Aarnu Valtteri

DIGITAALISEN TRANSFORMAATION KESKEISET TEKNOLOGIAT JA NIIDEN KYBERTURVALLISUUS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Aarnu Valtteri
Digitaalisen transformaation keskeiset teknologiat ja niiden kyberturvallisuus
Jyväskylä: Jyväskylän yliopisto, 2022, 31 s.
Tietojärjestelmätiede, Kandidaatintutkielma
Ohjaaja(t): Kuusio, Ari

Organisaatiot sekä yhteiskunnat digitalisoituvat yhä enemmän ja uusien teknologioiden noustessa on hyvä tarkastella, mitkä niistä ovat tällä hetkellä yleisimmät digitaalisessa transformaatiossa. Maailman muuttunut turvallisuustilanne näkyy myös kybermaailmassa muun muassa kyberhyökkäyksien määrän nousulla, joten aiheen tarkastelu tästä näkökulmasta on todella ajankohtainen. Tässä kandidaatintutkielmassa tarkasteltiin kirjallisuuskatsauksen avulla digitaalisen transformaation keskeisiä teknologioita, niiden kyberturvallisuutta kyberuhkien kautta, sekä näiden uhkien torjuntaa ja ehkäisyä strategisella tasolla. Kirjallisuuskatsausta hyödyntäen löydettiin kuusi digitaalisen transformaation teknologiaa sekä kuusi keskeistä kyberuhkaa, jotka haittaavat niin organisaatioita kuin myös yksityishenkilöitä. Tämän jälkeen tarkasteltiin löydettyjen teknologioiden alttiutta kyberuhille sekä käytiin läpi näiden uhkien torjumista yleisellä tasolla sekä yksittäisten uhkien näkökulmasta. Tällä tutkielmalla on pyritty tuomaan kokoava yleiskatsausta digitaalisen transformaation teknologioiden kyberturvallisuudesta.

Asiasanat: Digitaalinen transformaatio, Kyberturvallisuus, Tietoturva, Kyberuhka

ABSTRACT

Aarnu, Valtteri
Key technologies of digital transformation and their cybersecurity
Jyväskylä: University of Jyväskylä, 2022, 31 pp.
Information Systems, Bachelor's thesis
Supervisor(s): Kuusio, Ari

As societies and organizations keep on digitalizing and new technologies keep emerging, it is time to take look at the most common technologies of digital transformation. In the last few years world tension has risen significantly, so perspective of cybersecurity is very topical as organizations face ever-growing amount of cyberattacks. In this bachelor´s thesis I used literature review to take look at the key technologies of digital transformation, the cybersecurity of those technologies through cyberthreats and how to prepare and prevent for said threats on strategic level. This thesis presents six common technologies that are adopted in digital transformation and six cyberthreats that cause nuisance to organizations and individuals. After these findings I gathered from the literature the vulnerabilities of the technologies to the found cyberthreats and gathered ways to prepare and prevent these threats. This thesis has aimed to provide a comprehensive overview of the cyber security of digital transformation technologies.

Keywords: Digital transformation, Cybersecurity, Information security, Cyberthreat

KUVIOT JA TAULUKOT

SISÄLLYS

1 JOHDANTO

Yhteiskunnan digitalisoituminen näkyy jokapäiväisessä elämässämme. Esimerkiksi pankit sulkevat fyysisiä konttoreitaan ja palvelut ovat siirtyneet nettipankkeihin sekä mobiiliapplikaatioihin. Myös etätapaamiset yleistyvät ja nostavat suosiotaan yritysmaailmassa, kauppojen hintakyltit alkavat muuttumaan sähköisiksi ja fyysisten maksukorttien ohelle on alkanut syntymään digitaalisia pankkikortteja.

Vuonna 2021 pankkien henkilöasiakkaita palvelevia konttoreita oli Suomessa 740 kappaletta (Finanssivalvonta, 2022). Konttoreita on suljettu muutaman viimevuoden ajan noin 30 kpl vuodessa, ja syynä tähän on pankkipalveluiden digitalisoituminen ja niiden jatkuva parantuminen (Finanssivalvonta, 2022). Finanssivalvonnan (2022) mukaan pankit tarjoavat kehittyviä tukiverkostoja asiakkaille, joilla on vaikeuksia päästä käsiksi digitaalisiin palveluihin ja tämän ansiosta konttoreita pystytään sulkemaan nykyisellä tahdilla.

COVID-19 pandemian aiheuttaman sulkutilan alkaessa lähes kaikki kokoukset muuttuivat etäkokouksiksi. Samalla etätyö alkoi tehdä tuloaan ihmisten koteihin ja toimistoja jouduttiin sulkemaan. Tämä toi uusia vaatimuksia niin yrityksille kuin kotitalouksille. Työn siirtyminen suojatusta toimiston verkkoympäristöstä koteihin luo uusia uhkia ja tietoturva-aukkoja. Pandemian hellittäessä yhä useammat yritykset tarjoavat etätyömahdollisuutta työntekijöilleen. Työn siirtyessä yhä enenevissä määrin ihmisten koteihin yrityksille voi avautua uusia mahdollisuuksia ottaa käyttöön uusia teknologiota ja strategioita. Tämän tapaisessa tilanteessa digitaalisella transformaatiolla voidaan saavuttaa mittavia hyötyjä niin yritykselle kuin sen työntekijöillekin.

Internet of things (IoT, suomeksi esineiden internet) on alati kasvava trendi IT-alalla. IoT laitteiden oikeanlainen implementointi organisaatioon ja sen strategiaan voi tuoda toimialoille massiivisia mullistuksia. IoT:n liittyy niin sanottuun ”Neljäs teollinen vallankumous” (Frank ym., 2019). Saadakseen IoT:n osaksi entiteetin toimintaa, vaaditaan toimijoilta digitaalista transformaatiota.

Maailman turvallisuustilanne on muuttunut paljon viimevuosien aikana. Tämä uusi turvallisuustilanne heijastuu myös organisaatioihin mm. kyberuhkina. Vieraat valtiot ja hakkeriryhmittymät pyrkivät saamaan arkaluontoista tie-

toa organisaatioilta tai häiritsemään niiden toimintaa lamauttamalla järjestelmiä ja infrastruktuuria. 77 % Kyberrikoksista kohdistuu Pk-yrityksiin näiden yleisesti heikomman kyberturvallisuuden takia verrattuna suuriin yrityksiin (Vakakis ym., 2019). Digitaalisen transformaation tuodessa uusia laitteita, järjestelmiä ja infrastruktuuria organisaatioihin mahdollisuudet erilaisiin kyberuhkiin kasvavat. Internetistä on tullut monelle eurooppalaiselle pakollinen työkalu työntekemiseen, opiskeluun, ja sosiaaliseen kanssakäymiseen (ENISA, 2022).

Tässä tutkielmassa tarkastellaan digitaalisen transformaation keskeisiä teknologioita ja niihin liittyviä turvallisuusuhkia. Tutkimuksen tehdään kirjallisuuteen perustuva katsaus digitaalisen transformaation keskeisiin teknologioihin, sekä näiden teknologioiden kyber- ja tietoturva uhkiin. Aihetta lähestytään seuraavien tutkimuskysymysten kautta:

- Mitkä ovat digitaalisen transformaation yleisimmät teknologiat?
- Minkälaisia tieto-/kyberturvauhkia teknologiat sisältävät?
- Kuinka näitä uhkia voidaan ehkäistä?

Tutkielma rakentuu viidestä luvusta. Toisessa luvussa avataan digitaalista transformaatiota ja tarkastellaan sen keskeisimpiä teknologioita. Kolmannessa luvussa avataan kyberturvallisuutta ja esitetään yleisiä kyberuhkia. Neljännessä luvussa tarkastellaan esitettyjen teknologioiden alttiuksia kyberuhille sekä kyberuhkien torjumista. Viimeisessä luvussa käydään läpi keskeisimmät tulokset ja esitetään aiheita mahdollisille jatkotutkimuksille.

Tutkielma toteutetaan kuvailevana, narratiivisena kirjallisuuskatsauksena. Se on yleinen kirjallisuuskatsauksen muoto ja sopii hyvin laajoihin alueisiin (Salminen. 2011, s. 7), luoden siltaa tutkimusten ja artikkeleiden välille (Templier, Pare. 2015, s. 118).

Hakusanoina lähteiden etsinnässä on käytetty seuraavia sanoja suomeksi, että englanniksi yksinään ja yhdisteltynä: Digitaalinen transformaatio, onnistunut digitaalinen transformaatio, Liiketoiminta strategia/malli, tietojärjestelmät, kyberturvallisuus, Big data, Internet of things, tekoäly, Kyberuhka, Pilvipalvelut, mobiilialustat, sosiaalinen media ja tehokas kyberturvallisuus. Lähteitä on etsitty seuraavista tietokannoista: Google Scolar, Scopus ja JYKDOK. Kriteereinä ovat olleet tieteelliset artikkelit, jotka ovat vertaisarvioituja. Valinnoissa on pyritty priorisoimaan laadukkaat tieteelliset julkaisut. Laadun arviointiin on käytetty muun muassa Julkaisufoorumin arviointia, tekstissä viitattujen lähteiden laatua sekä viittausten määrää tutkittavaan artikkeliin. Lähteinä on myös käytetty valtiollisten instituutioiden ja käytännön työelämän yritysten raportteja.

2 DIGITAALINEN TRANSFORMAATIO JA SEN KESKEISET TEKNOLOGIAT

Tässä luvussa käydään läpi digitaalista transformaatiota käsitteenä sekä digitaalisen transformaation keskeisiä teknologioita. Teknologiat ja niiden strategiset merkitykset avataan lyhyesti ja niiden hyödyistä annettaan muutamat esimerkit menemättä sen syvemmälle taktisiin tai operatiivisiin prosesseihin.

2.1 Digitaalisen transformaation määritelmä

Digitaalista transformaatiota (digital transformation) ei ole määritelty täysin yksiselitteisesti. Yleisellä tasolla digitaalinen transformaatio kattaa syvällisesti muutokset yhteiskunnassa ja toimialoilla, jotka ovat muuttuneet käyttäen erilaisia teknologioita (Vial, 2019). Digitaalinen transformaatio tarkoittaa yleisesti maailman laajuista nopeutunutta teknologian käyttöönottoa organisaatioissa, yhteisöissä, yksilöillä ja kansakunnissa (Sivarajah ym., 2020). Nämä molemmat määritelmät ovat hyviä yleisen tason määritelmiä.

Monien lähteiden mukaan (esim. Gong ja Ribiere, 2021; Saarikko ym., 2020) digitaalinen transformaatio on usein sekoitettu digitointiin (digitization) ja digitalisaatioon (digitalization). Digitointi tarkoittaa analogisen tiedon muuttamista digitaaliseen muotoon, joita tietokoneet voivat hyödyntää (Gong & Ribiere, 2021). Digitalisaatio on seuraava askel digitoinnista. Digitalisaation myötä digitoitu tieto voidaan valjastaa liiketoimintaan, jonka seurauksena syntyy uusia liiketoimintamalleja, tuotteita tai prosesseja (Saarikko ym., 2020).

Digitalisaatio sekoitetaan usein digitaaliseen transformaatioon, koska digitaalista transformaatiota ei ollut määritelty yhtenäisesti (Gong & Ribiere, 2021). Gong ja Ribiere (2021) pyrkivät tekemään tähän muutoksen ”Developing a unified definition of digital transformation” tutkimuksessaan. He johtavat määritelmänsä digitaalisen transformaatioon analysoimalla 146 erilaista digitaalisen transformaation määritelmää tieteellisistä artikkeleista. Tutkimuksen lopputuloksena he määrittelivät digitaalisen transformaation seuraavasti: ”Olennainen

muutosprosessi, jonka mahdollistaa digitaaliset teknologiat, minkä tarkoituksena on tuottaa entiteetille (esim. Organisaatio, bisnesverkosto, toimiala tai yhteisö) radikaaleja parannuksia ja innovaatioita, joilla luodaan arvoa sidosryhmille käyttämällä organisaation resursseja ja kykyjä strategisena vipuvartena" (Gong & Ribiere, 2021). Samanlaisia elementtejä digitaalisen transformaation määritelmään voidaan löytää Vialin (2019) tutkimuksesta "Understanding digital transformation: A review and research agenda". Tässä tutkimuksessa digitaalisen transformaation määritelmä on johdettu 28 tutkimuksesta ja se on seuraava: "Prosessi, joka pyrkii parantamaan entiteettiä tekemällä suuria muutoksia sen ominaisuuksiin yhdistelemällä erilaisia tieto- ja viestintäteknologioita" (Vial, 2019).

Molemmat Vialin (2019) sekä Gong ja Ribiere (2021) ovat johtaneet määritelmänsä useiden aiempien tieteellisten artikkeleiden pohjalta. Määritelmät jakavat monia samankaltaisuuksia. Molempien mukaan digitaalinen transformaatio on muutosprosessi, joka ei rajoitu vain organisaatioihin ja sen mahdollistaa erilaiset teknologiat. Vaikka entiteetti on usein organisaatio, tulee muutkin mahdolliset kohteet huomioida määrittelyssä, kuten yhteisöt ja toimialat (Vial, 2019).

2.2 Digitaalisen transformaation keskeisimmät teknologiat

Uudet teknologiat ovat keskeinen osa digitaalista transformaatiota. Digitaalista transformaatiota käsittelevistä artikkeleista (esim. Vial, 2019; Frank, ym. 2019; Bouwman, 2019; Duc & Chirumamilla, 2019; Sivarajah ym. 2020) ja yritysten (esim. Accenture, 2022.) nettisivuja tutkimalla voidaan löytää useita keskeisiä teknologioita, joiden onnistunut käyttöönotto yleisesti vaatii digitaalista transformaatiota. Näitä teknologioita ovat:

- Sosiaalinen media (Vial, 2019; Bouwman ym., 2019, Sivarajah ym., 2020)
- Pilvipalvelut (Accenture, 2022; Duc & Chirumamilla, 2019; Vial, 2019; Frank, ym. 2019; Sivarajah ym., 2020)
- Big data ja data-analytiikka (Accenture, 2022; Duc & Chirumamilla, 2019; Vial, 2019; Frank, ym. 2019; Sivarajah ym., 2020)
- Mobiilialustat (Duc & Chirumamilla, 2019; Vial, 2019; Frank, ym. 2019; Sivarajah ym., 2020)
- Internet of Things (Accenture, 2022; Duc & Chirumamilla, 2019; Vial, 2019; Frank, ym. 2019)
- Tekoäly (Accenture, 2022; Duc & Chirumamilla, 2019; Vial, 2019)

Sosiaalinen media tuo parhaiten arvoa asiakaskokemuksen parantamiseen (Sivarajah ym., 2020). Sosiaalinen media voi muuttaa yrityksessä tapoja kommunikoida asiakkaidensa kanssa, palveluiden toimituksessa ja uuden IT:n integroinnissa (Bouwman ym., 2019). Sosiaalisesta mediasta on tullut ominainen alusta sekä julkiselle että organisaatioiden väliselle vuorovaikutukselle, tiedon-

siirrolle ja suhteille (Sivarajah ym., 2020). Sosiaalinen media voidaan myös valjastaa datan keräämiseen. Sen kautta pystytään mittaamaan muun muassa asiakasvirtoja, asiakasuskollisuutta sekä brändin mainetta ja merkkitietoisuutta (Sivarajah ym., 2020). B2C yritykset valjastavat sosiaalisen median datan big datan analyysin todennäköisemmin kuin B2B yritykset (Sivarajah ym., 2020). Tämä voisi johtua B2C yritysten asiakkaiden aktiivisemmasta sosiaalisen median käytöstä. Puskaradiossa (word of mouth) huhut ja arvostelut leviävät yhä nopeammin digitaalisten alustojen avulla. B2B yritykset eivät ole niin suuressa vuorovaikutuksessa keskenään sosiaalisen median kautta kuin B2C yritykset ja heidän yksityisasiakkaansa. Tämä arviot kuitenkin omia hypoteesejani, jota tulisi tarkastella tieteellisesti. Sosiaalisen median datan analysoinnin avulla voidaan organisaatioissa tehdä nopeita, oikein ajoitettuja ja merkittäviä liiketoiminnan päätöksiä (Sivarajah ym., 2020). Sosiaalisesta mediasta kasattua Big dataa käytetään yleensä trendien ja mielipiteiden löytämiseen (Ghani ym., 2019). Trendien löytämistä voidaan hyödyntää esimerkiksi uusissa mainoskampanjoissa (Sivarajah ym., 2020) ja tuotteissa.

Pilvipalveluilla voidaan saada helposti pääsy dataan ja muihin palveluihin lähes miltä tahansa laitteelta, esimerkiksi mobiililaitteelta, tietokoneelta tai erilaisista terminaaleista (Frank ym., 2019; Zissis & Lekkas, 2012). Pilvipalveluiden avulla yritysten ei tarvitse hankkia omiin tiloihinsa laajaa teknologiainfrastruktuuria, kuten palvelimia, tietokantoja ja laajoja verkkoja, vaan ne voivat vuokrata niitä toisilta yrityksiltä. Lisäksi pilvipalvelut ovat hyvin skaalautuvia ja täten helppoja laajentaa ja supistaa tarvittaessa, toisin kuin organisaation omat konesalit ja datakeskukset. Keskeisimpiä pilvipalveluita ovat SaaS (software as a service), IaaS (Infrastructure as a service) ja PaaS (platform as a service) (Zissis & Lekkas, 2012). SaaS palvelut tarjoavat yrityksille järjestelmiä ja sovelluksia, joita voidaan käyttää erilaisilla alustoilla, kuten mobiililaitteilta tai selainpohjaisesta rajapinnasta (Zissis & Lekkas, 2012). IaaS palvelua käyttäessä asiakas vuokraa erilaista infrastruktuuria palvelun tarjoajalta, kuten palvelimia, laskentatehoa ja verkkoja, joita asiakas voi hallita omien tarpeidensa mukaan (Zissis & Lekkas, 2012). IaaS palveluiden avulla organisaatio voi ulkoistaa konesalinsa pois omista tiloistaan. PaaS palvelut tarjoaa infrastruktuurin lisäksi alustoja kehittämiseen (Microsoft Azure, 2022). PaaS palvelut eivät anna yhtä laajaa hallintaa infrastruktuurista kuin IaaS palvelut (Zissis & Lekkas, 2012). Pilvipalvelut ovat erittäin hyödyllisiä prosessien automatisoinnissa, esim. tuotantoprosessi voidaan virtualisoida siirtämällä aikaisemmin yrityksen tiloissa laiteistoissa sijainneet on-premise ohjelmistot pilveen, täten jättäen tehtaaseen vain tuotannossa tarvittavat laitteet, kuten robotit, valmistuslaitteet ja liukuhihnat (Borangiu ym., 2019). Tämän tapaisella laitteiden ja ohjelmiston erotuksella valmistusyksiköstä voidaan saada ketterämpiä ja joustavampia (Borangiu ym., 2019). SaaS-pohjainen järjestelmä mahdollistaa esimerkiksi toimitusketjussa tiedonkulun kaikkien ketjuun osallistujien välillä, jolloin tieto virtaa paremmin osapuolien kesken ilman kolmannen osapuolen alustoja tai henkilöitä (Sivarajah ym., 2020).

Big data tarkoittaa suuria määriä monimuotoista tietoa, jonka käsittely ja analysointi vaatii edistyneitä tietojenkäsittelyn teknologioita (Gartner, 2022a). Tieto voi olla strukturoitua, semi-strukturoitua tai strukturoimatonta (Ghani ym., 2019). Big data on yleensä jaettu internettiin ja digitaalisiin ekosysteemeihin (Pappas ym., 2018). Dataa kerätään muun muassa sosiaalisesta mediasta (Ghani ym., 2019), järjestelmistä ja IoT-sensoreista (Frank ym., 2019). Dataa kerätessä ei usein tiedetä mihin sitä ollaan käyttämässä (Sivarajah ym., 2020). Data-analytiikka pyrkii etsimään näistä valtavista data määristä tarvittavia tietoja.

Data ei itsessään ole arvokasta (Gandomi & Haider, 2015), vaan sen potentiaalin avaamiseksi vaaditaan data-analyysia. Data-analyysin tarkoituksena on analysoida ja kerätä relevantit tiedot datavarastoista ja -virroista (Gandomi & Haider, 2015). Data-analytiikalla voidaan saada kokonaisvaltaisia ja persoonallisia oivalluksia organisaation nykyisestä tilanteesta reaaliajassa, auttaen johtoa tekemään parhaat päätökset (Sivarajah ym., 2020), tai sillä voidaan ennustaa asiakkaiden toimintaa (Sestino ym., 2020). Analytiikan avulla yritykset voivat tarjota parempia ja kysyntää vastaavia palveluita kuluttajille (Vial, 2019).

Mobiililaitteilla voidaan saavuttaa niin asiakaskokemuksen parantamista, datan keräystä kuin prosessien helpotusta. Monet yritykset ovat luoneet mobiilisovelluksia asiakkaan ostoprosessin helpottamiseksi (Vial, 2019). Sovelluksilla voidaan kerätä yksilöistä tärkeää dataa, joka mahdollistaa persoonallisen kokemuksen luomisen (esim. paremmat suositukset tuotteista) parantaen näin asiakaskokemusta (Vial, 2019). Mobiililaitteen käyttäminen maksaessa voi parantaa asiakaskokemusta (Sivarajah ym., 2020). Mobiililaitteet helpottavat myös tiedon kulkua, tehden jokapäiväisistä prosesseista nopeampia ja sulavampia (Sivarajah ym., 2020). Ravintolat voivat tarjota mahdollisuutta tilata ruoka mobiililaitteen avulla, mikä nopeuttaa ruuan tilaamista (Fitzgerald ym., 2013.). Tällöin saadaan henkilökuntaa priorisoitua muihin tehtäviin tuoden yritykselle säästöjä. Asiakas voi saada sovelluksen kautta myös helposti ja nopeasti enemmän tietoa tuotteista. Mobiililaitteet ovat yhä suurempi osa arkipäiväämme. Esimerkiksi pankkitoiminnot, vero- sekä muut yhteiskunnalliset asiat hoituvat yhä kasvavissa määrin mobiilisovelluksissa ja selaimissa.

Gartner (2022b) määrittelee Internet of Thing:n seuraavasti: ”Fyysisten esineiden luoma verkosto, joka sisältää sulautettua teknologiaa kommunikoidakseen, aistiakseen tai ollakseen vuorovaikutuksessa keskenään tai ympäristönsä kanssa.”. IoT tuo erilaisia sensoreita valmistuslaitteisiin ja prosesseihin, jolloin niistä voidaan kerätä reaaliaikaista dataa (Tao ym., 2018). Tehtaassa IoT:ä voidaan käyttää yhteyden luomiseen laitteiden ja järjestelmien välille (Frank ym., 2019). IoT voi tuoda kriittisen muutoksen tuotantoon automatisoimalla prosessin ja korvaamalla ihmisen liukuhihnalta ja siirtämällä hänet toisiin tehtäviin (Abdellah ym., 2022).

Tekoälyä voidaan käyttää prosessien automatisointiin ja datan käsittelyyn. Tekoälyällä, analytiikalla ja IoT-alustojen avulla voidaan löytää tietoja big datasta, jota ei muilla keinoilla pystyttäisi löytämään (Warner & Wäger, 2019). Tekoäly sopii hyvin esim. trendien löytämiseen ja ennustamiseen tai strategisen

päätöksen teon parantamiseen (Warner & Wäger, 2019). Tekoälyt muuttavat datavirrat liiketoiminnassa hyödylliseksi tiedoksi (Kaloudi & Li, 2020).

Edellä tarkastellun perusteella voidaan ajatella, että erilaisten teknologioiden implementointi voi mahdollistaa suuriakin kehitysaskeleita yrityksessä niin prosessien, strategioiden kuin toimintamallienkin kannalta. Esimerkkinä näiden teknologioiden yhteiskäytöstä voidaan nostaa tilanne, jossa IoT laitteet luovat useasta eri lähteestä big dataa, jonka tekoäly ja data-analytiikka tulkitsevat. IoT:n ja pilvipalveluiden yhteiskäytöllä voidaan yhdistää useita dataa keräämiä ja tuottavia laitteita yhteen, jolloin voidaan luoda big data varasto (Frank ym., 2019). Taulukkoon 1 on kerätty tässä luvussa käsiteltyjä teknologioita, esimerkkejä kyseisistä teknologioista, sekä niiden luomia hyötyjä entiteetille.

Taulukko 1 - Digitaalisen transformaation yleisimmät teknologiat

Teknologia	**Esimerkki**	**Hyödyt**
Sosiaalinen media (Vial, 2019; Bouwman ym., 2019, Sivarajah ym., 2020)	Asiakaspalvelukanava (Bouwman ym., 2019), Markkinointialusta (Sivarajah ym., 2020), Datan keräysalusta (Sivarajah ym., 2020)	Asiakaskokemuksen parantaminen (Sivarajah ym., 2020), Sisäisen ja ulkoisen kommunikoinnin parantaminen (Bouwman ym., 2019, Sivarajah ym., 2020), Datan keräys (Sivarajah ym., 2020; Ghani ym., 2019)
Pilvipalvelut (Accenture, 2022; Duc & Chirumamilla, 2019; Vial, 2019; Frank, ym. 2019; Sivarajah ym., 2020)	SaaS, IaaS ja PaaS (Zissis & Lekkas, 2012; Microsoft Azure)	Konesalien ulkoistaminen (Zissis & Lekkas, 2012; Borangiu ym., 2019), Pääsy applikaatioihin ja dataan usealta eri alustalta (Frank ym., 2019; Zissis & Lekkas, 2012)
Big data ja data-analytiikka (Accenture, 2022; Duc & Chirumamilla, 2019; Vial, 2019; Frank, ym. 2019; Sivarajah ym., 2020)	Datavarastot ja -virrat (Ghani ym., 2019; Frank ym., 2019), Asiakkaiden käytöksen ennustaminen (Sestino ym., 2020)	Trendien ennustaminen (Sestino ym., 2020; Sivarajah ym., 2020), Asiakaskokemuksen parantaminen (Sestino ym., 2020; Vial, 2019; Sivarajah ym., 2020), Tukea päätösten tekoon (Sivarajah ym., 2020)
Mobiilialustat (Duc & Chirumamilla, 2019; Vial, 2019; Frank, ym. 2019; Sivarajah ym., 2020)	Sovellukset (Sivarajah ym., 2020; Fitzgerald ym., 2013.), Datan keräysalusta (Vial, 2019)	Organisaation sisäisen kommunikaation parantaminen (Sivarajah ym., 2020), Asiakaskokemuksen parantaminen (Vial, 2019; Sivarajah ym., 2020; Fitzgerald ym., 2013.)

Internet of Things (Accenture, 2022; Duc & Chirumamilla, 2019; Vial, 2019; Frank, ym. 2019)	Tuotannon ja prosessien automatisointi (Abdellah ym., 2022), Datan keräysalusta (Tao ym., 2018; Frank ym., 2019)	Automatisointi (Abdellah ym., 2022), Datan keräys (Tao ym., 2018; Frank ym., 2019)
Tekoäly (Accenture, 2022; Duc & Chirumamilla, 2019; Vial, 2019)	Automatisointi (Abdellah ym., 2022)	Tukea päätösten tekoon (Warner & Wäger, 2019), automatisointi (Abdellah ym., 2022), Datan analysointi (Kaloudi & Li, 2020; Warner & Wäger, 2019)

3 KYBERTURVALLISUUS

Tässä luvussa käydään läpi kyberturvallisuutta, yleisimpiä kyberuhkia sekä turvallista digitaalista transformaatiota.

3.1 Kyberturvallisuuden käsite

Microsoft (2022) määrittelee kyberturvallisuuden tavoiksi, joilla suojataan digitaalisia tietoja, laitteita ja resursseja. Gartnerin (2022c) määritelmä on hyvin samankaltainen mutta laajempi: Kyberturvallisuus on kokoelma ihmisiä, käytäntöjä, prosesseja ja teknologioita, jotka suojaavat yrityksen kybervarallisuutta (Cyber assets). Kyberturvallisuus pitää sisällään informaatioteknologian-, operatiivisten teknologioiden- ja IoT turvallisuuden, sekä tietoturvan (Gartner, 2022c). Microsoftin määritelmä on enemmän yksityishenkilöille suunnattu yksinkertaistettu käsite, kun taas Gartnerin käsite kuvaa laajemmin etenkin yrityksen kyberturvallisuutta. Molemmissa käsitteissä tulee kuitenkin kyberturvallisuuden keskeinen näkökulma, eli digitaalisten laitteitten, ohjelmistojen ja tiedon suojaaminen ulkoisilta uhilta. Suojautumisessa voidaan hyödyntää muun muassa palomuureja, antivirus ohjelmia, lokitietoja sekä luvattoman tunkeutumisen tunnistamisen ohjelmilla (Mukhopadhyay ym., 2013). Tässä tutkielmassa termi kyberturva tulee sisältämään tietoturvan.

Kyberturvallisuuden tarkoitus on tuoda kolme eri ulottuvuutta datalle ja järjestelmille, tietosuoja, saatavuus ja koskemattomuus (Duc & Chirumamilla, 2019). Nämä ovat turvallisten systeemien rakentamisen tärkeät kulmakivet (Zissis & Lekkas, 2012).

Haavoittuvuuksilla tarkoitetaan informaatioteknologian tai muun teknologian heikkouksia, joita hakkerit voivat käyttää hyväkseen (Lezzi ym., 2018). Haavoittuvuus tarkoittaa kaikenlaisia heikkouksia tietojärjestelmissä, sovelluk-

sissa, laitteissa tai prosesseissa (mukaan lukien ihmisen toiminta), joita voidaan käyttää järjestelmien, infrastruktuurin, prosessien tai organisaation vahingoittamiseen (Kyberturvallisuuskeskus, 2020).

Ihmisen laiminlyövä toiminta tuo suuria haavoittuvaisuuksia ja voi vaarantaa koko yrityksen. Ihminen, joka ei ole töissä teknisellä puolella, voi vaarantaa koko järjestelmän ja sen sisältämät tiedot (ENISA, 2022). Tutkimuksista on tullut ilmi, että kaikki työntekijät eivät seuraa yrityksen antamia tietoturvakäytäntöjä vaaditulla tavalla (Li ym., 2019). Henkilöt, joille on annettu enemmän kyberturvallisuus koulutusta, eivät välttämättä harjoita muista poikkeavia toimia kyberturvallisuuden takaamiseksi (Li ym., 2019). Kuvaavana esimerkkinä voidaan nostaa esille vuonna 2020 paljastunut psykoterapiakeskus Vastaamon tietovuoto, joka johtui tutkimuksen mukaan ”turvallisen palvelun ylläpidon parhaiden käytäntöjen ja suojausmenetelmien laiminlyönnistä” (Tietovaltuutetun toimisto, 2021). Vastaamo asetettiin konkurssiin vuonna 2021.

Joihinkin järjestelmiin ei haluta lisätä uusimpia päivityksiä ja korjauksia, sillä ne voivat vaarantaa järjestelmän toimivuuden ja saatavuuden (Alghassab, 2022). Tämän tapainen toiminta jättää järjestelmään vanhoja, tunnettuja haavoittuvuuksia, joita hakkereiden on helppo hyödyntää. Nämä haavoittuvuudet luovat massiivisia tietoturvauhkia yrityksille.

Kyberrikollisuuden motiivi on usein taloudellinen tai haitan aiheuttaminen. Kyberrikolliset voivat hyödyntää edellä mainittuja teknologioita omissa hyökkäyksissään. Pilvipalveluita voidaan käyttää botnet-palveluiden luomiseen, jonka kautta voidaan suorittaa massiivisia ja hajautettuja palvelunestohyökkäyksiä (ENISA, 2022). Tekoälyä voidaan hyödyntää useissa erilaisissa hyökkäyksissä ja dataa voidaan käyttää kiertämään tunnettuja puolustautumismenetelmiä (Kaloudi & Li, 2020).

3.2 Yleisimmät kyberuhat

European union agency for cybersecurity (ENISA) (2022) esittää raportissaan kuusi eri typpistä kyberuhkaa. Samoja uhkia voidaan löytää TrafiCom:n (2020) ja Eurooppa neuvoston (2021) raporteista. Näitä ovat uhkia ovat:

- Kiristysohjelmat (ENISA, 2022; TrafiCom, 2020; Eurooppa-neuvosto, 2021)
- Haittaohjelmat (ENISA, 2022; TrafiCom, 2020; Eurooppa-neuvosto, 2021)
- Henkilöiden manipulointi (ENISA, 2022; TrafiCom, 2020; Eurooppa-neuvosto, 2021)
- Dataan kohdistuvat uhat (ENISA, 2022; Eurooppa-neuvosto, 2021)
- Saatavuuteen kohdistuvat uhat (ENISA, 2022; Eurooppa-neuvosto, 2021)
- Disinformaatio (ENISA, 2022; Eurooppa-neuvosto, 2021)

Kiristysohjelman tarkoitus on sulkea omistaja ulos järjestelmästä tai salata tietoja ja omaisuutta, ja vaatia niiden takaisin saamisesta rahaa (ENISA, 2022). Kiristysohjelmien motiivi on usein taloudellinen (TrafiCom, 2020). Kiristysohjelmat

ovat uhka sekä yrityksille, että yksityishenkilöille. Kiristysohjelma voi päästä järjestelmiin esim. erilaisten linkkien liitetiedostojen mukana (TrafiCom, 2020).

Haittaohjelmilla tarkoitetaan koodia tai logiikkaa, jolla pyritään saamaan luvaton pääsy tai aloittaa luvaton prosessi, joka voi vaarantaa järjestelmän saatavuuden, tietosuojan tai koskemattomuuden (ENISA, 2022). Haittaohjelmat voivat olla muun muassa troijalaista, viruksia, vakoiluohjelmia tai matoja (TrafiCom, 2020). Kryptovaluuttojen noustessa maailmanlaajuiseksi trendiksi syntyi myös uudenlaisia kryptovaluuttojen louhintaan tarkoitettuja haittaohjelmia, jolloin hyökkääjä pystyy käyttämään uhrinsa infrastruktuuria ja resursseja oman taloudellisen edun hankkimiseen (Eurooppa-neuvosto, 2021). Haittaohjelmien tarkoitus on nimensä mukaan aiheuttaa haittaa ja vahinkoja sen uhrille tai hyötyä sen käyttäjälle vakoilemalla, poistamalla ja/tai salaamalla tiedostoja tai lamauttamalla prosesseja (TrafiCom, 2020). Haittaohjelmia voi kiristysohjelmien tapaan asentua linkkien ja tiedostojen välityksellä huolimattomuuden seurauksena. Sosiaalisesta mediasta on tullut tehokas alusta haitta- ja kiristysohjelmien levittämiseen, ollen jopa 10 kertaa tehokkaampi kuin sähköpostilla tehdyt levittämisyritykset (He, 2012).

Henkilöiden manipuloinnin tavoitteena on saada arkaluotoisia tietoja, kuten salasanoja, pankkitunnuksia tai saada luvaton pääsy dokumentteihin ja järjestelmiin käyttämällä hyväksi ihmisen erehtyväisyyttä ja käytöstä (ENISA, 2022). Tietojenkalastelu kuuluu tähän uhkienluokkaan. Yleinen tapa tietojenkalasteluun on sähköpostiin lähetettävät linkit, jotka vievät huijaussivustoille (TrafiCom, 2020). Näillä sivuilla pyydetään yleensä käyttäjän kirjautumistietoja tai pankkitunnuksia. Ihminen, joka ei seuraa kyberturvallisuuteen luotuja käytäntöjä on erittäin haavoittuvainen tällaiselle toiminnalle. Muun muassa siirryttäessä etätyön aikaan arkaluontoista tietoa voi jäädä lojumaan paikkoihin, jossa sitä ei pitäisi olla. Tämä altistaa henkilöt ja yritykset tietovuodoille.

Dataan kohdistuvat uhkat koostuvat useista eri uhista, joiden tavoitteena on saada pääsy dataan tai sen tuottajiin ja manipuloida/häiritä sen tuotantoa. (ENISA, 2022). Esimerkiksi palvelunestohyökkäyksillä voidaan estää dataan pääsy tai disinformaatiota yrityksessä voidaan vahvistaa tietojen manipuloinnilla (ENISA, 2022). Näihin uhkiin kuuluu myös tietovuodot ja tietomurrot. Tietomurto on tarkoituksellinen hyökkäys, jonka tavoitteena on saada pääsy, varastaa ja mahdollisesti julkaista arkaluontoista tietoa, kun taas tietovuoto on vahingossa tapahtunut arkaluontoisen tiedon vuoto tai paljastus (ENISA, 2022).

Saatavuuteen liittyvät uhat tulevat lähinnä palvelunestohyökkäyksistä. Palvelunestohyökkäyksen tavoitteena on kaataa nettisivu tai palvelu ja mahdollisesti jopa hajottaa fyysistä infrastruktuuria kuormittamalla järjestelmä suurilla määrillä tietoliikennettä (F-secure, 2022). Näiden hyökkäysten tekijät ovat yksittäisiä henkilöitä, järjestöjä tai valtiollisia toimijoita (Kyberturvallisuuskeskus, 2022). Palvelunestohyökkäyksiin voi myös liittyä kiristämistä. Ryhmät uhkaavat yrityksiä heidän sivujen/järjestelmien kaatamisella, jos uhrit eivät suostu maksamaan hyökkääjille (ENISA, 2022). Palvelunestohyökkäykset ovat yksi kriittisimmistä uhista IT järjestelmille, sillä nämä hyökkäykset voivat poistaa dataa, poistaa kriittisiä palveluita käytöstä ja vaikuttaa pysyvästi laitteiden suo-

rituskykyyn (ENISA, 2022). Vuonna 2022 uutisiin on noussut useita artikkeleita merenalaisten verkkokaapeleiden häiriöistä. Näissä tapauksissa merikaapeleihin on tullut häiriöitä, ja tämän seurauksena useat saaret ovat jääneet ilman kriittisiä yhteyksiä. Häiriöistä on syytetty eri valtiollisia toimijoita ilman pitäviä todisteita. Tällainen mahdollinen toiminta luetaan myös saatavuuteen liittyväksi uhaksi.

Disinformaatiolla, eli väärällä tiedolla pyritään vaikuttamaan niin yrityksiin, yksilöihin kuin yhteiskuntiinkin. Yrityksiä voidaan mustamaalata väärällä tiedolla, yhteiskunnille ja ihmisille voidaan jakaa valeuutisia, joilla voidaan tehdä vaikeaksi oikean erottaminen väärästä ja ihmisisten mielipiteitä tai luottamusta voidaan manipuloida tai ohjailla (ENISA, 2022). Valtiolliset toimijat voivat levittää disinformaatiota tavoitteena aiheuttaa epävarmuutta, välinpitämättömyyttä totuutta kohtaan ja väsymystä totuuden löytämistä kohtaan (ENISA, 2022).

Digitaalisiin toimintoihin ja myös digitaaliseen transformaatioon liittyviä uhkia on monenlaisia ja ne kohdistuvat niin järjestelmiin, ohjelmiin, fyysiseen IT infrastruktuuriin ja ihmisiin. Näitä uhkia voidaan yhdistellä keskenään ja aiheuttaa näin vielä isompaa haittaa. Niiden motiivina on haitan tekeminen tai rahallisen hyödyn tavoittelu. Taulukkoon 2 on kasattu luvussa käsitellyt kyberuhat, sekä näistä uhista on annettu muutamia esimerkkejä.

Taulukko 2 - Yleisimmät kyberuhat

Kyberuhka	**Esimerkkejä**
Kiristysohjelmat (ENISA, 2022; TrafiCom, 2020; Eurooppa-neuvosto, 2021)	Tiedostojen/laitteiden/järjestelmien lukitseminen ja uhrin kiristäminen (ENISA, 2022; TrafiCom, 2020; Eurooppa-neuvosto, 2021)
Haittaohjelmat (ENISA, 2022; TrafiCom, 2020; Eurooppa-neuvosto, 2021)	Virukset, troijalaiset, vakoiluohjelmat (ENISA, 2022; TrafiCom, 2020; Eurooppa-neuvosto, 2021)
Henkilöiden manipulointi (ENISA, 2022; TrafiCom, 2020; Eurooppa-neuvosto, 2021)	Tietojenkalastelu (ENISA, 2022; TrafiCom, 2020; Eurooppa-neuvosto, 2021)
Dataan kohdistuvat uhat (ENISA, 2022; Eurooppa-neuvosto, 2021)	Datan manipulointi, varastaminen tai tuhoaminen. Tietomurrot ja -vuodot (ENISA, 2022; Eurooppa-neuvosto, 2021)
Saatavuuteen kohdistuvat uhat (ENISA, 2022; Eurooppa-neuvosto, 2021)	Palvelunestohyökkäykset, infrastruktuurin fyysinen vahingoittaminen (ENISA, 2022; Eurooppa-neuvosto, 2021)
Disinformaatio (ENISA, 2022; Eurooppa-neuvosto, 2021)	Valeuutiset, datan vääristäminen (ENISA, 2022; Eurooppa-neuvosto, 2021)

3.3 Digitaalisen transformaation turvallisuus

Digitaalinen transformaatio tuo paljon uutta teknologiaa ja infrastruktuuria entiteetille. Nämä teknologiat tuovat lisää tilaa haavoittuvuuksille ja täten lisäävät mahdollisuuksia kyberhyökkäyksille.

Kyberturvallisuuden ongelmat organisaation ottaessa käyttöön uutta teknologiaa voidaan jakaa kolmeen ryhmään: 1. Tiedon puute teknologiasta ja/tai kyberturvallisuudesta. 2. Tilanteet, joissa uusia ja vanhoja teknologioita käytetään yhdessä. 3. Riittämättömät resurssit kyberturvallisuuteen investoimiseen. Näihin edellä mainittuihin ongelmiin liittyy tieto jollain tavalla, ja niistä voidaan selvitä laajalla henkilöstön koulutuksella niin teknologioihin kuin kyberturvallisuuteen liittyen. (Almeida ym., 2020)

Pienet yritykset ovat etenkin alttiita kyberhyökkäyksille, sillä ne eivät näe kyberturvallisuutta muita yrityksen puolia ja ominaisuuksia tärkeämpänä, eikä niillä ole riittäviä resursseja tarvittavan kyberturvallisuuden saavuttamiseksi. Tämä tekee niistä houkuttelevia kohteita kyberrikollisille. (Teymourlouei & Harris, 2019)

Digitaalisen transformaation kyberturvallisuutta voidaan edistää ottamalla käyttöön tunnettuja ja turvallisia teknologioita. Nämä teknologiat tulee suojata hyvin, jotta ne ovat turvassa haavoittuvuuksilta, uhilta ja hyökkäyksiltä. Ohjesääntöjä seuraamalla (esim. GDPR) voidaan rajoittaa vahinkoja ja riskejä. (Duc & Chirumamilla, 2019)

Uusista järjestelmistä saadaan turvallisia lisäämällä niihin tarvittavat vastatoimet, joilla voidaan torjua uhkia ja haasteita. Nämä toimet tulee ottaa huomioon jo järjestelmän suunnittelussa. (Zissis & Lekkas, 2012).

Edellisten löydösten perusteella digitaalisen transformaation turvallisuutta voidaan edistää kattavalla muutosprosessin suunnittelulla. Organisaatiolla tulisi olla osaava tiimi, joka osaa neuvoa johtoa ja tutkia teknologia vaihtoehtoja sekä niiden kyberturvallisuutta ja varmistaa niiden turvallinen integrointi. Organisaation tulee luoda kattavat käytännöt työntekijöilleen uusiin prosesseihin, jotta niiden kyberturvallisuus voidaan varmistaa. Työntekijät tulee kouluttaa kattavasti uusien teknologioiden turvalliseen käyttöön, jolla voidaan pienentää teknologioiden sekä prosessien haavoittuvuutta (Li, ym. 2019). Käytänteitä on etenkin alkuun hyvä valvoa, jotta yksittäisten työntekijöiden käytäntöjä laiminlyövä toiminta ei tartu muihin (Li, ym. 2019).

4 DIGITAALISEN TRANSFORMAATION TEKNOLOGIOIDEN KYBERTURVALLISUUS

Tässä luvussa käsitellään Digitaalisen transformaation yleisten teknologioiden alttius uhille, sekä tarkastellaan näiden uhkien torjumista. Luvussa ei mennä teknisiin keinoihin, vaan asioita pohditaan hyvin yleisellä tasolla

4.1 Teknologioiden alttius kyberuhille

Sosiaalinen median kautta yritys voi joutua tietovuodon tai tietojenkalastelun kohteeksi. Työntekijöiltä voidaan yrittää saada arkaluontoista tietoa, tai heille voidaan jakaa linkkejä, joiden takana onkin kiristys- ja haittaohjelmia (He, 2012). Työntekijät voivat jakaa arkaluontoista tietoa epähuomiossa esimerkiksi viestiketjuissa juttelemalla tai kuvia jakamalla. Osaan työtehtävistä kuuluu sosiaalisen median käyttö, ja yritysten voi olla vaikea valvoa kaikkia tietoturvaan liittyviä käytäntöjä riskialttiissa sosiaalisessa mediassa (He, 2012). Yrityksen mainetta voidaan haitata tekemällä sosiaaliseen mediaan valetilejä. Twitterin omistajanvaihdoksen jälkeen verified-ikonin, joka ennen annettiin vain varmistetuille käyttäjille, pystyi ainakin marraskuussa 2022 ostamaan kuukausitilauspohjaisesti. Tämän seurauksena valetileistä on ollut mahdollista tehdä oikean näköisiä ja jakaa niiden kautta väärää tietoa, joka sosiaalisessa mediassa voi levitä räjähdysmäisesti.

Pilvipalveluista saadaan yleensä vääränlainen turvallisuuden tunne, joka voi johtaa siihen, että pilvipalveluita ei valvota niin tarkasti (ENISA, 2022). Kuitenkin pilvipalvelut ovat alttiita monille uhkille riippuen palvelusta. Yleisimpiä ovat datan häirintä ja poisto, luvaton käyttö, palvelun huono valvonta ja palvelunestohyökkäykset (Zissis & Lekkas, 2012). Pilvipalvelun tarjoajalla on pääsy asiakkaan tietoihin, joten luvattoman käytön riski laajenee oman organisaation toimijoiden ulkopuolelle (Kyberturvallisuuskeskus, 2014). Tietoja saattaa tuhoutua tahattomasti palveluntarjoajan puolen häiriöiden seurauksena. Pilvipal-

veluiden tarjoaja on yhtä lailla altis saatavuuteen liittyviin uhkiin kuin asiakaskin.

Big data ja data-analyysi voivat sisältää paljon arkaluontoista tietoa, kuten käyttäjätietoja (Zhang, 2018). Tiedot voivat tulla varastetuiksi, tai ne voivat päästä vuotamaan, jonka seurauksena yritykset voivat kokea suuria maineellisia tai taloudellisia haittoja. Big datan luotettavuus ja oikeellisuus on tärkeä turvallisuuden seikka. Dataa voidaan manipuloida jopa yhden yksittäisen hyökkääjän toimesta, minkä jälkeen data-analyysistä voi tulla virheellisiä tuloksia, mikä johdosta organisaatiossa voi syntyä huonoja päätöksiä, tai hyökkääjä voi yrittää muuttaa datan omalle kannalleen edulliseksi (Zhang, 2018).

Mobiililaitteet ovat haavoittuvaisia samoille asioille kuin normaalit tietokoneet (Abawajy ym., 2018). Mobiililaitteiden lukuisat sensorit (GPS, kamerat, mikrofonit ja erilaisia mittarit) tekevät siitä oivan kohteen vakoiluohjelmille, joilla voidaan kerätä tietoa henkilöstä tai yrityksestä, jossa hän työskentelee (Abawajy ym., 2018). Mobiililaitteet jakavat dataa ja tarjoavat laskentatehoa muille laitteille, jotka tekevät niistä osan verkkoa ja infrastruktuuria ja näin mobiililaitteet tekevät itsestään houkuttelevan kohteen hyökkääjille (Abawajy ym., 2018). Puhelin voi vierailla useassa, myös suojaamattomassa, verkossa päivän aikana, esim. työpaikan sisäinen verkko on suojatumpi kuin kahvilan julkinen verkko tai talouskohtainen kodin verkko (Abawajy ym., 2018). Hyökkääjä voi tartuttaa laitteen julkisessa verkossa ja päästä käsiksi muihin verkkoihin mobiililaitteen yhdistäessä näihin. Koska laitteen käyttäjä ei ole kokoajan samassa, turvatussa verkkoympäristössä, palomuurit ja luvattomaan tunkeutumiseen luodut keinot eivät välttämättä pysty tunnistamaan mahdollista tunkeutumista mobiililaitteen kautta (Abawajy ym., 2018).

IoT-laitteiden tuoma teknologinen lisäpinta ja yhteyksien määrä verkossa luo lisää hyökkäysalaa ja kohteita (Vakakis ym., 2019). IoT-laiteet ovat usein huonosti suojattua ja valvottuja, mikä tekee niistä suosittuja hyökkäyskohteita (Cisco, 2019; Lezzi ym, 2019). IoT-järjestelmien ja laitteiden kautta voidaan kaapata tietoa, niiden saatavuutta voidaan häiritä tai niihin voidaan asentaa kiristysohjelmia (Tsiknas ym., 2021).

Tekoälyn toiminta perustuu erilaisiin näytteisiin, dataan ja algoritmeihin, ja näitä häiritsemällä voidaan suorittaa kyberhyökkäyksiä tekoälyä ja koneoppimista vastaan (Li, 2018). Pienikin muutos datassa tai näytteissä (datan myrkyttäminen), joista tekoäly oppii, voi johtaa merkittäviin, virheellisiin tuloksiin, esimerkiksi virheisiin kasvojen tunnistamisessa, asiakkaan suosituksissa tai asioiden luokituksissa (Li, 2018).

Taulukkoon 3 on kasattu tutkielmassa esiin nousseet digitaalisen transformaation teknologiat, sekä niiden alttius käsitellyille kyberuhille tämän luvun löydösten perusteella. X sarakkeessa tarkoittaa teknologian olevan altis hyökkäykselle tai muuten haavoittuvainen sarakkeen kaltaiselle uhkatyypille. Taulukon tulokset on johdettu yllä olevan kappaleen löydöksistä.

Taulukko 3 - Teknologioiden alttius kyberuhille

	Kiristysohjelmat	**Haittaohjelmat**	**Henkilöiden manipulointi**	**Dataan kohdistuvat uhat**	**Saatavuuteen kohdistuvat uhat**	**Disinformaatio**
Sosiaalinen media	X	X	X			X
Pilvipalvelut	X	X	X	X	X	
Big data ja data-analyysi				X	X	X
Mobiilialustat	X	X	X	X	X	X
Internet of Things	X	X		X	X	
Tekoäly				X	X	X

4.2 Kyberuhkien torjuminen yleisellä tasolla

Yleisellä tasolla edellä käsiteltyjä uhkia voidaan ehkäistä seuraamalla yhteisöjen, yritysten ja valtiollisten instituutioiden asettamia kyberturvaan liittyviä käytäntöjä. Entiteetin tulisi tehdä omat säännöt ja käytännöt turvalliseen toimimiseen teknologioiden kanssa sekä valvoa näiden toteutumista (He, 2012). Käytännöt voivat sisältää muun muassa ohjeet salasanoihin Lisätyn turvan haasteina ovat usein hitaampi tiedonkulku verkon ja laitteiden välityksellä sekä prosessien hidastuminen (Vakakis ym., 2019). Entiteetillä olisi hyvä olla osaava tiimi, joka osaa reagoida ja antaa toimintaohjeita esimerkiksi palvelunestohyökkäyksen tai tietomurron tapahtuessa (ENISA, 2022). Tämän tiimin tulisi tuntea laitteistot, järjestelmät, toimintatavat ja toimitussopimukset hyvin, jotta tarvittavat toimet voidaan aloittaa välittömästi (ENISA, 2022). Teknologiat tulee olla hyvin suojattuja palomuureilla ja viruksentorjunta ohjelmilla, sekä järjestelmät ja ohjelmistot tulisi päivittää heti kun päivitykset tulevat saataville (TrafiCom, 2020). Työntekijöitä tulee kouluttaa teknologioiden turvalliseen käyttöön ja kyberturvaan liittyen (Li, ym. 2019).

4.3 Kyberuhkien torjuminen uhkaluokittain

Kiristys- ja haittaohjelmia pystytään välttämään pitämällä järjestelmät ja ohjelmistot päivitettyinä (TrafiCom, 2020). Päivityksillä korjataan löydettyjä haavoittuvuuksia. Jos päivityksiä ei suoriteta, nämä haavoittuvuudet jäävät avoimiksi ja entiteetti altistaa itsensä hyökkäyksille. Työntekijöiden toiminnalla voidaan ehkäistä kiristys- ja haittaohjelmille altistumista. Työntekijöiden olisi hyvä tunnistaa epäilyttävät linkit ja tiedostot, jotta ohjelmia ei pääse yrityksen järjestelmiin (TrafiCom, 2020). Lokitiedoilla, joita tulisi seurata aktiivisesti, voidaan jäljittää, mitä kautta haitalliset ohjelmat ovat voineet päätyä järjestelmiin, tai haittaohjelman toiminta voidaan huomata näistä tiedoista (ENISA, 2022). Sähköpostisuodattimilla voidaan vähentää haitallisten linkkien ja tiedostojen vastaanottamista (ENISA, 2022). Palomuureilla ja virustorjuntaohjelmilla voidaan torjua näitä uhkia. Kiristysohjelmien tuomaa haittaa voidaan torjua varmuuskopioiduilla ja salatuilla tiedostoilla (ENISA, 2022).

Ihmisten manipulointiin ja tietojenkalastelussa kattavia lokitietoja voidaan käyttää muun muassa sattuneen tietomurron tai -vuodon selvitystyössä (ENISA, 2022). Kolmansien osapuolien tarjoamien palveluiden lupia tulisi valvoa, jotta nämä järjestelmät eivät pääse liian syvälle yrityksen omiin järjestelmiin (ENISA, 2022). Jos kolmasosapuoli joutuisi hyökkäyksen kohteeksi, se vaarantaisi samalla myös yrityksen omat järjestelmät. Sähköpostien suodattimella voidaan yrittää suodattaa selvästi haitalliset yhteydenotot pois, tai sähköpostiin voidaan lisätä erilaisia toimintoja, jotka estävät tai varoittavat kommunikoimasta mahdollisen henkilön kanssa, joka imitoi esimerkiksi esimiestä tai ylempää johtajaa (ENISA, 2022). Etenkin etätyön ja mobiililaitteiden yleistymisen myötä entiteetin tulisi luoda kattavat säännöt tietoturvaan liittyen, kuten missä järjestelmiä saa avata, ja valvoa työntekijöiden toimintaa lokitietoja hyödyntäen lain sallimissa puitteissa (ENISA, 2022).

Dataan kohdistuvien uhkia voidaan pienentää valtuuksien hallinnalla eli varmistamalla, että vain tarvittavilla henkilöillä ja järjestelmillä on pääsy heidän tarvitsemiinsa tietoihin (ENISA, 2022). Salasanojen tulisi olla uniikkeja ja monivaiheisella tunnistamisella voidaan edistää käyttäjän tunnistamisen luotettavuutta (ENISA, 2022). Laadukkaan datan käytöllä ja datan arvioinnilla voidaan ehkäistä datan myrkyttämistä, jolloin tekoäly ja koneoppiminen ei opi virheellisiä asioita (ENISA, 2022). Varmuuskopioimalla voidaan pelastaa tiedot. Tiedot ja data voivat korruptoitua tai laitteisto, jolla data ja tiedot sijaitsee voi vahingoittua. Varmuuskopiot olisi hyvä hajauttaa laitteistollisesti, jotta yksi hyökkäys ei pääse käsiksi kopioihin, sekä maantieteellisesti esimerkiksi sähkökatkojen ja luonnonkatastrofien aiheuttamien vaurioiden varalta (ENISA, 2022).

Saatavuuden kohdistuvia uhkia voi olla vaikea ennaltaehkäistä, joten näiden varalle olisi hyvä olla varasuunnitelma, jolla tärkeät järjestelmät voidaan saada toimimaan (ENISA, 2022). Hyökkäyksiä voidaan yrittää estää dataliikenteen suodattimilla luomalla liikenteelle trendejä ja profiileja, lisäämällä järjestelmiin uusimmat päivitykset heti kun ne julkaistaan ja lisäämällä resursseja

(esim. skaalautuva pilvipalvelu), jotta palvelunestohyökkäyksen hinta nousee sietämättömäksi hyökkääjälle (ENISA, 2022).

Disinformaatiota vastaan voi toimia kouluttamalla työntekijöitä (ENISA, 2022). Tekoälyn voi valjastaa tunnistamaan tyypillisiä tuntomerkkejä manipuloidusta tiedosta ja kommunikoinnista (ENISA, 2022). Jotta dataa ei pystyttäisi manipuloimaan disinformaatiolla, tulisi lähteet varmistaa ennen tiedon keräystä ja tunnistaa disinformaatiota levittävät lähteet, jotta ne voidaan suodattaa pois (ENISA, 2022). Organisaatio voi tarkkailla internettiä saadakseen tietoa siitä, mitä ihmiset kirjoittavat heistä tai löytääkseen esimerkiksi heidän brändinsä väärinkäyttöä ja puutua asiaan välittömästi, jolloin voidaan estää mahdollisia mustamaalaus yrityksiä (He, 2012).

5 YHTEENVETO

Tässä tutkielmassa on tarkasteltu digitaalisen transformaation keskeisiä teknologioita, teknologioihin liittyviä kyberuhkia, sekä näiden uhkien torjuntaan ja ehkäisyyn liittyviä käytänteitä strategisella tasolla seuraavien tutkimuskysymyksien avulla:

- Mitkä ovat digitaalisen transformaation yleisimmät teknologiat?
- Minkälaisia tieto-/kyberturvauhkia teknologiat sisältävät?
- Kuinka näitä kyberuhkia voidaan ehkäistä?

Aihe on todella laaja ja esimerkiksi digitaalisesta transformaatiosta ja tässä tutkielmassa esiintyvistä teknologioista löytyy paljon tutkimuksia, jotka voivat olla todella yksityiskohtaisia ja rajattuja. Aiheesta ei löytynyt montaa yleisen tason kokoavaa tutkimusta, vaan ne keskittyivät usein todella pieniin aihealueisiin. Tällä tutkielmalla on pyritty tuomaan kokoavaa yleiskatsausta yhdistämällä nämä kaksi erittäin ajankohtaista aihetta. Tutkielmassa on otettu näkökulmaksi organisaatiot digitaalisessa transformaatiossa niiden ollessa keskeisin entiteetti.

Teknologioita tunnistettiin kuusi, ja niihin liittyviä kyberuhkia löytyi yleisellä tasolla kuusi. Nämä kyberuhat voivat kohdistua niin organisaatioihin, valtioihin kuin yksityishenkilöihin ja niiden motiivi on taloudellisen hyödyn tavoittelu tai haitan aiheuttaminen. Kyberuhkien torjuntaa ja ehkäisyä tarkasteltiin yleisellä tasolla sekä yksilöllisesti uhkien mukaan. Taulukoihin 4 ja 5 on kerätty keskeisimmät tulokset tutkimuskysymysten mukaan.

Taulukko 4 – Tulokset osa 1

Mitkä ovat digitaalisen transformaation yleisimmät teknologiat?
Sosiaalinen media (Vial, 2019; Bouwman ym., 2019, Sivarajah ym., 2020)
Pilvipalvelut (Accenture, 2022; Duc & Chirumamilla, 2019; Vial, 2019; Frank, ym. 2019; Sivarajah ym., 2020)
Big data ja data-analytiikka (Accenture, 2022; Duc & Chirumamilla, 2019; Vial, 2019; Frank, ym. 2019; Sivarajah ym., 2020)
Mobiilialustat (Duc & Chirumamilla, 2019; Vial, 2019; Frank, ym. 2019; Sivarajah ym., 2020)
Internet of things (Accenture, 2022; Duc & Chirumamilla, 2019; Vial, 2019; Frank, ym. 2019)
Tekoäly (Accenture, 2022; Duc & Chirumamilla, 2019; Vial, 2019)

Taulukko 5 – Tulokset osa 2

Minkälaisia tieto-/kyberturvauhkia teknologiat sisältävät?	**Kuinka kyberuhkia voidaan ehkäistä?**
Kiristysohjelmat (ENISA, 2022; TrafiCom, 2020; Eurooppa-neuvosto, 2021)	Järjestelmien ja ohjelmistojen päivitys, tietojen salaus ja varmuuskopiointi, henkilöstön koulutus, organisaation kyberturvallisuus säännöt ja käytännöt (TrafiCom, 2020; ENISA, 2022)
Haittaohjelmat (ENISA, 2022; TrafiCom, 2020; Eurooppa-neuvosto, 2021)	Järjestelmien ja ohjelmistojen päivitys, tietojen salaus ja varmuuskopiointi, henkilöstön koulutus, organisaation kyberturvallisuus säännöt ja käytännöt (TrafiCom, 2020; ENISA, 2022)
Ihmisten manipulointia (ENISA, 2022; TrafiCom, 2020; Eurooppa-neuvosto, 2021)	Käyttöoikeuksien valvonta, lokitiedot, suodattimet (esim. sähköposti), organisaation kyberturvallisuus säännöt ja käytännöt (ENISA, 2022)
Dataan kohdistuvat uhat (ENISA 2022, Eurooppa-neuvosto 2021)	Käyttöoikeuksien ja valtuuksien aktiivinen hallinta, varmuuskopiointi, hajautus ja salaus (ENISA 2022)
Saatavuuteen kohdistuvat uhat (ENISA 2022, Eurooppa-neuvosto 2021)	Tietoliikenteen suodattimet, päivitysten asentaminen, skaalautuva infrastruktuuri (ENISA, 2022)
Disinformaatio (ENISA 2022, Eurooppa-neuvosto 2021)	Datan ja -lähteiden reliabiliteetin ja validiteetin varmistaminen, työntekijöiden kouluttaminen, suodattimet (esim. Internet, sähköposti) (ENISA, 2022; He, 2012)

Tutkielma on toteutettu käyttäen toimivaksi ja luotettavaksi todettua tutkimusmenetelmää. Tutkielma on johdettu laadukkaista ja arvostetuista tieteellisistä julkaisuista, jonka osoittaa muun muassa viittausten määrä valittuihin julkaisuihin. Julkaisujen laatua on myös arvioitu niiden käyttämien lähdemateriaalien kautta. Tieteellisten julkaisujen lisäksi tutkielmassa on käytetty luotettavia valtiollisten ja monikansallisten instituutioiden sekä käytännön työelämään liittyvien yritysten julkaisuja ja raportteja, jotka liittyvät tutkimusaiheeseen. Näihin lähteisiin on pyritty viittaamaan oikeanlaisella tavalla. Näitä keinoja käyttäen tutkielman luotettavuutta on pyritty parantamaan.

Jatkotutkimuksena voisi esimerkiksi syventää tarkastelua yksityiskohtaisempiin operatiivisiin toimintoihin kyberuhkien torjunnassa. Aihe on laaja ja siihen löytyy monia näkökulmia niin erilaisista toimialoista, teknologiosta ja entiteeteistä.

LÄHTEET

Abawajy, J., Huda, S., Sharmeen, S., Hassan, M. M. & Almogren, A. (2018). Identifying cyber threats to mobile-IoT applications in edge computing paradigm. *Future Generation Computer Systems*, *89*, 525–538. https://doi.org/10.1016/j.future.2018.06.053

Abdellah, W., Kim, J.-G., Hassan, M. & Ali, M. (2022). The key challenges towards the effective implementation of digital transformation in the mining industry. *Geosystem Engineering*, *25*(1–2), 44–52. https://doi.org/10.1080/12269328.2022.2120093

Accenture, (2022). "What is digital transformation?" Haettu 18.11.2022 osoitteesta: https://www.accenture.com/us-en/insights/digital-transformation-index

Alghassab, M. (2022). Analyzing the impact of cybersecurity on monitoring and control systems in the energy sector. *Energies*, *15*(1). Scopus. https://doi.org/10.3390/en15010218

Almeida, F., Duarte Santos, J. & Augusto Monteiro, J. (2020). The Challenges and Opportunities in the Digitalization of Companies in a Post-COVID-19 World. *IEEE Engineering Management Review*, *48*(3), 97–103. https://doi.org/10.1109/EMR.2020.3013206

Borangiu, T., Trentesaux, D., Thomas, A., Leitão, P. & Barata, J. (2019). Digital transformation of manufacturing through cloud services and resource virtualization. *Computers in Industry*, *108*, 150–162. https://doi.org/10.1016/j.compind.2019.01.006

Bouwman, H., Nikou, S. & de Reuver, M. (2019). Digitalization, business models, and SMEs: How do business model innovation practices improve performance of digitalizing SMEs? *Telecommunications Policy*, *43*(9), 101828. https://doi.org/10.1016/j.telpol.2019.101828

Cisco. (2018). Annual cybersecurity report. Haettu 21.11.2022 osoitteesta: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

Duc, A., Chirumamilla, A. (2019). "Identifying Security Risks of Digital Transformation - An Engineering Perspective." Digital Transformation for a Sustainable Society in the 21st Century 2019: 677-688. https://doi.org/10.1007/978-3-030-29374-1_55

ENISA. (2022). "ENISA threat landscape, 2022." European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Eurooppa-neuvosto. 2022. "Infographic - Top cyber threats in the EU." Haeuttu 21.11.2022 osoitteesta: https://www.consilium.europa.eu/en/infographics/cyber-threats-eu/

Finanssivalvonta. (2022). "Fivan selvitys peruspankkipalveluista." Raportteja vuosilta 2019-2021. Haettu 1.11.2022 osoitteesta: https://www.finanssivalvonta.fi/kuluttajansuoja/pankkipalvelut/peruspankkipalvelut/fivan-selvitykset-peruspankkipalveluista/

Fitzgerald, M., Kruschwitz, N., Bonnet, D. & Welch, M. (ei pvm.). *Embracing Digital Technology*. 16.

Frank, A., Dalenogare, L. & Ayala, N. (2019). Industry 4.0 technologies: Implementation patterns in manufacturing companies. *International Journal of Production Economics*, *210*, 15–26. https://doi.org/10.1016/j.ijpe.2019.01.004

F-secure. (2022.) "Mikä on palvelunestohyökkäys (DDOS)?" Haettu 19.11.2022 osoitteesta: https://www.f-secure.com/fi/home/articles/what-is-ddos

Gandomi, A. & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, *35*(2), 137–144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Gartner. (2022a) Gartner Glossary: Big data. Haettu 18.11.2022 osoitteesta: https://www.gartner.com/en/information-technology/glossary/big-data

Gartner. (2022b) Gartner Glossary: Internet of Things. Haettu 17.11.2022 osoitteesta: https://www.gartner.com/en/information-technology/glossary/internet-of-things

Gartner. (2022c) Gartner Glossary: Cybersecurity. Haettu 20.11.2022 osoitteesta: https://www.gartner.com/en/information-technology/glossary/cybersecurity

Ghani, N., Hamid, S., Targio Hashem, I. & Ahmed, E. (2019). Social media big data analytics: A survey. *Computers in Human Behavior*, *101*, 417–428. https://doi.org/10.1016/j.chb.2018.08.039

Gong, C. & Ribiere, V. (2021). Developing a unified definition of digital transformation. *Technovation*, *102*, 102217. https://doi.org/10.1016/j.technovation.2020.102217

He, W. (2012). A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology*, *14*(2), 171–180. https://doi.org/10.1108/13287261211232180

Kaloudi, N. & Li, J. (2020). The AI-Based Cyber Threat Landscape: A Survey. *ACM Computing Surveys*, *53*(1), 20:1-20:34. https://doi.org/10.1145/3372823

Kyberturvallisuuskeskus. (2014). "Pilvipalveluiden turvallisuus." Haettu 21.11.2022 osoitteesta: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_tietoturva_organisaatioille.pdf

Kyberturvallisuuskeskus. (2020). "Haavoittuvuudet - miten niistä ilmoitetaan oikein". Haettu 21.11.2022 osoitteesta: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/haavoittuvuudet-miten-niista-ilmoitetaan-oikein

Kyberturvallisuuskeskus. (2022) "Palvelunestohyökkäykset ovat arkipäivää Suomessa". Haettu 21.11.2022 osoitteesta: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/palvelunestohyokkaykset-ovat-arkipaivaa-suomessa

Lezzi, M., Lazoi, M. & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature: A reference framework. *Computers in Industry*, *103*, 97–110. https://doi.org/10.1016/j.compind.2018.09.004

Li, J. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462–1474. https://doi.org/10.1631/FITEE.1800573

Li, L., He, W., Xu, L., Ash, I., Anwar, M. & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Microsoft Azure. (2022). "What is PaaS? Platform as a service". Haettu 20.11.2022 osoitteesta: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-paas/

Microsoft. (2022). "Mikä kyberturvallisuus on?". Haettu 21.11.2022 osoitteesta: https://support.microsoft.com/fi-fi/topic/mit%C3%A4-kyberturvallisuus-on-8b6efd59-41ff-4743-87c8-0850a352a390

Mukhopadhyay, A., Chatterjee, S., Saha, D., Mahanti, A. & Sadhukhan, S. K. (2013). Cyber-risk decision models: To insure IT or not? *Decision Support Systems*, *56*, 11–26. https://doi.org/10.1016/j.dss.2013.04.004

Pappas, I. O., Mikalef, P., Giannakos, M., Krogstie, J. & Lekakos, G. (2018). Big data and business analytics ecosystems: paving the way towards digital transformation and sustainable societies. *Information Systems and E-Business Management*, *16*(3), 479–491. https://doi.org/10.1007/s10257-018-0377-z

Saarikko, T., Westergren, U. H. & Blomquist, T. (2020). Digital transformation: Five recommendations for the digitally conscious firm. *Business Horizons*, *63*(6), 825–839. https://doi.org/10.1016/j.bushor.2020.07.005

Salminen, A. (2011). Mikä kirjallisuuskatsaus? johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan ylioisto

Sestino, A., Prete, M. I., Piper, L. & Guido, G. (2020). Internet of Things and Big Data as enablers for business digitalization strategies. *Technovation*, *98*, 102173. https://doi.org/10.1016/j.technovation.2020.102173

Sivarajah, U., Irani, Z., Gupta, S. & Mahroof, K. (2020). Role of big data and social media analytics for business to business sustainability: A participatory web context. *Industrial Marketing Management*, *86*, 163–179. https://doi.org/10.1016/j.indmarman.2019.04.005

Tao, F., Qi, Q., Liu, A. & Kusiak, A. (2018). Data-driven smart manufacturing. *Journal of Manufacturing Systems*, *48*, 157–169. https://doi.org/10.1016/j.jmsy.2018.01.006

Templier, M., & Paré, G. (2015). A Framework for Guiding and Evaluating Literature Reviews. Communications of the Association for Information Systems, 37, 112–137. https://aisel.aisnet.org/cais/vol37/iss1/6/

Teymourlouei, H. & Harris, V. (2019). Effective Methods to Monitor IT Infrastructure Security for Small Business. *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, 7–13. https://doi.org/10.1109/CSCI49370.2019.00009

Tietovaltuutetuntoimisto. (2021). " Psykoterapiakeskus Vastaamolle seuraamusmaksu tietosuojarikkomuksista". Haettu 21.11.2022 osoitteesta: https://tietosuoja.fi/-/psykoterapiakeskus-vastaamolle-seuraamusmaksu-tietosuojarikkomuksista

TrafiCom. (2020) "Pienyrityksen kyberturva opas". Traficomin julkaisuja 228/2020. Haettu 21.11.2022 osoitteesta: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

Tsiknas, K., Taketzis, D., Demertzis, K. & Skianis, C. (2021). Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. *IoT*, *2*(1), 163–186. https://doi.org/10.3390/iot2010009

Vakakis, N., Nikolis, O., Ioannidis, D., Votis, K. & Tzovaras, D. (2019). Cybersecurity in SMEs: The Smart-Home/Office Use Case. *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 1–7. https://doi.org/10.1109/CAMAD.2019.8858471

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, *28*(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003

Warner, K. S. R. & Wäger, M. (2019). Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal. *Long Range Planning*, *52*(3), 326–349. https://doi.org/10.1016/j.lrp.2018.12.001

Zhang, D. (2018). Big Data Security and Privacy Protection. Advances in computer Science research, volume 77. https://www.atlantis-press.com/article/25904185.pdf

Zissis, D. & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006