Tampereen yliopisto

Jade Karrila

ORGANISAATIOIDEN KYBER-RESILIENSSIN KEHITTÄMINEN

Kandidaatintyö
Johtamisen ja talouden tiedekunta
Tarkastaja: Krista Sorri
Toukokuu 2023

TIIVISTELMÄ

Jade Karrila: Organisaatioiden kyberresilienssin kehittäminen
Kandidaatintyö
Tampereen yliopisto
Tietojohtaminen
Toukokuu 2023

Tämän kandidaatintyön tarkoituksena on selvittää miten organisaatiot voivat kehittää kyberresilienssiään digitalisaation neljännen aallon toimintaympäristöön tuomien muutosten myötä. Kyberresilienssillä tarkoitetaan organisaatioiden kykyä säilyttää suorituskykynsä kyberhäiriötilanteista huolimatta. Työn tarkoituksena oli selvittää mitä kyberturvallisuuden johtamisessa ja hallinnassa organisaatioiden tulisi muuttaa kyberresilienssin kehittämiseksi.

Tutkimus toteutettiin kirjallisuuskatsauksena, jossa hyödynnettiin Finkin määrittelemää kirjallisuuskatsauksen prosessimallia. Tutkimusaineisto haettiin Scopus-, Web of Science-, ScienceDirect- ja Andor-tietokannoista. Tutkimusaineisto koostuu vertaisarvioiduista tutkimusartikkeleista, joista pyrittiin tunnistamaan yhteneviä tekijöitä ja termejä, jotka liitettiin kyberresilienssin kehittymiseen organisaatioissa. Aiheen rajaamiseksi kyberresilienssin tutkimuksessa on hyödynnetty NIST-kyberturvallisuusmallia, jonka avulla voidaan tunnistaa kyberturvallisuuden osa-alueita ja näin löytää merkittäviä kehityskohteita kyberresilienssin rakentamisessa.

Tutkimuksessa tunnistettiin NIST-kyberturvallisuusmallin osa-alueiden ja kyberresilienssin rinnakkaisuuksia. Erityinen yhtymäkohta molemmille oli reagointi- ja toipumisosa-alueet. Pelkkä kyberturvallisuuden kehittäminen ei yksiselitteisesti paranna kyberresilienssiä, sillä se on suurilta osin ennaltaehkäisevää, lyhyen aikavälin ongelmanratkaisua siinä missä kyberresilienssi pyrkii ensisijaisesti tukemaan organisaation liiketoiminnan jatkuvuutta. Tämän turvaaminen digitalisaation neljännen aallon tuomien muutosten myötä on organisaatioille välttämätöntä, sillä neljäs aalto luo suuria haasteita kyberturvallisuudelle muun muassa laskentatehon nousulla, liitettävyyden ja verkottuneisuuden yleistymisellä sekä automatisaatiolla. Kyberresilienssi ei kuitenkaan voi kehittyä ilman perustavanlaatuista kyberturvallisuutta, jonka takia niitä molempia tulee kehittää organisaatioiden liiketoiminnan jatkuvuuden turvaamiseksi.

Organisaatioiden kyberresilienssin kehittämiseksi organisaatioilta vaaditaan strategista kyberturvallisuusjohtamista, sisäistä ja ulkoista seurantaa, järjestelmäarkkitehtuurin ja puolustuksen dynaamisuutta sekä analytiikan hyödyntämistä kyberturvallisuudessa. Kaikki nämä tekijät tukevat reagointi- ja toipumissuunnittelua, joka on avainasemassa kyberresilienssin ja kyberturvallisuuden kehityksessä. Organisaatioilta vaaditaan näkökulman muutosta resurssien allokoinnissa, puolustusteknologian implementoinnissa sekä tietoisuuden kehittämisessä, jotta ne voivat kehittää kyberresilienssiään nykyiset ja tulevat haasteet huomioiden. Organisaatioiden on siirryttävä reaktiivisesta toiminnasta proaktiiviseen, jotta niillä on parhaat mahdolliset kyvykkyydet turvata toimintansa tulevaisuuden kybertoimintaympäristössä, jossa kyberhyökkäyksiltä ei voida puolustautua vain ehkäisevillä toimintamenetelmillä.

Avainsanat: kyberresilienssi, kyberturvallisuus, digitalisaation neljäs aalto.

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

APT	Advanced persistent threat, kehittynyt jatkuva uhka
DMZ	Demilitarized zone, Demilitarisoitu vyöhyke
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
IDS	Tunkeutumisen havainnointijärjestelmä
IoT	Esineiden Internet
IPS	Tunkeutumisen ennaltaehkäisyjärjestelmä
NIST	Yhdysvaltain kauppaministeriön kansallinen instituutti teknologia-astandardien luomiselle
TI	Threat Intelligence. Kyberuhkia koskevan tiedonhallinta. Verrattavissa liiketoimintatiedon hallintaan (business intelligence).
VPN	Virtual private network, Virtuaalinen erillisverkko

1. JOHDANTO

Tieto- ja viestintäteknologiat ovat internetin keksimisen jälkeen kehittyneet eksponentiaalisesti ja kehitystä voidaan kuvata suurina harppauksina, joita voidaan huomattavien maailmanlaajuisten vaikutusten takia kuvata digitalisaation aaltoina (Samoilenko, 2022). Kehitys ole pysähtymässä, sillä Mooren lain mukaan tietotekniikka kokee eksponentiaalista kasvua vuosittain (Brennan et al., 2019). Digitalisaation neljäs aalto tulee haastamaan organisaatiot ja niiden liiketoimintamallit seuraavan kymmenen vuoden sisään kovemmin kuin koko teknologian kehitys viimeiseen 30 vuoteen yhteensä (Henry-Biabaud, 2020). Tällä aallolla tarkoitetaan muun muassa tekoälyn ja laskentatehon räjähdysmäistä kasvua, jolla on odotettavissa laajoja sosioekonomisia vaikutuksia (Winter, 2020). Tämän kehityksen mukana kyberhyökkäysten syklit kasvavat ja teknologian kehitys sekä kyberuhat uhkaavat ohittaa kapasiteetin ottaa käyttöön nykyaikaisia järjestelmiä (Brennan et al., 2019; Coden et al., 2023)

Organisaatioiden kyberturvallisuutta voidaan jo nyt pitää huolestuttavan puutteellisena, sillä niillä on edelleen haasteita integroida kyberturvallisuutta tavallisiin jokapäiväisiin toimintajärjestelmiin (Lee & Trim, 2022). 2010-luvun hyökkäykset ovat osoittaneet kyberrikollisten olevan hyvin resursoituja, sivistyneitä ja järjestäytyneitä. 2010 Stuxnet-mato sabotoi Iranin ydinaseohjelmaa (Cimpanu, 2019) kohteenaan nollapäivänhyökkäyksiä vastaan tehokkaina pidetyt SCADA-valvomojärjestelmät (Ridout, 2016), 2016 hakkerit ryöstivät bangladeshilaisen pankin tienaten 81 miljoonaa dollaria jäämättä kiinni (Cimpanu, 2019), 2017 NotPetya-virus iski yli 80 globaaliin yritykseen ja johti yli 10 miljoonan dollarin vahinkoihin yli toimialojen (Hepfer & Powell, 2020) ja 2021 tapahtui 8,4 miljardin kirjautumistietojen vuoto, joka tunnetaan nimellä RockYou2021 (Carter, 2021; Pellegrino, 2022).

Jatkuvan muutoksen johtaminen on yksi tämän vuosikymmenen suurimmista johtamishaasteista (Henry-Biabaud, 2020) ja vaikuttavan nopea kehitys haastaa organisaatioiden kyberturvallisuuden kautta kaiken sillä saavutettavan infrastruktuurin (Petrenko, 2019) . Kyberhyökkäykset nousivat 400 % vuonna 2020 verrattuna aikaisempiin vuosiin (Abraham & Sims, 2021), jonka lisäksi valtiollisten toimijoiden uhka kybertoimintaympäristössä on lisääntynyt (Abraham & sims, 2021). Tällaisessa ympäristössä suorituskyvyn ylläpitämiseksi, ympäristöön sopeutumiseksi ja tapahtumien ennakoimiseksi, organisaatioilta vaaditaan kyberresilienssiä (Petrenko, 2019).

1.1 Tutkimuksen tausta

Organisaatioiden resilienssin tutkimus lisääntyi huomattavasti Covid-19-pandemian seurauksena, sillä se haastoi monet organisaatiot koostaan huolimatta sopeutumaan ennalta arvaamattomiin (Abraham & Sims, 2021) tapahtumiin ja nopeisiin ympäristön muutoksiin. Tämä lisäsi tutkimusta myös kyberresilienssin tutkimuksesta.

Pandemia osoitti resilienssin välttämättömyyden organisaatioille kriiseissä selviytymiseen ja niistä toipumiseen, sillä pandemian seurauksena erityisesti pienet ja keskikokoiset organisaatiot ajautuivat konkurssiin (Abraham & Sims, 2021), joissa kyberhyökkäyksillä oli suuri rooli niiden maksaessa keskimäärin satoja tuhansia dollareita (Abraham & Sims, 2021)

Jotta organisaatioilla on tarpeeksi kyvykkyyksiä pysyä nykyisen muutoksen perässä, vaaditaan kyberturvallisuudelta enemmän kuin pelkkää riskienhallintaa (Ferdinand, 2015), jonka kyberresilienssi tarjoaa (Juan et al., 2020). Aikaisemmin organisaatioiden navigointia kyberympäristössä on ymmärretty kyberturvallisuuden näkökulmasta niin, että tärkeintä on puolustautua kaikilta mahdollisilta uhilta (Ferdinand, 2015). Tämä on kuitenkin epärealistista, sillä kyberhyökkäykset kehittyvät koko ajan vain hienostuneimmikseni (Ferdinand, 2015) ja arvioilta vain noin 45 % kyberuhista on organisaatioiden ennakoitavissa (Petrenko, 2019). Modernit järjestelmät ovat niin monimutkaisia, että haavoittuvuuksien löytyminen niistä on varmaa (Ridout, 2016). Tällöin suorituskyvyn säilyttämiseksi ja liiketoiminnan jatkuvuuden takaamiseksi tarvitaan kyberresilienssiä (Ferdinand, 2015; Tran et al., 2016). Haasteena on kuitenkin muun muassa organisaatioiden omat lähestymistavat kyberturvallisuuteen (Coden et al., 2023), jonka takia organisaatioilta vaaditaan suuria organisatorisia muutoksia.

Tässä tutkimuksessa kyberresilienssin tutkimiseen käytetään NIST-kyberturvallisuusmallia, joka kuvaa organisaation tärkeimpiä kyberturvallisuuden osa-alueita ja jota organisaatiot voivat käyttää viitekehyksenä parantaessaan kyberturvallisuuttaan (NIST, 2016). Viitekehyksen avulla pyritään kartoittamaan mitkä osa-alueet ovat kyberresilienssin kehittymiselle merkittävimpiä. Tutkimuksen tavoitteena on löytää tuloksia, joiden perusteella voidaan tehdä päätelmiä siitä, minkälaisia muutoksia organisaatioiden täytyy tehdä kyberturvallisuuden johtamiseen ja kehittämiseen saavuttaakseen kyberresilienssin digitalisaation neljännen aallon tuomien muutosten myötä.

1.2 Tutkimusongelma ja -rajaus

Tässä tutkimuksessa aiheen rajaamiseksi kyberresilienssin kehittämistä ja rakentumista käsitellään organisaatioiden johdon luomien ja mahdollistamien toimintamallien nä-

kökulmasta. Tämä tarkoittaa, että kyberresilienssin haasteet nähdään johtamisen hallinnollisena ja strategisena ongelmana, joka on kyberturvallisuuden hallinnassa yleistyvä näkökulma (Hepfer & Powell, 2020). Aiheen ulkopuolelle on rajattu henkilöstön tai yksilöiden henkilökohtaiset toimintatavat, jotka eivät edusta koko organisaation linjaa tai kuvaa organisaation kehittämää kyberturvallisuuspolitiikkaa. Kyberresilienssin käsittelemissä käytetään aiheen rajaamiseksi NIST-kyberturvallisuusmallia viitekehyksenä.

Tutkimusongelmana on, miten organisaatiot voviat kehittää kyberresilienssiään digitalisaatio neljännen aallon tuomat muutokset toimintaympäristöön huomioiden, sillä se tarkoittaa uusia ennalta odottamattomia mittakaavaltaan entistä suurempia ja vaikutuksiltaan tuhoisampia nollapäivän massahyökkäyksiä (Tran et al., 2016). Kyberresilienssin kehitykseen vaikuttavat tekijät ovat valikoituneet esiintymistiheyden perusteella vertaisarvioidussa tutkimusaineistossa ja niiden tarkoitus on luoda kattava kokonaiskuva organisaatioiden kyberresilienssin kehitysmahdollisuuksista. Viitekehyksen tarkoituksena on ettei tutkimus kuitenkaan keskity liikaa yhteen puolustus- tai havainnointiteknologiaan vaan tarkoituksena on luoda laajempaa kehityssuuntaa esittelevää kokonaiskuvaa. Kyberturvallisuuteen yhdistetään tämän takia myös organisaation resilienssin teoriaa kuten organisaation oppimisen ja systeemiajattelun perusteita.

Kirjallisuustutkimuksen päätutkimuskysymys on:

- Miten organisaatiot voivat kehittää kyberresilienssiään digitalisaation neljännen aallon tuomien muutosten myötä?

Tukevia alatutkimuskysymyksiä ovat:

- Minkälaisia muutoksia organisaation kyberturvallisuuden kehittämiseen organisaatiolta vaaditaan kyberresilienssin kehittymiseksi?
- Mitkä NIST-kyberturvallisuusmallin osa-alueet ovat toisia merkittävämpiä organisaatioiden kyberresilienssin kehittymiselle?

1.3 Käsitteet ja teoria

Kyberturvallisuuteen liittyy paljon käsitteisiin ja teknologiaan liittyvää teoriaa. Alla on esitetty niistä tyypillisimmät, joita kirjallisuuskatsauksessa käytetään runsaasti. Muut termit on esitetty tekstissä. Englanninkielisen lähdemateriaalin takia niiden alkuperäiset englanninkieliset merkitykset on esitetty yksikäsitteisyyden varmistamiseksi.

Kybertoimintaympäristö (cyber environment, cyberspace) on toimintaympäristö, joka muodostuu yhdestä tai useammasta tietojärjestelmästä, ja josta organisaation toimin-

not ovat usein riippuvaisia. Tavoitteena olisi tavoitetila, jossa kybertoimintaympäristön toimintaan voidaan luottaa ja sen toiminta voidaan turvata. (Turvallisuuskomitea, 2018)

Kybeuhka ja kyberhaavoittuvuus (Cyber threat, cyber vulnerability) kyberuhka on mahdollisesti toteutuva haitallinen tapahtuma tai kehityskulku, joka voi vaarantaa siitä riippuvaisen toiminnon. Haavoittuvuus on heikkous, joka mahdollistaa vahingon toteutumisen ja järjestelmän vaarantumisen. (Turvallisuuskomitea, 2018)

Kyberhäiriötilanne ja kyberhyökkäys (Cyber incident, Cyber attack) Häiriötilanne on toteutunut uhka, joka haittaa järjestelmän tai organisaation toimintaa tai toimintojen tapahtuma, jonka seurauksen tietojen tai palvelun tila on muuttunut ja joka saattaa vaikuttaa kyberturvallisuuteen. Hyökkäys on toimintaa, jolla pyritään esimerkiksi järjestelmään oikeudettomaan käyttöön, joka vaarantaa kyberturvallisuuden. (Turvallisuuskomitea, 2018)

Nollapäivähyökkäys ja -haavoittuvuus (zero-day attack, zero-day vulnerability) Nollapäivän haavoittuvuuksia ei voida määrällisesti mitata, mutta ne on otettava huomioon mahdollisina haavoittuvuuksina, jotka voidaan löytää ja joita voidaan hyväksikäyttää (Campbell & Robert, 2020).

2. TUTKIMUSMENETELMÄ JA -AINEISTO

Tutkimus suoritetaan kirjallisuuskatsauksena. Lähdeaineisto koostuu vertaisarvioiduista artikkeleista ja kyberturvallisuuden alan ammattilaisten ja professorien julkaisemista teoksista. Aineiston tietokantoina on muun muassa käytetty Scopus-, ScienceDirect- ja Web of Science-tietokantoja. Aineistojen löytämiseksi on käytetty myös Tampereen yliopiston kirjaston hakupalvelu Andoria sekä muutamia hakuja on tehty myös hyödyntämällä Google Scholaria. Hakutermit- ja rajaukset tietokantoihin on valittu aikaisemmassa luvussa esitetyn tutkimuskysymyksen ja sen alakysymysten avulla.

2.1 Tutkimusmenetelmä

Kirjallisuuskatsauksen tutkimusmenetelmänä käytetään Finkin (2014, s.3–5) määrittelemää kirjallisuuskatsauksen prosessimallia. Malli koostuu seuraavista seitsemästä vaiheesta.

1. Valitaan tutkimuksen aihe ja määritellään sen ympärille tutkimusongelmat ja alatutkimuskysymykset
2. Valitaan tietokannat
3. Valitaan hakutermit
4. Lisätään käytännön rajoittavia kriteerejä
5. Lisätään metodologisia rajoittavia kriteerejä
6. Tutustutaan aineistoon tarkemmin ja toteutetaan kirjallisuuskatsaus
7. Luodaan aineistosta synteesi

Ensin määritellään tutkimuksen aihe ja muodostetaan sen ympärille tutkimuskysymys, jonka jälkeen valitaan tietokannat, joista etsitään vertaisarvioitua aineistoa. Tämän jälkeen valitaan hakutermit. Hakutermeinä on käytetty kyberresilienssiin, kyberturvallisuuteen ja kyberstrategioihin liittyviä hakutermejä, kuten ”cyber security strategies”, ”cyber resilience” ja ”cyber security polic*”. Termejä on yhdistelty, sillä pelkällä ”cyber security” haulla tuloksia tulee liikaa ja niistä on haastava löytää relevanttia tietoa. Hakutulosten määrää on esitelty taulukossa 1, jolla samalla havainnollistetaan minkälaisilla hakutuloksilla aineistoa löydettiin.

Taulukko 1 – Hakutermien esiintyvyys eri tietokannoissa

Tietokanta	cyber security	cyber security industry 4.0	cyber resilience	cyber resilience industry 4.0	cyber resilience industry 4.0 NIST	cyber resilience industry 4.0 NIST AND (opportun* OR challenge*)	cyber security digitalization fourth wave	Valitut
Scopus	44 165 tulosta	884 tulosta	2 729 tulosta	107 tulosta	2 tulosta	Ei tuloksia	Ei tuloksia	9
ScienceDirect	30 480 tulosta	4 138 tulosta	5 920 tulosta	1 206 tulosta	141 tulosta	99 tulosta	965 tulosta	5
Web Of Science	36 020 tulosta	632 tulosta	2 650 tulosta	83 tulosta	3 tulosta	Ei tuloksia	Ei tuloksia	2
Andor	36 612 tulosta (vertaisarvioidut)	745 tulosta (vertaisarvioidut)	2 260 tulosta (vertaisarvioidut)	81 tulosta (vertaisarvioidut)	2 tulosta (vertaisarvioidut)	Ei tuloksia	Ei tuloksia	8

Tämän lisäksi hakuihin on liitetty tarkentavia termejä kuten etsitty tiettyihin kyberturvallisuusmalleihin, strategioihin ja havaitsemisjärjestelmiin ja -teknologioihin liittyviä termejä aikaisempien aineistojen perusteella, joita ovat olleet esimerkiksi ”zero trust architecture”, ”Industry 4.0” ja ”zero day”. Huomionarvioista on, että kyberturvallisuudessa digitalisaation neljäs aalto ei ole vakiintunut käsite vaan aallon tuomista teknologioista puhutaan käsitteellä teollisuuden 4.0-teknologiat. Aineistoa valittiin tietokannoista etsimällä vertaisarvioitua, uusimpia ja relevanteimpia artikkeleita. Relevanttiuden kriteerit tietokannoissa perustuvat hakutermin esiintyvyyteen artikkelissa, julkaisuajankohtana, viittausten määrään sekä julkaisevan tahon arvostukseen alalla (Elsevier, 2023).

Hakua rajataan niin käytännön kuin metodologisilla kriteereillä. Ajankohtaisimman tiedon saamiseksi hakua on tehty 2015 vuodesta eteenpäin ja etsitty englannin kielellä julkaistua aineistoa. Nämä valinnat on tehty sen takia, jotta aineiston perusteella tehdyt päätelmät olisivat mahdollisimman ajankohtaisia. Lisäksi aineiston tiivistelmiin tutustumalla voidaan valikoida tarkemmin kirjallisuuskatsaukselle relevanteimmat lähteet, jotka eivät esimerkiksi keskity tietyn toimialan kyberturvallisuuden erityispiirteisiin. Tämän jälkeen aineistoon tutustutaan tarkemmin ja lajitellaan tarkemmin tulosten ja johtopäätösten kokoamiseksi. Lopuksi aineistoista luodaan synteesi. Vertaisarvioitua aineistoa on kerätty yhteensä 24 kappaletta.

2.2 Tutkimusaineisto

Tutkimusaineisto on etsitty ja kerätty edellisessä luvussa esitetyllä tavalla. Aineistossa on keskitytty artikkeleihin ja tutkimuksiin, joiden tulosten perusteella voidaan tehdä objektiivisia kuvauksia siitä, mitkä kyberturvallisuuden osa-alueista ovat kyberresilienssin rakentamiselle ja kehittämiselle kriittisempiä sekä minkälaisilla konkreettisilla toimintamalleilla voidaan kyberresilienssiä kehittä ja minkälaisia vaikutuksia digitalisaation neljännen aallolla teollisuuden 4.0 -teknologioiden kautta on kyberturvallisuudelle. Lähteiden luotettavuuden arvioinnissa on otettu huomioon muun muassa kuinka paljon läh-

teeseen on viitattu muissa aineistoissa. Teoreettisen aineiston avulla on pyritty luomaan kokonaiskuvaa siitä, mitä kyberresilienssi ja kyberturvallisuus ovat. Tutkimusaineiston perusteella on pyritty kartoittamaan kriittisempiä kehityskohteita modernien organisaatioiden kyberturvallisuudessa. Aineistoista on pyritty löytämään yhteneväisyyksiä taulukon 2 tulosten saamiseksi. Tarkoituksena on ollut kartoittaa kyberresilienssin kehitykselle kyberturvallisuuden kriittisemmät kehityskohteet, jotka ovat valittu esiintyvyyden perusteella aineistossa. Taulukossa 2 on esitetty kirjallisuustutkimuksen tukena tehty taulukko, jossa on pidetty kirjaa termien esiintyvyydestä ja tämän perusteella on valittu luvun 5 käsittelemät kyberresilienssin kehitykselle merkittävät tekijät. Aineiston englanninkielisyyden takia termit on esitelty taulukossa englanniksi, jotta käännösvirheiltä vältytään.

Taulukko 2 – Termien esiintyvyys vertaisarvioidussa aineistossa

Englannin kielinen termi	Strategic Management	System Architecture	System Defense Strategies	Risk Management	Resource Allocation	Analytics	Internal and External Monitoring	Respond and Recovery Capabilities	Testing
Esiintyvyys lähteissä	18	14	15	6	10	9	17	22	17

Taulukossa on huomioitu termien esiintyvyys eri 24 vertaisarvioidussa lähdemateriaalissa. Liitteessä 1 on esitetty vertaisarvioitu lähdemateriaali kokonaisuudessaan sekä termien esiintyvyys niissä. Taulukosta voidaan havaita, että reagointi- ja toipumiskyvykkyydet (respond and recovery capabilities) oli aineistossa eniten esiintynyt termi. Tällä tarkoitetaan muun muassa organisaatioiden reagointi- ja toipumissuunnittelua sekä henkilöstön ja laitteiston mahdollistamia kyvykkyyksiä vastata kyberturvallisuushyökkäyksiin ja -loukkauksiin. Aineistossa myös kyberresilienssin kehittyminen on rinnastettu ylimmän johdon tekemään strategiseen johtamiseen (strategic management) sekä resurssien allokointiin (resource allocation), jolla tarkoitetaan suurilta osin suhtautumisen muutosta kyberturvallisuusbudjetointiin ja -investointeihin. Tutkimuksen edetessä havaittiin, että aineistossa ei esiintynyt tiettyä kyberturvallisuusteknologiaa tai -järjestelmää, joka mahdollistaisi resilientin puolustautumisen. Tämän sijasta aineisto korosti arkkitehtuurisia päätöksiä ja dynaamisia puolustusstrategioita, jotka on sovitettu organisaation liiketoiminnallisiin tavoitteisiin ja jotka pyrkivät mahdollistamaan liiketoiminnan jatkuvuuden turvaamisen. Aineisto myös korosti sisäistä ja ulkoista seurantaa (internal and external monitoring) yhdessä testaamsien (testing) kanssa, joka käsitteenä oli pelkkää järjestelmien ja tietoverkkojen penetraatiotestausta laajempi käsite, sillä sen tavoitteena oli nimenomaan kasvattaa organisaation tietoisuutta kybertoimintaympäristön uhista ja toimijoista sekä omista kyvykkyyksistä ja heikkouksistaan. Riskien-

hallintaan aineisto keskittyi yllättävän vähän vaan seurannalla ja analytiikalla oli tätä suurempi rooli.

3. KYBERRESILIENSSI

Kyberresilienssiä voidaan pitää kyberturvallisuutta laajempana käsitteenä. Siinä missä kyberturvallisuudessa pääasiassa keskitytään vaaratilanteiden todennäköisyyden arviointiin ja mahdollisten tietoturva- ja kyberuhkien torjuntaan (Petrenko, 2019; Coden et al.,2023), kyberresilienssin tavoitteena on säilyttää tavoiteltu organisaation käyttäytyminen ja kyberjärjestelmien suorituskyky kriisien ja häiriötilanteiden keskellä (Petrenko, 2019). Kyberresilienssin kehittäminen vaatii perinteistä suojaa ja ehkäiseviä toimintatapoja enemmän, sillä se vaatii organisaatiolla muun muassa ketterämpää lähestymistä kyberturvallisuuteen ja sen johtamiseen (Hausken, 2020).

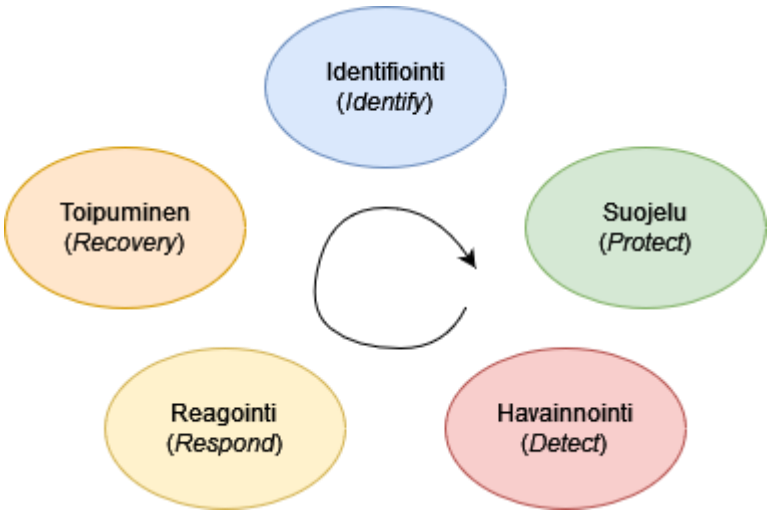
Kyberresilienssi merkitsee organisaation kykyä valmistautua ja suunnitella toimintaansa ympäristön muutoksia varten, absorboida niistä relevanttia informaatioita ja toipua muutoksien vaikutuksista suorituskykyyn sekä sopeutua paremmin toimintaympäristöönsä (Hausken, 2020). Tämän resilienssin kehittäminen tulisi olla organisaatioiden tavoitteena, sillä se edistää organisaation toimintaa jatkuvasti odottamilla tavoilla kehittyvässä kyberympäristössä (Ferdinand, 2015; Ducheck, 2020). Kyberresilienssiä tarkastellessa voidaan huomata keskittymisen olevan kyberturvallisuutta enemmän toipumis- ja reagointisuunnittelussa, sopeutumisessa ja jatkuvan kehityksen mahdollistamisessa (Coden et al., 2023).

3.1 NIST-kyberturvallisuusmalli viitekehyksenä

Kyberresilienssi on hyvin laaja kokonaisuus ja usein kehittämisen haasteena organisaatioissa on tiedon sirpaleisuus ja yhteisen kehityssuunnan puute (Ferdinand, 2015), Tämän kokonaisuuden tarkempaa tarkastelua varten, se jaetaan helpommin käsiteltäviin osa-alueisiin. Kyberresilienssi perustuu organisaation kyvylle jatkuvasti kehittää omaa kyberturvallisuuttaan, jonka takia sen tulee hallita ja kehittää kyberturvallisuuden ydinosa-alueita (Ferdinand, 2015; Campbell & Robert, 2020). Näiden osa-alueiden tarkastelua varten voidaan hyödyntää moria eri viitekehyksiä ja mallinnuksia. Tässä viitekehyksenä on hyödynnetty National Institute of Standards and Technologyn (NIST) luomaa kyberturvallisuusmallia, sillä se on hyvin laajalti hyödynnetty viitekehys ja on toiminut monien muiden kypsyysmallien ja standardien pohjana (Ferdinand, 2015, Tran et al., 2016; Coden et al., 2023).

NIST on Yhdysvaltain kauppaministeriötä osana oleva teknologiainstituutti ja -laboratorio. Se tarjoaa teknologian alalle lukuisia eri mittareita ja standardeja, joihin lukemattomat tuotteet atomikelloista nanomateriaaleihin ja tietokonesiruihin jollain tavalla perustuvat. Se on myös luonut laajasti käytetyn kyberturvallisuus mallin *NIST Cybersecurity Framework*, joka on monien organisaatioiden hyödyntämä lähestymistapa liiketoiminnan kyberturvallisuuden riskien ja kehityskohteiden havainnointiin. (NIST, 2009; NIST, 2016)

Viitekehyksen tarkoituksena on parantaa organisaation tietoisuutta ja oppimista mahdollistaen näin jatkuvan kehityksen (NIST, 2016), jotka ovat olennaisia tekijöitä organisaation resilienssin (Ducheck, 2020) ja näin myös kyberresilienssin rakentumisessa. Mallin mukaan jatkuvan kehityksen mahdollistamat identifiointi (identify), suojelu (protect), havainnointi (detect), reagointi (respond) ja toipuminen (recover).



Kuva 1 – NIST-kyberturvallisuusmalli (mukaillen lähteestä NIST, 2016)

Identifiointi tarkoitta organisaation ymmärrystä niin kyberriskeistä ja -järjestelmistä kuin omista resursseista, datasta ja kyvykkyyksistä (NIST, 2016). Osa-alue keskittyy esimerkiksi kriittisen infrastruktuurin tunnistamiseen ja ymmärtämiseen, informaatiovirtojen dokumentointiin sekä riskien ja haavoittuvuuksien hallintaan (NIST, 2016). Tässä osa-alueessa kyberresilienssin näkökulmassa korostuu ylimmän johdon merkitys sen rakentumisessa, sillä nämä päättävät toimielimet vaikuttavat suuresti sen kehitykseen vaikka eivät ole suoraan vastuussa organisaation kyberturvallisuudesta (Hepfer & Powell, 2020). Tämä johtuu siitä, että resurssien allokoinnin avulla ylin johto määrittelee minkälaisia resursseja ja kyvykkyyksiä organisaation kyberturvallisuudesta vastuussa olevilla tahoilla sekä muulla henkilöstöllä on käytössään.

Suojelu keskittyy sopivien turvaavien toimenpiteiden implementointiin, jotka mahdollistavat palveluiden tuoton ja turvaavat liiketoiminnot. Tähän osa-alueeseen kuuluvat esimerkiksi henkilöstön, laitteiston ja tiedon hallinta. Yleisiä turvallisuustoimenpiteitä voivat olla esimerkiksi varmuuskopiointi, henkilöstön kouluttautuminen ja turvallisuustekniikan, kuten palomuurien ja konfigurointijärjestelmien implementointi. (NIST, 2016)

Havainnointi pyrkii kehittämään organisaatioon toimintamalleja, jotka tunnistavat epätavallisuuksia ja mahdollisia kyberloukkauksia tai hyökkäyksen yrityksiä (NIST, 2016). Tähän osa-alueeseen kuuluvat esimerkiksi erilaiset IDPS (intrusion detection and prevention systems) -järjestelmät, väärinkäytön ja poikkeamien hallinta sekä tietoliikenteen seuranta ja hallinta.

Reagointi tarkoittaa vastatoimia, joita organisaatio ottaa käyttöönsä havaitessaan poikkeamia tai mahdollista väärinkäyttöä (NIST, 2016). Reagointi tapahtuu pääsoin reagointisuunnitelmien pohjalta ja siihen kuuluu vastatiedustelutekniikoiden ja uhkien eristämistekniikoiden (Tran et al., 2016) lisäksi muun muassa ulkoisten ja sisäisten sidosryhmien kanssa koordinoiminen (Ferdinand, 2015).

Viimeinen ja ehkä haastavin osa-alue on toipuminen. Se sisältää käytännöt ja toimintamallit, joilla organisaatio pyrkii säilyttämään liiketoimintansa kriisien keskellä ja turvaamaan kriittisen infrastruktuurin toiminnan (NIST, 2016). Erityisesti tämän vaiheen kehittäminen kehittää resilienssiä, sillä sen avulla organisaatio pyrkii turvaamaan kyberturvallisuuttaan myös ennalta arvaamattomia hyökkäyksiä ja tapahtumia vastaan, joita toiset osa-alueet eivät pysty kartoittamaan (Coden et al., 2023). Tähän osa-alueeseen kuuluvat esimerkiksi kommunikointi sisäisten ja ulkoisten sidosryhmien kanssa, toipumissuunnittelun päivittäminen ja aktiivinen päivittäminen ja testaus (Ferdinand, 2015; NIST, 2016).

Tätä viitekehitystä hyödynnetään kartoittamaan, minkälaisia muutoksia organisaation täytyy kyberturvallisuuden johtamiseen ja hallintaan tehdä erityisesti digitalisaation neljännen aallon näkökulmasta, sillä se mahdollistaa hyökkäyspolut ja -tekniikat, joita perinteinen kyberturvallisuus ei pysty ennakoimaan (Mazzara et al., 2019; Vaidya et al., 2020). NIST-malli antaa yleisen kuvan organisaation kyberturvallisuudesta ja antaa siihen yksinkertaisen lähestymistavan. Se ei kuitenkaan tarjoa suoraan toimintamalleja, jotka kehittäisivät nimenomaan kyberresilienssiä vaan tähän keskittyy ainoastaan toipumissuunnittelun huomioiva osa-alue (Coden et al., 2023).

Laajasta hyödynnettävyydestään huolimatta, malli ei ole täysin ongelmaton kyberresilienssin näkökulmasta, sillä siitä vain 20 % keskittyy organisaatioon kykyyn vastata ja toipua loukkauksista, joka kyberresilienssin kehittymisen kannalta on olennaisin osa

(Ferdinand, 2015; Coden et al., 2023). Lisäksi tämä on johtanut siihen, että kyberturvallisuuteen käytetyistä resursseista 72 % menee identifiointiin, suojaamiseen ja havainnointiin, ja 17 % vastatoimiin, toipumiseen ja liiketoiminnan jatkuvuuden turvaamiseen (Coden et al., 2023). Tämä epätasapainoisuus tekee organisaatioista haavoittuvaisia eivätkä ne ole valmiita esimerkiksi kansainvälisiin säännöksiin, jotka ohjeistavat liiketoiminnan jatkuvuuden mahdollistamiseen, satunnaisuuksiin valmistautumiseen ja toipumissuunnitteluun kyberloukkausten varalta (Coden et al., 2023).

3.2 Kyberresilienssin rakentuminen organisaatioissa

Organisaatioiden kokonaisvaltaisen resilienssin voidaan katsoa koostuvan kolmesta kyvykkyydestä, jotka ovat ennakointi, selviytyminen ja sopeutuminen. Näihin kuuluvat organisaation kyvykkyydet tunnistaa tärkeitä tapahtumia ja ennakoida riskien varalta valmistautumalla niihin, ongelmien hyväksyminen ja ratkaisuihin kehittäminen niihin sekä muutosten hyödyntäminen jopa kilpailuedun saavuttamiseksi. Organisaation resilienssin saavuttamisessa organisaation oppimisella, systeemiajattelulla ja esimerkiksi skenaarioiden ja simulaatioiden hyödyntämisellä on suuri merkitys. (Ducheck, 2020)

Taulukko 3 – Kyberresilienssin määritelmät suhteessa Duchekin (2020) organisaatioiden resilienssiin

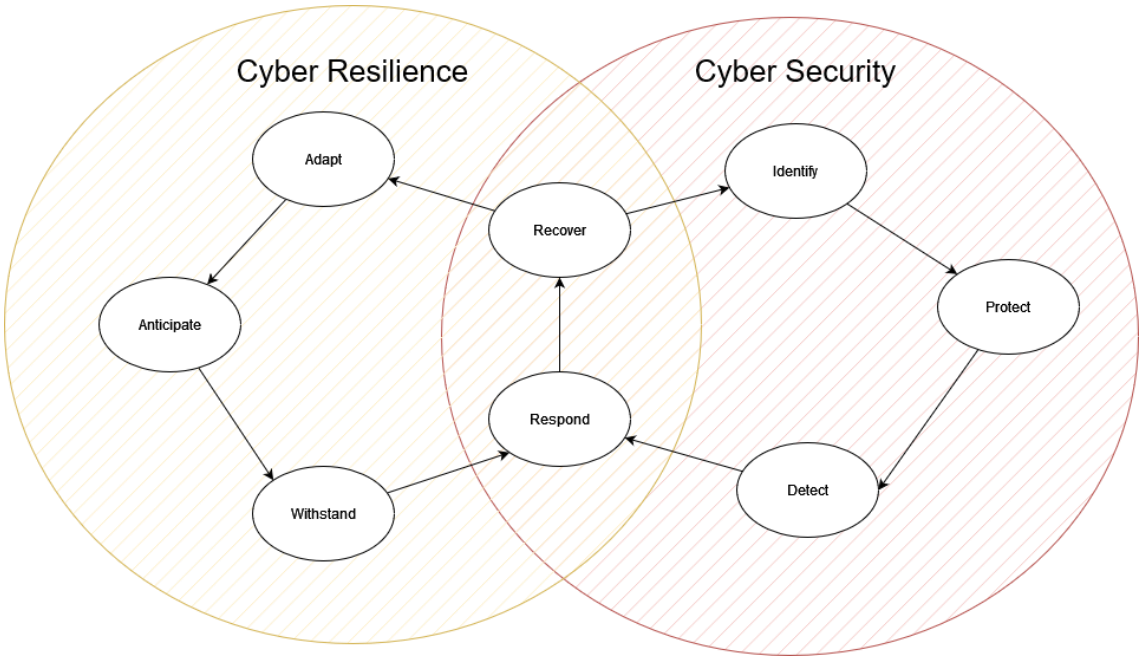
(Ducheck, 2020)	**Ennakointi**	**Selviytyminen**	**Sopeutuminen**	
(Brennan et al., 2019)	Ennakointi (Anticipate)	Sietäminen (Withstand)	Toipuminen (Recover)	Kehittyminen (Evolve)
(Hausken, 2020)	Valmistelu (Prepare)	Absorptio (Absorb)	Toipuminen (Recover)	Sopeutuminen (Adapt)
(Coden et al., 2023)	Ennakointi (Anticipation)	Absorptio (Absorption)	Reagointi (Responsiveness)	Muotoutuminen (Shaping)
(Hepfer & Powell, 2020)	Liiketoiminnan suojaaminen (Protecting the business)	Tietoisuuden laajentaminen (Broading awareness)	Seurauksien hallinta (Managing consequences)	Reagointi ja toipuminen (Responding and recovering)
(Abraham & Sims, 2021)	Nopea havainnointi (Rapid detection)	Voimakas reagointi (Effective response)	Tehokas palautuminen (Efficient Recovery)	

Kirjallisuudessa kyberresilienssistä puhuttaessa systeemiajattelun ja organisaation oppimisen periaatteita ei huomioida selkeästä yhteydestä huolimatta. Kyberresilienssillä ei ole vakiintunutta viitekehystä (Ferdinand, 2015; Ridout, 2016), mutta kyberresilienssin vaiheiden kuvauksissa eri kirjallisuuden lähteissä on havaittavissa paljon samankaltaisuuksia niin toistensa kuin Ducheckin (2020) resilienssin kyvyyksien kanssa. Näiden vertailemiseksi aineiston tulokset on esitetty taulukossa yhdessä Ducheckin resilienssin kyvykkyyksien kanssa. Brennan et al. (2019) esittelevät vaiheet ennakointina (anticiapte), sietämisenä (withstand), toipumisena (recover) ja kehittymisenä (evolve). Hausken (2020) mainitsee vaiheisiin kuuluvan valmistelun (prepare), absorboimisen

(absorb), toipumisen (recover) ja sopeutumisen (adapt). Coden et al. (2023) kyberresilienssin osa-alueiksi mainitaan ennakointi (anticipation), absorptio (absorption), reagointi (responsiveness) ja muotoutuminen (shaping). Näillä kuvauksilla on havaittavissa paljon yhteneväisyyksiä NIST-kyberturvallisuusmallin osa-alueiden kanssa. Näistä hieman poiketen Hepfer & Powell (2020) jakaa kyberresilienssin neljään osaan, jotka ovat liiketoiminnan suojaaminen (protecting the business), tietoisuuden laajentaminen (broadening awareness), seurauksien hallinta (managing consequences) sekä reagointi ja toipuminen (responding and recovering). Abraham & Sims (2021) kuvaavat tätä vielä suppeammin jakamalla kyberresilienssin nopeaan havainnointiin (rapid detection), voimakkaaseen reagointiin (effective response) ja tehokkaaseen palautumiseen (efficient recovery).

Kyberresilienssin kehittyminen vaatii organisaation toimivaa perustavanlaatuista kyberturvallisuutta (Petrenko, 2019). Tämä on myös havaittavissa kyberresilienssin rakentavien tekijöiden kuvauksissa, joissa otetaan riskienhallinta, turvaavat toimenpiteet ja havainnointi huomioon, jotka sen sijaan eivät organisaation kokonaisvaltaisen resilienssin kyvykkyyksiin kuulu. Kyberresilienssin ja kyberturvallisuuden rinnakkaisuus on esitetty kuvassa 2.

.



Kuva 2 – Kyberturvallisuuden ja -resilienssin rinnakkaisuus

NIST-mallin alueet vaikuttavat organisaatioiden kyberturvallisuuden kehitykseen pienellä aikavälillä (Ferdinand, 2015), sillä sen avulla voidaan esimerkiksi tunnistaa puutteita

varmuuskopiointikäytännöissä tai pääsynvalvonnan haavoittuvuuksia. Se ei kuitenkaan resilienssin periaatteiden tavoin pyri ymmärtämään organisaation systeemisyyttä ja näin vaikuttamaan organisaation oppimisen avulla systeemiin niin, että suorituskyky ja sen ylläpito paranee pysyvästi (Ducheck, 2020). Kyberturvallisuusmallit ja kyberresilienssin menneet viitekehykset saattavat auttaa vain pienessä ongelman ratkaisussa (Ridout, 2016). Lyhyen ja pitkän aikavälin kehityksen ja oppimisen kautta kyberturvallisuuden ja kyberresilienssillä voidaan havaita olevan rinnakkaisuuksia systeemiajatteluun double-loop oppimiseen, joka mahdollistaa resilienssin kehittymisen ja pitkän aikavälin muutoksen (Ducheck, 2020).

Organisaation oppimisen ja systeemiajattelun yhdistäminen tiukemmin kyberresilienssin rakentamiseen voisi edistää kehitystä, sillä systeemiajattelu muun muassa pyrkii ymmärtämään organisaation toimintaa, osien keskinäisiä riippuvuussuhteita ja vaikutuksia kokonaisuuteen syvemmin (Ducheck, 2020). Näiden ymmärtämisessä ja keskinäisten riippuvuussuhteiden hallinnassa organisaatioilla on erityisesti haasteita digitalisaation neljännen aallon tuomien muutosten myötä (Vaidya et al., 2020). Organisaatiot ovat systeemeinä samanaikaisesti sosiaalisia ja teknisiä kokonaisuuksia, jotka ovat läheisesti liitoksissa toisiinsa (Ducheck, 2020) ja kyberturvallisuudessa tämä korostuu hyökkäyspolkujen ollessa yleensä yhdistelmä sosiaalisia ja teknisiä elementtejä (Tran et al., 2016). Tunnukset kohdejärjestelmään voidaan hankkia käyttäjän manipuloinnilla, sosiaalisella hakkeroinnilla tai harhaanjohtamisella, kun taas varsinainen hyökkäys voi olla haittakoodin injektoiminen järjestelmään. Järjestelmien turvallisuus on perinteisesti ollut organisaatioiden IT-osastojen velvollisuus, joka on nähty sisäisenä palveluna, joka pitää järjestelmät toiminnassa (Hepfer & Powell, 2020). Tämä lähestymistapa on kuitenkin tehnyt organisaatioista haavoittuvaisia ja jonka korjaamiseen systeemiajattelun periaatteita olisi mahdollista hyödyntää, jotteivat organisaatiot väärinymmärtäisi kyberturvallisuuden strategista roolia kilpailuedun tuojana (Hepfer & Powell, 2020) ja järjestelmien elinehtona (Petrenko, 2019) kyberloukkausten ja digitalisaation kehityksen huomioiden (Hepfer & Powell, 2020). Kyberresilienssin rakentumiseen vaaditaan yhteistyötä sisäisten ja ulkoisten sidosryhmien kanssa (Coden et al., 2023) ja systeemiajattelun periaatteet auttavat ymmärtämään näiden merkitystä ja vaikutusta kyberresilienssin kehitykselle, sillä näin voidaan ymmärtää kyberturvallisuushäiriötilanteiden vaikutukset muun muassa organisaation toimitusketjuihin ja asiakkaisiin.

3.3 Nykytila moderneissa organisaatioissa

Digitalisaation neljäs aalto herättää mielenkiintoista keskustelua siitä, minkälaisia mahdollisuuksia organisaatioilla on rakentaa ja ylläpitää kyberresilienssiään teknologian

nopean kehityksen keskellä. Edelleen jopa arvostetuilla Fortune 500 -listauksen miljardien eurojen liikevaihdon organisaatioilla on ongelmia kyberturvallisuuden johtamisessa (Abraham & Sims, 2021; Martin, 2021), jolloin kyberresilienssin rakentaminen voi olla erityisen hankalaa. Modernien organisaatioiden kyberresilienssin nykytilaa voidaan yleisesti pitää suhteellisen heikkona, sillä suurillakin organisaatioilla on edelleen haasteita kyberturvallisuuden johtamisessa (Petrenko, 2019).

Haasteena yleisesti kyberturvallisuuden alalla on pula alan osaajista (Petrenko, 2019) ja henkilöstöstä, jolla tarvittavia kyberturvallisuuden kyvykkyyksiä (Wong, 2017). Ongelmana on etteivät koulutusohjelmat pysy nopean toimintaympäristön kehityksen perässä, sillä arviolta merkittäviä muutoksia teknologian saralla kyberturvallisuuden näkökulmasta tapahtuu kuudessa kuukaudessa (Petrenko, 2019). Tästä johtuen valmistuneilla alan opiskelijoilla on yleensä liian vähän tarvittavia taitoja työmarkkinoille eivätkä opintosuunnitelmat kouluta opiskelijoita tarpeeksi perusteellisesti käytännön todellisuutta varten eivätkä siihen miten todellisia moderneja tietoturvallisuuden ongelmia ratkaistaan tehokkaasti (Petrenko, 2019).

Lisäksi kyberresilienssin kehitystä moderneissa organisaatioissa hidastaa resurssien epätasainen allokointi. Kyberturvallisuuden resursseista vain 17 % investoidaan reagointi- ja toipumissuunnitteluun sekä liiketoiminnan jatkuvuuden turvaamiseen (Coden et al., 2023). Suurin osa kyberturvallisuuden kuluista menee suojaaviin toimenpiteisiin (Hepfer & Powell, 2020; Coden et al., 2023). Täydellisen puolustuksen renderöinti on mahdotonta ja tämän takia ensimmäisen tason suojelun ei pitäisi täysin viedä kyberturvallisuusbudjettia (Hepfer & Powell, 2020).

Organisaatiot pyrkivät usein olemaan kustannustehokkaita, jolloin esimerkiksi järjestelmäarkkitehtuurissa pyritään hyödyntämään yhtä toimivaa järjestelmää kaikkialla. Tämä johtaa tilanteisiin, jossa liiketoiminta vaarantuu tämän järjestelmän vaarantuessa. Kustannukset kyberloukkauksen iskiessä kuitenkin helposti ylittävät järjestelmän kokonaiskustannukset. Resilientin organisaation on löydettävä tasapaino resurssien allokoinnin suhteen. Tämä on haastavaa, sillä hyödyt eivät ole välittömät eivätkä välttämättä koskaan havaittavissa. (Coden et al., 2023)

Vuonna 2020 kyberhyökkäykset nousivat 400 % verrattuna aikaisempiin vuosiin, mikä ensisijaisesti johtui pahantahtoisen toimijoiden hyödyntäessä huonosti suojattuja virtuaalisia työympäristöjä ja IT-infrastruktuureja, joita oli jouduttu pandemian takia mukauttamaan organisaatioiden toimintaan äkillisesti. Keskimäärin nämä hyökkäykset maksoivat yrityksille satoja tuhansia dollareita. Tämä vaikutti suuresti monien pienien ja keskisuurten yritysten konkursseihin. Yhdysvaltalaisyrityksissä kyberhyökkäykset ai-

heuttivat yhteensä biljoonan dollarin menetykset raporttien mukaan vuoden 2020 lopulla. (Abraham & Sims, 2021)

Pandemian vaikutusten takia sitä voidaan käyttää esimerkkinä siitä, minkälaista resilienssiä organisaatioilta vaaditaan niiden suorituskyvyn ylläpitämiseksi sekä arviointikohteena niiden resilienssin nykytilasta. Pandemia-aikana organisaatioiden henkilöstön annettiin käyttää etätyöskentelyyn omaa laitteistoa, jonka seurauksena IT- ja turvallisuustiimit eivät tienneet mitä laitteita ja applikaatioita käytettiin organisaation verkossa, minkälaisia tietoturvapäivityksiä laitteissa oli, miten turvallisia WIFI-verkkoja henkilöstö käytti tai minkälaisia muita laitteita oli yhdistettynä verkkoon kuten kodin älylaitteistoa (Abraham & Sims, 2021). Tämä on antanut esimakua digitalisaation neljännen aallon tuomista haasteista, joihin kuuluu esimerkiksi laitteiden laaja linkittyneisyys ja verkottuneisuus, jolloin on erityisen haasteellista huomioida kaikki tietoverkkoihin kytkeytyneet laitteet sekä huomioida kaikki mahdolliset pääsykohdat (access point) verkkoon (Culot et al., 201).

4. DIGITALISAATION NELJÄS AALTO

Digitalisaation neljännestä aallosta puhuttaessa tarkoitetaan trendiä, joka teknologioiden kehityksessä tarkoittaa muun muassa liitettävyyden (connectivity), automatisaation ja laskentatehon nousua (Culot et al., 2019). Aineistossa trendin tuomista teknologioista käytetään käsitettä teollisuus 4.0 (Industry 4.0) tai 4.0 teknologiat. Näitä teknologioita ovat muun muassa esineiden internet (Internet of Things, IoT), pilvi- ja sumulaskenta, big data, tekoäly, uuden sukupolven robotiikka ja lohkoketjut (Dietrich, 2017; Culot et al., 2019; Mazzara et al., 2019; El-Kady et al., 2023). Kyberresilienssiä voidaan pitää näiden järjestelmien tärkeimpänä ominaisuutena, sillä niiden toiminta muun muassa liitettävyyden takia on riippuvainen tästä ominaisuudesta (Petrenko, 2019).

Digitalisaation neljännen aallon teknologiat luovat organisaatioille monimutkaisia haasteita hyökkäyspinta-alan kasvaessa ja järjestelmistä tullessa yhä monimutkaisempia (Lezzi et al., 2018). Tästä johtuen kyberturvallisuudessa reaktiivinen toiminta ei ole kannattavaa, sillä kriteerit onnistuvalla puolustusteknologialle liikkuvat jatkuvasti (Wong, 2017). Toisaalta muun muassa laskentatehon kasvu ja koneoppiminen tuovat puolustuksen käyttöön uusia mahdollisuuksia, kuten algoritmityökaluja (Bécue et al., 2021). Nämä teknologiat luovat organisaatioille uusia mahdollisuuksia toiminnan kehittämiseen ja kilpailuedun saavuttamiseen kyberturvallisuutta kehittämällä (Hepfer & Powell, 2020).

4.1 Uhat

Riskienhallinnassa käytetään muun muassa hyökkäyspinta-alan ja -vektorien mallintamiseksi visuaalisia kuvauksia mahdollisista hyökkäyspoluista (Lezzi et al., 2018; El-Kady et al., 2023). Näiden avulla voidaan myös arvioida todennäköisyyksiä, mistä hyökkäys todennäköisin on peräisin ja miten se järjestelmässä ja tietoverkoissa pyrkii etenemään. Tämä tekee 4.0-teknologioista erityisen haasteellisia kyberturvallisuuden kannalta, sillä niiden liitettävyys ja monimutkaisuus moninkertaistaa hyökkäyspinta-alan ja tekee riskien- ja haavoittuvuuksienhallinnasta hyvin haasteellista. (El-Kady et al., 2023)

Dynaamisessa toimintaympäristössä organisaatioita uhkaavat hienovaraiset erittäin kehittyneet jatkuvat uhat (Advanced Persistent Threat, APT). Erityisesti organisaatiot, jotka eivät monitoroi ympäristöään ja näin ole tietoisia muutoksien luonteesta ja kyberuhkien hienovaraisuuden tasosta ovat erityisen haavoittuvaisia APT-uhille (Ferdinand, 2015). Tämä aiheutuu muun muassa heikosta organisaation oppimisen tasosta ja siitä ettei ympäristön kehitystä huomioida edes perustavanlaatuisen kyberturvallisuustekniikan päivittämiseksi (Ferdinand, 2015). 4.0-teknologiat mahdollistavat yhä hienovaraisemmat hyökkäykset (Culot et al., 2019; Hausken, 2020), jolloin myös APT-uhat mahdollistavat, että organisaatioihin voidaan hyökätä ilman niiden tietämystä vaarantaen organisaation kyvyn tuottaa tuotteita ja palveluita (Ferdinand, 2015). Vuonna 2013 hyökkääjät pysyivät piilossa keskimäärin 229 päivää ja vain 33 % löysivät loukkauksen sisäisesti (Ferdinand, 2015). Kyberrikollisuuden kasvavan trendin huomioiden (Hepfer & Powell, 2020; Juan et al., 2020; Abraham & Sims, 2021) lukemien voidaan olettavaa olevan nousussa. Hyökkääjillä ollessa pääsy hyvin pitkiksi ajoiksi uhriinsa, se mahdollistaa muun muassa datan louhimisen, helpottaa pääsyä syvemmälle tietoverkkoihin ja mahdollisesti koko toimitusketjuun ja sitä kautta myös muihin organisaatioihin (Ferdinand, 2015). 4.0-teknologioiden mahdollistavan hakkerointikyvyn ja älykkään automaation huomioiden (Dietrich, 2017), APT-uhat ovat organisaatioille entistä suuremmassa roolissa, sillä ne nopeuttavat hyökkääjän kykyä edetä järjestelmissä.

IoT eli esineiden internet (Internet of Things) on monimutkainen turvallisuuden näkökulmasta, sillä se kasvattaa huomattavasti hyökkäyspinta-alaa, jolloin kaiken ollessa linkittynyttä hyökkäys voi olla mahdollinen mistä päin maailmaa tahansa (Ridout, 2016; Hausken, 2020). Tämän lisäksi pääsykohtien (access point) määrä järjestelmiin moninkertaistuu ja lisää järjestelmissä käynnissä olevia ohjelmistoja, mikä muun muassa monimutkaistaa epätavallisuuksien tunnistusta tietoliikenteessä (Ridout, 2016).

4.0-teknologiat myös mahdollistavat laajan automatisaation, jolloin perinteisien logiikkapommien sijaan voidaan hyökkäyksissä hyödyntää monimutkaisempia automatisoituja kyberhyökkäyksiä, jotka eivät vaadi aktiivista ihmisen osallistumista. Automatisaatio tekee ohjelmistoista polymorfisia, jolloin ne kykenevät jatkuvasti muuttamaan hienovaraisesti osia itsestään siten, että sen toiminnallisuus ei muutu, mutta sen allekirjoitus (signature) voi muuttua loputtomasti. Tällaiselta hyökkäykseltä puolustautuminen on vaikeaa, sillä se voi jopa aiheuttaa itsensä vahingoittamista väärällä identifioinnilla ja luoda kuvan puolustajasta, joka reagoi sattumanvaraisesti. (Ridout, 2016)

Yleisesti 4.0-teknologiat ovat haasteellisia kyberturvallisuuden näkökulmasta, sillä hyökkäyksen alkuperää ja kohdetta on vaikea ennustaa, jolloin erityisiesti nollapäivän haavoittuvuudet ja hyökkäykset yleistyvät (El-Kady et al., 2023), häiriötilanteiden seu-

raukset ovat yhä tuhoisammat (Vaidya et al., 2020) ja järjestelmät niin monimutkaisia, että toipumiseen tarvitaan erityistä ammattitaitoa (Wong, 2017).

4.2 Mahdollisuudet

Täydellinen kyberpuolustus on jo nyt mahdotonta (Hepfer & Powell, 2020) ja tulee sellaisena myös pysymään (Culot et al., 2019) digitalisaation neljännen aallon tuomien teknologian kehityksen trendien myötä. Tämä ei kuitenkaan tee puolustusmenetelmistä tarpeettomia, vaan muuttaa tapaa suhtautua puolustukseen ohjaamalla lähestymistapaa reaktiivisesta proaktiiviseen (Wong, 2017; Culot et al., 2019).

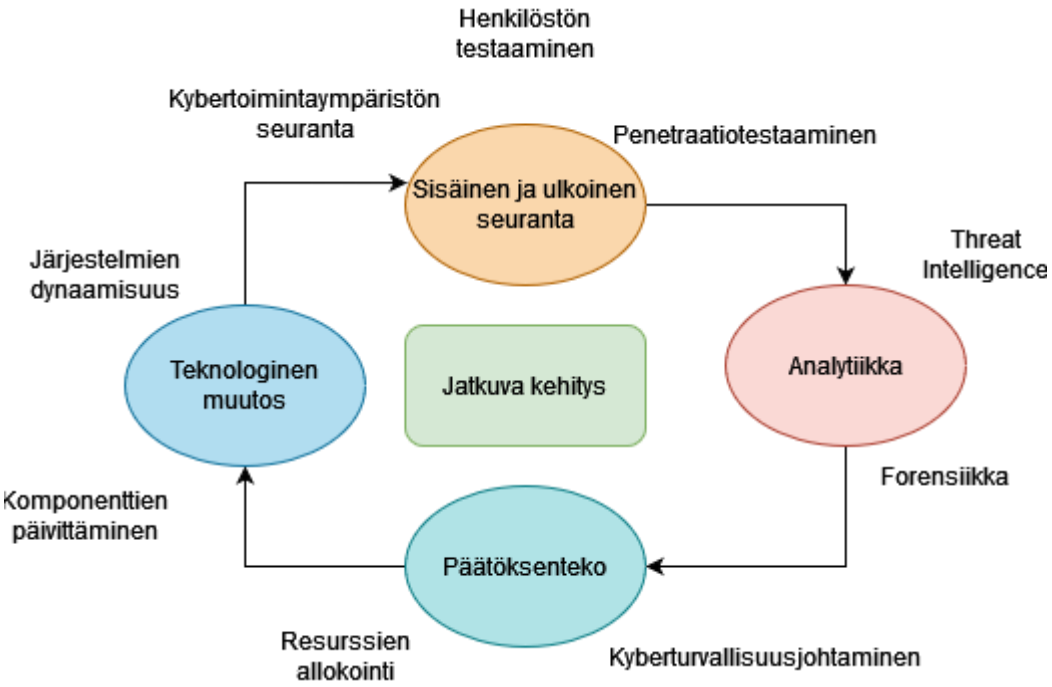
4.0-teknologioiden avulla voidaan muun muassa vähentää ihmisen tekemiä virheitä kaikissa organisaation liiketoiminnassa (El-Kady et al., 2023). Teknologian tuominen lähemmäs ihmisen toimintaa voi olla erittäin hyödyllistä, sillä yhä ihminen on usein suurin riskitekijä kyberturvallisuudessa (Petrenko, 2019). 4.0-teknologioilla voidaan myös kehittää turvallisuuden noudattamista, ylläpitoa ja valvontaa (El-Kady et al., 2023), poikkeavuuksien ja virheiden tunnistamista (Bécue et al., 2021; El-Kady et al., 2023) sekä kehittää turvallisuustilanteiden havainnointia konfiguroinnilla (El-Kady et al., 2023).

Syväoppimista, kuten neuroverkkoja voidaan hyödyntää haastavien multikanavahyökkäysten havaitsemisessa. Syväoppimisen avulla voidaan myös kehittää parempia algoritmeja arvioimaan onko tapahtunut loukkaus tai hyökkäyksen yritys. Hybridioppimista soveltamalla voidaan luoda järjestelmiä, jotka havaitsevat dynaamisesti nollapäivän kalastelusähköpostiviestejä (Hausken, 2020). Tekoäly voidaan myös asettaa järjestelmiin monitoroimaan ja tarjoamaan tarkempaa tietoa, tekemään kriittisiä päätöksiä jos tarpeellista ja antamaan todisteita toiminnasta sekä kehittämään resilienssiä. Tekoälystä huolimatta järjestelmiä hallinnoidaan tarkkaan ja niissä hyödynnetään tiukkoja kyberturvallisuuspolitiikkoja. Hyödyntämällä syväoppimista voidaan jo nyt monitoroida tietoverkkoliikenettä alueilla, joissa tarvitaan korkean tason henkilökohtaista tukea (Brennan et al., 2019)

Kvanttitietokoneet ja laskentatehon nousu tarjoavat puolustukselle uusia mahdollisuuksia muun muassa analytiikan ja algoritmien suhteen (El-Kady et al., 2023). Algoritmeja voidaan kouluttaa käsittelemään ihmistä tarkemmin mahdollisia uhkia louhimaan datasta yhteneväisyyksiä ja hyökkäyskuvioita (attack pattern) (Bécue et al., 2021). Kyberresilienssin kehitys vaatii 4.0-teknologiat tuntevaa ammattitaitoa, mutta sen lisäksi selkeitä politiikkoja ja toimintamalleja sekä koko organisaation kattavaa kyberturvallisuustietoisuutta, jotta uhkia voidaan tunnistaa ja mahdollisuuksia hyödyntää (Wong, 2017).

5. KYBERRESILIENSSIN JA KYBERTURVALLISUUDEN KEHITYS

Kyberresilienssin kehittymisen osa-alueet on esitelty kuvassa 2 ja taulukossa 2 on esitelty mitkä tekijät edistävät tämän kehityksen toteutumista vertaisarvioidun lähdemateriaalin perusteella. Merkittävimmät tekijät lähdemateriaalin perusteella ovat strateginen kyberturvallisuusjohtaminen, analytiikka, järjestelmäarkkitehtuuri ja dynaaminen puolustus sekä sisäinen ja ulkoinen seuranta, mitkä kaikki pyrkivät edistämään jatkuvaa kyberturvallisuuden kehitystä sekä erityisesti kyberresilienssille merkittävää reagointi- ja toipumissuunnittelua. Näitä tekijöitä on havainnollistettu kuvassa 3, joka pyrkii esittämään miten eri tekijät käytännössä toimivat yhdessä ja mitä näihin eri osa-alueisiin kuuluu.



Kuva 3 – Kyberresilienssin kehittymiseen vaikuttavat tekijät

Näillä tekijöillä voidaan havaita olevan yhteyksiä kyberresiliensin kehittymisen lisäksi myös kyberturvallisuuden kehittymiseen NIST-mallin osa-alueiden kautta, sillä esimerkiksi teknologiset muutokset puolustusjärjestelmiin eivät pelkästään paranna organi-

saation kykyä sietää häiriötilanteita vaan myös NIST-mallin osa-aluetta suojella sensitiivistä dataa.

5.1 Strateginen kyberturvallisuusjohtaminen

Organisaation ylimmän tason päätöksenteolla ja strategisella kyberturvallisuusjohtamisella on merkittävä vaikutus organisaation kyvylle kehittää kyberresilienssiä (Hepfer & Powell, 2020), sillä tällä tasolla tehdään muun muassa päätöksiä resurssien allokoinnista, kyberturvallisuusstrategioista ja -politiikoista sekä niiden suhteesta muuhun liiketoimintaan. Tämä päätöksenteko mahdollistaa sen, minkälaisia kyvykkyyksiä ja resursseja NIST-kyberturvallisuusmallin osa-alueilla on ja minkälaiset mahdollisuudet organisaatiolla on sopeutua kybertoimintaympäristönsä muutoksiin sen liiketoiminnalliset tavoitteet huomioiden (Ferdinand, 2015; Hepfer & Powell, 2020).

Yrityksen strategisesta päätöksenteosta vastuussa oleva johto vaikuttaa suuresti kyberresilienssin kehitysmahdollisuuksiin. Kyberresilienssin kehittämiseksi ylimmän johdon on nähtävä kyberturvallisuuden strategisuus (Culot et al., 2019; Hepfer & Powell, 2020) ja uhkien potentiaalinen vahinko kattavampien strategioiden luomiseksi erilaisten kyberkonfliktien estämiseksi (Ridout, 2016). Strateginen johto ei huomioi kyberturvallisuutta välttämättä ollenkaan, vaan se nähdään taustalla toimivana sisäisenä palveluna ja tämän lisäksi johdolla on usein kognitiivinen taipumus jatkaa samoilla strategisilla päämäärillä (Hepfer & Powell, 2020). Kyberresilienssin kehittämiseksi johdolta vaaditaan kyberturvallisuuden suunnittelussa muutosta toiminnallisesta näkökulmasta strategiseen ja reaktiivisesta proaktiiviseen toimintaan, mikä mahdollista vakavan suhtautumisen uhkiin korkeimmassa päätöksenteossa (Hepfer & Powell, 2020). Tutkimusten mukaan johdon luoma kattava kyberturvallisuusstrategia parantaa kokonaisvaltaista organisaation oppimista ja luo uusia mahdollisuuksia, sillä kyberhyökkäykset paljastavat heikkouksia järjestelmien lisäksi muussa liiketoiminnassa ja esimerkiksi johtajuuden kehityksessä (Hepfer & Powell, 2020). Organisaation oppiminen on välttämätöntä resilienssin kehitykselle (Ducheck, 2020) ja kyberturvallisuustietoisuus kyberturvallisuuden kehitykselle (Ferdinand, 2015; NIST, 2016; Abraham & Sims, 2021), joiden molempien kokonaisvaltaisesta kehityksestä organisaation ylin johto on vastuussa (Hepfer & Powell, 2020).

Tätä strategisen tason muutosta vaaditaan organisaatioissa, sillä ylin johto on vastuussa muun muassa resurssien allokoinnista, jolla on kirjallisuuden perusteella merkittävä vaikutus kyberresilienssin kehittymiseen. Kyberturvallisuuden kehitys vaatii investointipäätöksiä ja organisaation kokonaisvaltaisilla strategisilla linjauksilla on myös suuri vai-

kutus järjestelmäarkkitehtuurisiin ratkaisuihin, jotta ne voivat integroitua yhdessä liiketoimintojen kanssa hidastamatta niitä (Brennan et al., 2019; Hepfer & Powell, 2020). Organisaatioiden hallitusten ja johtojen täytyy vaihtaa kyberturvallisuuden resurssisuunnitteluaan ja lähestymistapaansa tasapainoisemmaksi, sillä nyt vain noin neljännes menee resilienssiä edistäviin toimiin (Coden et al., 2023). Pelkään puolustamiseen budjetointi ei edistä kyberresilienssiä, sillä nykyisen ja 4.0-teknologian monimutkaisuuden huomioiden nollapäivän haavoittuvuuksilta on mahdotonta puolustautua täysin (Wong, 2017; Culot et al., 2019). Ylin johto on myös suurilta osin vastuussa suurista ulkoistamista päätöksistä, joilla kyberresileinssin kehitystä voidaan mahdollisesti edistää (Abraham & Sims, 2021)

Kyberstrategian tulee täytyy olla moniulotteinen ja joustava, jolloin sen tulee sisältää niin puolustautumista kuin kyberresilienssiäkin, milloin siihen kuuluu tekniikan ja puolustuksen suunnittelun lisäksi henkilöstön kouluttaminen ja harjoittaminen (Ridout, 2016). Kyberresilienssin kehittäminen ei ole ainoastaan pohjapiirustus teknologia-arkkitehtuurille vaan koko organisaation laajemmalle ekosysteemille (Coden et al., 2023). Tässä ekosysteemissä toimivat uhat tulee ymmärtää, mutta myös toimitusketjujen ja sidosryhmien mahdollistavat resilienssiä kehittävät elementit tulee huomioida, sillä nämä suhteet monialaisiin ja -tieteisiin toimijoihin voivat edesauttaa organisaation palautumista kriisitilanteista yhteistyön ja tiedon jakamisen avulla (Ferdinand, 2015; Coden et al., 2023). Johdon mahdollistama avoin kommunikointi ulkoisiin sidosryhmiin on arvokasta, sillä se mahdollistaa kyberhyökkäysten vaikutusten arvioinnin myös niihin.

Hallinnollisilla päätöksillään organisaatiot voivat olla paremmin varustautuneita suojelemaan kriittistä infrastruktuuriaan ja dataansa implementoimalla selkeitä kyberturvallisuuden ja tiedonhallinnan käytäntöjä (Abraham & Sims, 2021). Organisaatioiden byrokratian, politiikkojen, direktiivien ei tule olla implementoitavien ketterien toimintatapojen esteenä, sillä ne mahdollistavat kyberresilienssiä kehittävät informaation jakamisen, yhteistyön ja kybertoimintojen synkronoinnin (Brennan et al., 2019). Nopean havainnoinnin, voimakkaiden vastatoimien ja tehokkaan palautumisen mahdollistamiseksi, niistä erityisesti jälkimmäisen suunnittelussa koko organisaation tulee olla osallisena (Abraham & Sims, 2021). Organisaatioiden ylimmällä johdolla on vastuu mahdollistaa organisaation sisäisten ja ulkoisten sidosryhmien välinen yhteistyö kyberresilienssin kehittämiseksi (Hepfer & Powell, 2020). Tämän takia strateginen kyberturvallisuusjohtaminen on tärkeä osa kyberresilienssin ja kyberturvallisuuden kehittymiselle, sillä tämä

ylimmän tason päätöksenteko mahdollistaa muiden osa-alueiden resurssit sekä koko organisaation kyvykkyydet sopeutua kybertoimintaympäristön vaativiin muutoksiin.

5.2 Sisäinen ja ulkoinen seuranta

Kyberresilienssin kehittyminen vaatii organisaatiolta ymmärrystä omasta kybertoimintaympäristöstään (Ferdinand, 2015). Sisäisellä ja ulkoisella seurannalla (internal and external monitoring) organisaatio pyrkii kasvattamaan ymmärrystään kybertoimintaympäristön uhista, omista haavoittuvuuksistaan ja kyvykkyyksistään puolustautua niitä vastaan (Ferdinand, 2015). Organisaation on seurattava toimintaa niin organisaation sisällä kuin ulkona mahdollistaakseen jatkuvan kehityksen kehittämällä kykyään ennakoida ja sopeutua (Vaidya et al., 2020). Testaaminen on olennainen osa tätä seurantaa ja mainittu useassa NIST-kyberturvallisuusmallin osa-alueissa (NIST, 2016).

Jatkuva testaaminen on yksi tärkeimmistä kehityskohteista organisaatioissa kyberresilienssin keittämiseksi (Campbell & Robert, 2020; Coden et al., 2023) ja sen ylläpitämiseki 4.0-teknologioiden kehittyessä (Lezzi et al., 2018; Culot et al., 2019). Kyberresilienssi vaatii testaamista niin käytettävyyden kuin suorituskyvynkin näkökulmasta (Brennan et al., 2019). Organisaatioilta vaaditaan sisäisiä kyvykkyyksiä kyberresilienssin kehittämiseen ja testaamiseen (Brennan et al., 2019), jotta voidaan parantaa puolustuksen ja reagoinnin lisäksi koko liiketoimintaa (Hepfer & Powell, 2020). Testausta voidaan tehdä esimerkiksi niin sanotuilla penetraatiotesteillä (penetration testing), joissa järjestelmään pyritään tunkeutumaan tai read teaming -tekniikalla, jossa simuloidaan hyökkäystilanteita (Ridout, 2016). Simulaatioita pidetään erittäin tehokkaana tapana löytää järjestelmähaavoittuvuuksia (Ridout 2016) ja Ducheckin (2020) mukaan niiden avulla voidaan organisaation kokonaisvaltaista oppimista tehostaa resilienssin kehittämiseksi.

Järjetelmien lisäksi toimintoja, prosesseja ja henkilöstöä voidaan testata penetraatiotestien tavoin. Kaikkien ongelmatilanteiden kuvittelu voi olla vaikeaa, sillä organisaatiot ensisijaisesti suunnitellaan olemaan menestyneitä ja tuottavia. Mahdollisten virheiden ja ongelmakohtien löytäminen on kuitenkin erityisen palkitsevaa, sillä tarkastelemalla miten toiminnot jatkuvat epätavallisten tilanteiden tapahtuessa, kyberresilientit organisaatiot löytävät uusia tapoja parantaa tuottavuutta ja tehokkuutta sekä suorituskykyä. (Coden et al., 2023)

Testaamalla löydetään organisaation kehityskohteita ja mahdollistetaan kehitys. Kehityskohteet voivat olla puolustusjärjestelmien lisäksi muun muassa johtamistavoissa,

vastuunjaossa, tiedon jakamissa tai henkilöstön koulutustarpeissa (Hepfer & Powell, 2020). Kyberresilienssin kehittämiseksi testaamisen on katettava nykyistä useampia osa-alueita, johon vaaditaan osallistumista myös alueilta, jotka eivät suoraan ole vastuussa koko organisaation kyberturvallisuudesta. Testaamisessa on myös erityisen tehokasta hyödyntää kolmansia osapuolia, joiden ydinosaaminen on nimenomaan haavoittuvuuksien löytäminen (Abraham & Sims, 2021). Ulkoistaminen saattaa tukea kyberresilienssiä, sillä se keventää johdon kuormitusta ei-kriittisiltä toiminnoilta kyvykkäämmille tuottajille, mikä yleensä tehostaa kyberturvallisuutta (Brennan et al., 2019). Ideaalitilanteissa testaamista voidaan myös laajentaa tärkeimpiin ulkoisiin sidosryhmiin toimitusketjujen kyberresilienssin kehittämiseksi, mutta tämä on harvoin mahdollista (Hepfer & Powell, 2020).

Sisäinen ja ulkoinen seuranta on erittäin tärkeää modernissa jatkuvasti ja odottamattomilla tavoilla kehittyvässä toimintaympäristössä (Ferdinand, 2015). Puolustaminen ja hyökkääminen perustuu tietoon vastapuolen toiminnasta, joten toimintaympäristön uhkaindikaattoreita seuraamalla organisaatiot voivat kehittää sopeutumis- ja ennakointikykyään tunnistamalla miten kybertoimintaympäristö muuttuu (Lezzi et al., 2018). Kouluttamalla, jakamalla tietoa ympäristön uhkaindikaattoreista ja jatkuvalla pahantahtoisen toiminnan valvonnalla voidaan mukauttaa puolustusta ja koettaa pysyä askeleen edellä, joka organisaatioille on tavoiteltavaa (Ridout, 2016).

Sisäisellä seurannalla voidaan myös kehittää olemassa olevia havainnointi- ja puolustusjärjestelmiä ja -menetelmiä, sillä näin voidaan parantaa teknisiä ratkaisuja (Ridout, 2016) sekä organisaation kokonaisvaltaista kyberturvallisuustietoisuutta (Ferdinand, 2015). Kyberresilienssin mahdollistamiseksi organisaatio tarvitsee käyttökelpoista dataa kaikkialta organisaation tietoverkosta, käyttäjien laitteista ja applikaatioista (Abraham & Sims, 2021). Käyttökelpoisen datan kerääminen vaatii ennakkosuunnittelua, jota voidaan edesauttaa sisäisellä valvonnalla (Abraham & Sims, 2021). Kirjallisuuden perusteella sisäisellä ja ulkoisella seurannalla on erityisen tärkeä tehtävä sisäisten ja ulkoisten uhkien arvioinnissa, kyberriskienhallinnan kehittämisessä ja kehityskohteiden löytämisessä. NIST-kyberturvallisuusmallissa, sillä on suuri merkitys erityisesti identifioinnin, suojelun ja havainnoinnin osa-alueisiin.

5.3 Järjestelmäarkkitehtuuri ja dynaaminen puolustus

Kyberresilienssin kehittämiseksi organisaatiolta vaaditaan toimivaa perinteistä kyberturvallisuustekniikka, johon kuuluvat esimerkiksi palomuurit, VPN (Virtual Private Ne-

towrk), haavoittuvuusskannerit, anti-viruspalvelut ja tunkeutumisen havainnointityökalut (Brennan et al., 2019). Kyberympäristön dynaamisuus sekä modernien järjestelmien monimutkaisuus ja verkottuneisuus takaavat ettei kaikilta kyberuhilta voida kuitenkaan puolustautua (Tran et al., 2016) eikä mikään järjestelmä ole täysin turvallinen (Lezzi et al., 2018). Mikään tunnettu teknologia, metodi tai toimintatapa ei pysty kategorisesti ehkäisemään kyberhyökkäyksiä (Campbell & Robert, 2020). Tämän takia 4.0-teknologiatkaan eivät tarjoa yhtä kaikenkattavaa teknologiaa vastauksena digitalisaation neljännen aallon trendeihin vaan kirjallisuuden perusteella puolustuksessa on kyse kyberresilienssin dynaamisuudesta ja järjestelmäarkkitehtuurisista päätöksistä.

Järjestelmäarkkitehtuuri määrittelee järjestelmän osat, niiden ominaisuudet sekä niiden väliset yhteydyt ja riippuvuudet. Se määrittelee rungon järjestelmän suunnittelulle ja toteutukselle sekä lisäksi ohjaa järjestelmän kehityssuuntia. (Petrenko, 2019) Arkkitehtuuriset valinnat vaikuttavat järjestelmän kykyyn ylläpitää kyberresilienssiä saatavilla olevien rajapintastandardien käytön, dynaamisen verkonhallinnan mahdollisuuksien, prosessien kypsyyden ja alustan kyvyn kehittyä uusia kyberuhkia vastaan avulla (Brennan et al., 2019). Nämä valinnat näkyvät niin NIST-mallin mukaisissa kyvyissä suojella järjestelmiä ja havaita uhkia sekä kyberresilienssille olennaisessa kyvykkyydessä sietää hyökkäyksiä.

Teknologian kehityksen ja kyberuhkien ohittaessa kapasiteetin ottaa käyttöön nykyaikaisia järjestelmiä yhtenä vaihtoehtona on siirtyä avoimeen arkkitehtuuriin, jossa käytetään avoimia standardeja, jotka tukevat modulaarista, löyhästi kytkettyä ja erittäin yhtenäistä järjestelmärakennetta, johon kuuluu järjestelmän keskeisten rajapintojen julkaiseminen ja suunnittelun täydellinen julkistaminen. (Brennan et al., 2019).

Tavoitteena on nopeampi käyttöönoton sykli, jolloin komponentteja voidaan päivittää ja korvata teknologian kehittyessä ilman että koko järjestelmää täytyy uudelleen suunnitella (Brennan et al., 2019). Tämä lisää resilienssiä, sillä nopealla komponenttien korvauksella voidaan toiminta palauttaa uuden järjestelmän kautta, joka ei ole identtinen alkuperäisen kanssa (Coden et al., 2023). Arkkitehtuurin on tämän lisäksi perustuttava vankkoihin ja hyvin määriteltyihin standardeihin (Brennan et al., 2019). Näin voidaan arkkitehtuuria hyödyntämällä pienentää hyökkäyspinta-alaa (Brennan etal., 2019), joka on yksi 4.0-teknologioiden suurimmista kyberturvallisuushuolista (Ridout, 2016; Lezzi et al., 2018; Culot et al.,2019; Bécue et al., 2021). Avoin arkkitehtuuri myös tarjoaa tarkkaa uhkiin perustuvaa tietoa, mikä kehittää vastatoimien räätälöintiä, reagointia ja turvallisuusvalvontaa (Brennan et al., 2019).

Muita järjestelmäarkkitehtuurin suunnittelussa huomioitavia tekijöitä ovat tietoverkkojen kerrostuneisuus, järjestelmäkomponenttien heterogeenisyys ja fragmentaatio (El-Kady et al., 2023), tietovirrat (Capbell & Robert, 2020), hajautuneisuus (Hepfer & Powell, 2020) sekä erilaiset järjestelmien väliset riippuvuussuhteet (El-Kady et al., 2023). Kerroksien lisääminen ja komponenttien välisten yhteyksien vähentäminen lisää monimutkaisten järjestelmien turvallisuutta (Zou et al., 2021). Eri heterogeenisten komponenttien integrointi järjestelmään tulisi suunnitella huolellisesti, jotta järjestelmää voidaan ymmärtää kyberturvallisuuden mahdollistamiseksi (Vaidya et al., 2020).

Avoin arkkitehtuuri ei kuitenkaan ole yksiselitteisesti kyberresilienssin näkökulmasta tehokkain ratkaisu ja lopullinen päätös järjestelmäarkkitehtuurista tulisi tehdä suunnitellun elämänkaaren ja liiketoimintaprosessien sekä strategisten tavoitteiden perusteella (Brennan et al., 2019). Arkkitehtuuriset ratkaisut ovat kuitenkin kyberresilienssin kehityksen kannalta merkittäviä päätöksiä, sillä sen avulla voidaan ehkäistä haittaohjelmien leviämis- ja etenemismahdollisuuksia (Tran et al., 2016) ja ne määrittävät millä puolustuskeinoilla järjestelmiä voidaan parhaiten suojella (Campbell & Rober, 2020).

Puolustusmenetelmien ja -järjestelmien tulee olla dynaamisia kyberresilienssin kehittämiseksi (Ridout, 2016; Tounsi & Rais, 2018). Dynaamisen puolustukseen kuuluvat esimerkiksi defence in depth -käytännöt, jotka perustuvat puolustuksen kerrostuneisuuteen (Lezzi et al., 2018). Tämä voidaan toteuttaa esimerkiksi tietoverkoissa demilitarisoiduilla vyöhykkeillä (demilitarized zone, DMZ), jotka sijaitsevat tietoverkon ja tietokoneen välissä, ja joissa palomuurit ja IDS (Intrusion Detection System) toimivat (Tran et al., 2016). DMZ-vyöhykkeet ovat esimerkki tietoverkkojen segmentoinnista, joka on huomioitava moderneissa järjestelmissä kyberturvallisuuden mahdollistamiseksi (Lezzi et al., 2018; Campbell & Robert, 2020). Suurena uhkana verkottuneissa ja toisiinsa liittyneissä laitteissa on, että pääsemällä ydinverkkoon haittaohjelma voi levitä ja liikkua verkosta ja laitteesta toiseen (Tran et al., 2016; Lezzi et al., 2018). Segmentoinilla pyritään eristämään puolustusjärjestelmien avulla laitteita ja järjestelmiä hidastamatta liiketoimintoja (Lezzi et al., 2018).

Järjestelmäarkkitehtuuriin ja puolustusmenetelmiin liittyvillä ratkaisuilla voidaan tukea organisaation kykyä sietää hyökkäyksiä, sillä arkkitehtuurin avulla voidaan muun muassa mahdollistaa harhautusalustojen (deception platforms) käyttöönotto ja haittaohjelmien eristäminen, joilla voidaan huomattavasti hidastaa hyökkäyksen etenemistä ja leviämistä (Tran et al., 2016; Steingartner, 2021). Tämä tukee kyberresilienssiä kehittävää reagointi- ja toipumissuunnittelua antamalla enemmän aikaa päätöksentekoon. Lisäksi arkkitehtuuri luo pohjan NIST-mallin havainnointi- ja puolustusjärjestelmille. Jär-

jestelmäarkkitehtuurin ja puolustusmenetelmien tueksi tarvitaan kuitenkin jatkuvaa arviointia ja investointia testaamiseen sekä uhkien tunnistamiseen (Brennan et al., 2019).

5.4 Analytiikka kyberturvallisuudessa

Analytiikka on suuressa osassa kyberturvallisuutta, sillä sen perusteella havaitsemisjärjestelmät tunnistavat poikkeavuuksia (Brennan et al., 2019), sitä voidaan hyödyntää hyökkäyspolkujen todennäköisyyksien arviointiin riskienhallinnan tukena (Steingartner, 2021; El-Kady et al., 2023) ja muun muassa hyökkääjän alkuperän selvittämiseen (Ridout, 2016). Kyberturvallisuutta voidaan kuvata hyökkääjän ja puolustajan kilpavarusteluna, jossa tärkeimpänä aseena on informaatio. Hyökkääjä ja puolustaja toimivat vuorovaikutuksessa, jossa toiminta perustuu informaatioon vastapuolesta. Tämän takia hyökkäystapaa voidaan pitää heti vanhentuneena kun siitä tiedetään. (Ridout, 2016)

Monet havainnointi- ja puolustusjärjestelmät tunnistaavat analyyttisten menetelmien avulla haitallisia toimijoita niiden allekirjoituksen (signature) perusteella. Analytiikan avulla voidaan myös tunnistaa poikkeavuuksia hyödyntämällä koneoppimista väärinkäytön paljastavien kuvioiden perusteella, vertailemalla ennalta määriteltyjä sääntöyhdistelmiä tai esimerkiksi yhdistämällä ryhmäoppimiseen (ensemble clearing) perustuvia algoritmeja yhdessä poikkeavuuksien tunnistuksessa. (Bécue et al., 2021) Erityisen huomionarvioista, on miten digitalisaation neljännen aallon tuomat teknologiat tuovat uusia menetelmiä kyberturvallisuuden tueksi esimerkiksi vähentämällä ihmisen virheitä, tarkentamalla päätöksentekoa ja reaaliaikaista järjestelmänvalvontaa sekä organisaation kokonaisvaltaista ymmärrystä sen kyberympäristöstä ja siinä toimivista järjestelmistä (Mazzara et al., 2019; Vaidya et al., 2020; Bécue et al., 2021; El-Kady et al., 2023). Tämän takia analytiikalla on niin merkittävä rooli kyberresilienssin kehityksessä, sillä analytiikalla on potentiaalia muun muassa automatisoida ja tarkentaa NIST-kyberturvallisuusmallin identifiointia, suojelua ja havainnointia, jolloin organisaatioilla on mahdollisesti enemmän resursseja käytettävänä pitkän aikavälin jatkuvan kehityksen edistämiseen (Bécue et al., 2021).

Analytiikalla on myös tärkeä rooli vastatoimien suunnittelussa. Vastatoimien tarkoituksena on vähentää loukkauksen kestoa ja parantaa organisaation kykyä palautua odottamattomista uhista. Palautumiseen vaaditaan nopeita oppimisympyröitä, tietämyksen muodostamista kehittyvästä tilanteesta ja jatkuvaa uusien toimintatapojen testaamista. (Coden et al., 2023) Analytiikan avulla tätä tietämystä voidaan kehittää ja tuottaa informaatiota organisaation sisäisille sidosryhmille, kuten reagointi- ja suunnittelutiimien, järjestelmäarkkitehtien ja ylimmän johdon päätöksenteon tueksi (Bécue et al., 2021). Analytiikka tehostaa valvonnan epäsäännöllisyyksien tunnistamista esimerkiksi tietolii-

kenteessä (Abraham & Sims, 2021), ennustaa hyökkäyspolkuja ja parantaa ennaltaehkäisevää toimintaa uhkiin perustuvan tiedonhallinnan (threat intelligence) avulla (Steingartner et al., 2021).

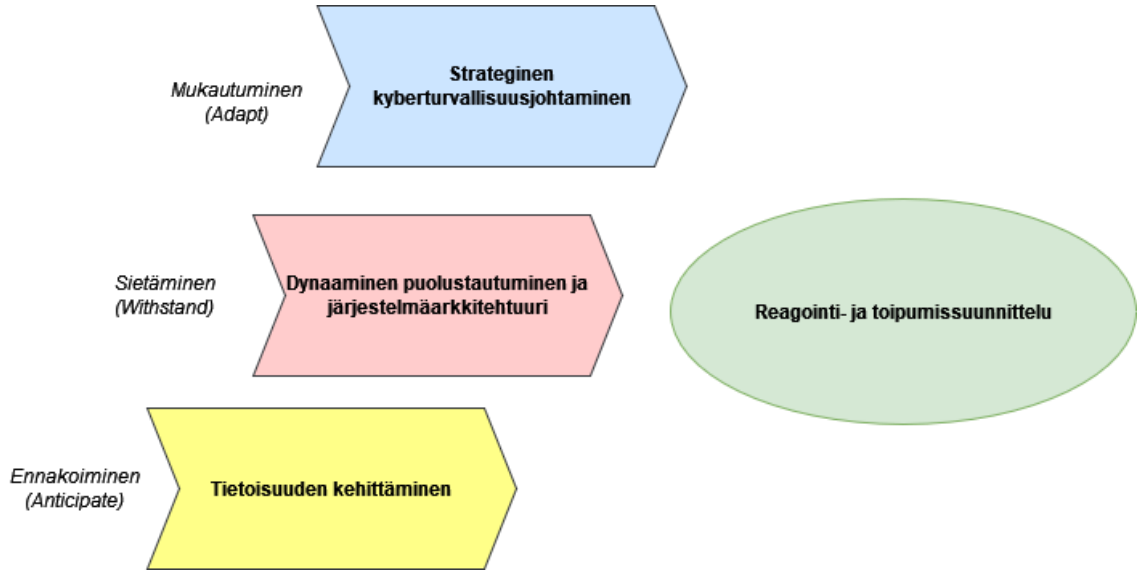
Analytiikalla on hyvin monipuolisia rooleja osana organisaatioiden kyberturvallisuutta. Esimeriksi forensiikka-analyysien avulla puolustaja voi selvittää tunkeutumisen takana olevan tahon alkuperän, mikä avaa mahdollisuuden hyökkäävään puolustukseen (Ridout, 2016). Hyökkäävän puolustuksen tehokkuus kyberresilienssin näkökulmasta on kuitenkin kyseenalaista, sillä se ei suoranaisesti paranna organisaation kykyä palauta konflikteista tai vastata niihin seuraavalla kerralla nopeammin (Ferdinand, 2015). Toisaalta kyberresilienssillä voi olla ratkaisevan varoittava rooli kyberrikollisuuden vähentämisessä, varsinkin jos siihen liittyy uskottava uhka rangaistuksesta. Jos osoitetaan että isku voidaan absorboida, siitä voidaan palautua nopeasti ja myös iskemään takaisin, resilienssi ja pelote (deterrence) voivat olla voimakasta yhdistelmä yhä kehittyneempiä, hienovaraisempia ja järjestäytyneempiä hyökkäyksiä vastaan. (Ridout, 2016)

Analytiikan avulla organisaation kyky tunnistaa uhkia ja haavoittuvuuksia sekä niiden yhtenäisyyksiä keskenään kehittyy ja mahdollistaa organisaation kyberturvallisuustietoisuuden lisääntymisen, mikä ehkäisee niin sanottuja social engineerig- ja käyttäjän manipulointi -hyökkäyksiä (Wong, 2017). Analytiikalla on myös tärkeä osa riskienhallinnassa, sillä pelkkien haavoittuvuuksien löytäminen esimerkiksi testaamalla ei aina riitä. Erityisesti pienillä ja keskisuurilla organisaatioilla ei välttämättä ole käytössää resursseja kaikkien mahdollisten hyökkäyspolkujen estämiseksi, vaan niiden tavoitteena on todennäköisyyksien ja vaikutusten arvioinnin avulla löytää kriittisimmät ja todennäköisimmät ketjut (Fluri & Tagarev, 2020). Analytiikka on kyberresilienssin kehittymisen kannalta relevanttia, sillä se mahdollistaa NIST-kyberturvallisuusmallin lyhyen aikavälin ongelmanratkaisun lisäksi pitkän aikavälin organisaation oppimisen.

5.5 Reagointi- ja toipumissuunnittelu

Kyberturvallisuuden ja kyberresilienssin yhtenevä kohta kuvan 2 esittämällä tavalla on reagointi- ja toipumissuunnittelu. Tämä on kyberresilienssin kannalta olennaisin osaalue, sillä nimenomaan reagointi- ja toipumissuunnittelu tukee kyberresilienssin merkitystä organisaation kykynä säilyttää toimintakykynsä kyberhäiriötilanteista ja -hyökkäyksistä huolimatta (Hausken, 2020; Sepúlveda Estya et al., 2020). Tätä osaaluetta tukevat ylimmän johdon tekemät päätökset kyberturvallisuusresurssien allokoinnista ja strategisista linjauksista (Hepfer & Powell, 2020), näitä liiketoiminallisia strategisia tavoitteita tukeva järjestelmäarkkitehtuuri (Brennan et al., 2019) sekä infor-

maation avulla organisaation tietoisuuden kehittäminen (Wong, 2017; Hausken, 2020). Tietoisuuden kehittämiselle alla olevassa kuvassa tarkoitetaan sisäistä ja ulkoista seurantaa sekä analytiikkaa, jotka tuottavat informaatiota reagointi- ja toipumissuunnittelun tueksi ja näin liittyvät vahvasti toisiinsa. Kuvassa 3 on havainnollistettu sitä, miten kaikki kyberturvallisuuden eri tekijät yhdistyvät kyberresilienssin kanssa ja miten ne pyrkivät tukemaan reagointi- ja toipumissuunnittelua.



Kuva 3 – Reagointi- ja toipumissuunnittelua kehittävät tekijät

Kyberresilienteillä järjestelmillä täytyy olla liiketoiminnan jatkuvuussuunnittelua, joka kuvaa organisaation strategioiden käyttöä, toimenpiteitä, teknisiä mittareita ja suunnitelmia, joita tarvitaan kadonneiden tietojen, toimintojen ja järjestelmien palauttamiseksi liiketoimintahäiriöiden sattuessa. Suunnitelma sisältää hallintasuunnitelman, tietojen varmuuskopiointisuunnitelman, katastrofipalautussuunnitelman ja hätätilan toimintasuunnitelman. Suunnitelmien tulee sisältää rooleja, vastuita ja viestintästrategioita kompromissin tai katastrofin sattuessa, mukaan lukien asiaankuuluvien ulkopuolisten kumppanien ilmoittaminen. (Campbell & Robert, 2020)

Kyberresilienssi vaatii jatkuvuussuunnittelua kaikille ekosysteemin jäsenille niin toimintaketjuissa kuin ydintoiminnoissakin (Ridout, 2016; Coden et al., 2023). Laaja ekosysteemi myös antaa organisaatiolle enemmän resursseja avunantoon loukkausten keskellä. Kyberresilienteillä organisaatioilla on valmiina suhteita lainvalvojiin, forensiikka-asiantuntijoihin, neuvonantajiin ja kommunikaation asiantuntijoihin. Näin loukkauksen tapahtuessa, organisaatio voi hyödyntää näitä olemassa olevia suhteita ja sidosryhmiä, jotka muuten saattaisivat vaatia aikaa kehittyä. (Coden et al., 2023) Ekosysteemin jat-

kuvuussuunnittelun kehittämiseksi tarvitaan yhteisiä termejä ja yksinkertaisia konsepteja tehokkaamman kommunikoinnin saavuttamiseksi, jotta eri ammatilliset toimijat saavat yhteisen sanaston vuorovaikutukseen ja ymmärtääkseen toisiaan. Tässä on vielä paljon kehitettävää kyberturvallisuuden alalla, jotta ekosysteemin kokonaisvaltainen yhteistyö ja kommunikointi voidaan saavuttaa. (Ridout, 2016) Tämä voisi myös edesauttaa yhteisten viitekehitysten kehityksessä, joista reagointi- ja toipumissuunnittelussa on puutetta (Sepúlveda Estay et al., 2020).

Toimiva reagointi- ja toipumissuunnittelu vahvistaa järjestelmän resilienssiä. Sen täytyy kestää hyökkäyksiä, sopeutua muutoksiin ja kehittyä paremmaksi prosessiksi. Toimivalla toipumissuunnittelulla täytyy olla liiketoiminnallinen rooli organisaatioissa. Sen täytyy olla tehokas, kustannustehokas, toistettava riskien pienentämiseksi ja sen täytyy edistää jatkuvaa prosessien kehitystä. Esimerkiksi implementoimalla organisaatioihin CSIRT- (Computer Security Incident Response Team) tai CERT- (Computer Emergency Response Team) tiimejä hoitamaan kyberhyökkäyksiä voidaan parantaa tapausten käsittelyprosesseja ja menetelmiä. Joustava palautumisprosessin on kehityttävä ajan mittaan. Toimivalla mallilla palautumisaste on korkeampi kuin häiriötilanteiden aste. (Tran et al., 2016)

Kyberresilienssiä ei ole ilman reagointi- ja toipumissuunnittelun mahdollistavaa tietopääomaa, jonka tietotekniikka-ammattilaiset voivat tarjota rakentamalla ratkaisuja järjestelmien turvaamiseksi ja parhaimpien toimintamallien toteuttamiseksi murron tapahtuessa (Wong, 2017). Kyberturvallisuusalan osaajapulan, teknologian nopean kehityksen ja koulutusohjelmien vanhentuneen tiedon takia organisaatioilta vaaditaan enemmän yhteistyötä kouluttavien tahojen kanssa, jotta tätä tietopääomaa ammattilaisten muodossa saadaan organisaatioiden käyttöön (Petrenko, 2019).

Liiketoiminnan jatkuvuuden ja jatkuvan kehityksen mahdollistaminen kuuluu muotoutuminen, jolla tarkoitetaan loukkauksen jälkeiseen toimintaan keskittymistä, mitä organisaatiot arvioivat sen tarvitsemalla painoarvolla (Campbell & Robert, 2020). Liiketoiminnan jatkuvuuden mahdollistaminen reagointi- ja toipumissuunnitelmien avulla on kuitenkin ydinkyvykkyyksiä, joita organisaatioilta vaaditaan kyberresilienssin kehittymiseksi (Ferdinand, 2015; Campbell & Robert, 2020; Abraham & Sims, 2021; Coden et al., 2023). Reagointi- ja toipumissuunnittelu on kriittinen osa sitä, miten organisaatiot kehittävät kyberturvallisuuttaan, oppivat ja valmistautuvat tulevaan (Campbell & Robert, 2020). Tämän takia muut tekijät kirjallisuuden perusteella ikään kuin pyrkivät tukemaan nimenomaan reagointi- ja toipumissuunnittelua kyberresilienssin kehittämiseksi. Stra-

teginen kyberturvallisuusjohtaminen investoimalla siihen enemmän resursseja ja linjaamalla sitä osaksi liiketoiminnallisia strategioita, järjestelmäarkkitehtuuri ja dynaaminen puolustus edistämällä reagoinnin ja toipumisen teknologisia elementtejä sekä seuranta ja analytiikka tuottamalla informaatiota suunnittelun tueksi kyberympäristöstä.

6. PÄÄTELMÄT

Tutkimuksen tarkoituksena oli selvittää miten organisaatiot voivat kehittää kyberresilienssiään digitalisaation neljännen aallon tuomien muutosten myötä. Vastauksena tähän saatiin, että organisaatioilta vaaditaan perustavanlaatuista näkökulman muutosta koko kyberturvallisuuden rooliin organisaatiossa, jotta pysyvää muutosta voidaan saada aikaan. Lisäksi selvitettiin mitkä NIST-kyberturvallisuusmallin osa-alueista olivat kyberresilienssin kehitykselle merkittävimmät, jotka olivat reagointi ja toipuminen. Vastaus siihen minkälaisia muutoksia organisaatioilta vaaditaan saatiin kokoamalla tärkeitä tekijöitä, joita olivat strateginen kyberturvallisuusjohtaminen, sisäinen ja ulkoinen seuranta järjestelmäarkkitehtuuri ja dynaaminen puolustus, analytiikka kyberturvallisuusjohtamisessa, jotka kaikki yhdessä tukevat reagointi- ja toipumissuunnittelua. Tarvittava muutos kyberresilienssin saavuttamiseksi tulisi erityisesti suuntautua reagoinnin ja toipumisen kehittämiseen.

6.1 Yhteenveto

Kyberresilienssin kehittyminen vaatii erityisesti strategista kyberturvallisuusjohtamista, sisäistä ja ulkoista seurantaa, järjestelmäarkkitehtuurin ja puolustuksen dynaamisuutta sekä analytiikka. Nämä kaikki ovat aineistossa esille nousseita tekijöitä, jotka mahdollistavat organisaation reagointi- ja toipumissuunnittelun kehittymisen. Nämä edistävät kyberturvallisuuden jatkuvaa kehitystä ja näin myös kyberresilienssiä, joka on välttämätöntä organisaatioiden toimintakyvyn säilyttämiselle digitalisaation neljännen aallon tuomien muutosten myötä.

Organisaatioiden ylimmältä johdolta vaaditaan kyberturvallisuuden käyttämien resurssien uudelleen allokointia, sillä kyberresilienssin kehityksen kannalta merkittävään reagointi- ja toipumissuunnitteluun menee NIST-kyberturvallisuusmallin mukaisesti vain neljäsosa, mikä ei riitä vastaamaan digitalisaation neljännen aallon tuomiin haasteisiin. Ylin johto on myös vastuussa siitä etteivät organisaation liiketoiminnalliset strategiat tai organisaatiopolitiikat ole ristiriidassa kyberturvallisuuden kanssa. Ylin johto on vastuussa kyberturvallisuutta tukevasta organisaatiokulttuurista ja ulkoisten sidosryhmien roolista kyberturvallisuuteen, joilla molemmilla on merkittävä rooli kyberresilienssin kehittymiselle.

Sisäisellä ja ulkoisella seurannalla tarkoitetaan organisaation sisäisen toiminnan valvomista sekä kybertoimintaympäristön tarkkailua ja datan keräämistä molemmista ympäristöistä. Kyberresilienssin kehittymisen kannalta on tärkeää, että organisaatio on tietoinen siitä, minkälaisessa kybertoimintaympäristössä se toimii, minkälaisia kyvykkyyksiä kyberturvallisuuden suhteen se omistaa ja minkälaisia haavoittuvuuksia organisaatiossa on. Sisäisessä seurannassa olennaisessa roolissa on testaaminen. Tätä voidaan penetraatiotestein harjoittaa järjestelmien lisäksi henkilöstöön kehityskohteiden löytämiseksi.

Mikään järjestelmä tai tietoverkko ei ole läpitunkeutumaton eikä tule sellaiseksi kehittymään digitalisaation neljännen aallon kasvavan linkittyneisyyden ja monimutkaisuuden takia. Tämän takia kyberturvallisuuden haasteita ei ole mahdollista ratkaista kaiken kattavalla kyberturvallisuusteknologialla. Tätä merkittävämpää on organisaation järjestelmäarkkitehtuurin suunnittelu organisaation liiketoiminalliset tavoitteet huomioiden yhdessä kyberturvallisuuden mahdollisimman tehokkaan, mutta dynaamisen implementoinnin kanssa. Järjestelmäarkkitehtuurissa tulee huomioida kerrostuneisuus, komponenttien linkittyneisyys ja hajauttaminen. Puolustusteknologiassa kirjallisuuden perusteella perinteiset IDPS-järjestelmät eivät ole menettäneet tehokkuuttaan, mutta ne vaativat jatkuvaa päivittämistä edistääkseen organisaation häiriöiden sietokykyä, mukautumista uudenlaisiin uhkiin ja kybertoimintaympäristön muutosten ennakointia.

Analytiikka on aina ollut suuri osa kyberturvallisuutta, sillä niin hyökkäys kuin puolustuskin perustuu tietoon vastapuolesta. Analytiikan avulla organisaatio voi hyödyntää sisäisellä ja ulkoisella seurannalla kerättyä informaatiota ja ohjata päätöksentekoa sekä kyberturvallisuuden kehitystä. Analytiikassa digitalisaation neljäs aalto tuo organisaatioille uusia mahdollisuuksia muun muassa koneoppimisalgoritmien, tekoälyn ja laskentatehon nousun avulla.

Tärkeimpänä päämääränä on kuitenkin kehittää organisaation reagointi- ja toipumissuunnittelua. Tähän organisaatio tarvitsee yhteistyötä sisäisiltä ja ulkoisilta sidosryhmiltä sekä kyberturvallisuuden alan ammattilaisten asiantuntijuutta. Huomionarvoista on, että myös reagointi- ja toipumissuunnitelmia on päivitettävä ja testattava jatkuvasti, jotta organisaation kyberresiienssiä voidaan ylläpitää jatkuvasti muuttuvassa kybertoimintaympäristössä.

6.2 Tutkimuksen arviointi ja jatkotutkimusehdotukset

Kirjallisuustutkimus antoi paljon uusia näkökulmia kyberturvallisuuden johtamiseen ja hallintaan. Oli yllättävää miten vähän yhteisiä linjauksia kyberturvallisuuden alalla vai-

kuttaa olevan kyberresilienssin kehityksen suhteen. Aihe on toisaalta hyvin tuore, sillä se on saanut suurta huomiota vasta viime aikoina pandemian ja 4.0-teknologioiden kehityksen myötä. Erityisen yllättävän miten vähän kyberresilienssin kehittämisessä huomioitiin kokonaisvaltaista organisaation resilienssiä ja systeemiajattelun periaatteita.

Tutkimuksessa haasteita toi muun muassa englanninkielinen aineisto, jonka suomentamisessa oli ajoittain suuria haasteita puuttuvien suomennosten takia. Lisäksi aineistossa saatettiin käyttää jo vakiintuneita käsitteitä ristiriitaisesti, joka teki välillä tulosten vertailusta haasteellista. Tämä vaikuttaa suoraan myös tutkimustulosten luotettavuuteen, sillä aineistosta tehdyt suomennokset eivät välttämättä ole täsmällisiä, yksiselitteisiä ja vertailtavia. Aineiston teknisen teorian takia on myös mahdollista, että sen tuloksista on tehty virheellisiä johtopäätöksiä, sillä sen täsmälliseen ja syvälliseen analysointiin olisi ollut tarvetta suuremmalle ammattitaidolle ja asiantuntijuudelle. Myös suhteellisen pieni vertaisarvioidun aineiston otanta vaikuttaa suoraan tulosten luotettavuuteen. Kuitenkin tutkimuksesta saatiin myös hyödynnettäviä tuloksia, jotka ottavat kantaa siihen mitä konkreettisia kehityskohteita organisaatioissa on kyberresilienssin kehittämiseksi. Tulokset vaativat kuitenkin suurempaa ja kattavampaa tarkastelua ennen kuin niitä voidaan suoraan hyödyntää kyberresilienssin kehittämiseksi.

Kyberturvallisuus on räjähdysmäisesti kasvava ala (Wong, 2017), joten tutkimusta alalla tullaan varmasti näkemään vielä paljon. Kirjallisuuden perusteella näkökulma perinteistä kyberturvallisuutta kohtaan on kokemassa muutosta ja resilienssin kehittymiseksi tämä on välttämätöntä. Todennäköisesti digitalisaation neljännen aallon tuomien trendien kasvaessa, kuten liitettävyyden ja automatisaation, tullaan näkemään enemmän tutkimusta aiheeseen kyberturvallisuuden näkökulmasta.

Kirjallisuuden perusteella kyberturvallisuuden alalla on puute yhteisymmärryksestä sen suhteen, mihin suuntaan alan tulisi kehittyä ja miten organisaatioiden tulisi kehittää kyberresilienssiä (Ferdinand, 2015). Tämän takia jatkotutkimusta voisi tehdä esimerkiksi eri kyberresilienssimallien ja -viitekehyksien arvioinnista, käytännön testaamista ja yhtenäistämisestä. Jatkotutkimuksien tarkoituksena voisi olla luoda organisaatioille helposti hyödynnettäviä NIST-mallin kaltaisia viitekehyksiä, jotka keskittyvät kyberresilienssin kehitykseen. Tämä voisi myös auttaa kyberturvallisuuden haasteisiin yhteisen kielen löytämisessä eri ammattilaisten ja sidosryhmien välillä yhteistyön kehittämiseksi.

Myös eri digitalisaation neljännen aallon tuomat 4.0-teknologiat vaativat jatkotutkimusta kyberturvallisuuden kannalta, sillä niiden ollessa yhä tiiviimmin liittyneitä yhteiskunnalle kriittiseen infrastruktuuriin niiden turvallisuus ja resilienssi on välttämätöntä. Monet 4.0 -

teknologiat eivät ole vielä saavuttaneet täyttä potentiaaliaan ja ovat vasta kehittymässä, joten niiden osalta kattavaa arviointia niiden kyberturvallisuudesta on tuskin mahdollista tehdä. Tästä esimerkki voisi olla kvanttitietokoneet. Tutkimus kyberresilienssiin tulee mahdollisesti lisääntymään tulevaisuudessa, kun 4.0-teknologioiden yleistyessä vaaditaan uusia lähestymistapoja organisaatioiden toimintakyvyn säilyttämiseksi.

LÄHTEET

Abraham, C. & Sims R. R. (2021) A Comprehensive Approach to Cyber Resilience. MIT Sloan management review. Vol.62 (4), p. 1-4.

Bécue, A., Praça, I. & Gama, J. (2021). Artificial Intelligence, cyber-threats and Industry 4.0: challenges and opportunities. The artificial Intelligence review. Vol.54 (5), p. 3849-3886. https://doi.org/10.1007/s10462-020-09942-2

Brennan, G., Joiner, K. & Sitnikova, E. (2019) Architectural choices for cyber resilience. Australian journal of multi-disciplinary engineering. Vol. 15 (1), p. 68-74. https://doi.org/10.1080/14488388.2019.1664210

Cambell, S. & Robert, E. (2020) The Need for Cyber Resilient Enterprise Distributed Ledger Risk Management Framework. The Journal of The British Blockchain Association. Vol.3 (1), p. 1-9. https://doi.org/10.31585/jbba-3-1-(5)2020

Carter, L. (2021). 10 Biggest cyber Attacks in History. Clear Insurance. Saatavilla: https://clearinsurance.com.au/10-biggest-cyber-attacks-in-history/ (26.3.2023)

Cimpanu, C. (2019) A decade of hacking: The most notable cyber-security events of the 2010s. ZDNET Special Feature: 2010s: The Decade Review. Saatavilla: https://www.zdnet.com/article/a-decade-of-hacking-the-most-notable-cyber-security-events-of-the-2010s/ (26.3.2023)

Coden, M., Reeves, M., Pearlson, K., Madnick, S. & Berriman, C. (2023) An Action Plan for Cyber Resilience. MIT Sloan management review. Vol.64 (2), p. 1-6.

Culot, G., Fattori, F., Podrecca, M. & Sartor, M. (2019). Addressing Industry 4.0 Cybersecurity Challenges. IEEE engineering management review. Vol.47 (3), p. 79-86. https://doi.org/10.1109/EMR.2019.2927559

Dietrich, S. (2017). Cybersecurity and the Future. Computer (Long Beach, Calif.). Vol.50 (4), p.7-7. https://doi.org/10.1109/MC.2017.114

Ducheck, S. (2020) Organizational resilience: a capability-based conceptualization. Vol. 12 (1), p.215-246. Business Research. https://doi.org/10.1007/s40685-019-0085-7

El-Kady Hamdy, A., Halim, S., El-Halwagi, M., M. & Khan, F. (2023). Analysis of safety and security challenges and opportunities related to cyber-physical systems. Process Safety ad Environmental Protection. Vol. 173, p. 384-413. https://doi.org/10.1016/j.psep.2023.03.012

Elsevier (2023). How Scopus works. Saatavilla: https://www.elsevier.com/solutions/scopus/how-scopus-works (6.5.2023).

Ferdinand, J. (2015). Building organizational cyber resilience: A strategic knowledge-based view of cyber security management. (2015). Journal of business continuity & emergency planning. Vol.9 (2), p.185-195.

Fluri, P. & Tagarev, T. (2020) The Concept of Resilience: Security Implications and Implementation Challenges. Connections: The quarterly journal. Vol.19 (3), p. 5-12. https://doi.org/10.11610/Connections.19.3.00

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. Internet of Things. Vol. 11, p.100-2024. https://doi.org/10.1016/j.iot.2020.100204

Hepfer, M. & Powell, T. C. (2020). Make Cybersecurity a Strategic Asset. MIT Sloan management review. Vol.62 (1), p. 40-45.

Juan, C., Arrizabalaga, S., Labaka, L. & Hernantes, J. (2020). Cyber Resilience Progression Model. Applied sciences. Vol.10 (21), p.73-93. https://doi.org/10.3390/app10217393

Lee, Y-I & Trim, P. (2022). Strategic Cyber Security Management. 1. painos. Taylor and Francis, Lontoo. 268 s.

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

Martin, D. (2021). CyRM: Mastering the Management of Cybersecurity. 1. painos. Taylor and Francis, Boca Raton. 146 s.

Mazzara, M., Bruel, J-M., Meyer, B. & Petrenko, A. (2019). Cyber-Resilience Concept for Industry 4.0 Digital Platforms in the Face of Growing Cybersecurity Threats. Software Technology: Methods and Tools. Vol. 11771, p.281-294. https://doi.org/10.1007/978-3-030-29852-4_23

National Institute of Standards and Technology (2016) Cybersecurity Framework. Päivitetty 4.19.2022. Saatavissa: https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide (6.3.2023).

National Institute of Standards and Technology (2009). About NIST. Päivitetty 1.11.2022. Saatavissa: https://www.nist.gov/about-nist (6.3.2023).

Pellegrino, S. (2022) The six biggest cyberattacks in history. TechMonitor. Päivitetty: 9.3. 2023. Saatavilla: https://techmonitor.ai/technology/biggest-cyberattacks-in-history#h-1-rockyou2021-the-biggest-password-leak-yet-2021 (26.3.2023)

Petrenko, S. (2019). Cyber Resilience. 1. painos. River Publishers, Gistrup. 494 s.

Ridout, T. (2016). Building a Comprehensive Strategy of Cyber Defense, Deterrence , and Resilience. The Fletcher forum of world affairs. Vol.40 (2), p. 63-83.

Sepúlveda Estay, D. A., Sahay, R., Barford, M. B. & Jensen, C. D. (2020) A systematic review of cyber-resilience assessment frameworks. Computers & Security. Vol. 97. https://doi-org.libproxy.tuni.fi/10.1016/j.cose.2020.101996

Steingartner, W., Galinec, D. & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. Symmetry (Basel). Vol13 (4), p.5-97. https://doi.org/10.3390/sym13040597

Tounsi, W. & Rais H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security. Vol.72, p. 212-233. https://doi.org/10.1016/j.cose.2017.09.001

Tran, H., Campos-Nanez, E., Fomin, P & Wasek, J. (2016). Cyber resilience recovery model to combat zero-day malware attacks. Computers & Security. Vol.61, p. 19-31. https://doi.org/10.1016/j.cose.2016.05.001

Turvallisuuskomitea (2018). Kyberturvallisuuden sanasto. Saatavissa: https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

Vaidya, J., Zhang, X. & Li, J. (2020). Main Enabling Technologies in Industry 4.0 and Cybersecurity Threats. Cyberspace Safety and Security. Vol.11983, p.588-597. https://doi.org/10.1007/978-3-030-37352-8_53

Winter, J. (2020). The evolutionary and disruptive potential of industry 4.0. Hungarian geographical bulletin. Vol.69 (2), p.83-97. https://doi.org/ 10.15201/hungeobull.69.2.1

Wong, A. (2017). Industry Insight: Cyber Resilience. The Australian Financial Review. Melbourne. p. 3.

Zou, B., Choobchian, P. & Rozenberg, J. (2021). Cyber resilience of autonomous mobility systems: cyber-attacks and resilience enhancing strategies. Journal of Transportation Security. Vol. 14 (3-4), p.137-155. https://doi.org/10.1007/s12198-021-00230-w

LIITTEET

Liite 1: Tutkimuksen vertaisarvioitu aineisto

	Strategic Management	System Architecture	System Defense Strategies	Risk Management	Resource Allocation	Analytics	Internal and External Monitoring	Respond and Recovery Capabilities	Testing
(Ferdinand, 2015)	X	X	X	X	X	X	X	X	X
(Hausken, 2020)	X				X				
(Campbell & Robert, 2020)	X	X	X	X	X		X	X	X
(Coden et al., 2023)	X	X	X	X	X	X	X	X	X
(Abraham & Sims, 2021)	X		X	X	X	X	X	X	X
(Brennan et al., 2019)	X	X	X	X			X	X	
(Tran et al., 2016)	X	X	X	X			X	X	
(Tounsi & Rains, 2018)		X			X				X
(Ridout, 2016)	X		X		X	X	X	X	X
(Hepfer & Powell, 2020)	X		X		X		X	X	
(Culot et al., 2019)	X	X	X		X		X	X	
(Lezzi et al., 2018)	X	X	X				X	X	X
(Juan et al., 2020)	X						X	X	X
(Fluri & Targarev, 2020)	X					X		X	X
(Steingartner et al., 2021)	X					X		X	X
(Bécue et al., 2021)	X		X			X	X	X	X
(Mazzara et al., 2019)							X	X	X
(Vaidya et al., 2020)	X	X	X			X	X	X	X
(Dietrich, 2017)		X						X	
(Wong, 2017)								X	
(El-Kady et al., 2023)	X	X	X		X	X	X	X	X
(Benz et al., 2020)		X	X				X	X	X
(Zou et al., 2021)		X	X					X	X
(Sepúlveda Estay et al., 2020)	X	X					X	X	X
Lukumäärä	18	14	15	6	10	9	17	22	17