksi järjestelmiksi, joka on luonut uusia haavoittuvuuksia. Tämä muutos on nostanut kyberturvallisuuden merkittävään asemaan. Tutkielmassa tarkastellaan digitaalisiin toimitusketjuihin kohdistuvia kyberuhkia ja -onnettomuuksia, keskittyen erityisesti toimitusketjuhyökkäyksiin ja inhimillisen virheen aiheuttaneisiin kyberonnettomuuksiin. Lisäksi arvioidaan uusien teknologioiden, kuten tekoälyn, Big Data -analytiikkan, lohkoketjuteknologian, pilvipalveluiden ja IoT:n potentiaalia kyberturvallisuuden parantamiseksi uhkien ennaltaehkäisyssä ja tunnistamisessa, tietoturvan vahvistamisessa sekä reagointi- ja palautumiskyvyn tehostamisessa.

Digitaalisiin toimitusketjuihin kohdistuvat kyberhyökkäykset ja -onnettomuudet saavat aikaan suurta tuhoa maailmanlaajuisasti. SolarWindsin toimitusketjuhyökkäys ja CrowdStriken IT-katkos havainnollistavat, miten vakavia seurauksia organisaatiot kokevat laajalle levittyvistä kriiseistä. SolarWindsin tapaus vaikutti yli 18 000 organisaatioon, joiden joukossa oli suuria monikansallisia yrityksiä ja valtiollisia virastoja. CrowdStrike aiheutti sen sijaan lähes 100 miljardin dollarin kustannukset. Näitä kahta esimerkkitapausta hyödynnetään läpi tutkielman, kun tarkastellaan erityyppisiä haavoittuvuuksia ja uhkia sekä uusien teknologioiden tarjoamia ratkaisuja.

Tutkielman muoto on kirjallisuuskatsaus. Lähteinä käytettiin pääasiallisesti alan teoreettista kirjallisuutta sekä luotettavien julkisten organisaatioiden raportteja ja julkaisuja tapausten havainnollistamiseksi. Tulokset osoittavat, että Industry 4.0:n teknologioilla on merkittävä potentiaali parantaa digitaalisten toimitusketjujen kyberturvallisuutta. Tuloksissa kuitenkin korostuu käsitys, että pelkkä teknologiaan keskittyminen ei riitä. Kyberturvallisuuden tulee olla kokonaisvaltainen strategia, joka kattaa kaikki organisaation ihmiset, prosessit ja teknologiset ratkaisut. Lisäksi syntyy tarve kehittää organisaatiokulttuuria, jossa tietoturva nähdään kaikkien vastuulla ja jossa virheistä oppiminen on tärkeämpää kuin syyllisten etsiminen.

Avainsanat: digitaalinen toimitusketju, kyberturvallisuus, kyberuhka, uudet teknologiat

SISÄLLYS

KUVIOT

TAULUKOT

1 Johdanto

Digitaalinen transformaatio on muovannut yhteiskuntaa ja liiketoimintaa ennennäkemättömällä tavalla. Tiedonsiirron nopeus on lisääntynyt eksponentiaalisesti, mahdollistaen yritysten reaaliaikaisen vuorovaikutuksen maailmanlaajuisesti. Uusien innovatiivisten teknologioiden, kuten tekoälyn, Big Data -analytiikan, esineiden internetin (IoT) ja pilvilaskennan, käyttöönotto on tehostanut liiketoimintaa ja muuttanut perinteisiä toimintatapoja. Tämä globaali muutos on johtanut myös toimitusketjujen digitalisoitumiseen, kun perinteisistä maantieteellisesti hajautuneista rakenteista on siirrytty kohti verkottuneita ja integroituja ekosysteemejä. Digitaalinen toimitusketju ei ole pelkästään digitaalisia palveluita tarjoava tai hyödyntävä järjestelmä, vaan uudenlainen prosessi, joka toimii älykkäästi, tehokkaasti ja arvolähtöisesti. Tämä digitalisoitunut rakenne luo organisaatioille uusia tulonlähteitä ja edistää niiden liiketoimintaa. Digitaalisissa toimitusketjuissa korostuu ominaisuudet kuten joustavuus ja ketteryys organisaation digitaalisten valmiuksien kasvaessa. (Büyüközkan & Göçer, 2018; Nasiri ym., 2020; Queiroz ym., 2021.)

Digitalisaatio on kuitenkin luonut uusia haavoittuvuuksia ja riskejä, joista kyberuhkat ovat nousseet merkittäväksi huolenaiheeksi niin yksityishenkilöille, yrityksille kuin hallituksillekin. Erityisesti huomio tulisi suunnata digitaalisten toimitusketjujen kyberturvallisuuteen. Kyberturvallisuus tarkoittaa arkaluonteisten tietojen, ohjelmistojen ja järjestelmien suojaamista kyberuhilta, kuten kyberhyökkäyksiltä, tietovuodoilta ja muilta kybertapauksilta. Toimitusketjuihin kohdistuvat kyberhyökkäykset aiheuttavat laajoja taloudellisia vahinkoja ja yhteiskunnallisia häiriöitä globaalisti. Yritysten ja muiden digitaalisia alustoja hyödyntävien toimijoiden onkin ryhdyttävä ennakoivasti torjumaan kyberuhkia ja parantamaan omaa kyberturvallisuuttaan. (Nygård & Katsikas, 2022; Kumar ym., 2023; Khokhar ym., 2024.) Maailman talousfoorumin riskiraportin mukaan kyberturvallisuuden vaarantumiseen liittyvät huolenaiheet kuuluvat nykyään viiden suurimman maailmanlaajuisen riskin joukkoon (World Economic Forum, 2024). Tämä korostaa kyberturvallisuuden kriittistä merkitystä digitaalisessa maailmassa ja toimitusketjujen suojaamisessa. Digitaalisten toimitusketjujen kyberturvallisuuden tutkiminen onkin entistä tärkeämpää.

Alan kirjallisuudessa on yhä puutteita, vaikka digitaalisten toimitusketjujen kyberturvallisuuden tutkimus on lisääntynyt viime vuosina. Pandey ym. (2020) toteavatkin, että toimitusketjujen kyberturvallisuus on noussut valokeilaan vasta viime vuosina, ja akateemista tutkimusta, joka painottuisi digitaalisiin toimitusketjuihin, on edelleen niukasti. Aarland (2024) puolestaan huomauttaa, että tutkimuksessa on puutteita sen suhteen, mitkä digitaalisten toimitusketjujen osa-

alueet vaatisivat kohdennettua hallintaa kyberriskien minimoimiseksi. Melnyk ym. (2022) korostavat samansuuntaisesti tarvetta lisätä kyberturvallisuustutkimusta läpi koko digitaalisen toimitusketjun, jotta saavutettaisiin kaikkien toimijoiden keskinäinen ymmärrys ja yhteinen käsitys kattavasta kyberturvallisuudesta. Cheung ym. (2021) painottavat, että suurin osa toimitusketjujen kyberturvallisuutta koskevista tutkimuksista käsittelee ennaltaehkäiseviä toimenpiteitä, kun taas kriiseihin reagointia ja toiminnan palauttamista koskevia tutkimuksia on vähän. Näiden lähteiden yhtenevä viesti, esittää kyberturvallisuustutkimuksen merkittävää tarvetta digitaalisissa toimitusketjuissa.

Tutkielmassa tarkastellaan digitaalisten toimitusketjujen kyberturvallisuuteen liittyviä haavoittuvuuksia ja siihen kohdistuvia merkittävimpiä kyberuhkia ja -onnettomuuksia. Kyberuhkista analysoidaan erityisesti toimitusketjuhyökkäyksiä ja ihmisten virheiden aiheuttaneita kyberonnettomuuksia. Tarkastelussa on kaksi tosielämän tapausta: CrowdStriken IT-katkos ja SolarWindsin toimitusketjuhyökkäys, jotka korostavat toimitusketjujen kyberonnettomuuksien laajuutta. Näissä tapauksissa yhden haavoittuvan osapuolen takia koko toimitusketju on kokenut vakavat seuraukset. Lisäksi tutkitaan, miten Industry 4.0:n avainteknologiat, kuten tekoäly, Big Data -analytiikka, lohkoketjut, pilvipalvelut ja IoT, voivat parantaa kyberturvallisuutta uhkien ennaltaehkäisyssä ja tunnistamisessa, tietoturvan vahvistamisessa sekä reagointikyvyssä ja palautumisessa kyberhyökkäysten jälkeen. Tutkielmassa pyritään vastaamaan seuraaviin tutkimuskysymyksiin olemassa olevan tieteellisen kirjallisuuden avulla:

1) Millaisia kyberuhkia ja -onnettomuuksia digitaaliseen toimitusketjuun kohdistuu?

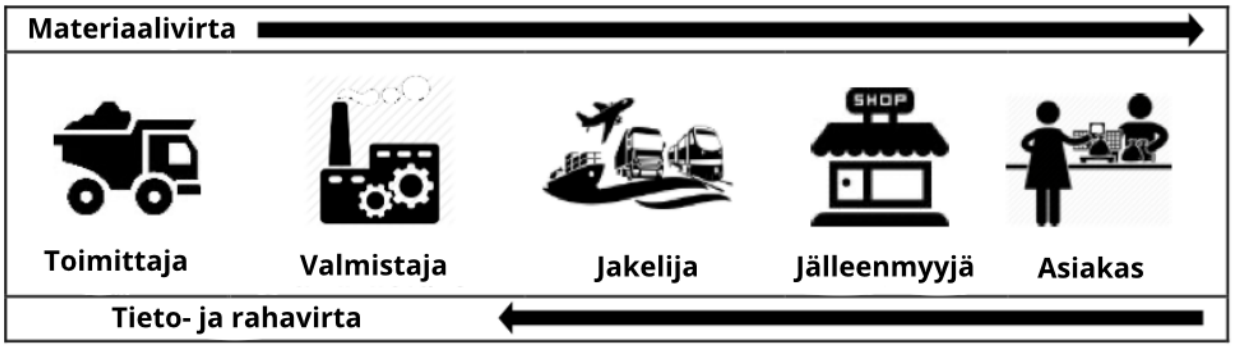
2) Miten digitaalisen toimitusketjun kyberturvallisuutta voitaisiin parantaa uusien teknologioiden avulla?

Tutkielma toteutetaan kirjallisuuskatsauksena. Artikkelien ja muiden tutkielmassa käytettyjen tieteellisten lähteiden etsinnässä on pääosin käytetty Google Scholarin ja Scopuksen tietokantoja. Ajoittain käytössä on ollut lisäksi Emerald, Volter ja ProQuest -tietokannat. Pääasiassa käytössä olivat englanninkieliset hakutermit, koska suomenkielisen kirjallisuuden havaittiin olevan rajoittunutta. Kantavina hakutermeinä vaihtelevin muodoin toimivat muun muassa: ’’supply chain’’, ’’digital supply chain’’, ’’cybersecurity’’, ’’cyberthreat’’, ’’cyberrisk’’, ’’indystry 4.0’’, ’’cyber resilience’’. Näitä on käytetty katkaisemalla ja Boolen operaattoreita hyödyntämällä. Lähteiden valintaa on rajattu vertaisarvioituihin ja JUFO-portaalin kautta tarkastettuihin lähteisiin. Lisäksi paikoittain hahmottamisen tukena on käytetty luotettavien organisaatioiden, kuten Statistan ja World Economic Forumin, raportteja.

2 Digitaalinen toimitusketju

2.1 Perinteisestä digitaaliseen toimitusketjuun

Toimitusketju on verkosto, joka koostuu useista organisaatioista, jotka tekevät tiivistä yhteistyötä toimittaakseen tietyn tuotteen tai palvelun asiakkaalle. Se on sarja toisiinsa kytkettyjä toimintoja, joihin kuuluu mm. tuotteiden tai palveluiden suunnittelu, valmistus, varastointi ja kuljetus. Toimitusketju pitää siis sisällään kaikki mahdolliset vaiheet alkutuottajalta loppuasiakkaalle asti. Toimitusketjun hallinta (engl. supply chain management) on näiden toimintojen optimointia, jolla pyritään parantamaan koko toimitusketjun tehokkuutta ja laatua sekä vähentämään kustannuksia. Perinteisesti toimitusketjut ovat koostuneet useista hajautuneista ja epäyhtenäisistä vaiheista. Kuvio 1 osoittaa, miten materiaalivirta kulkee perinteisissä toimitusketjuissa vertikaalisesti alkupään toimittajilta asiakkaille päin, kun samanaikaisesti tieto- ja rahavirta liikkuu vastakkaiseen suuntaan. (Büyüközkan & Göçer, 2018; Menon & Shah, 2019.)



Kuvio 1 Malli perinteisestä toimitusketjusta (mukaillen: Menon & Shah, 2019)

Digitalisaatio on haastanut perinteiset toimitusketjumallit, joiden vertikaalinen rakenne ei enää vastaa dynaamisen maailmantalouden vaatimuksia. Nämä toimitusketjut kohtaavat nykyisessä liiketoimintaympäristössä merkittäviä haasteita, sillä ne eivät pysty hyödyntämään digitalisoituneen ekosysteemin tuomia etuja. (Büyüközkan & Göçer, 2018; Menon & Shah, 2019.)

Ensinnäkin tiedon tehokas kulku on perinteisissä toimitusketjuissa usein hidasta ilman uusia teknologioita, mikä johtaa viivästyneeseen reagointiin ja heikentää koko toimitusketjun ketteryyttä. Tällöin muuttuviin markkinatilanteisiin reagointi ja kyky omaksua uusia teknologioita vaikeutuu entisestään. Lisäksi yhteistyön puute eri osapuolten välillä saattaa vaivata perinteisiä toimitusketjuja aiheuttaen ristiriitoja, jotka entisestään heikentävät toiminnan tehokkuutta. Asiakkaiden odotusten täyttäminen on haastavaa ilman monikanavaisia palveluita, joka laskee asiakaskokemusta. Puutteellinen teknologia voi johtaa myös läpinäkyvyyden puutteeseen ja epätarkkoihin ennusteisiin,

joista voi seurata ylimääräisiä kuluja ja huonoja päätöksiä. (Büyüközkan & Göçer, 2018; Menon & Shah, 2019.)

Nämä haasteet ovat ajaneet perinteiset toimitusketjut muutoksen partaalle. Digitaalinen muutoskin tuottaa itsessään haasteita. Alustavat investoinnit uuteen teknologiaan voivat olla korkeita ja osaaminen niiden käyttöön vähäistä. Muutosvastarinta saattaa hidastaa organisaation digitalisoitumista, kun työntekijät ovat edelleen tottuneita vanhoihin toimintatapoihin eivätkä halua muuttaa niitä. Tällöin johdon on oltava sitoutunut muutokseen, ja heillä tulee olla vahva näkemys tavasta sen toteuttamiseen. (Büyüközkan & Göçer, 2018; Boyson ym., 2022.)

Digitalisaation tuomat uudet innovaatiot ja älyteknologiat ovat mahdollistaneet kehityksen perinteisistä kömpelöistä toimitusketjuista, integroiduiksi ja tehokkaiksi järjestelmiksi, jotka luovat kilpailuetua nopean tiedonvälityksen ja korkean ketteryyden ansiosta. Digitaalinen toimitusketju on lisäarvoa tuottava, korkeasti integroitunut verkosto organisaatioita, joka hyödyntää älykkäästi uusia teknologioita internetpohjaisten alustojen avulla. Toimitusketjun digitaalisuus perustuu siis siihen, hallitaanko sitä digitaalisesti ja älykkäiden teknologioiden avulla, ei pelkästään sen läpi virtaavien palveluiden ja tuotteiden digitaalisuuden tasosta. (Büyüközkan & Göçer, 2018; Nasiri ym., 2020; Garay-Rondero ym., 2020; Queiroz ym., 2021; Boyson ym., 2022.) Tästä voidaan johtaa päätelmä, että lähes mikä tahansa toimitusketju voi kehittyä digitaaliseksi hyvin toteutetun muutoksen avulla.

2.2 Digitaalisten toimitusketjujen avainteknologiat

Industry 4.0, joka tunnetaan myös neljäntenä teollisena vallankumouksena, edustaa älykkään valmistuksen ja teollisuuden digitalisoitumista. Tämä ilmiö ei koske pelkästään yksittäisten teknologioiden käyttöönottoa, vaan se edustaa laajempaa paradigman muutosta, joka yhdistää fyysisen ja digitaalisen maailman sekä eri toimijat. Industry 4.0:n keskiössä ovat älykkäät teknologiat kuten lohkoketjut, Big Data, IoT, pilvipalvelut ja tekoäly. Nämä teknologiat ovat samalla digitalisoituneiden toimitusketjujen avainelementtejä. (Wang ym., 2016; Garay-Rondero ym., 2020; Queiroz ym., 2021.)

2.2.1 Tekoäly

Tekoälyn (engl. artificial intelligence) hyödyntäminen toimitusketjun hallinnassa on noussut keskeiseksi tutkimusaiheeksi. Tekoälyn kyky käsitellä suuria tietomääriä, tunnistaa kuvioita ja ratkaista kompleksisia ongelmia tarjoaa merkittäviä mahdollisuuksia parantaa useita toimitusketjun prosesseja. Merkittäviä tekoälymenetelmiä ovat mm. keinotekoiset neuroverkot (engl. artificial neural networks), sumea logiikka (engl. fuzzy logic) ja agenttipohjaiset järjestelmät (engl. agent-

based systems), joita käytetään ennustamisessa, optimoinnissa ja päätöksenteossa. Näitä menetelmiä ja muita tekoälyn sovelluksia on otettu laajasti käyttöön useilla toimitusketjun osa-alueilla, kuten markkinoinnissa, logistiikassa ja tuotannossa. Tarvetta lisätutkimukselle on havaittu erityisesti toimitusketjun integroinnin ja kustannusoptimoinnin alueilla. (Toorajipour ym., 2021.)

2.2.2 Big Data

Big Datalla viitataan erittäin suuriin ja monimutkaisiin tietomääriin, joiden käsittely tuottaa ongelmia perinteisten toimitusketjujen järjestelmille. Big Data -analytiikassa hyödynnetään edistyneitä menetelmiä, kuten ennustavaa analytiikkaa korrelaatioiden ja trendien paljastamiseksi laajoista tietoaineistoista. Toimitusketjuissa analytiikkaa sovelletaan muun muassa kysynnän ennustamisessa, hankinnassa ja varaston- sekä riskienhallinnassa. Sen merkitys toimitusketjun hallinnassa on kiistaton datan määrän kasvaessa vuosi vuodelta. Big Data -analytiikka kohtaa haasteita teknologiaan ja resursseihin liittyen, mutta sen potentiaali toimitusketjujen tehokkuuden parantamiseksi on huomattava ja parhaillaan toteutumassa. (Tiwari ym., 2018; Menon & Shah, 2019.)

2.2.3 Lohkoketju

Lohkoketjuteknologiaa (engl. blockchain) on esitetty lupaavana ratkaisuna digitaalisten toimitusketjujen tietoturvan ja kustannustehokkuuden parantamiseksi. Sen luoma hajautettu ja muuttumaton tapahtumakirjanpito helpottaa tuotteiden alkuperän varmistamisessa ja niiden seuraamisessa koko toimitusketjun läpi tuottajalta loppuasiakkaalle asti. Tietojen luotettava jakaminen ilman välikäsiä ja paljastamatta osapuolten identiteettejä tehostaa ja turvaa prosesseja. Lohkoketjun mahdollistamat älysopimukset (engl. smart contract) vähentävät ihmisen läsnäolon tarvetta, kun sopimusten täytäntöönpano voidaan automatisoida. Lohkoketjuja hyödynnetään jo logistiikassa ja maksujen suorittamisessa, mutta haasteet liittyen integrointiin, skaalautuvuuteen ja sääntelyyn hidastavat niiden laajaa käyttöönottoa. (Korpela ym., 2017; Wang ym., 2019.)

2.2.4 Esineiden internet (IoT)

Esineiden internet (engl. internet of things, IoT) on teknologia, joka yhdistää fyysisiä objekteja digitaaliseen maailmaan. Tämä mahdollistaa niiden välisen kommunikaation sekä datan keräämisen ja analysoinnin. IoT-teknologia hyödyntää monia teknologioita, kuten RFID-sensoreita, langattomia verkkoja sekä pilvipalveluita, tarjotakseen reaaliaikaista näkyvyyttä ja tehokkuutta toimitusketjujen eri vaiheisiin. IoT tuo useita hyötyjä toimitusketjun hallintaan, joihin kuuluu mm. nopeampi reagointi häiriötilanteisiin ja tehokkaampi kommunikaatio, jotka edistävät koko toimitusketjun

joustavuutta ja reagointikykyä. Lähteissä mainitaan, että mahdollisimman monet tehtävät tulisi suorittaa IoT:n avulla, koska se voi merkittävästi parantaa toimitusketjun suorituskykyä ja tuotannon turvallisuutta ihmisten välisen vuorovaikutuksen vähentyessä. Tällainen liiketoimintaprosessien automatisointi nousee elintärkeäksi tekijäksi kilpailukyvyn säilyttämisessä tulevaisuudessa. (Majeed & Rupasinghe, 2017; Menon & Shah, 2019; Queiroz ym., 2021.)

2.2.5 Pilvipalvelut

Pilvipalvelut (engl. cloud computing) ovat mullistaneet perinteisten toimitusketjujen järjestelmien käytön. Ne tarjoavat useita etuja informaatiojärjestelmien hallintaan, kuten kustannustehokkuutta sekä nopean ja ketterän käyttöönoton niiden skaalautuvuuden ansiosta. Pilvipalveluiden yleisimmät muodot ovat ohjelmistopalvelu (engl. Software as a System, SaaS), infrastruktuuripalvelu (engl. Infrastructure as a System, IaaS) ja alustapalvelu (engl. Platform as a System, PaaS). Ne ovat rakenteeltaan joustavia ja mukautuvat helposti erilaisten organisaatioiden tarpeisiin, jonka ansiosta liiketoiminnan keskeisimpiin prosesseihin keskittymiseen jää enemmän voimavaroja. Monet suuret palveluntarjoajat, kuten Amazon, Google ja IBM, tarjoavat julkisesti saatavia pilvipalveluita. Nämä voivat tukea kapasiteetin, koordinoinnin ja yhteistyön kehittämistä ilman ylimääräisiä kustannuksia. (Wu ym., 2013; Menon & Shah, 2019.)

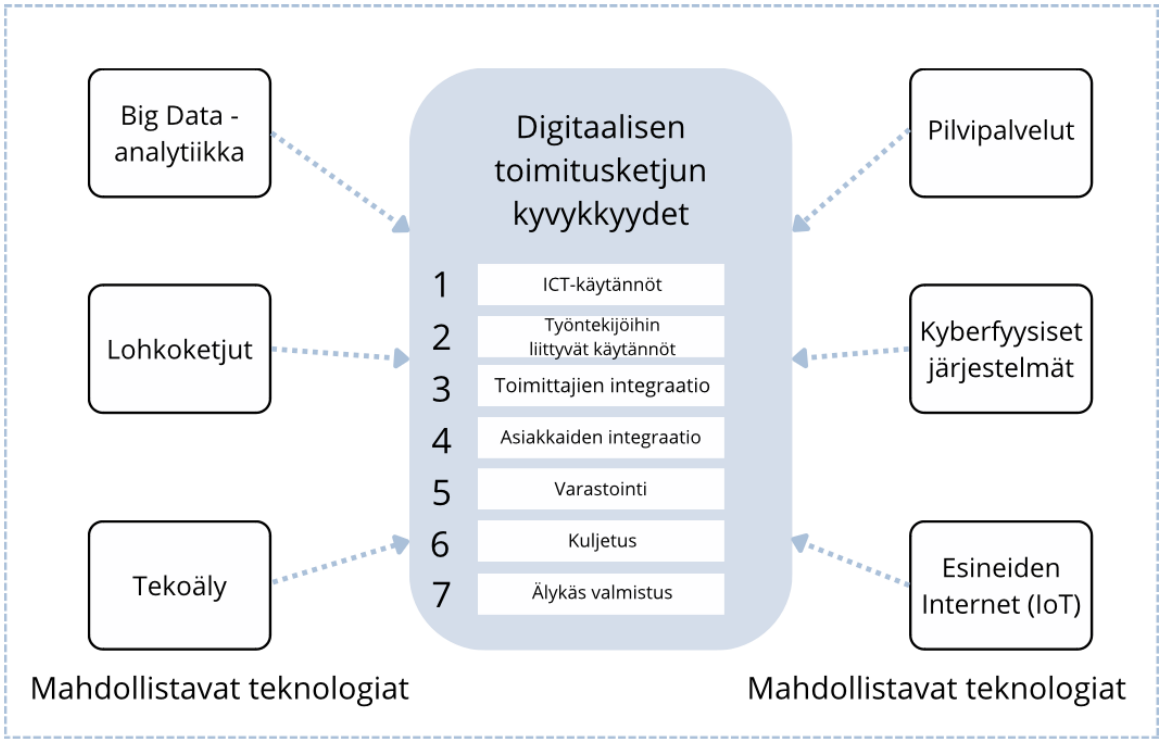
2.2.6 Kyber-fyysiset järjestelmät

Kyber-fyysiset järjestelmät (engl. cyber physical systems, CPS) ovat keskeisessä asemassa Industry 4.0:n aikakautena, koska ne mahdollistavat digitaalisten toimitusketjujen fyysisten ominaisuuksien ja digitaalisten järjestelmien yhteensovittamisen. Kyber-fyysiset järjestelmät kykenevät käsittelemään tietoa, jota älykkäät laitteet, kuten IoT-teknologialla varustetut koneet tuottavat sekä kommunikoimaan näiden kanssa saumattomasti toiminnanohjausjärjestelmän tai muiden pilvipalveluiden välityksellä. CPS:n, IoT:n ja pilvipalveluiden yhteistyö tukee integroituja toimitusketjuja parantamalla tehokkuutta ja turvallisuutta, jonka takia näiden teknologioiden käyttö yhdessä luo enemmän lisäarvoa kuin niiden käyttö erillään. (Wang ym., 2016; Pandey ym., 2020; Queiroz ym., 2021.)

2.3 Digitaalisten toimitusketjujen hyödyt ja haasteet

Queiroz ym. (2021) esittelevät artikkelissaan kuusi avainteknologiaa, jotka mahdollistavat toimitusketjujen digitalisoitumisen. Nämä teknologiat tukevat digitaalisen muutoksen vaatimia peruskyvykkyyksiä. Kuviossa 2 nähdään kyvykkyyksistä ensimmäisenä ICT-käytännöt, jotka ovat keskeisessä asemassa uusien toimintamallien kehittämisessä. Toisena on työntekijöihin liittyvät

voimavarat, joka korostaa, että työntekijät ovat edelleen strateginen voimavara organisaatioille, vaikka digitalisaatio automatisoi paljon tehtäviä. Kolmannes ja neljännes kyvykkyys osoittavat toimittajien sekä asiakkaiden integroinnin merkityksen koko toimitusketjun suorituskyvyn ja läpinäkyvyyden edistämiseen. Varastointia ja kuljetusta on myös mahdollista tehostaa älykkäillä ominaisuuksilla kuten älyvarastoilla, automaattisilla ajoneuvoilla ja reaaliaikaisella seurannalla ketteryyden parantamiseksi ja kustannusten laskemiseksi. Seitsemäntenä ja viimeisenä kyvykkyytenä älykäs tuotanto, joka tukee tuotantojärjestelmien nopeaa reagointia muutoksiin laitteiden itsenäisen päätöksentekokyvyn ansiosta, pääasiallisesti IoT:n ja CPS:n avulla.



Kuvio 2 Digitaalisen toimitusketjun kyvykkyydet ja mahdollistavat teknologiat (mukaillen: Queiroz ym., 2021)

Uudet teknologiat ja kyvykkyydet tarjoavat merkittäviä etuja perinteisiin malleihin verrattuna. Lohkoketjujen, asiakkaiden ja toimittajien integrointi osaksi digitaalista toimitusketjua lisää läpinäkyvyyttä. Tämä mahdollistaa tarkemmat ja reaaliaikaiset tiedot kysynnän ja tarjonnan osalta, mikä lisää kykyä ennakoida ja reagoida markkinoiden muuttuviin tarpeisiin tehokkaasti. Samalla asiakaskokemus paranee, kun asiakkaiden tarpeiden ymmärrys helpottuu ja heille voidaan tarjota personoituja palveluita. (Agrawal & Narain, 2018; Büyüközkan & Göçer, 2018; Wang ym., 2019; Garay-Rondero ym., 2020; Queiroz ym., 2021.)

Automaatio ja älysopimukset vähentävät manuaalista työtä, mikä puolestaan nopeuttaa prosesseja ja alentaa operatiivisia kustannuksia. Varastoinnin ja kuljetusten optimointi tukee just-in-time-hankintoja lyhentäen toimitusaikoja. Lisäksi globaali verkottuminen mahdollistaa hajautetun

varastoinnin, joka vähentää riippuvuutta kaukaisista toimituksista kasvattaen kilpailukykyä. Digitaaliset toimitusketjut tarjoavat myös luontevan alustan innovaatioille, mahdollistaen proaktiivisen ja ketterän sopeutumisen muutoksiin ja häiriöihin. Järjestelmien skaalautuvuus helpottaa toimitusketjujen mukauttamista tarpeiden mukaan ja edistää kustannustehokkuutta. Digitaalisten toimitusketjujen ekologinen jalanjälki on myös pienempi kuin perinteisten, koska ne edistävät resurssien tehokasta käyttöä ja ympäristöystävällisiä prosesseja. Kaiken kaikkiaan digitaaliset toimitusketjut parantavat tehokkuutta ja asiakasarvoa sekä alentavat kustannuksia. (Agrawal & Narain, 2018; Büyüközkan & Göçer, 2018; Wang ym., 2019; Queiroz ym., 2021.)

Vaikka digitaaliset toimitusketjut kykenevät vastaamaan perinteisten toimitusketjujen kokemiin haasteisiin kehittyneiden ominaisuuksiensa ansiosta, kohtaavat nekin uusia haasteita digitaalisten ja internetpohjaisten alustojensa takia. Büyüközkanin ja Göçerin (2018) mukaan digitaalisten toimitusketjujen toteuttamiseen liittyvät keskeiset haasteet ovat suunnittelun, yhteistyön, tiedon jakamisen ja integroinnin puute sekä epätarkka kysyntäennuste. Nygård ja Katskikas (2022) sen sijaan korostavat digitaalisiin toimitusketjuihin kohdistuvia kyberhyökkäyksiä merkittävänä huolenaiheena. Kyberturvallisuuteen tulisi kiinnittää nyt entistä suurempaa huomiota toimitusketjujen digitalisoituessa. Voidaan päätellä, että Büyüközkanin ja Göçerin esiin nostamat haasteet luovat myös itsessään uhkia digitaalisen toimitusketjun kyberturvallisuudelle. Heikko suunnittelu voi johtaa järjestelmien ja prosessien heikkoon tietoturvaan. Heikko yhteistyö sekä tiedon jakamisen puute vaikeuttavat kyberuhkien tunnistamista ja niihin reagointia. Tiedon integroinnin puute voi luoda tietoturva-aukkoja, joita kyberrikolliset voivat hyödyntää. Epätarkka kysyntäennuste puolestaan voi johtaa varastojen ylikapasiteettiin ja varastoturvallisuuden heikkenemiseen, altistaen järjestelmät kyberuhille. Täten kaikkien näiden haasteiden ratkaiseminen on tärkeää digitaalisten toimitusketjujen kyberturvallisuuden vahvistamisessa.

3 Kyberturvallisuus

3.1 Kyberturvallisuuden määritelmä

Kyber-sana toimii määriteosana useissa digitaalista informaatiota käsittelevissä, jotka liittyvät organisaatioiden tietojärjestelmiin ja yleisesti tietotekniikkaan (Sanastokeskus, 2018). Kyberturvallisuus voidaan nähdä kaikkina niinä työkaluina, käytäntöinä, menetelminä, teknologioina ja muina turvallisuutta ylläpitävinä toimina, jotka varmistavat kyberympäristön, organisaatioiden ja käyttäjien resurssien saatavuuden, eheyden ja luottamuksellisuuden kyberriskejä vastaan (International Telecommunications Union [ITU], 2008). Kyberuhka viittaa ilmiöihin tai tapahtumiin, jotka uhkaavat kybertoimintaympäristön normaalia toimintaa toteutuessaan (Sanastokeskus, 2018). Kyberympäristö (engl. cyberspace) on globaali informaatioverkosto, jota luonnehtii digitaalisten laitteiden käyttö informaation luomiseen, tallentamiseen, muokkaamiseen, vaihtamiseen ja hyödyntämiseen (Kramer ym., 2011).

Tietoturva (engl. information security) ja kyberturvallisuus ovat läheisesti toisiinsa liittyviä, mutta eivät synonyymejä. Arkikielessä näitä termejä käytetään usein sekaisin, vaikka niiden välillä on selvä ero. Tietoturva on perinteisesti määritelty CIA-mallin (engl. CIA triad) mukaan. Malli koostuu kolmesta tekijästä, jotka ovat luottamuksellisuus, eheys ja saatavuus (engl. confidentiality, integrity, availability). Luottamuksellisuus tarkoittaa, että vain valtuutetut käyttäjät voivat käsitellä tietoja. Eheys takaa, että tiedot ovat muuttumattomia, eli niitä ei ole muokattu luvatta. Saatavuus varmistaa, että valtuutetut käyttäjät pääsevät käsiksi tietoihin aina tarvittaessa. Tietoturva keskittyy siis tiedon suojaamiseen luvattomalta käytöltä, muokkaamiselta ja hävittämiseltä. Kyberturvallisuus on sen sijaan laajempi käsite. CIA-malli on ollut tärkeä perusta kyberturvallisuudelle, mutta sen kapea-alaisuus ei enää riitä määritelmäksi lähes täysin digitalisoituneessa yhteiskunnassa. Tämän takia kyberturvallisuus tulisi nähdä nykyään jatkumona, toisin kuin tavoitteena tai yksittäisinä tietoturvakäytäntöinä, jota tietoturvan määritelmä enemmänkin painottaa. (Samonas & Coss, 2014; Galinec ym., 2017; Sanastokeskus, 2018; Ham, 2021.)

Cybersecurity Venturesin (2020) raportin mukaan globaalin kyberrikollisuuden arvioidut kustannukset kasvavat 3 biljoonasta dollarista vuonna 2015, jopa 10,5 biljoonaan dollariin vuoteen 2025 mennessä. Ennuste korostaa kyberturvallisuuden kasvavaa merkitystä kaikilla yhteiskunnan tasoilla. Kyberuhkien jatkuva kehittyminen ja niiden aiheuttamat taloudelliset vahingot sekä mainehaitat vaativat yrityksiltä ja organisaatioilta yhä kehittyneempiä kyberturvallisuusvalmiuksia. Accenturen (2023) tutkimuksessa havaittiin, että vaikka 96 % toimitusjohtajista ymmärtää kyberturvallisuuden keskeisen merkityksen nykypäivän liiketoiminnassa, niin vain 33 %:lla on

syvällinen ymmärrys kehittyvistä kyberuhkista. Tämä osoittaa selkeän kuilun tiedon ja ymmärryksen välillä, mikä korostaa kyberturvallisuuskoulutuksen ja -osaamisen kehittämisen tärkeyttä yrityksissä. Kyberturvallisuuden vahvistaminen on siis entistä tärkeämpää varmistaakseen yritysten jatkuvuutta ja kilpailukykyä.

Kyberhyökkäykset eivät enää rajoitu ainoastaan yksittäisten organisaatioiden ja yksityishenkilöiden väliseen toimintaan, vaan ne ovat saaneet geopoliittisen ulottuvuuden. Valtioiden kyberturvallisuuden merkitys on kasvanut huomattavasti kyberympäristön noustessa viidenneksi operatiiviseksi ulottuvuudeksi avaruuden, ilman, meren ja maan lisäksi. Valtiot käyttävät kyberkeinoja puolustus- ja hyökkäystarkoituksissa, joka on nostanut kyberkonfliktien riskiä. Tämä korostaa kyberturvallisuuden merkitystä myös kansallisessa turvallisuudessa ja kansainvälisissä suhteissa. (Welch, 2011.)

3.2 Kyberuhkat

Kyberuhkat koskettavat kaikkia teollisuuden aloja, mutta erityisesti terveydenhuolto, rahoitusala ja valmistava teollisuus ovat tällä hetkellä kyberhyökkäysten ensisijaisia kohteita (Statista, 2024). Terveydenhuolto houkuttelee kyberrikollisia sen heikon suojauksen ja suuren arkaluonteisen tiedon määrän ansiosta. Muita vahvasti kyberhyökkäyksille alttiita aloja ovat IT ja telekommunikaatio sekä energiantuotanto. Hyökkäysten motiivit vaihtelevat taloudellisesta tai poliittisesta hyödystä aina organisaatioiden heikkouksien paljastamiseen. Kyberhyökkäysten laajuus ja niiden aiheuttamat taloudelliset sekä maineelliset vahingot ovat kasvussa, mikä tekee kyberturvallisuudesta entistä kriittisemmän tekijän kaikilla teollisuuden aloilla. Jatkuvasti kehittyvät kyberhyökkäykset vaativat organisaatioilta kehittyneitä tietoturvastrategioita ja -järjestelmiä. (Alharam & Elmedany, 2017; Coventry & Branley, 2018.)

Haittaohjelmilla (engl. malware) viitataan laajasti kaikenlaisiin haitallisiin sovelluksiin ja ohjelmiin, jotka on suunniteltu vahingoittamaan kohteen järjestelmiä tai murtautumaan niihin luvattomasti. Kyberrikolliset käyttävät niitä tietoturvahyökkäysten välineinä muun muassa tietokoneiden kaappaamiseen, tietojen varastamiseen ja kriittisten infrastruktuurien lamauttamiseen. Tunnetuimpia haittaohjelmia ovat troijalaiset, virukset, botit, vakoiluohjelmat ja kiristyshaittaohjelmat. (Ye ym., 2018.)

Kiristyshaittaohjelmat (engl. ransomware) ovat yksiä yleisimpiä haittaohjelmia ja kyberuhkia, jotka lukitsevat kohteen tiedostot ja vaativat lunnaita niiden vapauttamiseksi. Hyökkääjä pitää tietokonetta tai tiedostoja ikään kuin panttivankina tilanteessa. Taloudellisten menetyksien lisäksi

organisaatioiden liiketoiminnan jatkuvuus ja sen asiakassuhteet voivat kärsiä, tai pahimmassa tapauksessa lukitut tiedot voi menettää lopullisesti. (Brewer, 2016.)

Edellä mainittujen kiristysohjelmien lisäksi myös viruksilla, madoilla ja troijalaisilla on merkittävä rooli kyberuhkien maisemassa. Virukset ovat haittaohjelmia, jotka vaativat jonkin alustan, johon kytkeytyä. Ne eivät ole haitallisia yksinään, vaan vaativat toisen ohjelman tuhotyönsä suorittamiseksi. Kun tällaisen ohjelman käynnistää, virus saastuttaa sen. Toisin kuin virukset, madot ovat itse haitallisia, ja voivat lisääntyä täydellisinä kopioina itsestään autonomisesti. Troijalaiset naamioituvat vaarattomiksi ohjelmiksi, mutta osoittautuvat lopulta haitallisiksi. Näiden ohjelmien kyky pettää käyttäjät helposti selittävät niiden vaarallisuuden. (Ye ym., 2018.)

Tietojenkalastelu (engl. phishing) perustuu sosiaaliseen manipulointiin, jossa uhri pyritään johtamaan harhaan. Hyökkääjä esiintyy laittomasti luotettavana organisaationa voittaakseen uhrin luottamuksen, esimerkiksi tekstiviestin tai sähköpostin muodossa. Viestissä oleva linkki ohjaa uhrin luovuttamaan henkilökohtaisia tietoja tai lataamaan haittaohjelmia laitteilleen. Tietojenkalastelussa yleistynyt muoto on nykyään ’’spear-phisfing’’, jossa joukkoviestien lähettämisen sijasta hyökätään kohdennetusti vain yhteen henkilöön. (Alkhalil ym., 2021.)

Palvelunestohyökkäyksessä (engl. denial of service attack) hyökkääjä pyrkii estämään jonkin verkossa toimivan palvelun käytön. Hyökkäys toteutetaan ylikuormittamalla palvelu tai verkko liiallisella liikenteellä, tai hyödyntämällä siinä olevaa teknistä heikkoutta. Suurin osa tänä päivänä toteutetuista palvelunestohyökkäyksistä ovat hajautettuja (engl. distributed denial of service attack), joissa liikennettä ohjataan kohteeseen yhtäaikaisesti useista eri lähteistä. Hajautetuissa palvelunestohyökkäyksissä käytetään usein bottiverkkoa, johon kuuluu internetiin liitettyjä laitteita, jotka on kaapattu hyökkäyskäyttöön omistajien tietämättä. (Kyberturvallisuuskeskus, 2022.)

3.3 Kyberonnettomuudet ja kyberresilienssi

Yritysten informaatiojärjestelmien toimintaa eivät uhkaa ainoastaan kyberhyökkäykset, sillä samanlaista tuhoa aiheutuu esimerkiksi järjestelmien kaatuessa. Kyberonnettomuus (engl. cybersecurity incident/cyber-event) on reagointia ja toipumista edellyttävä kybertapahtuma, jolla on todettu olevan vaikutusta organisaatioon esim. suorituskyvyn heikentymisen tai kapasiteetin laskun seurauksesta. (Boyes, 2015; National Institute of Standards and Technology [NIST], 2018.) Kyberonnettomuuden määritelmä käsittää laajemman kirjon tapahtumia kuin vain kyberhyökkäykset, joten se sopii paremmin erilaisten kybertapahtumien, kuten CrowdStriken IT-katkoksen ja SolarWindsin kyberhyökkäyksen, tutkimiseen.

Kyberresilienssi on tärkeässä osassa organisaatioiden kyvyssä kestää, sitä uhkaavia kyberonnettomuuksia ja toipua niistä. Hyvä kyberresilienssi edellyttää vahvaa kyberturvallisuutta. Siihen kuuluu kyky tunnistaa uhat ja haavoittuvuudet, sopeutua muuttuviin olosuhteisiin ja palauttaa järjestelmät nopeasti toimintakuntoon häiriötilanteiden jälkeen, jotka ovat kaikki itsessään kyberturvallisuutta parantavia ominaisuuksia. (Boyes, 2015; Cheung ym., 2021.) Näin ollen vahva kyberturvallisuus edistää myös kyberresilienssiä.

Boyes (2015) esittelee uhkia ja haavoittuvuuksia yrityksen kyberresilienssille, jotka altistavat järjestelmän kyberonnettomuuksille tai pahimmassa tapauksessa itse aiheuttavat sellaisen. Uhkiin ja haavoittuvuuksiin kuuluu ihmisen tekemät virheet kuten heikko ohjelmistokehitys sekä luonnonilmiöt, jotka voivat aiheuttaa häiriöitä viestintäinfrastruktuurissa kuten aurinkomyrskyt ja maanjäristykset.

Kaikista mainituista kyberonnettomuuksista, tässä tutkielmassa keskitytään erityisesti odottamattomiin käyttökatkoksiin (engl. unplanned IT outages). Ne voivat aiheutua esimerkiksi viallisesta päivityksestä, kuten tapahtui CrowdStriken tapauksessa (George, 2024). Käyttöjärjestelmän katkokset tapahtuvat, kun organisaation laitteistossa tai ohjelmistossa tapahtuu yllättäen toimintahäiriö. Katkokset edellyttävät välitöntä toimintaa perustilan palauttamiseksi. Yleisimpiä käyttökatkoksen syitä ovat luonnonilmiöt, laitteisto- tai ohjelmistoviat, inhimilliset virheet, järjestelmän ylikuormitus ja ilkivalta. Tällaiset katkokset voivat johtaa merkittäviin taloudellisiin tappioihin ja vahingoittaa yrityksen mainetta. (O’Callaghan & Mariappanadar, 2008.)

4 Kyberuhkat ja –onnettomuudet digitaalisissa toimitusketjuissa

Digitaalinen toimitusketju on yhtä vahva kuin sen heikoin lenkki (Pandey ym., 2020). Viimeaikaiset tapaukset, kuten SolarWinds sekä CrowdStrike (Raponi ym., 2021; George, 2024), ovat osoittaneet, että toimitusketjun heikoin lenkki voi paljastua niin sisältä kuin ulkopuoleltakin. Siksi organisaation henkilöstö ja sen ulkoiset toimittajat, tulisi suojata yhteisellä koko toimitusketjun kattavalla kyberturvallisuus strategialla. (Melnyk ym., 2022; Aarland, 2024.)

Suurimpaa tuhoa kylvävät kyberuhkat ja -onnettomuudet, jotka kohdistuvat laajamittaisia globaaleja toimitusketjuja kohtaan (Pandey ym., 2020). Digitaaliset toimitusketjut ovat erityisen haavoittuvaisia, koska mahdollisten hyökkäysvektoreiden lukumäärä on moninkertaistunut järjestelmien digitalisoitumisen seurauksesta (Cheung ym., 2021). Tämä tarkoittaa, että ne sisältävät monen tyyppisiä haavoittuvuuksia, joihin tulisi keskittyä kyberresilienssin vahvistamiseksi (Boyes, 2015). Siispä pelkkiin ulkoisiin haavoittuvuuksiin keskittyminen ei riitä, sillä kyberonnettomuudet saavat usein alkunsa sisäisistä heikkouksista, joka korostaa organisaation oman henkilöstön koulutuksen ja järjestelmien turvallisuusprosessien merkitystä (Evans ym., 2019).

4.1 Toimitusketjuhyökkäykset

Toimitusketjuhyökkäykset ovat kaikista organisaatioita uhkaavista kyberuhkista brutaaleimpia. Ne määritellään kirjallisuudessa kyberhyökkäyksiksi, jotka koostuvat vähintään kahdesta johonkin toimitusketjun osaan kohdistetusta iskusta. Paikoittain niitä kutsutaan myös kolmannen osapuolen hyökkäyksiksi, koska usein alustavana kohteena on toimitusketjun heikoksi tai haavoittuvaksi tunnistettu kolmasosapuoli kuten ohjelmistopalveluntarjoaja. Ensisijainenhyökkäys voi kohdistua mihin tahansa ketjun sidosryhmään, joka toimii hyökkäysvektorina mahdollisesti haitallisemmalle hyökkäykselle itse pääkohteeseen. Tämä on joko ketjun loppuasiakas tai ketjun toinen toimittaja. Vaikka hyökkäys kohdistuisi aluksi vain yhteen toimittajaan, niin silti sen yhteistyökumppanit sekä asiakkaat joutuvat vaaraan, koska asiakkaiden ja muiden ketjun yritysten arkaluonteisia tietoja on usein tallennettuina yrityksen järjestelmissä tai palveluntarjoajan pilvipalvelussa. Hyökkäys voi tällöin levitä normaalista kyberhyökkäyksestä toimitusketjuhyökkäykseksi. (Raponi ym., 2021; Nygård & Katsikas, 2022; Khokhar ym., 2024.)

Khokar ym. (2024) luokittelevat eri hyökkäystyypit sen mukaan kohdistuuko hyökkäys ensisijaisesti asiakkaaseen vai toimittajaan. Nygård ja Katsikas (2022) sen sijaan luokittelevat hyökkäykset suoriin ja epäsuoriin. Samassa toimitusketjuhyökkäyksessä voidaan siis hyödyntää sekä suoria, että epäsuoria hyökkäystekniikoita ja niiden kohteena voivat olla asiakkaat sekä

toimittajat, minkä takia toimitusketjuhyökkäykset voivat olla luonteeltaan hyvinkin toisistaan poikkeavia ja vaikeasti ennakoitavissa tai tunnistettavissa.

Taulukko 1. on luokiteltu merkittävimmät hyökkäystekniikat sen mukaan, kohdistuvatko ne toimittajiin vai asiakkaisiin ja ovatko hyökkäykset suoria vai epäsuoria. Suorissa hyökkäyksissä vahinkoa aiheutetaan fyysisesti esim. peukaloimalla laitteistoja tai digitaalisesti esim. hyödyntämällä ohjelmiston haavoittuvuutta ja syöttämällä haitallista SQL-koodia web-sovelluksen syöttökenttään. Muita suoria hyökkäystekniikoita ovat muun muassa väsytyshyökkäystekniikka (engl. brute-force attack), jossa tavoitteena on salasanan arvaaminen ja sen avulla luvaton pääsy järjestelmään, sekä jo aiemmassa luvussa esitelty palvelunestohyökkäys, jonka tavoitteena on häiritä ja estää palvelun tavanomainen toiminta. Epäsuorat hyökkäykset, kuten virukset tai troijalaiset, voivat pysytellä huomaamattomina järjestelmässä pitkiä aikoja odottaen aktivoitumistaan. Haittaohjelmat pääsevät järjestelmään usein sosiaalisen manipuloinnin kautta, kun organisaation sisällä joku lankeaa huijaukseen tai vaihtoehtoisesti esim. korruptoituneen toimittajan ohjelmistoon asentaman takaoven kautta. Sosiaalisen manipuloinnin keinot luokitellaan myös epäsuoriksi kyberhyökkäyksiksi, kun tavoitteena on houkutella uhri luovuttamaan tietoja tai suorittamaan hyökkääjän motiivin mukainen teko. (Nygård & Katsikas, 2022; Khokhar ym., 2024.)

Taulukko 1 Toimittajiin ja asiakkaisiin kohdistuvat suorat ja epäsuorat hyökkäykset (mukaillen: Nygård & Katsikas, 2022; Khokhar ym., 2024)

	Toimittajiin kohdistuvat suorat hyökkäykset	**Toimittajiin kohdistuvat epäsuorat hyökkäykset**	**Asiakkaisiin kohdistuvat suorat hyökkäykset**	**Asiakkaisiin kohdistuvat epäsuorat hyökkäykset**
Tekniikka	Fyysinen hyökkäys (väärentäminen, varkaudet, peukalointi)	Sosiaalinen manipulointi (huijaushyökkäykset (engl. Spoofing), tietojenkalastelu)	Fyysinen hyökkäys (väärennettyjen laitteiden luonti, laitteiston peukalointi)	Tietojenkalastelu (esim. henkilöityminen toimittajan henkilökuntana)
Tavoite	Laitteiston muokkaaminen tai tuhoaminen	Teeskentely ja uhrin houkutteleminen suorittamaan jokin teko tai pääsy luvattomiin tietoihin	Arkaluonteisten tietojen saanti ja hyödyntäminen	Arkaluonteisten tietojen saanti ja hyödyntäminen
Tekniikka	Ohjelmiston tai konfiguraation haavoittuvuuden hyödyntäminen	Haittaohjelmat (virukset, madot, troijalaiset, kiristysohjelmat)	Avoimen lähdekoodin tiedustelu (engl. Open-Source Intelligence)	Haittaohjelmat (kiristysohjelmat, troijalaiset)
Tavoite	Luvaton pääsy järjestelmään ja haitallisen koodin tai komentojen syöttö	Järjestelmän saastuttaminen, työntekijöiden vakoilu tai kiristäminen	Tunnusten tai API-avainten löytäminen verkosta ja niiden väärinkäyttö	Arkaluonteisten tietojen saanti ja hyödyntäminen tai kiristäminen

Toimitusketjuhyökkäyksistä erityisen vakavia tekevät sen, että ne voivat saada alkunsa mistä tahansa pienestä haavoittuvuudesta, joko asiakkaan tai toimittajan päädyssä. Khokhar ym. (2024) viittaavat artikkelissaan ENISA:n tutkimukseen, jossa selvisi, että yli puolissa tapauksissa toimittajat eivät olleet tietoisia hyökkäyksistä. Lisäksi tutkimuksessa selvisi, että haittaohjelmat olivat eniten käytetty hyökkäystyyppi. Asiakkaiden luottamuksen väärinkäyttö oli sen sijaan asiakkaisiin kohdistuneiden hyökkäysten yleisin syy. Tämä korostaa myös käsitystä siitä, että digitaalisessa toimitusketjussa asiakkaat tulisi ottaa huomioon kyberturvallisuus ratkaisujen käytäntöönpanossa.

SolarWindsin tapaus on usein esillä toimitusketjuhyökkäyksiä käsittelevässä kirjallisuudessa. Se on yksi viime vuosien vakavimpia kyberhyökkäyksiä, joka vaikutti yli 18 000 organisaatioon mukaan

lukien Nvidian ja Intelin kaltaisiin monikansallisiin yrityksiin sekä moniin valtiollisiin virastoihin. Hyökkäyksen seurauksena monet yritykset ja hallitukset alkoivat kiinnittämään enemmän huomiota turvallisuuskäytäntöihin, kyberresilienssiin sekä jopa lainsäädäntöön. Yhdysvaltalainen SolarWinds on tunnettu IT-alan yritys, joka tarjoaa ohjelmistopalveluita järjestelmien ja verkkojen hallintaan. Hyökkäyksessä Orion-ohjelmiston kehitysprosesseissa esiintyvään DLL-tiedostoon päästiin käsiksi ja sinne saatiin lisättyä huomaamaton ja viaton koodinpätkä, joka ei vaikuttanut ohjelmiston tavanomaiseen toimintaan. Haitallinen koodi, aktivoitui kahden viikon kuluttua luoden takaoven Orion-ohjelmiston kehitysprosesseihin, jonka kautta hyökkääjille aukesi rajoittamaton pääsy järjestelmään. Koodi levisi troijalaisena, kun saastunutta tiedostoa käytettiin uusimmassa ohjelmistopäivityksessä, jonka asiakkaat latasivat sinisilmäisinä tiedostamattaan vaarasta. Hyökkääjät kykenivät takaoven kautta suorittamaan monia ilkivaltaisia tekoja kuten varastamaan sensitiivistä tietoa merkittäviltä toimijoilta, joihin kuului muun muassa Yhdysvaltain eri ministeriöitä. (Raponi ym., 2021; Nygård & Katsikas, 2022; Khokhar ym., 2024.)

Tämä osoittaa, kuinka tärkeää on suojata koko ohjelmistokehityksen ja -toimituksen ketju, eikä vain lopputuotteet tai käyttäjien päätelaitteet. Raponin ym. (2021) mukaan kriittisten infrastruktuureiden hallinnan haasteena on ohjelmistojen toimitusketju. Artikkelissa käsitellään SolarWindsin-toimitusketjuhyökkäystä, joka osoitti, että ohjelmistokehitykseen ei kiinnitetä tarpeeksi huomiota. Raponi ym. korostavat, että vaikka ohjelmisto olisi tarkastettu ennen sen liittämistä kriittiseen infrastruktuuriin, niin vahinko on voinut jo tapahtua, sitä ennen jonkin toisen ohjelmiston tai järjestelmän haavoittuvuuden takia.

Näiden lisäksi IoT-laitteet muodostavat merkittävän haavoittuvuuden digitaalisten toimitusketjujen kyberturvallisuudelle järjestelmiin kytketyn internetpohjaisen luonteensa takia. IoT-laitteiden ja muiden uusien teknologioiden, kuten pilvipalveluiden integroituminen osaksi toimitusketjuja on lisännyt mahdollisia hyökkäysvektoreita. IoT-laitteita uhkaa erityisesti riski manipulaatiosta. Aitojen laitteiden korvaaminen väärennetyillä tai peukaloiduilla voi johtaa epätarkkoihin tietoihin ja uhata sekä toimitusketjun toimintaa että loppuasiakkaita. Lisäksi IoT-laitteiden toimittajat eivät aina tiedosta tuotteidensa kaikkia mahdollisia haavoittuvuuksia, mikä tekee hyökkäysteiden määrittämisestä ja riskien analysoinnista haastavaa. (Raponi ym., 2021; Nygård & Katsikas, 2022; Boyson, 2023; Khokhar ym., 2024.)

IoT-laitteita käytetään nykyään paljon valmistavassa teollisuudessa ja toimitusketjuissa. Tällöin niiden muodostamaa verkostoa kutsutaan nimellä Industrial Internet of Things (IIoT). Tämän teollisen verkoston käyttö lisää entisestään toimitusketjuhyökkäyksen uhkaa monimutkaisuudellaan,

sillä IIoT ei ole yhden toimijan hallinnoima järjestelmä, vaan se koostuu useiden toimijoiden kuten erilaisten komponenttivalmistajien sekä pilvipalveluntarjoajien osista ja palveluista. Useiden eri toimijoiden mukanaolo lisää erilaisia epävarmuustekijöitä ja potentiaalisia heikkouksia, joita voidaan hyödyntää koko infrastruktuurin tasolla, ei pelkästään yksittäisissä laitteissa. Tämän takia yhteisen tietoturvastrategian kehittäminen toimijoiden kesken on välttämätöntä, jotta mahdolliset tietoturvaloukkaukset voidaan ennaltaehkäistä ja torjua ennen kuin suurempaa tuhoa ehtii tapahtua. (Cheung ym., 2021; Nygård, 2022; Melnyk ym., 2022; Camacho, 2024.)

4.2 Inhimilliset virheet

Kyberonnettomuudet eivät ole aina peräisin tarkasti järjestelmän haavoittuvuuksiin kohdistetuista ulkoisista hyökkäyksistä, kuten troijalaisista tai muista haittaohjelmista, jotka aiheuttavat laajamittaisen toimitusketjuhyökkäyksen. Evansin ym. (2019) mukaan kyberonnettomuudet saavat usein alkunsa organisaation sisäisistä puutteista, joissa inhimillisillä virheillä on keskeinen rooli. Evans ym. esittivät tutkimuksessaan, että ihmisten tekemät virheet aiheuttivat julkisen sektorin organisaatioissa keskimäärin 79 % kyberonnettomuuksista ja yksityisen sektorin organisaatioissa 89 %. Tutkimus osoittaa, että ihmisten tekemät virheet, joihin kuuluu muun muassa huolimattomuusvirheet sekä liiallinen järjestelmiin luottaminen, ovat useimmiten pääsyynä kyberonnettomuuksissa. Digitaalisten toimitusketjujen näkökulmasta erityistä huolellisuutta vaaditaan suurilta palveluntarjoajilta, joilla on kytköksiä kriittiseen infrastruktuuriin ja talouden merkittäviin sektoreihin.

Heinäkuussa 2024 paljastui, kuinka hallitsevan markkina-aseman omaavan kyberturvallisuusalan jättiläisen, CrowdStriken, oman viallisen ohjelmistopäivityksen takia koettiin historian suurin IT-katkos. George (2024) mukaan yrityksen asiakkaisiin kuuluu yli 75% Fortune 500 -yrityksistä, lukuisilla tärkeimmillä aloilla kuten ilmailussa, terveydenhuollossa, rahoitusjärjestelmissä ja globaalissa merenkuljetuksessa. Toimitusketjun näkökulmasta katkos aiheutti dominoefektin, joka viivästytti tavaroiden ja palvelujen oikea-aikaista toimittamista, kun Windows-järjestelmät kaatuivat samanaikaisesti ympäri maailmaa. Tämä näkyykin sen aiheuttamissa taloudellisissa tappioissa, jotka tutkimuksen mukaan lähestyvät arviolta 100 miljardia dollaria. O'Flahertyn (2024) kirjoittamassa uutisartikkelissa kyberasianasiantuntijat kommentoivat CrowdStriken julkaisemaa perusteellista selvitystä tapauksesta. Heidän mukaansa virheellinen päivitys laskettiin liikkeelle testaamisen sekä vaiheittaisen käyttöönoton puutteiden takia. Näiden puutteiden juurisyynä voidaan olettaa olevan inhimilliset virheet suunnitteluvaiheessa.

Tapaus korostaa, että vaikka teknologiset ratkaisut ovat keskiössä, on tärkeää myös tunnistaa ja hallita riskit, jotka liittyvät inhimillisiin tekijöihin, koska samalla tavalla toimitusketjuhyökkäysten tapaan, virheistä johtuvat onnettomuudet häiritsevät tai keskeyttävät koko ketjun normaalin toiminnan. George (2024) painottaa, että organisaatiot ovat yliriippuvaisia ulkoisista palveluntarjoajista, joka luo merkittävän riskin koko toimitusketjun kyberturvallisuudelle, kun käytössä ei ole ajantasaisia varajärjestelmiä tai varmuuskopiokäytäntöjä. Suuressa roolissa koko toimitusketjun kyberturvallisuudessa on sen toimittajan, kuten tietoruvapalveluntarjoajan, kyberresilienssin taso. Kaur ym. (2024) mukaan toimittajat tulisi valita heidän kyberturvallisuuden tason mukaan. Toimittajien tulisi myös olla sitoutuneita jatkuvaan parantamiseen yhteistyössä koko toimitusketjun kanssa. Tähän kuuluu työntekijöiden kouluttaminen ja investoinnit toimittajien tietoturvajärjestelmiin. Näin tekemällä toimitusketjun heikoin lenkki vahvistuu ja koko toimitusketjun kyberresilienssi paranee.

5 Uusien teknologioiden hyödyntäminen kyberturvallisuudessa

Digitaalisten toimitusketjujen kyberturvallisuutta tulisi käsitellä ikään kuin jatkumona, jonka kehitys on enemmänkin jatkuva prosessi kuin savutettava tavoite, sillä kyberriskit kehittyvät nopeammin kuin ratkaisut niiden hallintaan (Alani, 2021; Ham, 2021). Industry 4.0 on kiihdyttänyt toimitusketjujen muutosta perinteisestä digitaaliseen muotoon, mikä on tehnyt niistä entistäkin monimutkaisempia ja verkottuneempia, altistaen ne yhä monimuotoisemmille kyberuhille. Muutoksen taustalla olevat avainteknologiat, kuten lohkoketjut, Big Data -analytiikka ja IoT, ovat samalla haavoittuvuuksien syy ja ratkaisu niiden torjuntaan. (Büyüközkan & Göçer, 2018; Nasiri ym., 2020; Pandey ym., 2020.)

Gartnerin (2024) ennustus tukee tätä näkökulmaa, jonka mukaan kaikista kyberhyökkäyksistä 17% käyttää hyödyksi generatiivista tekoälyä vuoteen 2027 mennessä. Toimitusketjujen kyberturvallisuuden merkitys on korostunut viime vuosina, jonka vuoksi sen edistäminen edellyttää innovatiivisia ja proaktiivisia ratkaisuja (Melnyk ym., 2022; Kumar ym., 2023). Yritykset ovat tämän tiedostaen kasvattaneet investointejaan kyberturvallisuuteen. Tämä näkyy Gartnerin ennusteessa, jonka mukaan loppukäyttäjien taloudellinen panostus tietoturvan kehittämiseen tulee nousemaan 15% tämän vuoden aikana, saavuttaen ensi vuonna 212 miljardin dollarin kokonaissumman.

5.1 Uhkien ennaltaehkäisy ja tunnistus

Tekoälyn ja Big Data- analytiikan käyttö kyberturvallisuudessa tarjoaa tehokkaita menetelmiä kyberuhkien ennaltaehkäisyyn toistuvien kaavojen havaitsemiseksi tietoverkoissa. Suurten tietomäärien reaaliaikaisen analysoinnin on mahdollistanut Big Datan ja kehittyneiden koneoppimismallien (engl. machine learning) yhteiskäyttö. Tämä luo pohjan ennustavalle analytiikalle. Tekoälyalgoritmit kykenevät oppimaan ja mukautumaan uusiin uhkiin historiallista ja reaaliaikaista dataa käsittelemällä, mikä parantaa kykyä ennakoida kyberriskejä ennen niiden toteutumista. Tämä dynaamisuus tarkoittaa, että järjestelmät voivat automaattisesti päivittää puolustusstrategioitaan oppimalla uusia hyökkäysvektoreita. Tämä tekoälyteknologioiden mahdollistama proaktiivisuus on erityisen hyödyllistä monimutkaisissa ja muuntuvissa ympäristöissä, kuten Industry 4.0:ssa. (Ullah & Ali Babar, 2019; Radanliev ym., 2020; Alani, 2021; Yeboah-Ofori ym., 2021; Camacho, 2024.)

Ennustavaan analytiikkaan kuuluu lisäksi haavoittuvuuksien ja uhkien tunnistaminen, jossa tekoälyalgoritmit analysoivat järjestelmän dataliikennettä poikkeavuuksien havaitsemiseksi. Yeboah-Oforin ym. (2021) tutkimuksessa arvioitiin eri koneoppimismallien kykyä tunnistaa

erilaisia kyberuhkia, kuten haittaohjelmia ja vakoiluohjelmia. Neljästä eri koneoppimismallista logistinen regressio (engl. logistic regression) ja tukivektorikone (engl. support vector machine) suoriutuivat parhaiten tunnistaen haittaohjelmat 85% tarkkuudella. Radanliev ym. (2020) sekä Khokhar ym. (2024) mainitsevat tekoälyteknologioiden hyödyntämisestä IoT-sensoreiden tuottaman reaaliaikaisen datan analysoinnissa, joka voi edesauttaa epäilyttävän toiminnan tunnistamisessa ja mahdollisten uhkien ehkäisyssä. IoT-laitteet tuottavat jatkuvaa tietovirtaa, josta niiden sensorit voivat paljastaa esimerkiksi verkkoliikenteen odottamattomat piirteet, jotka saattavat muuten jäädä huomaamatta perinteisillä menetelmillä.

Kyberfyysiset järjestelmät (CPS) tuovat lisäulottuvuuden digitaalisten toimitusketjujen kyberturvallisuuteen integroimalla fyysiset, internetpohjaiset IoT-laitteet digitaalisiin järjestelmiin, jolloin reaali- ja virtuaalimaailmoista saadaan yhtenäinen kokonaisuus. CPS:n avulla voidaan luoda kattavampia tietoturvastrategioita, jotka huomioivat sekä ohjelmistojen että laitteistojen suojauksen. (Radanliev ym., 2020.) De Azambujan ym. (2024) esittelevät digitaalisten kaksosten käytön uudenlaisena kyberturvallisuusratkaisuna, erityisesti kyberfyysisten järjestelmien suojauksessa. Digitaalinen kaksonen tarjoaa virtuaalisen kopion fyysisestä järjestelmästä, jonka avulla voidaan turvallisesti simuloida, testata ja ennakoida erilaisia tilanteita. Ennustavaa analytiikkaa hyödyntämällä ja erilaisia uhkaskenaarioita simuloimalla, voidaan kehittää tehokkaampia ennakoivia turvatoimia kyberuhkien varalta sekä tunnistaa heikkouksia järjestelmästä. Lisäksi simuloimalla koko CPS ja siihen liitetyt IoT-laitteet, voidaan reaaliaikaisesti seurata niiden tuottamaa dataa ja toimintaa eri tilanteissa. Digitaalinen kaksonen mahdollistaa myös ohjelmistopäivitysten testaamisen kontrolloidussa ympäristössä ennen niiden liikkeelle laskua. Vastaavanlaisen testausympäristön käyttö olisi mahdollisesti voinut estää CrowdStriken ja SolarWindsin kyberonnettomuudet, joissa molemmissa viallinen tai saastunut päivitys levitti vahinkoa koko toimitusketjussa.

5.2 Reagointi ja palautuminen

Kyberuhkiin ja -onnettomuuksiin reagointi sekä niistä palautuminen ovat toimitusketjujen kontekstissa suhteellisen vähän tutkittuja alueita (Cheung ym., 2021). Kuitenkin uusien teknologioiden, erityisesti tekoälyn ja automatisoinnin, on todettu tarjoavan huomattavia mahdollisuuksia tässä yhteydessä. Digitaalisten toimitusketjujen tulisi saavuttaa niin sanottu itsetietoisuus uhkista ja niihin pohjautuvista reagointitoimista, jotta suojaus ja palautuminen olisivat nykyisten kehittyneiden uhkien tasolla. Tämä edellyttää innovatiivisten teknologioiden, kuten

tekoälyn, IIoT-verkkojen ja pilvipalveluiden, hyödyntämistä. (Radanliev ym., 2020; Kaur ym., 2023.)

Tekoäly voi automaattisesti eristää verkon osia tai yksittäisiä laitteita kyberhyökkäyksen aikana haittaohjelmien leviämisen estämiseksi (Radanliev ym., 2020). Lisäksi tekoälyä voidaan käyttää uhkien luokittelussa ja priorisoinnissa, jotta vakavimpiin uhkiin voidaan reagoida ensisijaisesti (Kaur ym., 2023). Big Datan ja tekoälyn kyky analysoida suuria tietomääriä reaaliaikaisesti tekee niiden integraatiosta tehokkaan työkalun uhkiin reagoinnissa. Mahdollisen kriisin sattuessa automatisaation avulla voidaan nopeasti hälyttää tietoturva-asiantuntijoita tai suoraan käynnistää toimenpiteet uhkien neutraloimiseksi. (Ullah & Ali Babar, 2019; Alani, 2021.)

Digitaalinen kaksonen tarjoaa mahdollisuuden simuloida ja testata järjestelmien kestävyyttä tunkeutumishyökkäyksiä vastaan, esim. tilanteet, joissa hyökkääjä on päässyt luvattomasti järjestelmään. Testaus voidaan suorittaa ilman, että tuotannon toiminta häiriintyy, mikä on erityisen tärkeää kriittisiä prosesseja tai infrastruktuuria ylläpitävälle yritykselle, sillä toiminnan katkoksia on aiemmin esiintynyt vastaavanlaisten testausten yhteydessä. Samalla digitaalinen kaksonen voi analysoida hyökkäysten vaikutuksia, joiden pohjalta voidaan kehittää tehokkaita reagointistrategioita ja palautumisprosesseja. (de Azambuja ym., 2024.)

Tekoälyn ja pilvipalveluiden merkitys korostuu myös kriiseistä palautumisessa. Jälkitoimet, kuten varmuuskopioiden palauttaminen, voidaan automatisoida tekoälyn avulla, mikä nopeuttaa toipumista. Pilvipalveluiden skaalautuvuus, kustannustehokkuus sekä niiden tarjoama välitön pääsy verkossa tallennettuihin varmuuskopioihin tuovat lisäarvoa kriisin kokeneelle organisaatiolle. Lisäksi tekoälyllä on potentiaalia automatisoida viestintä sisäisten ja ulkoisten sidosryhmien välillä, mikä tukee muun muassa tiedon jakamista, resurssien koordinointia ja tilannekuvan ylläpitämistä. Tehokas toiminnan palauttaminen minimoi seisokkiaikaa, joka on suoraan yhteydessä yrityksen taloudelliseen tilanteeseen ja asiakassuhteisiin. (Radanliev ym., 2020; Kaur ym., 2023.) Samalla tämän tyyppiset toimet edistävät digitaalisten toimitusketjujen kyberresilienssiä eli kykyä kestää kyberhyökkäyksiä ja palautua niistä nopeasti, joka on ensiarvoisen tärkeää nykymaailmassa, jossa organisaatiot tulevat väistämättä kokemaan kyberkriisejä (Boyes, 2015).

5.3 Yleinen tietoturvan vahvistaminen

Digitaalisen toimitusketjun tietoturvan vahvistamisessa lohkoketju on toimivia työkalu oikein sovellettuna. Se edistää jokaista perinteisen tietoturvan määritelmän ominaisuutta; luottamuksellisuutta, eheyttä ja saatavuutta (Samonas & Coss, 2014). Lohkoketjujen tieto on

luottamuksellista, koska vain valtuutetut osapuolet eli avaimenhaltijat pääsevät käsiksi tietoihin. Tiedon eheys säilyy, sillä lohkoketjuun tallennettuja tietoja ei voida muuttaa tai poistaa jälkikäteen. Jokainen tapahtuma kirjaa merkinnän lohkoketjuun pysyvästi, jolloin kaikki muutokset ovat läpinäkyviä ja jäljitettävissä. Tiedot ovat lisäksi saatavilla aina kaikille valtuutetuille käyttäjille yksittäisen laajan järjestelmän kautta. (Korpela ym., 2017; Wang ym., 2019; Ham, 2021.) Tietoturvan vahvistuminen edistää osapuolten luottamusta tietojen oikeellisuuteen vähentäen samalla virheiden ja petosten riskiä, joiden voidaan todeta vahvistavan digitaalisten toimitusketjujen kyberturvallisuutta.

Lohkoketjun hajautettu ja muuttumaton rakenne vaikeuttaa toimitusketjun tietojen peukalointia jälkikäteen ja järjestelmien heikkouksien hyödyntämistä. Siihen kirjatut tapahtumatiedot kopioidaan kaikkiin lohkoketjun solmuihin, ja jos niihin yritetään tehdä muutoksia, ne mitätöityvät virheellisinä. Lisäksi lohkoketjuteknologia mahdollistaa anonyymin, turvallisen ja tehokkaan tiedonjaon toimitusketjun eri osapuolten välillä, kun mukana ei ole keskitettyä välittäjää, eikä lohkoketju sisällä henkilökohtaisia tietoja osapuolista. (Korpela ym., 2017; Wang ym., 2019.)

Lohkoketju hyödyntää julkisen avaimen infrastruktuuria (engl. public key infrastructure, PKI), jonka ansiosta vain tapahtumaan osallistuvilla osapuolilla on pääsy tietoihin. Käytännössä tämä toimii, kun ostotilanteessa myyjä lähettää PKI-ohjelmiston ostajalle, joka sisältää turvaviestin. Ostajan tulee muistaa turvaviesti, jottei transaktio mitätöidy. Avain toimii siis tapahtuman tunnistetietojen salaamisessa ja salauksen purkamisessa. (Korpela ym., 2017; Wang ym., 2019.)

Älysopimukset ovat lohkoketjuteknologian sovelluksia, jotka suorittavat automaattisesti sopimuksen ehdot, vähentäen kolmansien osapuolten tarvetta ja tehden tapahtumista suojattuja sekä kustannustehokkaita. Esimerkiksi toimitusketjuissa älysopimukset voivat varmistaa, että maksu suoritetaan vasta toimituksen jälkeen. Yhdistämällä älysopimuksiin IoT –teknologia, osapuolten välinen tiedonvälitys automatisoituu, joka vähentää ihmisten välistä vuorovaikutuksen tarvetta entisestään. Tämän avulla voitaisiin minimoida ihmisten tekemiä virheitä, joka on suurin syy kyberonnettomuuksiin organisaatioissa (Evans ym., 2019). Älysopimuksia on tähän mennessä ollut pääsääntöisesti kokeilussa vasta rahoitusliiketoimissa. Niiden kokonaisvaltainen integrointi osaksi toimitusketjuja voi kestää vielä vuosia, sillä ne mullistaisivat koko toimitusketjurakenteen perinpohjaisesti. (Korpela ym., 2017; Wang ym., 2019.)

Lohkoketju ei ole kuitenkaan täysin haavoittumaton. Se on mahdollista hakkeroida, jos joukko hyökkääjiä saa tilapäisesti yli puolet lohkoketjun verkoston solmuista hallintaansa, jolloin sen tietojen manipulointi on mahdollista. Hakkerointi vaatii merkittävän laskentatehon ja paljon

resursseja, jotka usein vähentävät sen todennäköisyyttä. Haasteita lohkoketjuteknologian käyttöönotossa ovat muun muassa skaalautuvuus, tiedonhallinta, yhteentoimivuus ja puutteet taloudellisissa resursseissa, henkilöstön halukkuudessa, osaamisessa sekä sääntelyssä. (Wang ym., 2019; Cheung ym., 2021.)

Muutkin Industry 4.0 teknologiat kohtaavat samantyyppisiä haasteita ja riskejä. Big Data -analytiikka ja koneoppimisalgoritmit vaativat merkittäviä resursseja, kuten laskentakapasiteettia, osaavaa henkilökuntaa ja rahoitusta (Ullah & Ali Babar, 2019; Alani, 2021). Suurin haaste tekoälymallien kouluttamisessa on riittävän ja laadukkaan datan valitseminen (Kaur ym., 2023). Muita tekoälyn tuomia haasteita ovat muun muassa yksityisyyden suoja, vastuunalaisuus ja algoritmiset vinoumat, jotka voivat johtaa ennakkoluuloiseen tai virheelliseen päätöksentekoon. Digitaalisen kaksosen käyttöönottoon liittyy samoja haasteita kuin edellä mainittuihin teknologioihin kuten puutteelliset standardit ja järjestelmien yhteentoimivuuden ongelmat. (de Azambuja ym., 2024; Camacho, 2024.) IoT-laitteiden keräämän valtavan datamäärän takia niiden suurimmat riskit liittyvät yksityisyyden suojaan ja niiden haavoittuvuuksiin, joista jälkimmäistä käsiteltiin tutkielman alaluvussa 4.1 (Radanliev ym., 2020). Loppujenlopuksi, kaikkia näitä teknologioita yhdistää niiden luomat riskit digitaalisten toimitusketjujen kyberturvallisuuteen (Pandey ym., 2020).

Tulevaisuudessa uusien teknologioiden käyttöönotto tietoturvajärjestelmissä on enemmänkin välttämättömyys, kuin vain uusi hieno trendi. Organisaatioiden kyberresilienssi jää kehityksessä muista jälkeen, ellei käyttöön oteta pilvipalveluita, Big Data-analytiikkaa ja tekoälyalgoritmeja. Big Datan rooli kyberturvallisuuden vahvistamisessa korostuu, kun analysoitavan datan määrä kasvaa tulevaisuudessa entisestään, johon tarvitaan tekoälyä tehokkaan analysoinnin, uhkien torjunnan ja automatisoidun järjestelmien palauttamisen tueksi. Pilvipalvelut voivat lisätä digitaalisen toimitusketjun kustannustehokkuutta ja edesauttaa muiden teknologioiden, kuten lohkoketjujen ja IoT:n, integrointia tietoturvaratkaisuihin sekä muihin prosesseihin. Lohkoketjujen tulevaisuudennäkymät toimitusketjujen tietoturvan vahvistajana ovat lupaavat. (Korpela ym., 2017; Alani, 2021; Camacho, 2024; Khokhar ym., 2024.)

6 Yhteenveto ja johtopäätökset

Tässä tutkielmassa tarkasteltiin digitaalisten toimitusketjujen kyberturvallisuutta, sitä uhkaavia kyberuhkia ja sitä, miten Industry 4.0:n teknologioita voidaan hyödyntää digitaalisten toimitusketjujen kyberturvallisuuden tehostamisessa. Kyberuhkista ja -onnettomuuksista keskityttiin erityisesti toimitusketjuhyökkäyksiin ja kyberkriiseihin, jotka ovat seurausta ihmisten tekemistä virheistä. Uusista teknologioista tutkittiin tekoälyä, Big Data -analytiikkaa, IoT:ta, pilvipalveluita ja lohkoketjuja sekä niiden mahdollisuuksia kyberturvallisuusratkaisuissa. Nämä Industry 4.0 teknologiat ovat olleet toimitusketjujen digitalisoitumisen pääasiallinen syy. Ne mahdollistavat toimitusketjujen tehokkaamman ja ketterämmän hallinnan, joka moninkertaistaa niiden kyvyn tuottaa lisäarvoa asiakkaille, täten lisäten asiakas tyytyväisyyttä. (Büyüközkan & Göçer, 2018; Menon & Shah, 2019.)

Tutkielmassa selvisi, että digitaalisten toimitusketjujen monimutkaisuus, verkottuminen sekä internetpohjaisuus lisäävät niiden alttiutta kyberuhkille. Nämä ominaisuudet ovat seurausta toimittajien ja muiden toimitusketjun osapuolten määrän moninkertaistumisesta sekä uusien teknologioiden käyttöönotosta. Uusilla innovaatioilla on siis myös varjopuolensa, kuten näilläkin uusilla teknologioilla. Toimitusketjun monimutkaistumisesta on seurannut uusien toimittajasuhteiden syntymistä, mikä tarkoittaa uusia haavoittuvuuksia. (Büyüközkan & Göçer, 2018; Pandey ym., 2020; Nygård, 2022.) Kyberhyökkäykset ja muut kybertapaukset voivat saada alkunsa mistä tahansa toimitusketjun osasta, mutta kuten SolarWinds- ja CrowdStrike -tapaukset havainnollistavat, ne saavat usein alkunsa toimitusketjun heikoimmasta lenkistä, joka lopulta vaarantaa koko ketjun (Raponi ym., 2021; George, 2024). Havaittiin, että tämä heikoin lenkki on useimmiten ihminen eli kyberuhkat syntyvät suurimman osan ajasta oman henkilöstön inhimillisitä virheistä (Evans ym., 2019).

Tutkimus osoitti, että Industry 4.0:n teknologiat tarjoavat lupaavia ratkaisuja digitaalisten toimitusketjujen kyberturvallisuuden parantamiseen. Tekoälyn ja Big Data -analytiikan mahdollistama ennustava analytiikka voi parantaa uhkien ennaltaehkäisyä ja tunnistamista, lohkoketju vahvistaa tietoturvaa ja parantaa läpinäkyvyyttä, pilvipalvelut tarjoavat skaalautuvuutta ja joustavuutta, digitaalinen kaksonen tarjoaa turvallisen virtuaalitestausympäristön kyberturvallisuusratkaisuille sekä IoT-laitteet parantavat reaaliaikaista tiedonsiirtoa ja vähentävät ihmisten vuorovaikutuksen tarvetta. Lisäksi tekoälyn mahdollistama toimintojen automatisointi voi nopeuttaa kriiseihin reagointia ja toiminnan palauttamista normaaliin. (Korpela ym., 2017; Wang ym., 2019; Radanliev ym., 2020; Kaur ym., 2023; de Azambuja ym., 2024.)

On kuitenkin tärkeää huomata, että pelkkä teknologia ei takaa hyvää kyberturvallisuutta organisaatiolle. Kyberturvallisuuden on oltava kokonaisvaltainen lähestymistapa, joka kattaa ihmiset ja prosessit sekä fyysiset ja teknologiset näkökohdat. Ensiarvoisen tärkeää on organisaatiokulttuurin kehittäminen, jossa tietoturva nähdään kaikkien vastuulla ja jossa virheistä oppiminen on tärkeämpää kuin syyllisten etsiminen. (Boyes, 2015; Evans ym., 2019.)

Tutkimuksesta selvisi, että digitaalisten toimitusketjujen kyberturvallisuuden tutkimukselle olisi lisätarvetta, erityisesti reaaliaikaisiin reagointi- ja palautumistoimenpiteisiin liittyen (Cheung ym., 2021). Jatkossa olisi tärkeää tutkia tarkemmin toimitusketjujen kyberresilienssin parantamista. Tämä johtuu siitä, että kyberhyökkäysten ja -onnettomuuksien uhkat lisääntyvät tulevaisuudessa entisestään, jolloin niiden kohtaamisesta tulee lähes varmaa. Siispä kyky kestää kyberhyökkäyksiä ja toipua niistä on ensiarvoisen tärkeää, jotta väistämättömät onnettomuudet voidaan torjua siististi ja tehokkaasti jatkossa tai kriisin sattuessa toiminta on mahdollista palauttaa nopeasti normaaliin. (Boyes, 2015.) Tutkimuksissa tulisi käsitellä myös inhimillisen tekijän roolia kyberonnettomuuksissa, ja miten se voitaisiin minimoida, sillä ihminen on organisaatioiden kyberturvallisuuden suurin uhka (Evans ym., 2019). Lisäksi tulisi keskittyä uusien teknologioiden käytännön sovelluksiin kyberturvallisuudessa, teknologian ja kyberuhkien tason kehittyessä nopeasti (Büyüközkan & Göçer, 2018; Gartner 2024). Erityinen fokus tulisi kohdistua siihen, miten eri teknologioita voidaan parhaiten integroida osaksi digitaalisia toimitusketjuja ja miten voidaan varmistaa kaikkien toimitusketjun osapuolten saumaton yhteistyö sekä tiedonjako kyberturvallisuuden parantamiseksi. Tämä vaatii myös päättäjiltä standardien ja sääntelyn uudistamista.

Yrityksille suositellaan kokonaisvaltaista kyberturvallisuusstrategiaa, joka kattaa kaikki toimitusketjun osapuolet, inhimillisen tekijän, prosessit ja teknologiset ratkaisut. Säännölliset tietoturvakoulutukset ja -harjoitukset, kyberhyökkäyksiin valmistautuminen sekä jatkuva kyberturvallisuuden seuranta ja kehittäminen ovat keskeisiä keinoja uhkien minimointiin. Toimitusketjun toimittajien valintaan ja heidän kyberturvallisuuden tasoonsa tulisi kiinnittää erityistä huomiota. Lisäksi on tärkeää hyödyntää uusimpia teknologioita uhkien torjumisessa. (Cheung ym., 2021; Kaur ym., 2024.)

Lähteet

Aarland, M. (2024). Cybersecurity in digital supply chains in the procurement process: Introducing the digital supply chain management framework. *Information & Computer Security, ahead-of-print*(ahead-of-print). https://doi.org/10.1108/ICS-10-2023-0198

Accenture, 'The Cyber-Resilient CEO' (2023). https://www.accenture.com/content/dam/accenture/final/accenture-com/document-2/Accenture-The-Cyber-Resilient-CEO-Final.pdf#zoom=40

Agrawal, P., & Narain, R. (2018). Digital supply chain management: An Overview. In *IOP conference series: materials science and engineering* (Vol. 455, No. 1, p. 012074). IOP Publishing.

Alani, M. M. (2021). Big data in cybersecurity: A survey of applications and future trends. *Journal of Reliable Intelligent Environments*, *7*(2), 85–114. https://doi.org/10.1007/s40860-020-00120-3

Alharam, A. K., & Elmedany, W. (2017). *The effects of cyber-security on healthcare industry*. 1–9. The effects of cyber-security on healthcare industry. In 2017 9th *IEEE-GCC Conference and Exhibition (GCCCE)* (pp. 1-9). IEEE.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*. https://doi.org/10.3389/fcomp.2021.563060

Boyes, H. (2015). Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review, 5(4), 28.*

Boyson, S., Corsi, T. M., & Paraskevas, J.-P. (2022). Defending digital supply chains: Evidence from a decade-long research program. *Technovation*, *118*, 102380. https://doi.org/10.1016/j.technovation.2021.102380

Brewer, R. (2016). Ransomware attacks: Detection, prevention and cure. *Network Security*, *2016*(9), 5–9. https://doi.org/10.1016/S1353-4858(16)30086-1

Büyüközkan, G., & Göçer, F. (2018). Digital Supply Chain: Literature review and a proposed framework for future research. *Computers in Industry*, *97*, 157–177. https://doi.org/10.1016/j.compind.2018.02.010

Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *3*(1), Article 1. https://doi.org/10.60087/jaigs.v3i1.75

Cheung, K.-F., Bell, M. G. H., & Bhattacharjya, J. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, *146*, 102217. https://doi.org/10.1016/j.tre.2020.102217

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–52.

Cybersecurity Ventures, 'Cybercrime To Cost The World $10.5 Trillion Annually By 2025' (2020). https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

de Azambuja, A. J. G., Giese, T., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2024). Digital Twins in Industry 4.0–Opportunities and challenges related to Cyber Security. *Procedia CIRP*, *121*, 25–30.

Evans, M., He, Y., Luo, C., Yevseyeva, I., Janicke, H., Zamani, E., & Maglaras, L. A. (2019). Real-time information security incident management: A case study using the IS-CHEC technique. *IEEE Access*, *7*, 142147–142175.

Garay-Rondero, C. L., Martinez-Flores, J. L., Smith, N. R., Morales, S. O. C., & Aldrette-Malacara, A. (2020). Digital supply chain model in Industry 4.0. *Journal of Manufacturing Technology Management*, *31*(5), 887–933.

Gartner, 'Gartner Forecasts Global Information Security Spending to Grow 15% in 2025' (2024). https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025

George, D. A. S. (2024). When Trust Fails: Examining Systemic Risk in the Digital Economy from the 2024 CrowdStrike Outage. *Partners Universal Multidisciplinary Research Journal*, *1*(2), Article 2. https://doi.org/10.5281/zenodo.12828222

Ham, J. V. D. (2021). Toward a Better Understanding of "Cybersecurity". *Digital Threats: Research and Practice*, *2*(3), 1–3. https://doi.org/10.1145/3442445

International Telecommunications Union, 'ITU-T X.1205, Overview of cybersecurity' (2008). https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

Kaur, H., Gupta, M., & Singh, S. P. (2024). Integrated model to optimize supplier selection and investments for cyber resilience in digital supply chains. *International Journal of Production Economics*, *275*, 109338. https://doi.org/10.1016/j.ijpe.2024.109338

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, *97*, 101804.

Khokhar, R., Rankothge, W., Rashidi, L., Mohammadian, H., Frei, B., Ellis, S., Freitas, I., & Ghorbani, A. (2024). A Survey on Supply Chain Management: Exploring Physical and Cyber Security Challenges Threats Critical Applications and Innovative Technologies. *International Journal of Supply and Operations Management*, *Online First*. https://doi.org/10.22034/ijsom.2024.110219.2975

Korpela, K., Hallikas, J., & Dahlberg, T. (2017). *Digital Supply Chain Transformation toward Blockchain Integration*. http://hdl.handle.net/10125/41666

Kramer, F. D., Starr, S. H., & Wentz, L. K. (2011). *Cyberpower and National Security*. University of Nebraska Press. https://doi.org/10.2307/j.ctt1djmhj1

Kumar, G., Pandey, S. K., Varshney, N., Kumar, A., Kumar, M., & Singh, K. U. (2023). Cybersecurity Education: Understanding the knowledge gaps based on cyber security policy, challenge, and knowledge. In 2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT) (pp. 735-741). IEEE. https://doi.org/10.1109/CSNT57126.2023.10134610

Kyberturvallisuuskeskus, ’Toimintaohje – Palvelunestohyökkäys’ (2022). https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Palvelunestohy%C3%B6kk%C3%A4ysToimintaohje.pdf

Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: Cybersecurity across the supply chain. *International Journal of Production Research*, *60*(1), 162–183. https://doi.org/10.1080/00207543.2021.1984606

Menon, S., & Shah, S. (2019). An Overview of Digitalisation in Conventional Supply Chain Management. *MATEC Web of Conferences, 292*, 01013. https://doi.org/10.1051/matecconf/201929201013

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*, *Version 1.1* (No. NIST CSWP 04162018; s. NIST CSWP 04162018). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Nygård, A. R., & Katsikas, S. (2022). SoK: Combating threats in the digital supply chain. *Proceedings of the 17th International Conference on Availability, Reliability and Security*, 1–8. https://doi.org/10.1145/3538969.3544421

O’Callaghan, K., & Mariappanadar, S. (2008). Restoring service after an unplanned IT outage. *IT Professional*, *10*(3), 40–45.

O'Flaherty, K. (2024). CrowdStrike Reveals What Happened, Why—And What's Changed. *Forbes*, https://www.forbes.com/sites/kateoflahertyuk/2024/08/07/crowdstrike-reveals-what-happened-why-and-whats-changed/

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: Conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103–128.

Queiroz, M. M., Pereira, S. C. F., Telles, R., & Machado, M. C. (2021). Industry 4.0 and digital supply chain capabilities. *Benchmarking: An International Journal*, *28*(5), 1761–1782. https://doi.org/10.1108/BIJ-12-2018-0435

Radanliev, P., De Roure, D., Page, K., Nurse, J. R. C., Mantilla Montalvo, R., Santos, O., Maddox, L., & Burnap, P. (2020). Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*, *3*(1), 13. https://doi.org/10.1186/s42400-020-00052-8

Raponi, S., Caprolu, M., & Pietro, R. D. (2021). *Beyond SolarWinds: The Systemic Risks of Critical Infrastructures, State of Play, and Future Directions*.

Samonas, S., & Coss, D. (2014). Samonas, S., & Coss, D. (2014). The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security,* 10(3).

Sanastokeskus ry, 'Kyberturvallisuuden sanasto' (2018). https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

Statista, 'Distribution of cyberattacks across worldwide industries in 2023' (2024). https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/

Tiwari, S., Wee, H. M., & Daryanto, Y. (2018). Big data analytics in supply chain management between 2010 and 2016: Insights to industries. *Computers & Industrial Engineering*, *115*, 319–330. https://doi.org/10.1016/j.cie.2017.11.017

Toorajipour, R., Sohrabpour, V., Nazarpour, A., Oghazi, P., & Fischl, M. (2021). Artificial intelligence in supply chain management: A systematic literature review. *Journal of Business Research*, *122*, 502–517. https://doi.org/10.1016/j.jbusres.2020.09.009

Ullah, F., & Ali Babar, M. (2019). Architectural Tactics for Big Data Cybersecurity Analytics Systems: A Review. *Journal of Systems and Software*, *151*, 81–118. https://doi.org/10.1016/j.jss.2019.01.051

Wang, S., Wan, J., Li, D., & Zhang, C. (2016). Implementing Smart Factory of Industrie 4.0: An Outlook. *International Journal of Distributed Sensor Networks*, *12*(1), 3159805. https://doi.org/10.1155/2016/3159805

Wang, Y., Han, J. H., & Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: A systematic literature review and research agenda. *Supply Chain Management: An International Journal*, *24*(1), 62–84.

Welch, L. D. (2011). Cyberspace–The fifth operational domain. *IDA Research Notes*, 2–7.

World Economic Forum, 'The Global Risks Report 2024 14th Edition' (2024). https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

Wu, Y., Cegielski, C. G., Hazen, B. T., & Hall, D. J. (2013). Cloud Computing in Support of Supply Chain Information System Infrastructure: Understanding When to go to the Cloud. *Journal of Supply Chain Management*, *49*(3), 25–41. https://doi.org/10.1111/j.1745-493x.2012.03287.x

Ye, Y., Li, T., Adjeroh, D., & Iyengar, S. S. (2018). A Survey on Malware Detection Using Data Mining Techniques. *ACM Computing Surveys*, *50*(3), 1–40. https://doi.org/10.1145/3073559

Yeboah-Ofori, A., Islam, S., Lee, S. W., Shamszaman, Z. U., Muhammad, K., Altaf, M., & Al-Rakhami, M. S. (2021). Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security. *IEEE Access*, *9*, 94318–94337. https://doi.org/10.1109/ACCESS.2021.3087109

HUOM* Tekoälypohjaista ohjelmaa käytetty lähteiden etsinnän sekä tekstin alustavan rakenteen suunnittelun tukena