TURUN YLIOPISTO
Kauppakorkeakoulu

Digitaalinen resilienssi kriittisen infrastruktuurin yrityksissä: digitaalisuuden merkitys häiriötilanteissa energiasektorilla

Tietojärjestelmätieteen
pro gradu -tutkielma

Laatija:
Niilo Tulkki

Ohjaaja:
KTT Jonna Järveläinen

26.8.2024
Turku

Pro gradu -tutkielma

Oppiaine: Tietojärjestelmätiede
Tekijä: Niilo Tulkki
Otsikko: Digitaalinen resilienssi kriittisen infrastruktuurin yrityksissä: digitaalisuuden merkitys häiriötilanteissa energiasektorilla
Ohjaaja: KTT Jonna Järveläinen
Sivumäärä: 90 sivua + liitteet 13 sivua
Päivämäärä: 26.8.2024

Tämä pro gradu -tutkielma käsittelee digitaalista resilienssiä kriittisen infrastruktuurin yrityksissä keskittyen erityisesti energiasektoriin. Tutkielmassa perehdytään digitaaliseen resilienssiin kriittisen infrastruktuurin näkökulmasta eli siihen, miten digitaaliset teknologiat ja tietojärjestelmät auttavat Suomen kriittisen infrastruktuurin kannalta keskeisiä energiasektorin yrityksiä selviytymään erilaisista häiriötilanteista. Tutkielmassa käsitellään myös sitä, minkälaiset tapahtumat voivat aiheuttaa näitä häiriötilanteita.

Tutkielman aihe on ajankohtainen, sillä yhteiskunta ja organisaatiot kohtaavat nykypäivänä yhä useammin erilaisia normaalia toimintaa häiritseviä tilanteita ja tapahtumia, joista merkittävimpiä esimerkkejä viime vuosilta ovat koronaviruspandemia sekä Ukrainan sota. Keskeistä on myös se, että digitalisaation seurauksena tietojärjestelmät ja digitaaliset teknologiat ovat yhä suuremmassa roolissa häiriötilanteiden ja kriisien selvittämisessä. Näin on myös kriittisen infrastruktuurin yrityksissä, joiden häiriötön toiminta on yhteiskunnan toimivuuden kannalta ensisijaisen tärkeää. Tutkielman tarkoituksena on selvittää miten nämä kriittisen infrastruktuurin yritykset käyttävät digitaalisuutta avuksi häiriötilanteiden hallitsemissa, ja mitä digitaalisia teknologioita ja tietojärjestelmiä tässä hyödynnetään. Tähän pyritään vastamaan seuraavien tutkimuskysymysten avulla: Mitä digitaalinen resilienssi on? Mistä digitaalinen resilienssi muodostuu kriittisen infrastruktuurin yrityksissä?

Aiempi digitaalista resilienssiä käsittelevä kirjallisuus on keskittynyt digitaalisen resilienssin määrittelyyn sekä sen kehittämiseen erityisesti koronaviruspandemiaan liittyen. Kriittisen infrastruktuurin yritysten kontekstissa aiempi tutkimus on vähäistä, eikä kattavaa tutkimusta siitä, miten digitaalinen resilienssi toteutuu, ja mistä se muodostuu kriittisen infrastruktuurin yrityksissä ole. Tutkielma pyrkii osaltaan täyttämään tätä tutkimusaukkoa. Tutkielman teoreettinen viitekehys on muodostettu aikaisemman digitaalista resilienssiä sekä kriittisen infrastruktuurin resilienssiä käsittelevän kirjallisuuden perusteella. Viitekehyksessä digitaalisen resilienssin muodostavat digitaaliset teknologiat ja tietojärjestelmät on jaoteltu resilienssin eri vaiheisiin, joita ovat häiriöiden ennakoiminen ja ennaltaehkäiseminen, häiriöistä selviytyminen ja palautuminen sekä niistä oppiminen ja toiminnan kehittäminen.

Tutkielma toteutettiin laadullisena tapaustutkimuksena, jonka aineisto on kerätty haastatteluiden avulla. Haastatteluja pidettiin seitsemän, ja niihin osallistui eri työtehtävissä toimivia henkilöitä vaihtelevilta energiasektorin aloilta, jotka on tutkielmassa jaoteltu sähköön, lämpöön ja kaasuun. Tutkielman empiirisen aineiston analysoiminen toteutettiin temaattisen analyysin avulla.

Tutkielman tulosten perusteella digitaalinen resilienssi on monipuolinen ilmiö, joka koostuu kriittisen infrastruktuurin yrityksissä useista eri digitaalisista teknologioista ja tietojärjestelmistä. Häiriötilanteiden ennakoimisessa ja ennaltaehkäisemissä keskeisimpään rooliin nousivat erilaiset valvontajärjestelmät sekä IoT-teknologia. Häiriöistä selviytymisessä ja palautumisessa digitaalisuudella on tärkeä rooli erityisesti tilannekuvan ylläpitämisessä ja päätöksenteon tukemisessa. Häiriötilanteista oppimisen ja toiminnan kehittämisen kannalta digitaalisuuden rooli korostui erityisesti kykynä kerätä ja analysoida suuria määriä dataa, jonka avulla voidaan esimerkiksi pyrkiä ennakoimaan tulevia häiriöitä.

Avainsanat: Digitaalinen resilienssi, kriittinen infrastruktuuri, kriittisen infrastruktuurin resilienssi

SISÄLLYS

KUVIOT

TAULUKOT

1 Johdanto

1.1 Tausta

Viime vuosina alkunsa saaneet kriisit, kuten koronaviruspandemia sekä Ukrainan sota ovat korostaneet yhteiskunnan ja organisaatioiden resilienssiä eli kykyä selviytyä ja palautua tällaisista yllättävistä ulkopuolisista tapahtumista ja häiriötekijöistä (Boh ym. 2023). Arvioiden mukaan vastaavien kriisien ja häiriöiden määrä tulee todennäköisesti lisääntymään, ja niiden vaikutukset laajenemaan 2020-luvun edetessä. Esimerkkejä tällaisista potentiaalisista häiriöistä, joiden vaikutukset yhteiskunnan ja organisaatioiden toimintaan voivat olla suuria ovat muun muassa energiatuotannon ongelmat, inflaation nousu, elinkustannusten liiallinen nousu ja lisääntyvät kyberhyökkäykset erityisesti kriittistä infrastruktuuria vastaan. (World Economic Forum 2023.)

Digitalisaation seurauksena internet, tietojärjestelmät ja digitaaliset teknologiat ovat nykypäivänä keskeinen osa eri organisaatioiden toimintaa, ja ne auttavat myös kohtaamaan ja selviytymään tällaisten häiriöiden aiheuttamia haasteista (Gkeredakis ym. 2021). Tietojärjestelmien ja erilaisten teknologioiden, kuten tekoälyn ja data-analytiikan tehokas hyödyntäminen onkin yhä suuremmassa roolissa tämän selviytymis- ja palautumiskyvyn kehittämisessä. Tätä vuorovaikutusta tietojärjestelmien hyödyntämisen ja resilienssin parantamisen välillä kuvaa uusi käsite: digitaalinen resilienssi (engl. digital resilience). (Tim & Leidner 2023.) Digitaalisella resilienssillä tarkoitetaan siis tiivistetysti organisaatioiden tietojärjestelmiä ja digitaalisia teknologioita käyttämällä saavutettavaa kykyä selviytyä, mukautua ja palautua ulkoisten tapahtumien aiheuttamista häiriöistä ja ongelmista (Boh ym. 2023). Koska tällaisten ulkoisten häiriöiden odotetaan lisääntyvän jatkossa, on digitaalinen resilienssi ja sen kehittäminen tärkeää monille eri organisaatioille.

Yhteiskunnan toimivuuden kannalta erityisen tärkeässä roolissa ovat kriittisen infrastruktuurin yritykset ja organisaatiot, jotka ylläpitävät yhteiskunnan elintärkeitä toimintoja (Laugé ym. 2015). Kriittisen infrastruktuurin toimijoiden on siis pystyttävä varmistamaan toimintansa jatkuvuus sekä ylläpitämään kriittiset toimintonsa myös ulkoisia häiriöitä ja ongelmatilanteita kohdatessa. Tietojärjestelmillä on merkittävä rooli käytännössä kaikkien kriittisen infrastruktuurin organisaatioiden toiminnassa, ja monet niistä toimivatkin pitkälti digitaalisessa ympäristössä (Alcaraz & Zeadally 2014). Myös

Suomen kriittinen infrastruktuuri on erittäin teknistä ja yhteiskunta pitkälti digitalisoitunut, ja siihen kohdistuvan uhan katsotaan kasvaneen (Yle 2022). Kriittisen infrastruktuurin järjestelmiä, jotka toimivat digitaalisessa ympäristössä ovat esimerkiksi sähkö- ja ydinvoimalaitosten hallintajärjestelmät, terveydenhuollon tietojärjestelmät sekä pankki- ja maksujärjestelmät (Valtioneuvosto 2023). Jotta kriittisen infrastruktuurin organisaatiot pystyvät selviytymään mahdollisimman hyvin ulkoisista häiriöistä, on digitaalinen resilienssi niille tärkeää (Fernandes ym. 2023). Huoltovarmuuskeskus A (2023) ohjeistaakin kriittisen infrastruktuurin yrityksiä muun muassa tarkistamaan kyberturvallisuuden suojaustoimenpiteet ja poikkeamanhallintakäytännöt varsinkin kriittisten ydintoimintojen osalta, sekä varmistamaan kriittisen toiminnan kannalta riittävät tietoliikenneyhteydet myös häiriötilanteissa.

Digitaalinen resilienssi on käsitteenä varsin uusi, joten suuri osa aiheeseen liittyvästä aikaisemmasta tutkimuksesta liittyy sen määrittelyyn ja pyrkii selventämään mitä kaikkea käsite pitää sisällään. Monet tutkimukset selventävät mitä digitaalisella resilienssillä tarkoitetaan, miten se ilmenee ja millaisilla keinoilla sitä voidaan kehittää. (Boh ym. 2023, Dupin ym. 2023, Tim & Leidner 2023.) Useat aikaisemmat tutkimukset käsittelevät myös digitaalista resilienssiä Covid-19-pandemiaan liittyen, keskittyen siihen miten ja minkälaisia digitaalisia teknologioita erilaiset organisaatiot hyödynsivät selvitäkseen ja pystyäkseen jatkamaan toimintaansa pandemian aikana (Abidi ym. 2023, Gkeredakis ym. 2021, Tim ym. 2023). Kriittisen infrastruktuurin yritysten osalta digitaalista resilienssiä on tutkittu vain vähän, mutta esimerkiksi Fernandes ym. (2023) ovat tehneet aiheesta systemaattisen kirjallisuuskatsauksen. Aikaisempaa laadullista haastattelututkimusta ei kuitenkaan ole.

Digitaalinen resilienssi on käsitteenä uudehko, eikä siitä ole tehty vielä riittävästi tutkimusta, joten lisätutkimukselle on selkeä tarve. Pursiaisen (2017) mukaan Suomella on muiden pohjoismaiden ohella paremmat lähtökohdat kriittisen infrastruktuurin resilienssin parantamiseen kuin suurimmalla osalla muista Euroopan maista, minkä takia aiheen tutkiminen juuri Suomassa toimivissa kriittisen infrastruktuurin yrityksissä on kannattavaa. Vaikka nykyajan digitalisoituneessa yhteiskunnassa digitaalisen resilienssin merkitys on epäilemättä suuri ja sen kehittäminen tärkeää kriittisen infrastruktuurin yrityksissä, on aiheesta olemassa vain vähän aikaisempaa tutkimusta. Tutkimusta siitä, miten Suomessa toimivat kriittisen infrastruktuurin yritykset

varautuvat ennakoimattomiin tapahtumiin, ja miten niistä selviydytään digitaalisia teknologioita käyttämällä, ei ole juurikaan. On siis olemassa tutkimusaukko, jonka tutkielma pyrkii täyttämään syventämällä aikaisempaa tutkimustietoa kirjallisuuden ja haastatteluiden avulla. Tutkielma pyrkii selventämään millaisten ennakoimattomien tapahtumien aiheuttamien haasteiden kanssa kriittisen infrastruktuurin yritykset kamppailevat, ja miten niistä voidaan selvitä digitaalisen resilienssin avulla.

1.2 Tutkimuskysymykset

Tutkielman tavoitteena on selvittää miten digitaalinen resilienssi näkyy kriittisen infrastruktuurin yritysten toiminnassa eli miten ne voivat varautua ja selviytyä ennakoimattomista tapahtumista sekä häiriötekijöistä hyödyntämällä tietojärjestelmiä ja digitaalisia teknologioita – ja mitä nämä tähän tarkoitukseen käytettävät teknologiat ja tietojärjestelmät ylipäätään ovat. Koska digitaalinen resilienssi on uusi tutkimusalue, tutkielma selventää ja konkretisoi mitä digitaalinen resilienssi tarkoittaa käytännössä ja millaisista elementeistä se muodostuu. Tutkielmassa paneudutaan myös siihen, millaisia häiriötilanteita kriittisen infrastruktuurin yritykset kohtaavat ja minkälaiset tapahtumat voivat aiheuttaa niitä. Kriittinen infrastruktuuri muodostuu monesta eri osasta, kuten energian tuotannosta, tieto- ja viestintäjärjestelmistä sekä vesi- ja jätehuollosta, mutta tutkielmassa keskitytään erityisesti energiasektorin yrityksiin, jotka muodostavat yhden yhteiskunnan toimivuuden kannalta tärkeimmistä kriittisen infrastruktuurin aloista.

Tutkielman tutkimuskysymykset ovat:

Mitä digitaalinen resilienssi on?

Mistä digitaalinen resilienssi muodostuu kriittisen infrastruktuurin yrityksissä?

Ensimmäiseen tutkimuskysymykseen etsitään vastausta pääosin aikaisemman tieteellisen tutkimuksen avulla, ja sitä käsitellään erityisesti tutkielman kirjallisuuskatsausosiossa aikaisemman kirjallisuuden perusteella. Tutkielman varsinainen päätutkimuskysymys on *mistä digitaalinen resilienssi muodostuu kriittisen infrastruktuurin yrityksissä*, johon paneudutaan tarkemmin tutkielman empiriaosuudessa haastatteluilla kerätyn tutkimusaineiston pohjalta. Tutkielma pyrkii näin syventämään tietämystä siitä, mistä digitaalinen resilienssi muodostuu kriittisen infrastruktuurin yrityksissä ja millaisia digitaalisia teknologioita ja tietojärjestelmiä tähän käytetään. Tutkimus selventää siis millaisista elementeistä digitaalinen resilienssi koostuu näissä

energiasektorin yrityksissä. Koska aikaisempi tutkimus digitaaliseen resilienssiin liittyen on keskittynyt erityisesti Covid-19-pandemiaan ja sen aiheuttamiin haasteisiin, on myös oleellista selvittää minkälaisia muita häiriöitä energiasektorin yritykset kohtaavat, ja mitkä tapahtumat voivat aiheuttaa niille häiriötilanteita sekä miten niistä voidaan selviytyä digitaalisuuden avulla.

Tutkielma pyrkii vastaamaan tutkimuskysymykseen aikaisemman digitaaliseen resilienssiin ja kriittisen infrastruktuurin liittyvän kirjallisuuden ja tutkimustiedon, sekä erillisten haastatteluiden avulla. Tavoitteena on, että haastatteluiden avulla saadaan erityisesti tietoa siitä millaisia ongelmia nämä kriittisen infrastruktuurin yritykset kohtaavat tai valmistautuvat kohtaamaan, ja kuinka digitaaliset ratkaisut auttavat tässä varautumisessa sekä häiriöistä selviytymisestä ja palautumisessa.

1.3 Tutkielman rakenne

Tutkielman alkuvaiheessa johdantoa seuraavissa luvuissa 2 ja 3 tutustutaan aikaisempaan digitaalista resilienssiä ja kriittisen infrastruktuurin resilienssiä käsittelevään tieteellisen tutkimukseen kirjallisuuskatsauksen muodossa. Luku 2 keskittyy digitaaliseen resilienssiin, sen määritelmään ja ominaisuuksiin, ja tämän lisäksi luvun alussa käsitellään lyhyesti resilienssiä yleisemmällä tasolla. Luku 3 käsittelee resilienssin merkitystä tarkemmin juuri kriittisen infrastruktuurin näkökulmasta. Lisäksi siinä käydään läpi myös aikaisemmassa tutkimuksessa tunnistettuja uhkia kriittiselle infrastruktuurille ja sen resilienssille. Tämän luvuissa 2 ja 3 käsitellyn aikaisemman tieteellisen kirjallisuuden avulla muodostetaan myöhemmin metodologialuvussa esiteltävä viitekehys, jonka perusteella tutkielman empiirinen osuus toteutetaan. Luku 4 on tutkielman metodologialuku, jossa esitellään tutkielmassa käytetyt tutkimusmenetelmät sekä perustelut niiden valinnoille ja annetaan lisätietoa aineistonkeruusta, sen analysoinnista sekä tutkimusprosessin etenemisestä. Tutkielman tulokset esitellään luvussa 5. Tutkielman tulosten perusteella tehdyt johtopäätökset käydään läpi luvussa 6, jossa pyritään myös vastaamaan tutkielman päätutkimuskysymykseen. Lopuksi luku 7 sisältää tutkielman yhteenvedon sekä muutamia jatkotutkimusehdotuksia, joiden jälkeen tulevat vielä tutkielmassa käytetyt lähteet sekä tutkielman liitteet.

2 Digitaalinen resilienssi

2.1 Resilienssi yleisesti

Resilienssillä on perinteisesti tarkoitettu aineen, henkilön tai järjestelmän kykyä kestää, mukautua ja palautua yllättävistä iskuista (Comfort ym. 2010). Resilienssin kattava määritteleminen on kuitenkin haastavaa, sillä se esiintyy monissa eri muodoissa eikä sille ole vain yhtä yleisesti hyväksyttyä määritelmää. Sen sijaan resilienssillä on useita erilaisia merkityksiä, jotka vaihtelevat asiayhteydestä riippuen. Resilienssi on myös hyvin monitieteellinen käsite, joka on esiintynyt useilla eri aloilla (Lee ym. 2023). Nykytutkimuksessa resilienssin käsite onkin omaksuttu esimerkiksi ekologiassa, sosiologiassa, psykologiassa ja taloustieteessä (Schemmer ym. 2021) – sekä erityisesti viime vuosina resilienssin käsitettä on tutkittu laajalti myös tietojärjestelmätieteessä.

Resilienssin käsitettä alettiin alun perin edistämään erityisesti ekologiassa (Boh ym. 2023). Ekologi Holling (1973) määrittelee resilienssin ekologisen järjestelmän vahvuutena, joka lisää sen selviytymiskykyä. McAslanin (2010) mukaan resilienssi modernina tieteellisenä käsitteenä perustuukin pitkälti Hollingin (1973) edellä mainittuun määritelmään, ja hänen tutkimukseensa resilienssistä ekologisen järjestelmän ominaisuutena.

Pariès ym. (2013) esittelevät laajalle levinneen resilienssin määritelmän, jonka mukaan resilienssi tarkoittaa järjestelmän sisäistä kykyä sopeuttaa toimintaansa muutoksia tai häiriöitä ennen, niiden aikana taikka niiden jälkeen, jotta se pystyy ylläpitämään välttämättömät toimintonsa sekä oletetuissa että ennakoimattomissa olosuhteissa. Myös Hollnagelin (2009) mukaan resilientti järjestelmä pystyy tämän sopeutumiskyvyn avulla jatkamaan vaadittua toimintaansa häiriöiden tai vakavien onnettomuuksien jälkeen ja jatkuvan rasituksen alaisena. Euroopan komissio (2012) sen sijaan näkee resilienssin ennemminkin yhteiskunnallisesta kuin teknologisesta näkökulmasta: heidän mukaansa resilienssi tarkoittaa yksilön, kotitalouden, yhteisön, maan tai alueen kykyä kestää, mukautua ja toipua nopeasti iskuista ja rasituksesta.

Resilienssiin kuuluu olennaisena osana sen hyväksyminen, etteivät kaikki tapahtumat ole ennakoitavissa, vaan odottamattomia asioita tulee aina tapahtumaan (Wied ym. 2019). Myös Hollnagelin ym. (2006) mukaan resilienssin keskiössä on erityisesti odottamattomista ja yllättävistä tapahtumista selviytyminen ja kyky vastata nopeasti

tällaisiin tapahtumiin muun muassa tehokkaan tiedonvälityksen sekä resurssien oikea-aikaisen käyttämisen avulla. Heidän mukaansa resilienssiin kuuluu myös kyky ennakoida ja torjua tällaiset tapahtumat vastaavien keinojen avulla. Lisäksi resilienssi kuvaa miten organisaation tulisi hallita toimintojaan pystyäkseen ennakoimaan ja kiertämään organisaation olemassaoloa tai tavoitteita vaarantavia uhkia (Hollnagel ym. 2006).

Comfortin ym. (2010) mukaan resilienssiin kuuluu myös se, että tapahtumasta selvittyään resilientillä henkilöllä, yhteisöllä tai järjestelmällä on aiempaa parempi valmius estää ja selvitä vastaavista tapahtumista tulevaisuudessa. Vastaavasti Hollnagelin ym. (2006) mukaan ulkoisen tapahtuman aiheuttaman iskun kestämisen lisäksi myös kyky mukautua tästä seuranneisiin vaikeuksiin ja ongelmiin on oleellinen osa resilienssiä. Tähän mukautumiskykyyn on viitattu palautumisena joko entiseen tai optimitilanteessa entistä parempaan olotilaan (Woods 2015). Onnistuakseen tässä palautumisessa on pystyttävä toimimaan huomattavasti erilaisessa toimintaympäristössä, ja myös aikaisempien toimintojen ja prosessien on mukauduttava tähän muuttuneeseen ympäristöön (Boh ym. 2023).

Sen lisäksi, ettei resilienssille ole vain yhtä yleistä määritelmää, on sille myös useita eri alakategorioita (Schemmer ym. 2021). Näitä ovat esimerkiksi organisaation resilienssi, toimitusketjujen resilienssi, kyberresilienssi sekä digitaalinen resilienssi, johon tämä tutkielma keskittyy.

2.2 Digitaalisen resilienssin määritelmä

Digitaalinen resilienssi on käsitteenä melko uusi, eikä sille ole vain yhtä selkeää ja yleisesti hyväksyttyä määritelmää. Mehedintu ja Soava (2022) kertovat digitaalisen resilienssin olevan monen eri tekijän yhteistyön summa. Timin ja Leidnerin (2023) mukaan digitaalisen resilienssin käsite onkin edelleen kehittyvä, ja vain harvat aikaisemmista tutkimuksista ovat ylipäätään määritelleet sitä. Heidän mukaansa selkeän ja yhteneväisen määritelmän puuttuminen aiheuttaa haasteita tällä vielä kehittyvällä tutkimusalalla. Koska digitaalisen resilienssin määritelmä ei ole täysin selkeä ja toisistaan poikkeavia näkemyksiä esiintyy, määritellään digitaalinen resilienssi seuraavaksi mahdollisimman kattavasti.

Bohin ym. (2023) mukaan digitaalinen resilienssi viittaa organisaation digitaalisia teknologioita hyödyntämällä luotuun kykyyn selvitä ulkoisten tapahtumien aiheuttamista haitoista ja mukautua näistä tapahtumista aiheutuneisiin häiriöihin. Ulkoisten ja usein ennakoimattomien tapahtumien aiheuttamista iskuista pyritään siis selviytymään nopeasti tietojärjestelmien suunnittelun, kehittämisen ja käyttämisen avulla (Boh ym. 2020). Tämän lisäksi organisaatioiden kyky muuntautua ja kehittää toimintaansa ollakseen jatkossa entistä valmiimpia kohtaamaan ennakoimattomien ulkoisten tapahtumien aiheuttamia häiriöitä on oleellinen osa digitaalista resilienssiä (Boh ym. 2023).

Pohjautuen muun muassa Comfortin ym. (2010) esittämään perinteiseen resilienssin käsitteeseen, Tim ja Leidner (2023) viittaavat digitaalisella resilienssillä tietojärjestelmien ja resilienssin väliseen vuorovaikutukseen. He määrittelevät digitaalisen resilienssin yksilöiden, organisaatioiden ja yhteisöjen kyvyksi palautua ulkoisista iskuista ja häiriöistä tietojärjestelmien suunnittelemisen, kehittämisen ja käytön avulla. He jakavat tämän vielä tarkemmin siihen millaisia ominaisuuksia ja kyvykkyyksiä tulee olla, jotta pystytään suorittamaan tiettyjä tietojärjestelmien suunnitteluun, kehittämiseen ja käyttöön liittyviä toimintoja, jotka tukevat tätä palautumisprosessia. Vastaavasti myös Cuelin ym. (2022) mukaan digitaalisen resilienssin käsite viittaa tietojärjestelmien suunnitteluun ja käyttöön tarkoituksenaan auttaa yksilöitä, organisaatioita, yhteisöjä tai vastaavia palautumaan nopeasti häiriöistä tai ulkoisten tapahtumien aiheuttamista iskuista.

Myös poikkeavia digitaalisen resilienssin määritelmiä kuitenkin on. Kumarin ym. (2023) mukaan digitaalinen resilienssi viittaa organisaation kykyyn kestää ja palautua kyberhyökkäyksistä, tietomurroista ja muista vastaavista digitaalisessa ympäristössä tapahtuvista häiriöistä. Tremblay ym. (2023) taas määrittelevät digitaalisen resilienssin organisaation kyvyksi hyödyntää dataa, teknologiaa sekä analytiikkaa ennustaakseen, palautuakseen ja oppiakseen ennakoimattomien tapahtumien aiheuttamista iskuista. Näistä määritelmistä hieman poiketen, Parkin ym. (2023) mukaan digitaalinen resilienssi tarkoittaa IT:n käyttöä, hallinnointia sekä siihen investoimista tavalla, joka antaa organisaatiolle mahdollisuuden tuottaa korkealaatuisia palveluita ja ylläpitää asiakastyytyväisyyttä kriisin tai häiriön aikana vastaavalla tasolla kuin normaalisti.

Taulukko 1. Digitaalisen resilienssin määritelmiä

Lähde	Määritelmä
Boh ym. (2023)	Digitaalisia teknologioita hyödyntämällä luotu kyky selvitä ulkoisten tapahtumien aiheuttamista haitoista ja mukautua näistä tapahtumista aiheutuneisiin häiriöihin.
Kumar ym. (2023)	Organisaation kyky selvitä ja palautua digitaalisessa ympäristössä tapahtuvista häiriöistä.
Liu ym. (2023)	Tietojärjestelmien suunnittelu, käyttöönottaminen ja käyttö häiriöiden estämiseksi, vastustamiseksi ja niistä palautumiseksi.
Park ym. (2023)	Investointi IT:hen, sen käyttö ja hallinnointi, jotta voidaan mahdollistaa korkealaatuisten palveluiden tarjoaminen ja asiakastyytyväisyyden ylläpitäminen kriisitilanteessa normaaleja olosuhteita vastaavalla tasolla.
Tim & Leidner (2023)	Yksilöiden, organisaatioiden ja yhteisöjen kyky palautua ulkoisista iskuista ja häiriöistä tietojärjestelmien suunnittelemisen, kehittämisen ja käytön avulla.
Trembaly ym. (2023)	Organisaation dynaaminen kyky käyttää dataa, teknologiaa ja analytiikka ennakoidakseen, palautuakseen ja oppiakseen iskusta.

Aikaisemmasta kirjallisuudesta kerättyjä toisistaan eroavia digitaalisen resilienssin määritelmiä on kerätty taulukkoon 1. Digitaalisen resilienssin lisäksi on olemassa toinen hieman vastaava termi, tietojärjestelmien resilienssi (engl. IS resilience), jotka saatetaan helposti sekoittaa keskenään. Nämä käsitteet ovat hyvin lähellä toisiaan, ja tietojärjestelmien resilienssi on otettava huomioon, jotta digitaalinen resilienssi on mahdollista saavuttaa (Schemmer ym. 2021). Heeksin ja Ospinan (2019) mukaan tietojärjestelmän resilienssi on yleisesti määritelty itse tietojärjestelmän kyvyksi selvitä ja jatkaa toimintaansa siihen kohdistuneesta ulkoisesta iskusta huolimatta. Digitaalinen resilienssi taas mahdollistaa resilienssin tavoittelemisen kyseistä tietojärjestelmää käyttävälle organisaatiolle.

2.3 Digitaalinen resilienssi yleisesti

Timin ym. (2023) mukaan monet viimeaikaiset tapahtumat poliittisesta epävarmuudesta pandemiaan ovat korostaneet lisääntynyttä riippuvuuttamme tietojärjestelmistä, joiden avulla pystytään vastaamaan tällaisiin ulkoisten tapahtumien aiheuttamiin haasteisiin. Maailmanlaajuisten häiriöiden yleistyessä, kyvykkyys kestää ja mukautua häiriöitä aiheuttaviin tapahtumiin sekä muuttuvaan toimintaympäristöön on nykypäivänä erittäin tärkeää organisaation kestävyyden ja toiminnan ylläpitämisen kannalta (Pan ym. 2022). Timin ym. (2023) mukaan digitaalinen resilienssi on yksi tämän kyvykkyyden tärkeimmistä edellytyksistä, ja organisaatioiden kyky selvitä lisääntyneestä

epävarmuudesta sekä erilaisista teknologisista, taloudellisista ja geopoliittisista haasteita pohjautuu pitkälti digitaaliseen resilienssiin.

Digitaalinen resilienssi eli kyky ennakoida ja selviytyä ulkoisten tapahtumien aiheuttamista ongelmista tietojärjestelmiä ja digitaalisia teknologioita hyödyntämällä on kriittisen tärkeää sekä yksilöille että organisaatioille (Tim ym. 2023). Sen tavoitteena on minimoida organisaation kohtaamat häiriöt ja ylläpitää toiminta vakaana. Lisäksi tavoitteena on mukautua uusiin vallitseviin olosuhteisiin ja kehittyä uuteen vahvempaan olotilaan. (Tim & Leidner 2023.) Organisaatiot ja ihmiset ovatkin jatkuvasti enenevissä määrin riippuvaisia digitaalisesta teknologiasta, eikä tähän ole tiedossa muutosta (Cuel ym. 2022). Tim ja Leidner (2023) korostavat tietojärjestelmien hyödyntämisen suurta merkitystä häiriöistä selviytymisessä ja palautumisessa. Ihmiset ja organisaatiot eivät välttämättä ole aina tietoisia siitä, kuinka laajasti ne ovat digitaalisten teknologioiden varassa, mutta Cuel ym. (2022) esittävät, että tarve digitaaliselle resilienssille on suurempi kuin koskaan.

Aikaisemmin tietojärjestelmien on koettu lisäävän organisaatioiden haavoittuvuutta ja monimutkaisuutta, mikä voi aiheuttaa erilaisia ongelmia (Beese ym. 2016). Sakurain ja Chughtain (2020) mukaan nykyään on kuitenkin selvää, että tietojärjestelmien avulla voidaan parantaa merkittävästi organisaatioiden ja yhteiskunnan kykyä selvitä ulkoisten tapahtumien aiheuttamista haasteista. Timin ja Leidnerin (2023) mukaan tietojärjestelmiä ja digitaalisia teknologioita ei pitäisi kuitenkaan pitää automaattisesti vastauksena kaikkiin mahdollisiin kriiseihin ja häiriöihin, sillä se johtaa helposti nopeiden ja tilapäisten digitaalisen ratkaisujen tekemiseen sekä harkitsemattomien digitaalisten strategioiden toteuttamiseen. Lisäksi vaikka digitaalisten teknologioiden avulla pystytään parantamaan organisaation kykyä vastata häiriöihin tai onnettomuuksiin, voivat ne myös luoda uusia teknologisia riskejä (Spagnoletti & Za 2022).

Li ym. (2023) pitävät digitaalista resilienssiä merkittävänä ajurina yritysten menestykselle nykypäivän digiaikana, ja sitä tulisi kehittää yrityksen tai organisaation toiminnan parantamiseksi. Heidän mukaansa yritykset, jotka tiedostavat digitaalisen resilienssin merkityksen ja joilla on siihen liittyvä selkeä strategia, voivat näin parantaa merkittävästi kilpailukykyään ja kyvykkyyttä selvitä erityisesti digitaalisista häiriöistä. Digitaaliset teknologiat ovat merkittävä osa yritysten ja organisaatioiden jokapäiväistä

toimintaa, ja ne toimivat perustana haasteista selviytymisessä, muutoksiin mukautumisessa ja jatkuvassa kehityksessä häiriöiden vallitessa (Tim ja Leidner 2023). Digitaalinen resilienssi on yrityksille arvokas ja joskus myös harvinainen resurssi, joka voi myös luoda yrityksille kilpailuetua (Li ym. 2023).

Nykyään yksilöt, organisaatiot ja hallitukset ovat riippuvaisia digitaalisesta teknologiasta ja infrastruktuurista, ja erilaisten toisiinsa yhteydessä olevien laitteiden ja sensoreiden määrä on niin suuri, että digihankkeiden merkitys resilienssille on korvaamaton. Monet organisaatiot ovatkin käynnistäneet hankkeita, joiden avulla pyritään selvittämään kuinka digitaalisia teknologioita voidaan hyödyntää kriiseistä ja häiriöistä selviytymisessä. (Boh ym. 2020.) Digitaalisten työkalujen, kuten tekoälyn ja data-analytiikan tehokas hyödyntäminen on Timin ja Leidnerin (2023) mukaan edellytys resilienssin saavuttamiselle. Tietojärjestelmiin liittyvällä tehokkaalla suunnitelulla ja niiden käyttöönotolla ei ole tärkeää roolia vain arvon luomisessa kuten usein ajatellaan, vaan niillä on yhtä lailla tärkeä rooli resilienssin rakentamisessa. Organisaation kyky hyödyntää merkityksellisiä IT-resursseja tukeakseen organisaation häiriöistä selviytymiseen ja palautumiseen liittyviä toiminta mahdollistaa resilienssin saavuttamisen. (Tim & Leidner 2023.)

2.4 Teknologioiden ja tietojärjestelmien rooli digitaalisessa resilienssissä

Digitalisaation seurauksena ulkoisista tapahtumista seuranneista iskuista ja häiriöistä selviytyminen edellyttää entistä enemmän tietojärjestelmien ja digitaalisten teknologioiden, kuten esimerkiksi data-analytiikan ja tekoälyn tehokasta hyödyntämistä (Gkeredakis ym. 2021). Tällaisten teknologioiden avulla pystytään esimerkiksi havaitsemaan häiriöiden syntyminen ja puuttumaan niihin entistä nopeammin (Tim & Leidner 2023). Tietotekniikan kehittymisen myötä organisaatioiden kyky selvitä ulkoisista häiriöistä on parantunut merkittävästi. Digitaalisten teknologioiden nopean kehittäminen ja käyttöönotto voivat mahdollistaa esimerkiksi tuotteiden ja palveluiden monipuolistamisen, liiketoimintamallien mukauttamisen ja resurssien tehokkaamman sijoittamisen, ja näillä kyvyillä katsotaan olevan kriittinen rooli resilienssin rakentamisessa. (Boh ym. 2023.)

Tietojärjestelmiä ja erilaisia digitaalisia teknologioita, joiden avulla resilienssiä voidaan vahvistaa on lukuisia (Schemmer ym. 2021). Digitaalisten teknologioiden hyvä

saatavuus ja tärkeä rooli lähes kaikessa organisaatioiden toiminnassa ovat muuttaneet huomattavasti sitä, kuinka organisaatiot pystyvät mukautumaan ja selviämään ulkoisten tapahtumien aiheuttamista häiriöistä. Erilaisia digitaalisia teknologioita hyödyntämällä voidaankin siis kehittää organisaatioiden resilienssiä merkittävästi. Nykypäivänä datan ja erilaisten digitaalisten teknologioiden rooli on kriittinen, ja useiden organisaatioiden toiminta on niistä riippuvaista. Tämän kasvavan ja entistä kriittisemmän roolin seurauksena digitaaliset teknologiat, joita voidaan käyttää datan keräämiseen ja analysoimiseen, ovat oleellinen osa organisaatioiden resilienssin kehittämistä, sillä ne auttavat esimerkiksi hallitsemaan tähän tarvittavaa tietoa. Digitaalisten teknologioiden ominaisuudet mahdollistavat organisaatioille monenlaisia mahdollisuuksia resilienssin eri osa-alueiden kehittämiseen. (Boh ym. 2023.)

Monissa organisaatioissa otettiin käyttöön uusia digitaalisia teknologioita resilienssin parantamiseksi erityisesti Covid-pandemian seurauksena (Boh ym. 2023). Pandemian aikana tietojärjestelmiä pystyttiin hyödyntämään taudin torjumisessa monin eri keinoin, mikä korosti niiden merkitystä useiden organisaatioiden resilienssin parantamisessa (Schemmer 2021). Käytössä olevia teknologioita oli useita erilaisia, kuten tartuntaketjujen seuraamiseen käytettävät sovellukset, jotka hyödynsivät muun muassa bluetooth-teknologiaa, GPS:ää ja QR-koodeja (Min-Allah ym. 2021). Lisäksi tietojärjestelmien avulla pystyttiin parantamaan yhteiskunnan ja organisaatioiden resilienssiä korona-aikana esimerkiksi verkko-oppimisen (engl. e-learning) (Almaiah ym. 2020) sekä erilaisten etätyöskentelyn mahdollistavien teknologioiden avulla (Kylili ym. 2020). Georgen ym. (2020) mukaan juuri Covid-pandemia onkin muuttanut organisaatioiden digitaalista infrastruktuuria perusteellisesti sekä nopeuttanut digitaalisten teknologioiden ja pilvisovellusten käyttöönottoa. Heidän mukaansa uusien teknologioiden kehittäminen ja käyttöönotto ovat siis kiihtyneet huomattavasti pandemian aikana ja sen seurauksena.

Digitaalisen resilienssin kehittäminen on kuitenkin mahdollista myös monien muiden digitaalisten teknologioiden avulla. Tällaisia teknologioita ovat esimerkiksi esineiden internet (engl. Internet of Things, IoT) ja erilaiset sensorit, joiden avulla voidaan kerätä ja tuottaa tietoa, sekä data-analytiikka ja pilvipohjaiset tietojärjestelmät. (Boh ym. 2023.) Datan kerääminen ja analysoiminen voivat esimerkiksi auttaa havaitsemaan mahdolliset uhat ja häiriöt tehokkaammin (Xu ym. 2019). Lisäksi digitaalisen resilienssin saavuttamisessa voidaan hyödyntää tietokantoja, digitaalista infrastruktuuria

ja älykkäitä algoritmeja. Koska datan merkitys on nykypäivänä niin suuri, digitaalisista teknologioista, joiden avulla voidaan kerätä ja analysoida dataa on tullut luontainen työkalu tiedon keräämiseen mahdollisiin häiriöihin liittyen sekä resilienssin kehittämiseen. On kuitenkin myös oleellista huomioida, ettei näitä teknologioita ole välttämättä otettu käyttöön vain digitaalisen resilienssin saavuttamiseksi, vaan niillä on usein myös muita merkittäviä tehtäviä, kuten toimintojen ylläpitäminen ja tehokkuuden edistäminen. (Boh ym. 2023.)

Bohin ym. (2023) mukaan yksi merkittävä digitaalisten teknologioiden ominaisuus, joka auttaa organisaatioita parantamaan resilienssiään, on niiden älykäs mittaus- ja havaitsemiskyky. Tästä esimerkkinä on älykkäiden algoritmien hyödyntäminen analytiikassa ja päätöksenteon tukena. Tremblayn ym. (2023) mukaan tällaiset älykkäät mittaus- ja havaitsemisteknologiat tukevat harkittujen päätösten tekemistä epävarmassa toimintaympäristössä. Tätä näkemystä tukevat myös Spagnoletti ja Za (2022), jotka kertovat digitaalisten teknologioiden parantavan digitaalista resilienssiä erityisesti tukemalla päätöksentekoa sekä yhteistyötä ja toiminnan koordinointia. Digitaalisten teknologioiden jatkuvasti kehittyvä analytiikkaominaisuus mahdollistaa toimintaympäristön muutosten tarkkailun sekä datan keräämisen, varastoinnin ja analysoimisen (Yoo 2010). Näitä ominaisuuksia on käytetty esimerkiksi mobiililaitteita hyödyntävissä seuranta-applikaatioissa (Boh ym. 2023).

Vaddadin ym. (2023) mukaan myös tekoälyn ja koneoppimisen avulla voidaan parantaa organisaatioiden digitaalista resilienssiä sekä kyberturvallisuutta merkittävästi. Heidän mukaansa koneoppimisella ja tekoälyllä on ensisijaisen tärkeä rooli digitaalisen resilienssin vahvistamisessa, sillä niiden avulla pystytään havaitsemaan mahdollisia uhkia tehokkaasti sekä nopeuttamaan kyberhyökkäyksien torjumista ja lieventämään niiden haitallisia vaikutuksia. Tekoälyyn perustuvat järjestelmät auttavat tunnistamaan ja ennakoimaan erilaisia uhkia kyberturvallisuudelle, ja koneoppiminen mahdollistaa lyhyemmän vasteajan kyberhyökkäyksiä vastaan. Tämä on erityisen tärkeää, sillä nykyisessä digitaalisessa ympäristössä kyberhyökkäykset ovat entistä yleisempiä ja kehittyneempiä, ja datan suojaaminen sekä digitaalisen resilienssin vahvistaminen vaatii uusia keinoja. Tekoälyn ja koneoppimisen avulla voidaan siis vahvistaa organisaatioiden digitaalista resilienssiä ja parantaa kriittisen infrastruktuurin suojausta. Niiden tehokas käyttäminen digitaalisen resilienssin parantamiseksi edellyttää kuitenkin yhteistyötä eri sidosryhmien välillä. (Vaddadi ym. 2023.)

Vaikka digitaaliset teknologiat ovatkin nykyään helpommin saatavilla, organisaatioiden on oltava valmiita tekemään muutoksia toimintaansa pystyäkseen hyödyntämään näitä teknologioita mahdollisimman hyvin. Organisaatiot, jotka ovat varautuneita tekemän nopeitakin muutoksia esimerkiksi toimintaprosesseihin tai henkilöstöön liittyen, ja joiden digitaalinen osaaminen on korkealla tasolla, pystyvät hyödyntämään digitaalisia teknologioita kaikkein tehokkaimmin. Toimintaympäristön muutokset edellyttävät usein organisaatioita hyödyntämään olemassa olevia teknologioita uudella tavalla tai yhdistelemään eri teknologioita keskenään selviytyäkseen ja palautuakseen ulkoisesta häiriöstä (Boh ym. 2023). Tässä auttaa esimerkiksi järjestelmien modulaarisuus, joka helpottaa toiminnallisten muutosten tekemistä, jolloin järjestelmiä voidaan siten käyttää helpommin erilaisiin tarkoituksiin. Modulaarisuus helpottaa siis digitaalisten teknologioiden konfiguroimista uusiin käyttötarkoituksiin. (Yoo ym. 2010.) Bohin ym. (2023) mukaan tämä mahdollisuus käyttää digitaalisia teknologioita tarvittaessa uudenlaisiin tarkoituksiin on tärkeä osa digitaalisen resilienssin kehittämistä. Digitaalisten teknologioiden käyttäminen uudella poikkeavalla tavalla voi kuitenkin olla myös haitaksi. Muutokset digitaalisiin teknologioihin tulisi tehdä huolellisesti ja keräämällä aktiivisesti tietoa jatkoa varten. Näin organisaatio ymmärtää kuinka digitaalisia teknologioita voidaan käyttää mahdollisimman tehokkaasti tulevista häiriöistä selviämiseen. (Boh ym. 2023.)

2.5 Digitaalisen resilienssin kehittämisen edellytykset

Boh ym. (2023) esittelevät digitaalisen teknologian ominaisuuksia ja olosuhteita, joita tarvitaan organisaation digitaalisen resilienssin kehittämiseksi. Esimerkiksi IT-resurssien saatavuus, vallitsevat toimintatavat sekä IT:n hallinnointi muokkaavat organisaation kykyä selvitä kriiseistä tietojärjestelmien hyödyntämisen avulla. Digitaalinen resilienssi ei kuitenkaan koostu vain olemassa olevien avujen ja kykyjen hallitsemisesta, vaan siihen kuuluu myös uusien kykyjen ja taitojen käyttöönottaminen kriisejä tai häiriöitä kohdatessa. (Tim & Leidner 2023). Ottaakseen vastaan ennakoimattomien tapahtumien aiheuttamia iskuja, oleellisia digitaalisten teknologioiden ominaisuuksia ovat niiden monipuolisuus eli se, että on useita eri vaihtoehtoja jatkuvuuden varmistamiseksi, sekä jatkuva datan kerääminen ja analysointi iskujen ennakoimista ja kestämistä varten. Mukautuakseen iskusta seuranneisiin uusiin olosuhteisiin, organisaation on pystyttävä reagoimaan häiriöihin nopeasti sekä opittava, kehitettävä ja otettava käyttöön uusia teknologioita tarvittaessa nopeallakin aikataululla.

Myös iskuista toipuminen ja organisaation muutos entistä resilientimmäksi edellyttävät digitaalisten teknologioiden hyödyntämistä. Tässä muutos- ja kehitysprosessissa oleellisia ominaisuuksia digitaalisten teknologioiden kannalta ovat niiden modulaarisuuden ja uudelleenjärjestettävyyden hyödyntäminen sekä digialustojen skaalautuvuus. (Boh ym. 2023.) Modulaarisuuden avulla voidaan varmistaa se, että kehitettävän järjestelmän eri osia pystytään päivittämään itsenäisesti ilman, että se vaikuttaa koko järjestelmän toiminnallisuuteen (Tim ym. 2023).

Bohin ym. (2023) mukaan organisaatiossa tulisi olla tietynlaiset olosuhteet, jotta digitaalista resilienssiä voidaan kehittää mahdollisimman hyvin. Selvitäkseen ulkoisten tapahtumien aiheuttamista iskuista organisaation on oltava hyvin koordinoitu ja yhteistyön toimittava läpi organisaation. Sisäisten toimintojen optimoimisen, mahdollisten ylimääräisten resurssien tunnistamisen ja uudelleen sijoittamisen sekä resurssien nopean hyödyntämisen tulisi olla oleellinen osa koko organisaation toimintaa. Myös tiedonhallinnalla (engl. Data governance) on oleellinen merkitys resilienssin kehittämisessä, sillä sen avulla voidaan parantaa eri yksiköiden välistä luottamusta, jota tarvitaan datan tehokkaaseen hyödyntämiseen. Muuttuneisiin olosuhteisiin mukautuminen edellyttää teknologioiden tehokasta hyödyntämistä ja saattaa vaatia organisaation sisäisiä uudelleenjärjestelyitä. Jotta resilienssin rakentaminen onnistuu ja pystytään mukautumaan muuttuneisiin olosuhteisiin, olisi organisaatiossa Bohin ym. (2023) mukaan myös hyvä vallita mukautuva ja positiivinen ilmapiiri, jossa ollaan avoimia kokeilemaan uusia toimintatapoja. Mehedintun ja Soavan (2022) mukaan digitaalinen resilienssi onkin sosio-tekninen käsite eli se pitää sisällään teknologian lisäksi myös ihmiset. Jotta organisaatio pystyy muuttumaan entistä resilientimmäksi, tulisi uusien teknologioiden vaikutuksia olemassa oleviin ja mahdollisiin tuleviin liiketoimintamalleihin pystyä arvioimaan, sekä kehittämään strategia, joka mahdollistaa vahvemman resilienssin tulevaisuuden iskuja ja häiriöitä varten (Boh ym. 2023).

Digitaalisen teknologioiden ominaisuudet mahdollistavat organisaatioiden digitaalisen resilienssin kehittämisen. Bohin ym. (2023) mukaan näiden ominaisuuksien pitäisi kuitenkin olla olemassa jo ennen häiriötä, jotta organisaatio voi ottaa iskun vastaan, mukautua siihen ja muuttaa tarvittaessa toimintaansa. Tämän takia organisaatioiden tulisi valmistautua tähän jo ennen häiriötä. Heidän mukaansa on siis tarpeen suunnitella digitaalisen resilienssin rakentamista jo etukäteen, jotta ennakoimattomien tapahtumien häiriöt pystytään kestämään. Tarkkaa tietoa siitä, kuinka tämä valmistautuminen tulisi

suorittaa kaikkein tehokkaimmin ei ole, mutta Bohin ym. (2023) mukaan tämän valmistautumisprosessin on oltava jatkuva.

Se kuinka hyvällä tasolla digitaalinen resilienssi on organisaatiossa riippuu sen kyvystä järjestellä resurssinsa, osaamisensa ja teknologiansa tavalla, joka auttaa sitä selviytymään tietystä häiriöstä tai kriisistä. Digitaalinen resilienssi ei siis tarkoita vain tiettyjen kykyjen omaamista, vaan siitä kuinka laajasti näytä kykyjä pystytään hyödyntämään kriiseistä ja häiriöistä palautumisessa, esimerkiksi myöhemmin käsiteltävien jatkuvuuden, mukautumisen tai kehittämisen osalta. (Tim & Leidner 2023.) Mehedintun ja Soavan (2022) mukaan digitaalisen resilienssin rakentaminen edellyttää organisaatioilta digitaaliseen transformaatioon ja digitaalisiin innovaatioihin keskittyvää strategiaa.

Erilaiset iskut ja kriisit aiheuttavat organisaatioille monenlaisia haasteita (Tremblay ym. 2023). Kriisit voivat olla akuutteja tai pitkäaikaisia, ja digitaaliselta resilienssiltä vaaditaan näissä hieman erilaisia asioita. Akuutit kriisit, jotka voivat johtua esimerkiksi luonnonkatastrofeista tai organisaation sisäisistä hätätapauksista edellyttävät nopeaa ja tehokasta päätöksentekoa, jolla voidaan minimoida vahingot sekä palauttaa organisaation normaali toiminta (Kotlarsky ym. 2020). Tällaisissa tapauksissa digitaalisen resilienssin kannalta oleellisinta on kyky palautua häiriöstä ja jatkaa normaalia toimintaa mahdollisimman nopeasti (Tim & Leidner 2023). Pitkäaikaisemmat kriisit kuten ilmastonmuutoksen aiheuttamat ongelmat ja geopoliittinen epävarmuus edellyttävät jatkuvaa ja strategisempaa lähestymistä resilienssiin. Tämä korostaa organisaation kykyä kestää pidempiaikaisia häiriöitä samalla vahvistaen kykyä selviytyä mahdollisista uusista häiriöistä. Se mitä digitaalisen resilienssin rakentaminen näihin pidempikestoisiin kriiseihin edellyttää, ja kuinka organisaatiot voivat ylläpitää digitaalista resilienssiään sekä äkillisissä että pitkäkestoisissa kriiseissä edellyttävät Timin ja Leidnerin (2023) mukaan vielä enemmän tutkimusta.

Digitaalinen resilienssi ei ole täysin muuttumaton ominaisuus, vaan se kehittyy ajan kuluessa (Tim & Leidner 2023). Kriisin aikana käyttöönotetut tietojärjestelmät tai digitaaliset teknologiat voivat auttaa luomaan uusia toimintamalleja, jotka auttavat organisaatiota selviytymään uusista kriiseistä tai häiriöistä jatkossa (Floetgen ym. 2021). Strategiat ja käytännöt tietojärjestelmien suunnitteluun ja käyttöönottoon liittyen voivat myös vaihdella kriisin eri vaiheissa (Liu ym. 2023).

Nykyajan digitaalisessa yhteiskunnassa, jossa erilaiset häiriöt ovat yleisiä, digitaalinen resilienssi on Timin ja Leidnerin (2023) mukaan edellytys menestymiselle eikä ainoastaan selviytymiselle. He toivovatkin, että jatkossa ei keskityttäisi enää siihen kuinka vaikeuksista voidaan vain selvitä, vaan siihen miten kriisien jälkeen pystytään kehittymään entistä paremmaksi digitaalisen resilienssin avulla.

2.6 Ulkoisista iskuista ja häiriöistä selviytyminen digitaalisen resilienssin avulla

Yksi digitaalisen resilienssin ominaispiirteistä on, että se keskittyy erityisesti ulkoisten tapahtumien aiheuttamiin iskuihin ja niistä selviytymiseen (Tim & Leidner 2023). Carugati ym. (2020) kuvaavat näitä ulkoisia iskuja tapahtumiksi, joiden todennäköisyys on pieni, mutta seuraukset voivat olla erittäin laajat ja vakavat. Ne ovat siis poikkeuksellisia tapahtumia, jotka voivat aiheuttaa merkittävän uhan organisaation toiminnalle. Nämä iskut voivat olla esimerkiksi luontoon tai teknologiaan liittyviä taikka taloudellisia tai geopoliittisia. Digitaalinen resilienssi kiteyttää siis millaisia tietojärjestelmiin liittyviä ilmiötä tällaisiin iskuihin ja shokkeihin liittyen esiintyy. Tämä sisältää esimerkiksi millaisia tietojärjestelmien suunnitteluperiaatteita ja käyttöönottostrategioita, joiden tavoitteena on palautua näistä iskuista, on olemassa. (Tim & Leidner 2023.) Mangalarajin ym. (2022) mukaan IT:llä onkin kriittinen rooli resilienssin rakentamisessa sekä erityisesti odottamattomista tapahtumista ja häiriöistä selviytymisessä.

Timin ja Leidnerin (2023) mukaan onnistunut ulkoisista iskuista palautuminen tapahtuu jatkuvuuden *(engl. continuity*), mukautumisen (*engl. adaptation)* ja/tai kehittämisen (*engl. advancement*) kautta, ja digitaalinen resilienssi muodostuu pitkälti näistä osa-alueista. Jatkuvuuden ominaispiirre on vankkuus häiriöitä ja iskuja kohdatessa sekä vakaan tilan ylläpitäminen myös kriisitilanteissa. Jatkuvuudella ja resilienssillä onkin siis selvä yhteys (Liu ym. 2023). Jatkuvuuteen liittyen resilienssi nähdään organisaation välttämättömien toimintojen turvaamisena kriisin aikana, tavoitteena minimoida sidosryhmien kohtaamat häiriöt (Carugati ym. 2020). Tällainen resilienssi voi ilmetä kahdella eri tavalla: Ensinnäkin on mahdollista, että isku tapahtuu, mutta se ei juurikaan haittaa organisaation normaaleja toimintoja korostaen näin organisaation selviytymiskykyä (Duchek 2020). Tällaisessa tapauksessa resilienssi näkyy siten,

etteivät iskujen haittavaikutukset pääse toteutumaan (Darkow 2019). Toiseksi on myös tapauksia, joissa iskuilla on merkittäviä seurauksia, mutta resilienssi näkyy siinä, miten organisaatio pystyy palautumaan nopeasti takaisin normaaliin tilaansa (Heeks & Ospina 2018). Digitaalisen resilienssin käsite kattaa siis sen, kuinka tehokkaasti organisaatio pystyy saavuttamaan tällaisen jatkuvuuden tietotekniikkaa hyödyntämällä (Tim & Leidner 2023).

Jatkuvuuden ylläpitämisen ja normaaliin tilaan palaamisen lisäksi mukautuminen eli kyky kehittää ja luoda uusia käytäntöjä sopeutuakseen muuttuneisiin olosuhteisiin on oleellinen osa resilienssiä (Duchek 2020). Mukautuminen tarkoittaa olemassa olevien toimintatapojen muokkaamista ja uusien kehittämistä tietojärjestelmien ja digitaalisen teknologioiden avulla, jotta organisaatio pystyy vastaamaan kriisistä tai häiriöistä seuranneisiin uudenlaisiin tarpeisiin ja vaatimuksiin (Tim & Leidner 2023).

Kolmas digitaalisen resilienssin osa-alue eli kehittäminen tuo esiin resilienssin organisaatiota uudistavan puolen (Tim & Leidner 2023). Kehittämisestä oleellista on se, ettei tavoitteena ole palata aikaisempaan tilaan tai luoda vain hetkellisiä ratkaisuja, vaan pystyä luomaan kestävä, uusi olotila (Floetgen ym. 2021). Tämä digitaalisen resilienssin organisaation kehittämiseen keskittyvä osa-alue on näkynyt erityisesti Covid-pandemian aikana, kun organisaatiot ovat luoneet uusia digitaalisia toimintatapoja selviytyäkseen pandemian aiheuttamasta kriisistä, jotka ovat myös jääneet osaksi normaalia toimintaa (Tim & Leidner 2023).

Tremblayn ym. (2023) mukaan organisaation kyky hyödyntää sen dataresursseja ja rakentaa digitaalista resilienssiä määrittelevät, kuinka hyvin se pystyy selviämään ulkoisten tapahtumien aiheuttamista iskuista. Datan oikeanaikaisen saatavuuden varmistaminen on tärkeää, jotta ennakoimattomasta tapahtumasta johtunut isku pystytään ottamaan onnistuneesti vastaan. Tämä auttaa päätöksentekijöitä tarkkailemaan organisaation toimintaympäristöä ja yhdistelemään eri lähteistä peräisin olevaa dataa, mikä auttaa selviytymään tällaisesta iskusta. (Tremblay ym. 2023.) Heidän mukaansa data toimii tärkeimpänä digitaalisen resilienssin rakennusaineena, mutta ongelmana on kuitenkin usein datan kerääminen ja sen integrointi eri lähteistä. Datan vaihtaminen toisen organisaation kanssa vaatii luottamuksen luomista organisaatioiden välillä. Näihin datan jakamiseen liittyvien ongelmien selvittäminen vaatii yhteistyötä tekevien

toimijoiden välisen luottamuksen ja suhteen kehittämistä tiedonhallinnan rakenteiden avulla. (Tremblay ym. 2023.)

Kriisitilanteet ja ennakoimattomat tapahtumat tulevat usein yllättäen, ja resilienssin kehittäminen nopeasti on haastavaa. Siksi ensimmäinen askel tällaisesta tapahtumasta selviytymiseen ja digitaalisen resilienssin saavuttamiseen on usein tukeutuminen olemassa oleviin järjestelmiin ja muihin digitaalisiin resursseihin. (Lee ym. 2023.) Organisaatiot voivat mukautua ulkoisten tapahtumien aiheuttamiin häiriöihin ja reagoida niihin nopeasti valmiiksi käytettävissä olevien teknologioiden ja järjestelmien avulla, jotka ovat lähes kaikessa toiminnassa läsnä (Boh ym. 2023). Näiden järjestelmien muokkaaminen on myös usein mahdollista, jolloin niiden normaalien käyttötarkoitusten lisäksi niitä voidaan usein muokata tukemaan myös kriisin hallintaan tarvittavia toimintoja ilman merkittäviä teknisiä muutoksia. (Lee ym. 2023.) On kuitenkin myös mahdollista, että ulkoiset tapahtumat aiheuttavat järjestelmille liian äkillisiä ja merkittäviä haittoja (Tim ym. 2023). Silloin olemassa olevat järjestelmät ja teknologiat saattavat olla riittämättömiä selviytymään toiminnoista, joita vaaditaan tapahtumasta selviytymiseen (Fogli ym. 2017). Tästä seuraa usein tarve uusien tietojärjestelmä- ja teknologiaratkaisujen kehittämiselle (Tim ym. 2023). Kohdatessaan merkittävän ulkoisen häiriön organisaatioissa ymmärretään usein kuinka toimintaan on tehtävä merkittäviä muutoksia. Tällaisten muutoksien tekeminen ei kuitenkaan välttämättä onnistu pelkillä pienillä korjauksilla, vaan voi vaatia perusteellisempia muutoksia esimerkiksi organisaation rakenteisiin tai toimintatapoihin. (Boh ym. 2023.)

Mukautuakseen ulkoisten tapahtumien aiheuttamiin häiriöihin, organisaatiot kokeilevat usein uusia palveluita ja tuotteita erilaisten ketterien menetelmien, kuten DevOpsin tai Scrumin avulla. Häiriöiden aiheuttamasta epätietoisuudesta ja tarpeesta uusien teknologioiden käyttöönottamiseen johtuen organisaatioiden ei ole aina helppo tietää kuinka parhaiten selviytyä häiriöistä, joten tällainen eri vaihtoehtojen kokeilu on hyödyllistä. (Boh ym. 2023.) Bohin ym. (2023) mukaan kykyjä ottaa ennakoimattoman tapahtuman aiheuttama isku vastaan ja mukautua sen takia muuttuneeseen toimintaympäristöön, sekä iskun jälkeistä muuntautumiskykyä ei välttämättä tarvitse pyrkiä kehittämään peräkkäin, vaan niiden kehittäminen tapahtuu usein päällekkäin. Heidän mukaansa eri tahot saattavat lisäksi keskittyä erityisesti yksittäiseen resilienssin osa-alueeseen eli panostaa esimerkiksi kykyyn ottaa isku vastaan ja jättää muut osa-alueet vähemmälle huomiolle. Digitaalisen resilienssin kehittämisprosessi vaihtelee siis

eri organisaatioiden välillä, ja siihen vaikuttaa muun muassa käytössä olevien digitaalisen teknologioiden ominaisuudet tai organisaatiossa vallitsevat olosuhteet digitaalisen resilienssin rakentamiselle.

3 Kriittisen infrastruktuurin resilienssi

3.1 Kriittisen infrastruktuurin perusteet

Kriittisellä infrastruktuurilla tarkoitetaan yhteiskunnan elintärkeiden toimintojen ylläpitämisen kannalta välttämättömiä perusrakenteita ja palveluita, kuten esimerkiksi energiantuotannon järjestelmiä, tieto- ja viestintäjärjestelmiä sekä terveydenhuoltoa. Kriittinen infrastruktuuri muodostuu fyysisten laitosten ja rakenteiden lisäksi myös digitaalisista toiminnoista sekä palveluista. Suomessa valtaosa kriittisestä infrastruktuurista kuuluu yksityiselle sektorille. (Huoltovarmuuskeskus A 2023.)

Kriittisen infrastruktuurin toiminta on yhteiskunnalle niin tärkeää, että näihin palveluihin kohdistuvalla häiriöllä voi olla merkittävä vaikutus muun muassa kansalliseen turvallisuuteen, taloudelliseen hyvinvointiin tai kansalaisten terveyteen (Alcaraz & Zeadally 2014). Kriittistä infrastruktuuria löytyy modernin yhteiskunnan eri alueilta, eikä se siis ole vain tietyn organisaation, yrityksen tai järjestelmän vastuulla. Sen sijaan useat eri kriittisen infrastruktuurin organisaatiot ja järjestelmät vastaavat näistä kriittisistä tuotteista ja palveluista. (Nan & Sansavini 2015.) Luonteensa vuoksi on erityisen tärkeää, että kriittisen infrastruktuurin organisaatioilla ja järjestelmillä on olemassa keinoja, joiden avulla ne voivat käsitellä niihin kohdistuvia riskejä, vaaroja ja haavoittuvuuksia (Lichte ym. 2022).

Suomessa kriittisen infrastruktuurin suojaamisesta vastaavat organisaatiot ja yritykset itse. Kriittisen infrastruktuurin yritykset voivat ulkoistaa suojaamiseen tai ylläpitämiseen liittyvien palvelujen toteutuksen, mutta ovat kuitenkin itse siitä vastuussa. (Huoltovarmuuskeskus A 2023.)

3.2 Resilienssin merkitys kriittiselle infrastruktuurille

Nyky-yhteiskunta on hyvin pitkälti riippuvainen kriittisen infrastruktuurin tarjoamista korkeaa elämänlaatua ylläpitävistä palveluista, kuten energiatuotannosta, tietoliikenneyhteyksistä ja terveydenhuollosta (Katina ym. 2014, Ouyang ym. 2012). Tämän takia on äärimmäisen tärkeää, että kriittisen infrastruktuurin järjestelmien ja toimijoiden resilienssi on korkealla tasolla sekä tapaturmaisia että tahallisesti aiheutettuja häiriöitä vastaan. Niillä on siis oltava kyky välttää toimintahäiriöitä tai

palauttaa niiden normaali toiminta nopeasti tällaisia tapahtumia kohdatessa. (McDaniels ym. 2008.)

Kriittiseen infrastruktuurin toiminnan estyminen tai pahimmassa tapauksessa sen tuhoutuminen aiheuttaisi suurta vahinkoa ihmisten terveydelle ja turvallisuudelle, joten niiden saatavuus ja toiminta on pystyttävä varmistamaan yhtäjaksoisesti (Nan & Sansavini 2017). Koska yhteiskunnan hyvinvointi on siis pitkälti riippuvainen kriittisen infrastruktuurin kunnollisesta toiminnasta, kriittiseen infrastruktuuriin kohdistuvat häiriöt tai kriisit voivat olla todella haitallisia (Labaka ym. 2015). Tästä johtuen kriittinen infrastruktuuri on altis monenlaisille uhille, joiden vaikutukset voivat olla suuria (Brucherseifer ym. 2021). Mahdollisten kriisien ja häiriöiden lisääntyessä, resilienssin merkitys kasvaa. Kriittisen infrastruktuurin resilienssin tulee olla erinomaisella tasolla, jotta se pystyy vastaamaan näihin uhkiin. (Fernandes ym. 2023.) Kriittisen infrastruktuurin toiminnan turvaaminen ja sen resilienssin kehittäminen onkin erityisen tärkeää. (Labaka ym. 2015.) Alkhaleelin (2024) mukaan kriittisen infrastruktuurin elintärkeä rooli korostaa tarvetta uusien työkalujen ja teknologioiden käyttämiselle parhaan mahdollisen resilienssin tavoittamiseksi.

Tilanteessa, jossa kriittinen infrastruktuuri tai sen osa joutuu kriisitilaan ja sen normaali toiminta estyy joudutaan suorittamaan aikaa ja resursseja vaativia hätätoimenpiteitä, jotta pystytään palauttamaan se takaisin normaaliksi (Nieuwenhuijs ym. 2008). Kriittisen infrastruktuurin puutteellisen toiminnan vaikutuksia voidaan mitata esimerkiksi sen keston osalta, taloudellisten menetysten määrältä, sen vaikutusalueen laajuudelta tai sen vaikutuksen alaisten ihmisten lukumäärän osalta (Curt & Tacnet 2018). Jotta kriittisestä infrastruktuurin resilienssiä voidaan parantaa, kriittisestä infrastruktuurista vastaavien yritysten ja organisaatioiden tulee sijoittaa sekä ihmis- että pääomaresursseja luodakseen prosesseja häiriöiden välttämiseen, niiden vaikutusten minimoimiseen ja niistä palautumiseen (Fernandes ym. 2023).

Aikaisemmin pääpaino on ollut kriittisen infrastruktuurin suojaamisessa (engl. critical infrastructure protection), mutta viime vuosien aikana on sen sijaan alettu painottaa kriittisen infrastruktuurin resilienssiä. Tämä johtuu pääosin siitä, että on ymmärretty kriittisen infrastruktuurin täydellisen suojauksen takaamisen mahdottomuus. Tästä huolimatta sekä kriittisen infrastruktuurin suojaamiselle että sen resilienssille on kuitenkin olemassa tarve, eikä kumpaakaan näistä tule laiminlyödä. (Pursiainen 2017.)

3.3 Kriittisen infrastruktuurin resilienssin määritelmä

Kriittisen infrastruktuurin resilienssin määrittelyssä ei ole samanlaisia merkittäviä eroavaisuuksia kuin digitaalisen resilienssin käsitteen kanssa, jota käsiteltiin luvussa 2.2. Vaikka kriittisen infrastruktuurin eri sektorit toimivat eri tavalla, NIAC:n (2009) mukaan kriittisen infrastruktuurin resilienssille voi silti olla yksi yhteinen määritelmä. He esittelevätkin yhden ensimmäisistä määritelmistä, jonka mukaan kriittisen infrastruktuurin resilienssi tarkoittaa kykyä vähentää häiriöitä aiheuttavien tapahtumien vaikutuksien laajuutta ja kestoa kriittisen infrastruktuurin organisaatioissa ja järjestelmissä. Kriittisen infrastruktuurin järjestelmän tai yrityksen resilienssi on riippuvainen sen kyvystä ennakoida, kestää, mukautua ja palautua mahdollisesti vahingollisesta tapahtumasta. Kyky kestää häiriöitä ja haitallisia tapahtumia tarkoittaa organisaation tai järjestelmän kykyä kestää häiriö ilman, että se vaikuttaa merkittävästi normaaliin suoritustasoon. Mukautumiskyky viittaa siihen, että häiriöön pystytään sopeutumaan ja ylläpitämään normaalia toimintaa myös muuttuneissa olosuhteissa. Palautumiskyky taas tarkoittaa järjestelmän tai organisaation kykyä palautua häiriöstä nopeasti ja mahdollisimman pienin kuluin. (NIAC 2009.)

Kriittisen infrastruktuurin kontekstissa resilienssi kuvaa kykyä jatkaa välttämättömien palvelujen tuottamista luotettavasti ja ilman – tai mahdollisimman pienin – keskeytyksin erilaisia häiriöitä kohdatessa. Tämän lisäksi siihen kuuluu kyky palauttaa täysi toiminnallisuus iskun jälkeen. (Ouyang ym. 2012, Ouyang & Wang 2015.) Myös Labaka ym. (2015) määrittelevät kriittisen infrastruktuurin resilienssin järjestelmän kyvyksi estää kriisin tapahtuminen ylipäätään, tai kriisin tapahtuessa kyvyksi ottaa sen aiheuttama isku vastaan ja palata takaisin normaaliin tilaan tehokkaasti. Kriittisen infrastruktuurin osalta resilienssi keskittyy ennaltaehkäiseviin, lieventäviin ja valmiutta parantaviin toimiin ennen kriisin tai häiriön tapahtumista, sekä myös toimiin kriisin aikana. Lisäksi palautuminen kriisistä tai muusta tapahtumasta, joka on häirinnyt kriittisen infrastruktuurin toimintaa kuuluu resilienssiin. (Pursiainen 2017.) Jos kriittisen infrastruktuurin resilienssi on korkealla tasolla, on kohdatuista häiriöistä mahdollista oppia, ja sitten tehdä muutoksia vallitseviin toimintatapoihin tai teknologioihin ollakseen jatkossa entistä paremmin valmistautunut kohtaamaan uusia häiriöitä (Rehak ym. 2019).

Kriittisen infrastruktuurin järjestelmien resilienssi voidaan Rehakin ym. (2018) mukaan nähdä ominaisuutena, joka vähentää sen haavoittuvuutta, minimoi erilaisten uhkien ja vaarojen vaikutuksia, parantaa uhkiin vastaamista ja niistä toipumista sekä edistää vahingollisiin tapahtumiin mukautumista. Heidän mukaansa resilienssi edustaa kriittisen infrastruktuurin kontekstissa erityisesti osajärjestelmien sisäistä varautumista haitallisiin tapahtumiin. Näiden järjestelmien tulee siis olla kykeneviä suoriutumaan tehtävistään ja ylläpitämään toimintaansa huolimatta ulkoisten tai sisäisten tekijöiden aiheuttamasta haitasta. He pitävät resilienssiä eräänlaisena haavoittuvuuden vastakohtana.

3.4 Kriittisen infrastruktuurin resilienssin osa-alueet

Hollnagelin (2009) mukaan kriittisen infrastruktuurin järjestelmien ja organisaatioiden resilienssi perustuu pitkälti neljään kulmakiveen. Ensimmäinen näistä on kyky vastata pysyviin sekä yllättävästi syntyneisiin häiriöihin, keskeytyksiin ja muutoksiin. Toisena on kyky monitoroida ja valvoa järjestelmän tilaa teknisen ja inhimillisen suoriutumisen osalta sekä valvoa ympäristön olosuhteita erityisesti niiden muutosten osalta, jotka vaikuttavat suorituskyvyn vaatimuksiin. Tämä mahdollistaa potentiaalisten vaarojen havaitsemisen sekä kehittyvien uhkien tunnistamisen. Kolmas keskeinen kyky on pystyä ennakoimaan tulevia sekä positiivisia että haitallisia tapahtumia, jotka vaikuttavat järjestelmän suoriutumiseen. Myös uusien mahdollisuuksien etsiminen on tärkeää, jotta toimintaa voidaan kehittää. Neljäntenä kulmakivenä on kyky oppia menneistä tapahtumista, jotta voidaan laajentaa ja parantaa käytössä olevaa osaamismallia. Lichten ym. (2022) mukaan pelkästään näiden neljän kyvyn olemassaolo ei kuitenkaan vielä sellaisenaan riitä halutun resilienssin saavuttamiseksi. Heidän mukaansa on lisäksi pystyttävä löytämän operatiivisesti toteuttamiskelpoisia ratkaisuja näiden kykyjen saavuttamiseksi sekä koordinoida niiden käyttöä ottaen huomioon myös niiden väliset riippuvuudet ja vuorovaikutukset sekä tulevat olosuhteet. Heidän mukaansa ei siis tulisi keskittyä ainoastaan resilienssin mahdollistavien kykyjen olemassaoloon, vaan panostaa myös niiden operatiiviseen hallitsemiseen.

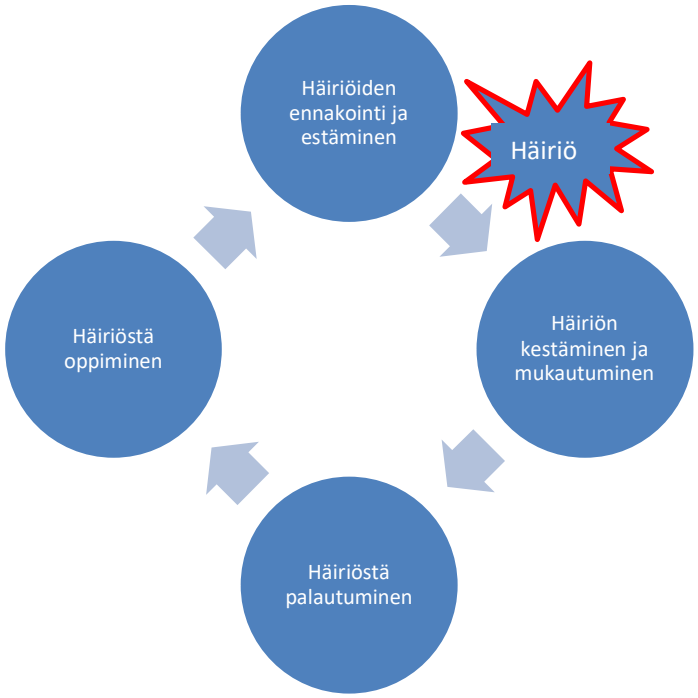
Petit ym. (2013) jakavat aikaisemmin luvussa 3.3 käsitellyt NIAC:n (2009) esittelemät kriittisen infrastruktuurin resilienssin kannalta oleelliset kyvyt eli häiriöiden tai haitallisten tapahtumien ennakoimisen, kestämisen, niihin mukautumisen ja niistä palautumisen neljään ryhmään. Nämä ryhmät ovat varautuminen (engl. preparedness), vaikutusten lieventämistoimenpiteet (engl. mitigation measures), vastauskyky (engl.

response capabilities) ja palautumismekanismit (engl. recovery mechanisms). Varautumisella viitataan toimintoihin, joita suoritetaan uhkien ja vaarojen sekä niiden mahdollisten seurausten ennakoimiseksi. Varautuminen voidaan jakaa vielä kahteen osaan, jotka ovat tietoisuuden parantaminen ja suunnittelu. Tietoisuuden parantamisen eteen tehtyjä toimia ovat muun muassa tiedon jakaminen ja erilaisten menetelmien käyttäminen mahdollisten luonnollisten tai ihmislähtöisten vaarojen ennakoimiseksi. Suunnitteluun liittyviä toimia taas ovat esimerkiksi hätätilanteiden toimintasuunnitelmien tekeminen ja jatkuvuuteen liittyvät toimet, kuten jatkuvuudenhallintasuunnitelmien luominen. Vaikutusten lieventämistoimenpiteet kuvaavat kykyä vastustaa uhkaa tai häiriötä taikka kykyä lieventää sen aiheuttamia seurauksia. Ne koostuvat erityisesti toimista, joita tehdään ennen haitallisen tapahtuman realisoitumista vähentääkseen sen seurausten vakavuutta. Vastauskyky muodostuu välittömistä ja jatkuvista toiminnoista, tehtävistä ja järjestelmistä, joihin on ryhdytty ja joita on kehitetty, jotta pystytään vastaamaan ja mukautumaan haitallisen tapahtuman aiheuttamiin vaikutuksiin. Neljännen ryhmän muodostavat palautumismekanismit, jotka sisältävät toimintoja ja ohjelmia, joiden on tarkoitus pystyä palauttamaan toiminnan taso normaalille ja hyväksyttävälle tasolle mahdollisimman nopeasti ja tehokkaasti. (Petit ym. 2013.)

Rehakin ym. (2018) mukaan lajittelu näihin neljään edellä mainittuun ryhmään ei ole kuitenkaan täysin kattava, sillä siitä puuttuu yksi merkittävä resilienssin osa-alue. Heidän mukaansa tämä lajittelu jättää huomiotta kriittisen infrastruktuurin osajärjestelmien kyvyn oppia ja kehittää sopeutumiskykyään aikaisempien haitallisten tapahtumien perusteella. Kuten luvussa 2.1 esiteltiin, resilienssiin kuuluu merkittävästi myös se, että haitallisesta tapahtumasta selvittyään järjestelmällä tulisi olla aikaisempaa parempi valmius estää niiden tapahtuminen ja selviytyä niistä jatkossa (Comfort ym. 2010), mikä korostaa tämän Rehakin ym. (2018) mainitseman puuttuvan osa-alueen merkitystä.

Kuvassa 1 esitellään näitä kriittisen infrastruktuurin resilienssin eri vaiheita ja osa-alueita. Ensimmäisenä vaiheena on haitallisten tapahtumien ja häiriöiden ennakoiminen ja estäminen. Ennakoiminen vähentää organisaation tai järjestelmän haavoittuvuutta tulevia häiriöitä vastaan. Häiriön tapahtumista seuraa siirtyminen ennakointivaiheesta häiriön kestämiseen ja siitä selviytymiseen sekä muuttuneisiin olosuhteisiin mukautuminen, jos häiriö on vaikuttanut organisaation tai järjestelmän toimintaan

haitallisesti. Palautumisvaihe alkaa, kun häiriö ei enää aktiivisesti haittaa toimintaa, ja normaaliin toimintaan ja suorituskykyyn voidaan palata. Viimeisenä vaiheena on kohdatusta häiriöstä oppiminen: kuinka organisaatio tai järjestelmä pystyy kehittämään toimintaansa, jotta jatkossa vastaavista häiriöistä pystytään selviämään entistä paremmin. (Rehak ym. 2018.)



Kuva 1. Kriittisen infrastruktuurin resilienssin vaiheet (mukaillen Rehak ym. 2018)

Vastaavasti Fernandesin ym. (2023) mukaan kriittisen infrastruktuurin resilienssin vahvistaminen koostuu kolmesta päävaiheesta. Ensimmäinen vaihe on riskienhallinta, jonka tavoitteena on tunnistaa mahdollisia vaaroja ja selvittää niiden todennäköisyyksiä sekä oletettuja vaikutuksia. Kriittisen infrastruktuurin resilienssin osalta tämä on kriittinen vaihe, jotta voidaan minimoida näiden vaarojen ja riskien mahdollisuus. On kuitenkin huomioitava, että on hyvin vaikea ennustaa milloin ja miten erilaiset nykypäivän kriisit tapahtuvat. Kriittisen infrastruktuurin organisaatioiden ei siis pitäisi varautua ainoastaan tiedossa olevia uhkia vastaan, ja on mahdotonta tunnistaa kattavasti kaikki mahdolliset uhat ja vaarat. Toinen vaihe on turvallisuudenhallinta, jonka tarkoituksena on estää ja lieventää kriittisen infrastruktuurin kohtaamia mahdollisia uhkia. Tämä sisältää haavoittavaisuuksien tunnistamisen ja niiden huomioimisen sekä suojatoimenpiteiden kehittämisen esimerkiksi kyberhyökkäyksiä vastaan.

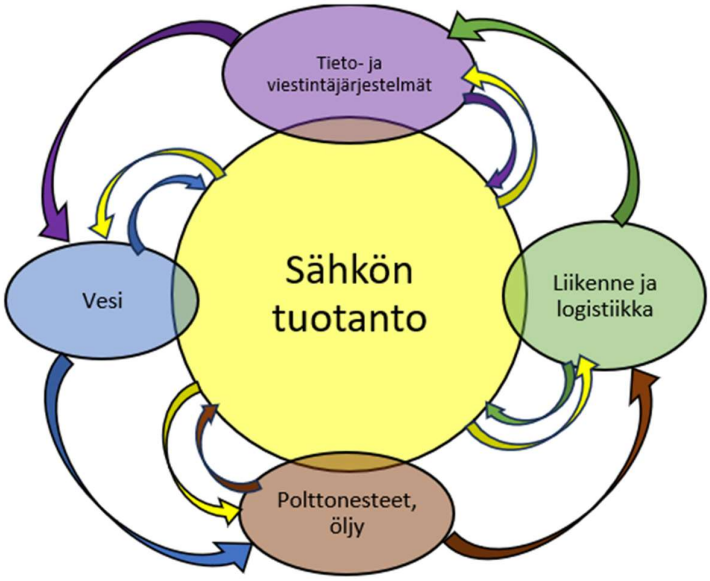
Suojatoimenpiteet ovat välttämättömiä, jotta toimintaa pystytään jatkamaan myös ennennäkemättömiä haasteita ja uhkia kohdatessa. Kolmas vaihe on toiminnan jatkuvuuden varmistaminen, joka keskittyy organisaation ydintoimintojen palauttamiseen normaalille tasolle häiriön kohtaamisen jälkeen, tai parhaassa tapauksessa häiriö ei vaikuta näihin toimintoihin ollenkaan. (Fernandes ym. 2023.)

Pursiaisen (2017) mukaan kriittisen infrastruktuurin resilienssin voi jakaa kolmeen osittain päällekkäiseen alueeseen: yhteiskunnalliseen, organisatoriseen ja teknologiseen. Tämä jako perustuu siihen, mitkä organisaatiot tai toimielimet ovat vastuussa tarvittavien toimien suorittamisesta haitallisen tapahtuman aikana, sitä ennen ja sen jälkeen. Yhteiskunnallisessa resilienssissä tärkeimmät toimijat ovat kansalliset hallitukset, yhteisöt ja kotitaloudet. Organisatorisessa resilienssissä toimijat ovat yrityksiä, jotka ovat vastuussa kriittisestä infrastruktuurista ja toimitusketjuista. Teknologisessa resilienssissä toimijat taas koostuvat yksilöistä ja organisaatioista, jotka vastaavat kriittisen infrastruktuurin laitosten ja välineiden toiminnasta. (Pursiainen 2017.)

Kuten aikaisemmin luvussa 2.1 mainittiin, resilienssiin kuuluu olennaisena osana sen hyväksyminen, etteivät kaikki tapahtumat ole ennakoitavissa, vaan odottamattomia asioita tulee aina tapahtumaan (Wied ym. (2019). Myös kriittisen infrastruktuurin resilienssi osalta joudutaan käsittelemään laajaa kirjoa erilaisia mahdollisia häiriöitä ja tapahtumia, joiden todennäköisyys on hyvin epävarma tai joissain tapauksissa täysin tuntematon (Brucherseifer ym. (2021).

3.5 Kriittisen infrastruktuurin riippuvuussuhteet

Kriittisen infrastruktuurien järjestelmät ja palvelut ovat yhteydessä toisiinsa ja pitkälti jopa riippuvaisia toisistaan. Tämä tarkoittaa sitä, että tietyn kriittisen infrastruktuurin osan tai järjestelmän toiminta riippuu siitä, että myös muut osat toimivat kunnolla. (Ouyang & Wang 2015.) Esimerkiksi vedenjakelun ja tietoliikenneyhteyksien järjestelmien toiminta edellyttää sähkötuotannon ja -jakelun jatkuvaa toimintaa (Ouyang 2014). Kuva 2 tarjoaa esimerkin kriittisen infrastruktuurin eri osien ja toimijoiden välisestä yhteydestä ja riippuvuudesta. Digitalisaation myötä tämä keskinäinen riippuvuus on kasvanut entisestään, ja tämä voi vaikeuttaa muun muassa riskien hahmottamista ja arviointia (Aven 2016).



Kuva 2. Esimerkki kriittisen infrastruktuurin riippuvuussuhteista (mukaillen Rinaldi ym. 2001)

Kriittiset infrastruktuurit muodostavatkin tiukasti yhteen punoutuneen ja yhdessä toimivan sosio-teknisen verkoston (Brucherseifer ym. (2021). Ne ovat siis monimutkaisia järjestelmiä, joissa ihmiset ovat vuorovaikutuksessa erilaisten teknologioiden kanssa (Zio 2016). Yhteys kriittisen infrastruktuurin eri järjestelmien välillä mahdollistaa niiden tehokkaan toiminnan, mutta lisää samalla niiden haavoittuvuutta. Yhden kriittisen infrastruktuurin järjestelmän pettäminen tai vastaavat ongelmat voivat johtaa toimintahäiriöihin myös muissa järjestelmissä. Tästä johtuen kriittisen infrastruktuurin resilienssissä on tärkeää ottaa huomioon niiden keskinäiset yhteydet. (Ouyang & Wang 2015.) Koska kriittisen infrastruktuurin eri toimijoiden ja järjestelmien väliset verkostot ovat hyvin monimutkaisia ja paikoin epäselviä, voi olla vaikea arvioida kuinka tiettyyn kriittiseen infrastruktuuriin kohdistuva häiriö vaikuttaa muihin (Gilpin & Murphy 2008). Kyky tunnistaa ja analysoida eri kriittisen infrastruktuurin järjestelmien välisiä riippuvaisuuksia ja yhteyksiä on oleellinen osa kriittisen infrastruktuurin resilienssiä (Pursiainen 2017).

Rinaldi ym. (2001) jakavat kriittisen infrastruktuurin verkostojen keskinäisen riippuvuuden neljään eri kategoriaan: fyysinen riippuvuus, kyberriippuvuus, maantieteellinen riippuvuus ja looginen riippuvuus. Fyysinen riippuvuus tarkoittaa sitä, että kriittisen infrastruktuurin osa hyödyntää omassa toiminnassaan jonkin toisen

kriittisen infrastruktuurin osan tuottamaa palvelua tai tuotetta. Kyberriippuvuudella tarkoitetaan sitä, että kriittisen infrastruktuurin osa hyödyntää tietoliikenneinfrastruktuurin tuottamaa informaatiota. Maantieteellinen riippuvuus taas on olemassa, jos samalla alueella tapahtuva häiriö vaikuttaa kahteen tai useampaan kriittisen infrastruktuurin osaan samanaikaisesti. Looginen riippuvuus pitää sisällään muiden kategorioiden ulkopuolelle jääneet riippuvuudet, esimerkiksi jos kriittisen infrastruktuurin osien välillä on jokin sosiaalinen yhteys.

3.6 Digitaaliset teknologiat kriittisen infrastruktuurin resilienssissä

Kriittisen infrastruktuurin organisaatioissa on nykyään paljon internet-yhteydellä toimivaa teknologiaa, mikä on luonut niille uuden haasteen: organisaatioiden on tutustuttava ja otettava käyttöön uusia teknologioita, mutta samalla myös hallittava riskejä, joita tähän digitaaliseen ympäristöön kuuluu. Käytännössä kaikki kriittisen infrastruktuurin toimijat ovatkin riippuvaisia tietojärjestelmistä. (Alcaraz & Zeadally 2014.) Erilaisten teknologioiden ja tietojärjestelmien rooli tärkeänä osana kriittistä infrastruktuuria aiheuttaa kuitenkin myös uudenlaisia riskejä, jotka täytyy ottaa huomioon, mikä korostaa digitaalisen resilienssin merkitystä myös kriittiselle infrastruktuurille (Fernandes ym. 2023).

Argyroudisin ym. (2022) mukaan ottamalla käyttöön ja hyödyntämällä uusia digitaalisia teknologioita, kuten esimerkiksi esineiden internetiä, tekoälyä ja koneoppimista, voidaan huomattavasti nopeuttaa kriittisen infrastruktuurin kehittymistä entistä resilientimmäksi. Hyödyntämällä näiden uusien teknologioiden tarjoamat mahdollisuudet ja niiden avulla kerättyä dataa, voidaan parantaa kriittisen infrastruktuurin resilienssiä merkittävästi erityisesti luonnonkatastrofeja vastaan (Achillopoulou ym. 2020). Uusien teknologioiden avulla voidaan tehdä nopeampia ja luotettavampia arvioita resilienssistä, sekä tukea päätöksentekoa ennen häiriötä, sen aikana ja sen jälkeen (Argyroudis ym 2022).

Kriittisen infrastruktuurin resilienssin kannalta on oleellista, että on käytettävissä järjestelmiä, joiden avulla voidaan kerätä sen toimintaan liittyvää dataa ja tarkkailla vallitsevaa olotilaa (Labaka ym. 2015). Jotta pystytään palauttamaan kriittisen infrastruktuurin järjestelmän toiminta ja suorituskyky iskun kohtaamisen jälkeen, on

tehtävä huolto- ja korjaustoimia. Näiden toimenpiteiden toteuttaminen vaatii kunnollisen informaation ja datan tunnistamista, prosessointia sekä hallintaa. Tätä informaatiota voidaan käyttää analytiikkajärjestelmissä, jotka tukevat kriittisen infrastruktuurin resilienssin kehittämistä. (Croope & McNeil 2011.) Tarvittavien mittauslaitteistojen ja ohjelmistojen avulla voidaan kerätä tietoa kriittisen infrastruktuurin järjestelmistä ja tarkkailla, että sen suorituskyky on normaalilla tasolla, sekä parhaassa tapauksessa pystytään ennakoimaan tulevia häiriöitä. Lisäksi tällaisten järjestelmien avulla voidaan kerätä dataa siitä, kuinka hyvin kriittisen infrastruktuurin palautuminen kohdatusta iskusta etenee. (Labaka ym. 2015.) Tässä kriittisen infrastruktuurin resilienssillä on selkeä yhtymäkohta digitaalisen resilienssin kanssa.

Massadataa (engl. big data) voidaan hyödyntää kriittisen infrastruktuurin järjestelmien resilienssin parantamisessa esimerkiksi koneoppimisen tai muiden dataa hyödyntävien analytiikkamenetelmien avulla. Kriittisen infrastruktuurin järjestelmät tuottavatkin jatkuvasti suuria määriä dataa, jota voidaan hyödyntää niiden resilienssin parantamisessa. (Eisenberg ym. 2019.) Barker ym. (2017) käyttävät tästä termiä resilienssianalytiikka (engl. resilience analytics), joka tarkoittaa edistyneiden datapohjaisten menetelmien järjestelmällistä käyttämistä infrastruktuurien hallintaan, tavoitteenaan niiden resilienssin parantaminen. Heidän mukaansa analytiikkaa voidaan käyttää erityisesti kriittisen infrastruktuurin toimintojen sekä niihin liittyvän päätöksenteon tukena.

Data-analytiikan eri menetelmät on luokiteltu kolmeen kategoriaan, jotka ovat kuvaileva analytiikka (engl. descriptive analytics), ennakoiva analytiikka (engl. predictive analytivs) ja ohjaileva analytiikka (engl. prescriptive analytics) (Duan & Da Xu 2021). Tätä mukaillen, Barker ym. (2017) jakavat myös resilienssianalytiikan edellä mainittuihin kolmeen alakategoriaan. Kuvailevan analytiikan avulla voidaan kuvata ja visualisoida kriittisen infrastruktuurin järjestelmän toimintakykyä. Ennakoivaa analytiikkaa voidaan käyttää esimerkiksi tulevien tapahtumien todennäköisyyksien laskemiseen ja näin ennakoida niitä. Ohjailevan analytiikan avulla taas voidaan tunnistaa ja arvioida mahdollisia toimintasuunnitelmia ottaen samalla mahdolliset rajoitteet ja tavoitteet huomioon. (Barker ym. 2017.) Resilienssianalytiikan selkeä heikkous on kuitenkin siinä, ettei sen avulla voida ennustaa täysin yllätyksellisiä ja ennennäkemättömiä tapahtumia (Eisenberg ym. 2019).

Alkhaleelin (2024) mukaan on olemassa useista koneoppimisen sovelluksia, joiden avulla voidaan parantaa sekä uusien että olemassa olevien kriittisen infrastruktuurin järjestelmien resilienssiä. Hänen mukaansa koneoppimisen tekniikoita voidaan käyttää resilienssin parantamiseen erityisesti kehittämällä päätöksentekoa ja vähentämällä häiriöistä aiheutuvia sosioekonomisia menetyksiä. Koneoppimisen avulla voidaan parantaa päätöksentekoprosessia tutkimalla dataa tavalla, joihin perinteisemmät analytiikan työkalut eivät kykene, ja Alkhaleel (2024) pitää koneoppimisen mahdollisuuksia kriittisen infrastruktuurin resilienssin parantamiseksi lähes rajattomina.

Digitalisaatio ja kriittisen infrastruktuurin organisaatioiden ja järjestelmien verkottaminen tarjoaa kriittiselle infrastruktuurille paljon uusia mahdollisuuksia, mutta toisaalta lisää myös sen monimutkaisuutta ja jo ennestään vaikeasti hahmotettavia keskinäisiä riippuvuuksia (Lichte ym. 2022). Uusien nousevien teknologioiden käyttämisessä kriittisen infrastruktuurin resilienssin parantamiseen on kuitenkin myös haittapuolensa. Ensinnäkin nämä uudet teknologiat ovat haavoittuvaisia kyberhyökkäyksiä vastaa, mikä voi pahimmillaan johtaa tietosodankäyntiin. Nämä teknologiat vaativat myös yleisesti ottaen virtalähteen toimiakseen. Lisäksi päätöksiä tehdessä ihmiset eivät välttämättä pysty täysin luottamaan näihin uusiin teknologioihin. (Argyroudis ym. 2022.)

3.7 Uhat kriittiselle infrastruktuurille ja sen resilienssille

Suuren merkityksensä ja julkisuutensa takia kriittinen infrastruktuuri on altis useille eri uhille ja häiriöille, kuten luonnonkatastrofeille, onnettomuuksille, terrorismille ja muulle rikolliselle toiminnalle (Mauro ym. 2010). Tällaiset lukuisat uhat voivat aiheuttaa kriittiselle infrastruktuurille merkittäviä häiriöitä ja näin laittaa sen resilienssin koetukselle, mikä voi aiheuttaa suuria negatiivisia vaikutuksia niin yksittäisille ihmisille kuin yhteiskunnille ja kansalliselle taloudelle. Näiden mahdollisten uhkien tunnistaminen ja ymmärrys niiden vaikutuksista on ensisijaisen tärkeää kriittisen infrastruktuurin resilienssin kehittämisen kannalta. (Osei-Kyei 2021.)

Tutkimuksessaan Osei-Kyei ym. (2021) tunnistavat yhteensä 31 erilaista uhkaa tai vaaraa kriittisen infrastruktuurin resilienssille, mikä kuvastaa hyvin niiden suurta määrää ja vaihtelevuutta. He jakavat nämä uhat ja vaarat kahdeksaan ryhmään, joita ovat sosiaaliset, poliittiset, hallinnolliset, tekniset, toiminnalliset, taloudelliset ja ympäristöön vaikuttavat uhat. Heidän mukaansa yleisimpiä vaaroja kriittiselle

infrastruktuurille ja sen resilienssille ovat luonnonkatastrofit, vanheneminen ja ränsistyminen, kyberuhat, sekä terrorismi.

Luonnonkatastrofien määrä on ollut viime vuosikymmenen aikana nousussa (Shakou ym. 2019), ja niillä on laajoja haitallisia vaikutuksia, jotka voivat johtaa kriittisen infrastruktuurin toimintahäiriöihin tai pahimmillaan sen tuhoutumiseen (Laugé ym. 2015). Ne voivat aiheuttaa suoraan tai epäsuorasti taloudellisia, yhteiskunnallisia ja ympäristöllisiä haittoja. Kriittisen infrastruktuurin resilienssin parantamisesta juuri luonnonkatastrofeja vastaan on tullut viime vuosina tärkeä tavoite, ja Shakoun ym. (2019) mukaan hallitusten sekä päätöksentekijöiden tulisi kiinnittää tähän erityistä huomiota niiden yleistymisestä ja laajoista vaikutuksista johtuen. Tällä hetkellä kriittisen infrastruktuurin resilienssissä keskitytään luonnonkatastrofien osalta erityisesti minimoimaan äärimmäisten sääilmiöiden aiheuttamia häiriöitä ja palautumaan niistä mahdollisimman nopeasti. (Shakou ym. 2019.)

Terrorismi ei ole uusi ilmiö, mutta se on vakava uhka kriittisen infrastruktuurin resilienssille, sillä sen vaikutukset voivat olla todella tuhoisia ja kauaskantoisia (Osei-Kyei 2021). Pursiaisen (2017) mukaan Euroopassa alettiin erityisesti kehittämään valmiutta suojata kriittistä infrastruktuuria ja ihmisiä terrori-iskuilta erityisesti vuosina 2004 ja 2005 tapahtuneiden Madridin ja Lontoon pommi-iskujen jälkeen. Terrorismin tarkoituksena on luoda kohdemaahan pelkoa, paniikkia ja häiritä sen toimintaa, minkä takia kriittinen infrastruktuuri on houkutteleva kohde terrori-iskulle. Monet eri infrastruktuurin osat, kuten rakennukset, laitokset ja lentokentät ovat alttiita terroriuhalle. (Stewart 2010.) Zimmermanin ym. (2009) mukaan tulevien terrori-iskujen todennäköisyyksien ja niiden mahdollisten vaikutusten ymmärtäminen edellyttää aikaisempien tapausten analysoimista, ja tässä voidaan hyödyntää riskienhallinnan viitekehyksiä.

Uusien kehittyneiden teknologioiden käyttöönoton myötä kriittisen infrastruktuurin suorituskyky ja toimintavarmuus on pitkälti riippuvainen digitaalisista ohjausjärjestelmistä ja verkkoyhteyksistä (Hurst ym. 2014). Erilaiset tieto- ja viestintäteknologiat ovatkin keskeinen osa modernia kriittistä infrastruktuuria (Genge ym. 2015). Tällaisia hallinta- ja ohjausjärjestelmiä käytetään laajalti monissa eri kriittisen infrastruktuurin osissa, kuten esimerkiksi sähkö- ja ydinvoimaloissa, jotka ovat tyypillisesti tietokoneistettuja laitoksia (Ryu ym. 2009). Koska kriittisen

infrastruktuurin ja sen järjestelmien hallinnointi ja seuranta on siis ainakin osittain riippuvainen internetistä, muodostuu erilaisista kyberhyökkäyksistä sille merkittävä uhka (Gunduz & Das 2020). Kyberhyökkäyksistä kriittistä infrastruktuuria vastaan on Choong-Heen ym. (2019) mukaan tullut viime vuosina aikaisempaa yleisempiä, koska niiden suunnitteluun tarvittu aika on lyhentynyt ja kehittyneempien teknologioiden avulla hyökkäyksiä voidaan toteuttaa aikaisempaa helpommin. Ne voivat olla monimutkaisia sekä kehittyneitä ja aiheuttaa suurtakin vahinkoa sekä kriittisen infrastruktuurin fyysisille että digitaalisille osille (Genge ym. 2015). Choong-Hee ym. (2019) väittävät, että kriittiseen infrastruktuuriin kohdistuvien kyberhyökkäysten estäminen ja niiden välitön torjuminen on haastavaa tietoturvatapahtumien suuresta määrästä johtuen, mikä tekee niiden analysoimisesta vaikeaa.

Kriittisen infrastruktuurin vanheneminen on myös tyypillinen uhka sen resilienssille, sillä vanhentuneet sekä kuluneet osat tai järjestelmät voivat aiheuttaa sen toiminnan keskeytymisen. Esimerkiksi kriittisen infrastruktuurin laitteistojen, ohjelmistojen ja viestintäverkkojen vanheneminen voi tehdä sen järjestelmistä epäluotettavia, mikä lisää häiriöiden ja siihen kohdistuvien hyökkäyksien mahdollisuuksia. (Tweneboah-Koduah & Prasad 2020.) Myös ilmastonmuutoksen ja lisääntyneiden luonnonkatastrofien katsotaan kiihdyttävän kriittisen infrastruktuurin kulumista ja vanhenemista (Bellini ym. 2020).

4 Metodologia

Tutkielman empiirinen osuus muodostuu laadullisesta tutkimuksesta, jossa kerätään haastattelujen avulla tietoa siitä, miten digitaalisuus ja erilaiset digitaaliset ratkaisut tukevat häiriötilanteista selviämistä kriittisen infrastruktuurin parissa toimivissa energiasektorin yrityksissä. Tässä luvussa esitellään kattavasti tutkielman empiiriseen osioon valittu menetelmäsuuntaus ja tutkimusstrategia sekä aineiston keräämiseen ja analysoimiseen käytetyt tutkimusmenetelmät. Tutkielman metodologiaan liittyvät valinnat perustellaan tieteellisen kirjallisuuden avulla. Luku sisältää myös kuvauksen tutkimuksen etenemisestä ja sen eri vaiheista. Lopuksi käydään läpi myös tutkimuksen laatuun, rajoituksiin ja eettisyyteen vaikuttavia tekijöitä.

4.1 Tutkielman menetelmäsuuntaus

Tutkielma toteutetaan kvalitatiivisena eli laadullisena tutkimuksena. Laadullisen tutkimuksen tavoite on tutkia ja ymmärtää monipuolisia ilmiöitä kattavasti (Eriksson & Kovalainen 2008). Laadullisen tutkimuksen avulla on mahdollista saada syvällinen ymmärrys ihmisten kokemuksista ja näkemyksistä tiettyyn ilmiöön liittyen, minkä takia se sopii hyvin tähän tutkielmaan (Agius 2013).

Valitsemalla tämän menetelmäsuuntauksen tutkielmassa voidaan saada laaja-alaisempaa tietoa tutkimukseen osallistuvien yritysten ja henkilöiden näkemyksistä sekä kokemuksista digitaaliseen resilienssiin liittyen. Laadullisen tutkimuksen avulla on määrällistä tutkimusta helpompi saada syvällisempi käsitys siitä, minkälaisten haasteiden parissa kriittisen infrastruktuurin yrityksissä toimitaan, ja miten digitaalinen resilienssi voi haastateltavien kokemusten mukaan auttaa selviämään näistä haasteista. Määrällisellä tutkimuksella tällaisen tiedon kerääminen olisi haastavaa.

4.2 Tutkimusstrategia

4.2.1 Tapaustutkimus

Tutkielman tutkimusstrategiana toimii tapaustutkimus eli case-tutkimus, jossa pyritään selvittämään miten digitaalisuus ja erilaiset digitaaliset keinot auttavat kriittisen infrastruktuurin yrityksiä käsittelemään ja selviytymään häiriötilanteista. Tapaustutkimus on empiirinen tutkimus, jossa tutkitaan tiettyä nykyhetken ilmiötä eli tapausta syvällisesti ja reaalimaailman kontekstissa. Se on erityisen hyvä

tutkimusstrategia, kun tarkoituksena on pystyä vastamaan miten- ja miksi-kysymyksiin. (Yin 2014.) Tutkielmassa tarkasteltava tapaus ja perustelut sille miksi sen tutkiminen on tärkeää, on kuvattu tarkemmin seuraavassa luvussa 4.2.2.

Tapaustutkimus on suosittu tutkimusstrategia myös tietojärjestelmätieteessä (Williamson & Johanson 2018). Erikssonin ja Kovalaisen (2008) mukaan tapaustutkimus on suositeltava tutkimusmenetelmä monipuolisia yritysten toimintaan liittyviä kysymyksiä tutkittaessa, joten tapaustutkimus sopii tutkielman aiheeseen. Tapaustutkimus sopii reaalimaailman ilmiöiden tutkimukseen, ja tähän ilmiöön liittyvien sidosryhmien kokemukset ja näkemykset ovat keskeisessä roolissa. Tapaustutkimuksissa aineistonkeruu voi tapahtua eri tavoilla, mutta haastattelut ovat niissä yleisiä. (Williamson & Johanson 2018.) Koska tutkimuksessa aineistonkeruu tapahtuu haastatteluilla, joissa haastateltavien omat mielipiteet ja kokemukset tulevat esiin, on tapaustutkimus tälle tutkielmalle sopiva tutkimusmenetelmä. Tapaustutkimuksella pystytään myös usein esittämään haastaviakin asiakokonaisuuksia helpommin ymmärrettävässä muodossa (Eriksson & Kovalainen 2008), mikä sopii tutkielman varsin vähän aikaisemmin tutkittuun aiheeseen.

4.2.2 Tapauksen kuvaus

Tässä tutkielmassa tutkittavana ilmiönä eli tapauksena on miten digitaaliset teknologiat ja ratkaisut sekä tietojärjestelmät auttavat kriittiseen infrastruktuuriin kuuluvia energiasektorin yrityksiä hallitsemaan ja toimimaan erilaisissa häiriötilanteissa. Nyky-yhteiskunnan riippuvuus kriittisen infrastruktuurin ja sen järjestelmien toimivuudesta kasvaa jatkuvasti (Ouyang 2014), minkä takia on erityisen tärkeää, että kriittisen infrastruktuurin ja siitä vastaavien yritysten toiminta pystytään varmistamaan myös häiriöitä kohdatessa. Tästä johtuen on hyödyllistä tutkia aihetta juuri kriittisestä infrastruktuurista vastaavien yritysten näkökulmasta. Digitalisaation seurauksena digitaalisen resilienssin merkitys on kasvanut ja digitaalisten teknologioiden sekä tietojärjestelmien rooli näiden häiriötilanteiden selvittämisessä on entistä suurempi (Gkeredakis ym. 2021). On siis tärkeää tutkia millä eri tavoin niitä voidaan hyödyntää tässä selviytymisessä ja näin luoda syvällisempää ymmärrystä siitä, miten digitaalisuus voi parantaa kriittisen infrastruktuurin resilienssiä.

Kriittinen infrastruktuuri jakaantuu moneen eri alaan ja siitä vastaavia yrityksiä on usealla eri toimialalla. Tutkielma on kuitenkin rajattu käsittelemään vain

energiasektorilla toimivia kriittisen infrastruktuurin yrityksiä, sillä energiasektorin häiriötön toiminta ja resilienssi on yhteiskunnan toimivuuden kannalta erityisen tärkeää (Jasiūnas ym. 2021). Suomessa energian tarve on pohjoisen sijainnin seurauksena suuri, ja lisäksi teollisuus vaatii suuria määriä energiaa käyttöönsä. Suomen energiasektorin ja -huollon kivijalkoja ovat hajautettu energiantuotanto, monipuoliset energialähteet sekä korkean toimintavarmuuden siirto- ja jakelujärjestelmät, ja yksi sen tärkeimmistä tavoitteista on energian häiriötön saatavuus. (Huoltovarmuuskeskus B 2024.) Koska energian häiriötön saatavuus on yksi Suomen energiasektorin tärkeimmistä tavoitteista, on tärkeää tutkia miten digitaalisuus ja digitaaliset teknologiat auttavat tämän tavoitteen saavuttamisessa. Vaikka kaikki kriittinen infrastruktuuri on yhteiskunnan kannalta erittäin tärkeää, on energiasektorin merkitys erityisen suuri myös sen takia, että monet muut kriittisen infrastruktuurin osat ja toiminnot ovat riippuvaisia siitä. Merkittävät häiriöt esimerkiksi sähköntuotannossa ja -jakelussa voivat olla todella haitallisia muun kriittisen infrastruktuurin toiminnan kannalta ja pahimmillaan jopa estää niiden toiminnan kokonaan. Lisäksi erilaiset digitaaliset teknologiat ja ratkaisut ovat keskeisessä roolissa energiasektorin yrityksissä, joten digitaalisen resilienssin tutkiminen niiden näkökulmasta on hyödyllistä.

Tutkielmaan osallistuneiden haastateltavien edustamat yritykset ovat keskeinen osa Suomen kriittistä infrastruktuuria ja energiasektoria. Suomessa Huoltovarmuuskeskus on jakanut energiahuoltosektorin neljään pooliin, joita ovat kaasupooli, lämpöpooli, polttonestepooli ja sähköpooli. Tutkielmaan osallistui haastateltavia tämän jaon mukaisesti kaikista muista paitsi polttonestepoolista, mutta ainakin yhdellä haastateltavista oli aikaisempaa työkokemusta myös siihen kuuluvasta yrityksestä. Tutkielmaan osallistui suuria suomalaisia energiayhtiöitä, joiden toimintaan kuuluu esimerkiksi sähkön ja kaukolämmön tuotanto eri muodoissa, sähkön ja kaukolämmön jakelu, myynti sekä sähkönsiirto. Tutkielmaan osallistui myös teollisuuskaasujen tuotantoon ja jakeluun erikoistunut yritys. Yhtiöt ovat siis merkittäviä energiasektorin toimijoita, joilla on tärkeä rooli energian häiriöttömän saatavuuden varmistamisessa Suomessa.

4.3 Aineistonkeruu

4.3.1 Aineistonkeruumenetelmä

Tutkielman aineistonkeruu toteutettiin laadullisten haastatteluiden avulla. Haastattelut ovat tyypillinen aineistonkeruumenetelmä laadullisessa tutkimuksessa, ja niitä käytetään laajalti myös tietojärjestelmätieteessä (Williamson & Johanson 2018). Yinin (2014) mukaan haastattelut ovat myös tapaustutkimuksissa yksi merkittävimmistä aineiston ja informaation lähteistä.

Yksi haastatteluiden merkittävimmistä eduista on niiden joustavuus, sillä haastattelija voi esimerkiksi tarvittaessa toistaa kysymyksen tai muotoilla sen uudelleen ja käydä keskustelua haastateltavan kanssa (Tuomi & Sarajärvi 2018). Tämä oli tutkielman aineistonkeruussa oleellista, sillä osa kysymyksistä olivat melko haastavia, eivätkä haastateltavat aina pystyneet vastaamaan niihin suoraan. Paikoitellen kysymyksiä täytyi siis hieman muotoilla uudelleen, ja tiettyjä kohtia käytiin keskustelunomaisesti läpi tarkempien vastausten löytämiseksi. Koska haastattelujen tarkoitus on saada tutkittavasta aiheesta mahdollisimman paljon tietoa, on perusteltua antaa haastateltaville joko haastattelukysymykset tai haastattelussa käsiteltävät teemat etukäteen (Tuomi & Sarajärvi 2018). Tutkielmaan osallistuneet haastateltavat saivat tutkielman aiheen ja haastattelussa käsiteltävät teemat tietoonsa hyvissä ajoin ennen haastattelua, jotta heidän oli mahdollista tutustua niihin etukäteen. Tarkempia haastattelukysymyksiä ei esitelty haastateltaville etukäteen lukuun ottamatta kahta haastateltavaa, jotka toivoivat erikseen pääsevänsä tutustumaan myös haastattelukysymyksiin ennen haastattelua.

Haastattelut voidaan jakaa strukturoituihin, puolistrukturoituihin ja strukturoimattomiin eli avoimiin haastatteluihin. Puolistrukturoiduissa haastatteluissa, joita käytettiin tässä tutkielmassa, kaikkien haastateltavien kanssa käydään läpi samoja teemoja ja suurimmilta osin samoja kysymyksiä, mutta kysymysten muotoilu ja järjestys voi vaihdella hieman. (Eriksson & Kovalainen 2008.) Haastattelut toteutettiin siis puolistrukturoituina eli puolirakenteellisina yksilöhaastatteluina, jotta haastateltavilta oli tarvittaessa mahdollista kysyä lisäkysymyksiä ja tarkennuksia heidän vastauksiinsa liittyen. Puolirakenteellisiin haastatteluihin päädyttiin osaltaan myös sen takia, että haastateltavien erilaisten taustojen ja osittain arkaluontoisen aiheen johdosta ei ollut täysin varmaa, kuinka hyvin haastateltavat pystyisivät vastaamaan tiettyihin kysymyksiin, ja pitäisikö heiltä kysyä hieman toisistaan poikkeavia tai eri lailla

muotoiltuja kysymyksiä. Puolirakenteelliset haastattelut mahdollistavat myös vapaamman keskustelun haastateltavien kanssa, mikä auttaa syvemmän ymmärryksen saamisessa erityisesti miten-, miksi- ja kuinka-kysymysten osalta. Puolirakenteellisissa haastatteluissa voi myös syventyä tarkemmin esiin nouseviin mielenkiintoisiin asioihin tai yksityiskohtiin. (Iyamu & Mutudi 2022). Tätä puolirakenteellisen haastattelun ominaisuutta hyödynnettiin useassa haastattelussa, kun haastatteluissa esiin nousseisiin uusiin asioihin ja yksityiskohtiin voitiin paneutua tarkemmin lisäkysymyksin, vaikkeivat ne olisikaan olleet osana alkuperäistä kysymysrunkoa.

Tutkielman empiirinen aineisto kerättiin haastattelemalla seitsemää henkilöä, jotka työskentelevät kriittisen infrastruktuurin parissa toimivissa energiasektorin yrityksissä Suomessa. Haastateltavat toimivat eri energiasektorin alojen yrityksissä ja heidän työtehtävänsä vaihtelevat esimerkiksi IT:hen, tuotantoon ja turvallisuuteen liittyvien tehtävien välillä. Toisistaan poikkeavista työtehtävistä huolimatta kaikilla haastateltavilla on tietämystä ja kokemuksia huoltovarmuuskriittisten energiasektorin yritysten varautumisesta ja selviytymisestä vaihtelevista häiriötilanteista ja siitä millaisessa roolissa digitaaliset ratkaisut ja tietojärjestelmät ovat tässä. Haastateltavia etsittiin tutkimukseen hyödyntämällä energiasektorin yritysten julkisia verkkosivuja sekä LinkedIniä, ja potentiaalisiin haastateltaviin oltiin yhteydessä sähköpostitse. Tutkielmaan osallistuneet haastateltavat on esitelty tarkemmin taulukossa 2.

Taulukko 2. Haastateltavat

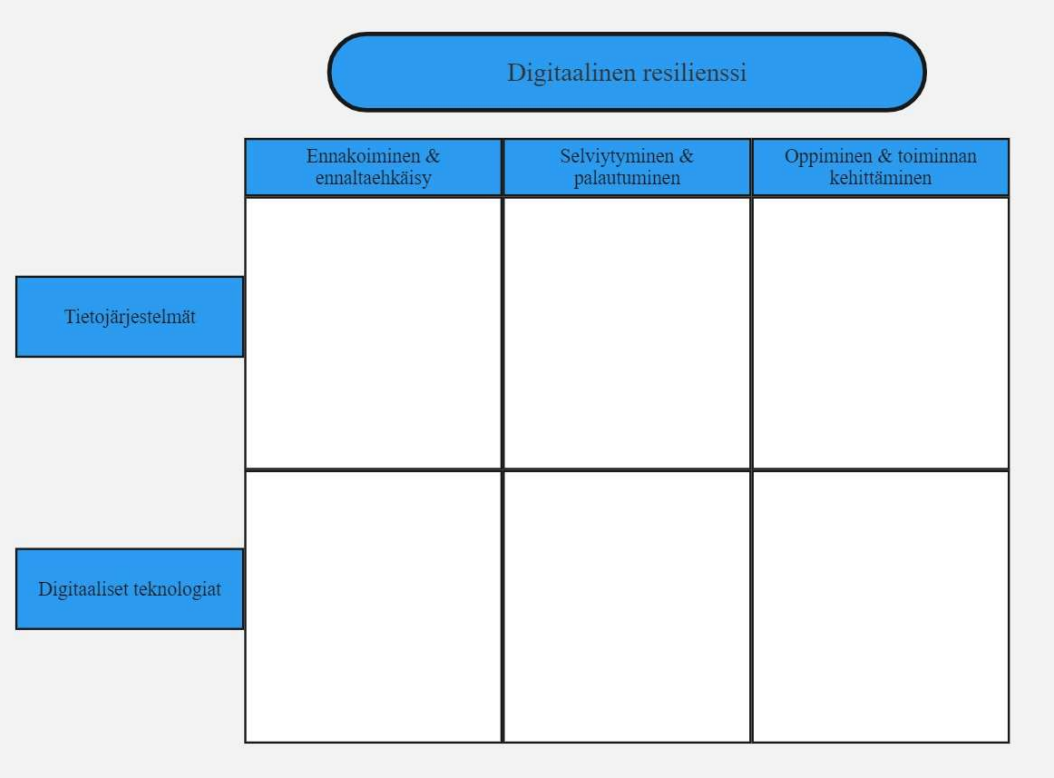
Haastateltava	Rooli yrityksessä	Energiasektorin osa	Haastattelun kesto	Haastattelun päivämäärä
H1	IT-palvelupäällikkö	Kaasu	40 min	22.4.2024
H2	Tietohallintojohtaja	Sähkö	32 min	10.5.2024
H3	Tuotantojohtaja	Kaasu	30 min	12.5.2024
H4	Turvallisuusjohtaja	Sähkö	38 min	29.5.2024
H5	Yksikön päällikkö	Sähkö	31 min	3.6.2024
H6	Turvallisuusjohtaja	Sähkö	30 min	3.6.2024
H7	Operatiivinen johtaja	Lämpö	28 min	7.6.2024

Haastattelut suoritettiin vuoden 2024 huhti-kesäkuussa etäyhteyksin pääosin Zoomin ja Microsoft Teamsin välityksellä, mutta teknisen ongelman seurauksena yksi haastatteluista pidettiin puhelimitse. Kestoltaan haastattelut olivat 28–40 minuuttia, ja

ne äänitettiin haasteltavien luvalla aineiston litterointia varten. Viiden ensimmäisen haastattelun äänityksen litterointi suoritettiin täysin manuaalisesti, ja kahden viimeisen haastattelun litteroinnissa käytettiin avuksi Turun yliopiston tarjoamaa UTU Transcribe -litterointityökalua. Nämäkin litteroinnit tarkastettiin manuaalisesti kahdesti laadun takaamiseksi.

4.3.2 Teoreettinen viitekehys

Tutkielman empiriaosuus perustuu teorialukujen perusteella luotuun teoreettiseen viitekehykseen, joka on esitelty alla kuvassa 3. Tutkielmassa digitaalista resilienssiä käsitellään Bohin ym. (2023) määritelmän mukaan, jossa digitaalisella resilienssillä viitataan organisaatioiden tietojärjestelmiä ja digitaalisia teknologioita käyttämällä saavutettavaan kykyyn selviytyä, mukautua ja palautua ulkoisten tapahtumien aiheuttamista häiriöistä ja ongelmista. Tutkielmassa pyritään siis selventämään käytännön tasolla mitä nämä määritelmässä mainitut digitaaliset teknologiat ja tietojärjestelmät ovat, ja miten niitä hyödynnetään kriittisen infrastruktuurin yrityksissä. Kuten tutkielman teoriaosuudessa huomattiin, sekä digitaalisen resilienssin että kriittisen infrastruktuurin resilienssin osa-alueet ja vaiheet ovat pitkälti samat, ja ne on otettu osaksi tutkielmassa käytettävää viitekehystä. Tutkielmassa selvitetään siis mitä nämä digitaaliset teknologiat ja tietojärjestelmät ovat kriittiseen infrastruktuuriin kuuluvissa energiasektorin yrityksissä, ja miten ne sijoittuvat resilienssin eri osa-alueisiin. Viitekehyksen avulla pyritään löytämään kattava vastaus tutkielman tutkimuskysymykseen: *Mistä digitaalinen resilienssi muodostuu kriittisen infrastruktuurin yrityksissä?*



Kuva 3. Teoreettinen viitekehys

Aikaisempi digitaalista resilienssiä käsittelevä tutkimus on tarjonnut esimerkkejä millaisia teknologioita siihen voi kuulua, mutta ne ovat keskittyneet hyvin pitkälti vain koronapandemiaan (Abidi ym. 2023, Gkeredakis ym. 2021, Tim ym. 2023). Pandemia on vain yksi esimerkki organisaatioiden toimintaan vaikuttavasta häiriöstä, joten on hyödyllistä tutkia digitaalisuuden roolia myös muunlaisiin häiriötilanteisiin liittyen. Voidaan olettaa, että erilaisissa häiriötilanteissa nousevat esiin eri teknologiat ja digitaaliset ratkaisut. Myös kriittisen infrastruktuurin yritysten näkökulmasta aikaisempi tutkimus on hyvin vähäistä, joten aihetta on hyödyllistä tutkia.

Tutkimus on operationalisoitu tutkielman liitteenä olevaan operationalisointitaulukkoon (liite 4). Operationalisointitaulukko kuvaa miten tutkielmassa pyritään löytämään vastauksia tutkimuskysymyksiin yhdistelemällä teoriaosuudessa kerättyä tietoa empiirisen aineistoon eli haastattelujen kautta saatuun uuteen tietoon. Aikaisemmassa aihetta käsittelevässä kirjallisuudessa digitaalinen resilienssi on jaettu eri osa-alueisiin, jotka toimivat myös tämän tutkielman empiriaosuuden pohjana ja haastatteluteemojen perustana. Tutkielman empiriaosuudessa pyritään löytämään konkreettisia vastauksia

siihen, miten digitaalinen resilienssi ja sen eri osa-alueet toteutuvat kriittisen infrastruktuurin yrityksissä ja mistä ne muodostuvat. Operationalisointitaulukossa on esitelty tarkemmin, miten aikaisempi kirjallisuus on auttanut luomaan haastatteluteemoja, ja miten näistä teemoista on sitten muodostettu haastattelukysymyksiä sekä varakysymyksiä.

4.4 Aineiston analysointi

Tutkielmassa aineiston analysoimiseen käytetään temaattista analyysiä. Temaattisen analyysin avulla voidaan analysoida laadullista aineistoa kuten haastatteluja tavoitteena löytää sieltä laajempia kokonaisuuksia eli teemoja, joiden avulla aineistoa voidaan ymmärtää paremmin (Riger & Sigurvinsdottir 2015). Temaattinen analyysi tarjoaa tutkijalle tavan luoda niin sanottuja koodeja, jotka muodostuvat tutkimuskysymyksen kannalta oleellisista aineiston osista. Näistä koodeista taas muodostuu laajempia merkityksellisiä teemoja, joiden avulla tutkija voi järjestää ja raportoida aineistosta tekemiään havaintoja. Tavoitteena ei ole ainoastaan tiivistää aineiston sisältöä, vaan tunnistaa ja tulkita aineiston keskeisiä piirteitä tutkimuskysymyksen johdattelemana. Yksi temaattisen analyysin vahvuuksista on sen joustavuus, sillä se on toimiva aineiston analysointikeino riippumatta esimerkiksi tutkimuskysymyksestä, aineiston laajuudesta tai aineistonkeruumenetelmästä. (Clarke & Braun 2016.)

Rigerin ja Sigurvinsdottirin (2015) mukaan temaattisessa analyysissä aineiston analysointiprosessi jaetaan useaan eri vaiheeseen, joita ovat aineistoon tutustuminen, alustavien koodien luominen, teemojen etsiminen, teemojen arvioiminen, teemojen määrittely sekä nimeäminen ja lopulta analyysin raportoiminen. Tutkielmassa aineiston analysoiminen toteutettiin edellä mainitun mukaisena prosessina näiden vaiheiden kautta.

Temaattisen analyysin ensimmäinen vaihe on siis aineistoon tutustuminen. Tämä toteutettiin tutkielmassa lukemalla litteroidut haastattelut läpi ensin sellaisenaan, jonka jälkeen haastattelut käytiin läpi yksi kerrallaan merkaten samalla tutkielman ja tutkimuskysymysten kannalta kiinnostavia kohtia. Nämä kohdat myös nimettiin lyhyesti erilaisin koodein eli alustava koodaus suoritettiin näin. Tämän jälkeen nämä haastatteluista löytyneet kiinnostavat osat ja koodit siirrettiin Excel-tiedostoon, jossa koodeja alettiin yhdistelemään ja jaottelemaan laajemmiksi teemoiksi, jotka myös nimettiin lyhyesti. Koodaustaulukko on esitelty kokonaisuudessaan tutkielman liitteissä (liite 5). Tunnistetut ja nimetyt teemat jaoteltiin sitten aiemmin esitellyn operationalisointitaulukon mukaisesti perustuen siihen, mihin digitaalisen resilienssin osa-alueeseen ne erityisesti liittyivät. Huomioitavaa on kuitenkin se, että tuloksissa on tämän lisäksi esitelty kuitenkin myös muita esiin nousseita teemoja, jotka voivat olla oleellisia esimerkiksi digitaalista resilienssiä käsittelevän jatkotutkimuksen kannalta.

Lopullinen analyysi kirjoitettiin tunnistettujen teemojen mukaisesti ja löytyy tutkielman luvusta 5.

4.5 Rajoitukset, tutkimuksen laatu ja eettisyys

4.5.1 Rajoitukset

Tutkielmaan liittyy tiettyjä rajoituksia, jotka tulee ottaa huomioon sen tuloksiin tutustuttaessa. Ensinnäkin tutkielmassa käsitellään melko sensitiivisiä aiheita, joten haastateltavat eivät voineet kaikilta osin mennä tarkkoihin yksityiskohtiin. Esimerkiksi kyberturvallisuuteen ja varautumiseen liittyvät järjestelyt ovat tietoturvasyistä salassa pidettäviä, eikä niitä voitu haastatteluissa käsitellä kovin yksityiskohtaisesti. Haastatteluissa oli myös pieniä eroja sen osalta, kuinka yleisellä tasolla haastateltavat halusivat vastauksissaan pysytellä: osassa haastatteluista käsiteltiin melko yksityiskohtaisiakin asioita, kun taas osassa pysyteltiin hieman yleisemmällä tasolla, joten haastattelut olivat luonteeltaan hieman erilaisia. Tämän takia haastatteluiden vertaaminen keskenään ei ollut täysin ongelmatonta.

Haastatteluja pidettiin kokonaisuudessaan seitsemän kappaletta, joten tutkielman empiirinen aineisto on rajallinen, eikä niiden avulla välttämättä pystytä tuottamaan täysin kattavaa kuvaa siitä, millä tavoin digitaalisuus voi auttaa häiriötilanteisiin liittyen. Tarkoituksena ei ole siis tarjota yksityiskohtaista kuvasta siitä millä kaikilla tavoin digitaalisuutta voidaan tässä hyödyntää, vaan nostaa esiin laajempia kokonaisuuksia tähän liittyen. Haastateltavia oli kuitenkin erilaisista työtehtävistä ja taustoista, joten tutkimukseen saatiin laajasti näkemyksiä ja kokemuksia erilaisista näkökulmista. Rajallisesta aineistosta huolimatta tutkielma pyrkii luomaan uutta tietoa tähän melko uuteen tutkimusalueeseen liittyen, jota voidaan hyödyntää esimerkiksi aihetta käsittelevässä jatkotutkimuksessa.

4.5.2 Tutkimuksen laatu

Erikssonin ja Kovalaisen (2008) mukaan laadullisen tutkimuksen laatua voidaan arvioida neljän laatukriteerin pohjalta, joita ovat tutkimuksen luotettavuus, siirrettävyys, uskottavuus ja yhdenmukaisuus. Näitä kriteerejä käytetään myös tämän tutkielman laadun arviointiin, jota käsitellään seuraavaksi yksi laatukriteeri kerrallaan.

Tutkimuksen luotettavuudella viitataan siihen, että tutkimuksessa tulee tarjota lukijalle tieto siitä, miten tutkimusprosessi on toteutettu. Tämän kannalta on tärkeää, että tutkimusprosessi on dokumentoitu ja se on toteutettu loogisesti sekä johdonmukaisesti. (Eriksson & Kovalainen 2008.) Tutkielman luotettavuuden lisäämiseksi tutkimusprosessin kulku ja siihen liittyen tehdyt päätökset perusteluineen on esitelty mahdollisimman kattavasti edellä tutkielman metodologialuvussa.

Tutkimuksen siirrettävyys kuvaa sitä, kuinka hyvin tutkimus tai sen osat vertautuvat ja liittyvät aikaisempaan aihetta käsittelevään tieteelliseen tutkimukseen. Tutkimuksen tuloksilla pitäisi siis olla ainakin jonkinlainen yhteys aikaisempaan vastaavaan tutkimukseen. Siirrettävyyden osalta ei ole tarkoitus, että oma tutkimus olisi täydellinen kopio aikaisemmasta tutkimuksesta, vaan ennemminkin tarkoituksena on löytää linkkejä ja yhteyksiä niihin. (Eriksson & Kovalainen 2008.) Tutkielmassa aikaisempaa tutkimusalueeseen liittyvää tutkimusta on esitelty laajasti teorialuvuissa 2 ja 3. Myös tutkielman tulosluvussa on pyritty vertailemaan saatuja tuloksia aikaisemman tutkimuksen perusteella siirrettävyyden parantamiseksi. Tutkielmassa tulosten vertaamista aikaisempaan tutkimukseen kuitenkin hankaloittaa se, että tutkimusalue on melko uusi eikä aikaisempaa vastaavaa tutkimusta ole kovinkaan paljoa.

Tutkimuksen uskottavuuden avulla arvioidaan ovatko tutkielmassa tehdyt johtopäätökset ja tulkinnat loogisia sekä tukeeko tutkielman aineisto näitä päätelmiä. Teoriassa muidenkin tutkijoiden pitäisi siis samaa aineistoa käyttämällä tehdä samankaltaisia tulkintoja ja olla samaa mieltä tutkielmassa tehtyjen väitteiden kanssa, jotta tutkimuksen uskottavuus on hyvällä tasolla. (Eriksson & Kovalainen 2008.) Tutkielman uskottavuuden kasvattamiseksi tutkielman tulosluvussa on esitelty suoria lainauksia aineistosta sekä taulukoita, joissa näkyy haastattelulainauksia sekä aineiston perusteella luotuja koodeja ja teemoja. Näiden tarkoituksena on havainnollistaa sitä, miten tutkimuksen tulkintoihin on päädytty aineiston perusteella.

Tutkimuksen yhdenmukaisuus viittaa siihen, että tuloksissa tehdyt tulkinnat perustuvat aidosti kerättyyn aineistoon, eikä niitä ole esimerkiksi keksitty itse (Eriksson & Kovalainen 2008). Tämän tutkielman osalta tuloksissa tehdyt tulkinnat perustuvat siis pidettyihin haastatteluihin, joita oli yhteensä seitsemän kappaletta. Yhdenmukaisuuden kasvattamiseksi tutkielmassa tehdyt tulkinnat on pyritty yhdistämään selkeästi aineistoon esimerkiksi lisäämällä tuloslukuun lainauksia haastatteluista sekä

taulukkomuodossa että osana tekstiä. Myös tutkielman johtopäätösluvussa on pyritty kuvaamaan tuloksien ja tulkintojen välillä olevaa linkkiä yhdenmukaisuuden lisäämiseksi.

4.5.3 Eettisyys

Tutkielma on sitouduttu tekemään eettisesti ja hyvän tieteellisen käytännön mukaisesti. Kaikki haastateltavat osallistuivat tutkielmaan vapaaehtoisesti, eikä heitä tai heidän edustamiaan yrityksiä voida tunnistaa tutkielmassa olevista tiedoista tai lainauksista. Haastateltaville oli kerrottu haastattelussa käsiteltävästä aiheesta ja haastatteluteemoista hyvissä ajoin etukäteen, sillä on eettisesti tärkeää, että tiedonantaja tietää mitä aihetta haastattelussa käsitellään (Tuomi & Sarajärvi 2018). Näin he tiesivät millaisia aihealueita haastattelussa käsitellään ja pystyivät halutessaan valmistautumaan haastattelua varten.

Ennen haastattelun aloittamista haastateltavien kanssa käytiin läpi haastattelusuostumuslomake (liite 2), ja he antoivat suostumuksensa haastatteluun ja sen äänittämiseen tutkimustarkoituksessa. Haastateltaville tarjottiin myös mahdollisuus keskeyttää haastattelu halutessaan milloin tahansa tai olla vastaamatta haastattelukysymyksiin. Ennen haastattelun aloittamista haastateltaville myös korostettiin, että he saavat itse määritellä kuinka yleisellä pysyttelevät vastauksissaan, sillä tutkielmassa käsiteltävät aiheet saattavat olla sensitiivisiä, eikä niitä välttämättä haluta kertoa yksityiskohtaisesti julkiseen tutkimukseen. Haastattelun lopuksi haastateltavilta kysyttiin myös haluavatko he saada haastattelun litteroinnin itselleen tarkistettavaksi. Tämän avulla he saivat mahdollisuuden käydä haastatteluissa kertomansa asiat läpi, jolloin he pystyivät halutessaan ilmoittamaan mahdollisista haastatteluissa kertomistaan asioista, joita pitäisi muokata tai ei saisi käyttää tutkielmassa ollenkaan esimerkiksi tietoturvasyistä. Haastateltavista kaksi halusi tarkistaa haastattelulitteroinnin haastattelunsa jälkeen, mutta litterointeihin ei tarvinnut tehdä muutoksia.

Tutkimusaineiston hallinta on myös oleellinen osa eettisesti toteutettua tutkimusta. Tutkielman aineistonhallintasuunnitelma valmisteltiin ennen aineiston keräämisen aloittamista tutkimusaineiston hallinnan tueksi. Lopullinen versio aineistonhallintasuunnitelma löytyy tutkielman liitteistä (liite 3). Aineistonhallintasuunnitelmaa myös päivitettiin tutkimuksen ja aineiston keräämisen

sekä käsittelyn edetessä, jotta suunnitelma pysyi ajan tasalla koko tutkimusprosessin ajan. Eettisyyden varmistamiseksi tutkielman tutkimusprosessi ja siihen liittyvät valinnat on myös pyritty kuvaamaan mahdollisimman kattavasti tutkielman metodologialuvussa.

5 Tulokset

Tässä luvussa käydään läpi tutkielman empiiriseen osuuden tulokset. Ensimmäisenä esitellään tarkemmin minkälaisia häiriöitä energiasektorin yrityksissä voidaan haastateltavien mukaan kohdata, ja minkälaiset tapahtumat voivat aiheuttaa häiriötilanteita. Näin voidaan paremmin hahmottaa minkälaisiin häiriöihin liittyen digitaalisia teknologioita ja tietojärjestelmiä voidaan hyödyntää. Tämän jälkeen perehdytään siihen miten digitaalisuutta, digitaalisia teknologioita ja tietojärjestelmiä hyödynnetään näissä häiriötilanteissa ja digitaalisen resilienssin eri vaiheissa, joita ovat häiriöiden ennaltaehkäisy, häiriötilanteessa selviytyminen ja niistä palautuminen sekä häiriöistä oppiminen ja toiminnan kehittäminen.

Tulokset sisältävät haastattelulainauksia, ja haastateltaviin viitataan lyhenteillä H1, H2, H3, H4, H5, H6 ja H7 sivulla 45 olevan taulukon 2 mukaisesti. Haastatteluaineiston analysoimisessa käytetty koodaustaulukko on kokonaisuudessaan tutkielman liitteissä (liite 5).

5.1 Häiriötilanteet energiasektorin yrityksissä

Haastatteluissa haastateltavat toivat esiin useita erilaisia tapahtumia ja tilanteita, jotka voivat aiheuttaa energiasektorin yrityksille vaikutustensa laajuudelta vaihtelevia toimintahäiriöitä. Erilaisia häiriötilanteita ja niiden aiheuttajia on hyvin paljon, joten jokaista niistä ei käydä tässä luvussa yksityiskohtaisesti läpi, vaan ne käsitellään pääpiirteittäin.

Potentiaalisia häiriötilanteita on siis hyvin paljon, ja ne voivat johtua sekä ulkoisista tapahtumista, kuten esimerkiksi tahallisesta ulkoisen toimijan sabotaasista että sisäisistä tapahtumista, kuten konfigurointivirheistä. Lisäksi on huomioitavaa, että osa häiriön aiheuttajista oli selkeästi digitaalisuuteen ja digiympäristöön liittyviä, josta esimerkkinä kyberhyökkäykset, kun taas toiset häiriötilanteet, kuten esimerkiksi tulipalon aiheuttamat häiriöt eivät liittyneet suoraan digitaalisuuteen. Huolimatta siitä liittyivätkö häiriöt itsessään digitaalisuuteen, haastatteluiden perusteella oli selvää, että erilaisilla digitaalisilla keinoilla pystyttiin vaikuttamaan molempiin ryhmiin kuuluviin häiriöihin eikä ainoastaan digitaalisuuteen liittyviin. Haastatteluissa esiin tulleet häiriöihin johtavat tapahtumat ja tilanteet on esitelty taulukossa 3, jossa ne on myös jaoteltu digitaalisuuteen liittyviin häiriöihin sekä niin sanotusti perinteisiin häiriöihin, jotka eivät

sellaisenaan liity digitaalisuuteen. Jaottelussa on kuitenkin huomioitava myös se, että osa näistä häiriöistä ja niiden aiheuttajista voivat kuulua molempiin näistä kategorioista. Esimerkiksi tahallinen häirintä voi olla sekä fyysistä että digitaalisessa ympäristössä tapahtuvaa.

Taulukko 3. Häiriötilanteiden aiheuttajat haastateltavien mukaan: Digitaaliset ja perinteiset

Digitaalinen häiriö	**Perinteinen häiriö**

• IT-ongelmat
  ○ Käytettävyysongelma, IT-teknologia ei käytettävissä
  ○ Ongelma ohjelmistossa/tietokannassa
  ○ Mahdollisesti hyökkäyksen aiheuttama
• Kyberhyökkäys
  ○ Palvelunestohyökkäys
  ○ Tietomurto
  ○ Verkkoon tunkeutuminen
  ○ Virus
• Tahallinen sabotaasi, haitan aiheuttaminen
• Tahallinen vaikuttaminen/häirintä
• Datavääristymä, datavuoto
• Internet alhaalla
  ○ Verkot poikki
  ○ Hyökkäys
• Kriittisen toimittajan ongelma
  ○ Tietoliikenneyhteydet
• Muutostilanteet (esim. päivitykset)
• Konfigurointivirheet, käyttövirheet, näppäilyvirheet
• Etäohjauksen toiminta/yhteyshäiriö
	• Laitevika, mekaanisten laitteiden vioittuminen
	• Sääolosuhteet, luonnonilmiöt
	  ○ Voimakas myrsky
	  ○ Jäätävä sade
	  ○ Kuurahuurre
	• Tahallinen sabotaasi, haitan aiheuttaminen
	• Tahallinen vaikuttaminen/häirintä
	• Tulipalo
	• Kriittisen toimittajan toimintahäiriö
	  ○ Sähkön saanti estynyt
	  ○ Maakaasun saanti estynyt
	• Pandemia, henkilöstöön liittyvä häiriö
	• Prosessin toimintahäiriö

Kysyttäessä siitä millaisia häiriöitä energiasektorin yrityksessä voidaan kohdata ja mitkä tapahtumat niitä voivat aiheuttaa kävi ilmi, että haastateltavan työtehtävällä ja roolilla oli vaikutus siihen millaisia häiriöitä he pitävät yleisimpinä tai todennäköisimpinä. Esimerkiksi tuotantojohtajana toimiva H3 piti yleisimpänä häiriönä tuotantolaitosten mekaanisten laitteiden vikaantumista, kun taas IT-roolissa toimiva H1 piti erilaisia IT-ongelmia kaikista todennäköisimpinä, mutta totesi lisäksi myös näin:

> ”Kyllähän nämä mulla menee tuonne IT-sektoriin kaikki ja mä rupesin miettimään johtuuko se siitä, että mä työskentelen niiden kanssa, niin mä en näe mitään muuta.”

Haastateltavat kokivat siis itsekin heidän työtehtävällään olevan yhteys siihen millaisia häiriöitä he pitävät erityisen yleisinä tai todennäköisinä. Haastateltavilla oli kuitenkin merkittävästi toisistaan poikkeavia työtehtäviä, eivätkä kaikki työskennelleet esimerkiksi ainoastaan IT-rooleissa, joten haastatteluissa tuotiin esiin laajasti erilaisia häiriöitä ja niiden aiheuttajia.

Osei-Kyei ym. (2021) tunnistivat tutkimuksessaan yhteensä 31 mahdollista uhkaa kriittiselle infrastruktuurille, mikä kuvastaa hyvin niiden suurta määrää. Koska näitä mahdollisia häiriötilanteita on niin runsaasti, voidaan niitä jaotella eri kategorioihin. Esimerkiksi kysyttäessä mistä häiriötilanteet voivat aiheutua, turvallisuusjohtajana toimiva H6 jakoi mahdolliset häiriöiden aiheuttajat näin:

> ”--kolmesta näkövinkkelistä voi tulla tämmöisiä häiriötilanteita. Toisaalta voi olla, että meillä on jotenkin, meidän teknologia hajoaa, joku kriittinen komponentti hajoaa, ja siitä seuraa sitten ongelmia. Toinen vaihtoehto on se, että jotenkin joku meidän ihmisistä tai meidän toimintaan liittyvistä ihmisistä tekee virheen ja siitä seuraa jotakin. Ja sitten kolmas on tietysti se näkökulma, että joku tarkoituksellisesti haluaa aiheuttaa pahaa meille.”

Nämä kolme näkökulmaa on tunnistettu myös Osei-Kyein ym. (2021) tutkimuksessa, jossa teknologian hajoaminen ja inhimilliset virheet ovat molemmat lajiteltu teknisiin uhkiin, ja tahallisesti aiheutettu haitta taas on määritelty sosiaaliseksi uhaksi. Tahallista haitantekoa voi esiintyä esimerkiksi fyysisenä sabotaasina, mutta myös digitaalisessa ympäristössä tapahtuvina kyberhyökkäyksinä. Inhimillisiin virheisiin liittyen haastatteluissa kävi ilmi, että niitä tulee aina tapahtumaan, mutta niitä voidaan pyritään minimoimaan digitaalisuuden avulla esimerkiksi testauksen automatisoinnin kautta.

Yksi mahdollinen vakavan häiriötilanteen aiheuttaja, joka nousi esiin jokaisessa haastattelussa liittyi kyberturvallisuuteen ja erilaisten kyberhyökkäysten riskiin ja yleistymiseen. Jokainen haastateltava piti kyberhyökkäyksiä aitona ja merkittävänä riskinä. Kyberturvallisuuden eteen tehdään yrityksissä jatkuvasti töitä ja hyökkäyksiin varautuminen on tärkeä osa jokapäiväistä toimintaa. Erilaisten digitaalisten järjestelmien yleistyminen ja jatkuvasti kasvava rooli kriittisessä infrastruktuurissa lisää sen houkuttelevuutta erilaisille kyberuhille (Genge ym. 2015). Käsiteltäessä mahdollisia häiriötilanteita H1 toi erilaisten kyberuhkien riskin esiin:

> ”voi olla myös jonkinlainen kyberjuttu, joka voisi olla virus, jonkinlainen tunkeutuminen meidän verkkoon, jolla voisi aiheuttaa merkittävän häiriön tai sitten tällainen denial of service -tyyppinen juttu, joka laittaisi järjestelmät kumoon.”

Vaikka mitään tarkkaa arviota onkin vaikea tehdä, olivat haastateltavat pitkälti sitä mieltä, että kyberuhkien riski on viime vuosien aikana kasvanut. Muun muassa World Economic Forum (2023) ennustaakin kriittiseen infrastruktuurin kohdistuvien kyberhyökkäysten lisääntyvän entisestään. Kyberhyökkäysten yleisyydestä kysyttäessä H3 totesi näin:

> ”On ilman muuta, (kyberhyökkäysten uhka) on merkittävästi lisääntynyt. Ja myös tavallaan konkreettiset uhat ovat sitä kautta kasvaneet paljon. Esimerkiksi äskettäin oli laaja palvelunestohyökkäys, joka kohdistui moneen julkisen sektorin toimijaan ja energiayhtiöön, ja me olimme yksi niistä. Tällaista ei siis ole aikaisemmin ollut ollenkaan.”

Aikaisemman kirjallisuuden sekä haastattelujen perusteella on siis selvää, että kyberhyökkäykset ovat nykypäivänä merkittävä uhka niin energiasektorille kuin muillekin kriittisen infrastruktuurin yrityksille ja niiden resilienssille. Kyberhyökkäykset tapahtuvat luonnollisesti digitaalisessa ympäristössä, joten erilaiset digitaaliset teknologiat ja tietojärjestelmät ovat merkittävässä roolissa näiden kyberuhkien torjumisessa. Kyberturvallisuutta ja kyberuhkien torjumista erilaisin keinoin voidaan siis pitää merkittävänä osana digitaalista resilienssiä.

5.2 Digitaalisuus häiriöiden ennakoimisessa ja ennaltaehkäisemisessä

Haastattelujen perusteella digitaalisuuden rooli oli erityisen merkittävä häiriötilanteiden ennakoimisessa ja ennaltaehkäisemisessä, joka on oleellinen osa resilienssiä. On luonnollisesti toivottavaa, että erilaisten häiriöiden syntyminen pystytään estämään proaktiivisesti, jolloin niiden haittavaikutukset eivät pääse realisoitumaan. Häiriöiden ennakoimiseen ja ennaltaehkäisemiseen liittyviä teemoja, jotka nousivat haastatteluaineistossa esiin ovat valvonta- ja monitorointijärjestelmien tärkeä rooli sekä mittausten ja IoT:n hyödyntäminen.

5.2.1 Valvontajärjestelmät osana digitaalista resilienssiä

Erilaiset digitaaliset valvonta- ja monitorointijärjestelmät ovat tärkeä osa häiriöiden havaitsemista ja estämistä, ja tämä nostettiin esiin usean eri haastateltavan osalta. Bohin ym. (2023) mukaan yksi tärkeimmistä digitaalisten teknologioiden ominaisuuksista häiriöihin ja ulkoisiin iskuihin liittyen onkin niiden älykäs havaitsemiskyky, joka voi auttaa organisaatioita havaitsemaan mahdollisia häiriötilanteita ennen kuin ne pääsevät toteutumaan. Kysyttäessä tietojärjestelmien ja digitaalisten teknologioiden roolista häiriötilanteiden ennakoimisessa, H2 korosti juuri valvomojärjestelmien merkitystä:

> ”Valvomojärjestelmät ovat meillä tosi iso IT-alue -- Jos oletettaisiin kaiken toimivan aina moitteitta, niin eihän meillä olisi koko valvomojärjestelmiä, emmehän me käyttäisi sellaisia mihinkään. Eli kyllä meillä käytetään paljon digitaalisia teknologioita tähän.”

Haastatteluissa kävi ilmi, että valvontajärjestelmien avulla voidaan seurata monenlaisia asioita, kuten esimerkiksi sovellusten ja järjestelmien toimintaa, tietokannan tai tietoliikenneyhteyksien tilaa taikka erilaisten laitteiden toimintaa ja mahdollisia ongelmia. Näiden lisäksi valvontajärjestelmiä voidaan käyttää verkon monitorointiin ja verkkoliikenteen valvomiseen, joka on tärkeää kyberhyökkäysten havaitsemiseksi ja estämiseksi. Valvontajärjestelmien toiminta on jatkuvaa, ja ne ovat tärkeässä roolissa häiriöiden estämisessä, sillä niiden avulla häiriöitä syntyminen pystytään välttämään kokonaan tai ainakin puuttumaan niihin mahdollisimman nopeasti. Kysyttäessä tilanteesta, jossa digitaalisen teknologian avulla on onnistuttu estämään häiriön syntyminen, H5 antoi konkreettisen esimerkin siitä, miten valvontajärjestelmää voidaan hyödyntää tässä:

> ”-- yhden muuntajan kanssa oli sellainen tilanne, että nähtiin siellä sellaiset vikakaasupitoisuudet rupesi selkeästi viikonlopun aikana nousemaan, niin otettiin se hallitusti ja suunnitellusti käytöstä pois, eikä niin, että se olisi häiriön omaisesti lauennut mahdollisesti huonolla hetkelläkin.”

Digitaaliset valvontajärjestelmät ovat siis merkittävä osa energiasektorin yritysten toimintaa, ja niiden avulla voidaan estää erilaisten häiriöiden syntyminen ja niiden eskaloituminen. Digitaalisuuden hyödyntäminen tässä valvonta- ja monitorointitarkoituksessa on havaittu myös aikaisemmassa digitaalista resilienssiä käsittelevässä tutkimuksessa (esim. Boh ym. 2023). Valvontajärjestelmien käyttämistä voidaan siis pitää yhtenä merkittävänä osana digitaalista resilienssiä, ja ne auttavat kriittisen infrastruktuurin yrityksiä ennakoimaan ja ennaltaehkäisemään häiriöitä.

Tämän lisäksi on huomioitavaa, että valvontajärjestelmien avulla voidaan myös varmentaa, että häiriötilanne on ohi ja normaaliin toimintaan palaaminen on mahdollista. Valvontajärjestelmiä voidaan häiriöiden ennaltaehkäisemisen ja ennakoimisen lisäksi hyödyntää myös häiriöistä palautumisessa. Haastattelulainauksia ja koodeja, joiden perusteella valvontajärjestelmien merkitystä ilmentävä teema on muodostettu on esitelty alla taulukossa 4.

Taulukko 4. Koodit ja teema: Valvontajärjestelmät

Lainaus	Koodi	Teema
”Onhan meillä kaikenlaisia järjestelmiä, joiden ainoa tehtävä on monitoroida, että asiat toimii kuten niiden pitäisi toimia. Eli tietojärjestelmät toimii niin kuin niiden pitää toimia. Varmaan tämä on sellainen sektori, joka olisi täysin mahdotonta ilman tietojärjestelmiä.” (H1)	Tietojärjestelmien toiminnan valvominen	Valvontajärjestelmät osana digitaalista resilienssiä
”Valvomojärjestelmät ovat meillä tosi iso IT-alue, joka nimenomaan on järjestelmä, joka on suunniteltu tähän. Jos oletettaisiin kaiken toimivan aina moitteitta, niin eihän meillä olisi koko valvomojärjestelmiä, emmehän me käyttäisi sellaisia mihinkään. Eli kyllä meillä käytetään paljon digitaalisia teknologioita tähän.” (H2)	Valvontajärjestelmät merkittävä IT-alue	Valvontajärjestelmät osana digitaalista resilienssiä
”Kyllähän me koko ajan verkkoa monitoroidaan ja sitten poikkeamia löydetään, ja siten niihin päästään voisi sanoa jopa yleensä puuttumaan proaktiivisesti eli ennen kuin kriisi tapahtuu.” (H2)	Verkon monitorointi valvontajärjestelmillä	Valvontajärjestelmät osana digitaalista resilienssiä
”Ja siis kyllähän kaikkea, mitä aikaisemmin asiat havaitaan, ja jos joku hyökkäys tai häiriö kohdistuu johonkin järjestelmään, niin silloinhan se, joko se tai joku valvova järjestelmä sitten sen huomaa, ja sitten pystytään aloittamaan torjuntatoimet. Tai voi olla jotain automaattisia torjuntatoimia tai eristystoimintoja, mitkä toimii sitten itsenäisesti siinä tilanteessa.” (H4)	Häiriön havaitseminen valvontajärjestelmällä	Valvontajärjestelmät osana digitaalista resilienssiä
”Että kyllähän ilman jotain digitaalista valvontaa, niin sitten tavallaan joku prosessihäiriö pääsee paljon isommaksi.” (H4)	Valvontajärjestelmä prosessihäiriön estämisessä	Valvontajärjestelmät osana digitaalista resilienssiä
” Ja kyllä se online-valvonta laitteille ja niiden seuranta, niiden kunnon seuranta ja tilanteen seuranta on kaiken a ja o” (H7)	Laitteiden seuranta valvontajärjestelmillä	Valvontajärjestelmät osana digitaalista resilienssiä

Lainaus	Koodi	Teema
”Mutta seurataan erinäköisillä etävalvontajärjestelmillä erinäköisiä laitteita, että ne kaikki on kunnossa.”(H7)	Laitteiden seuranta valvontajärjestelmillä	Valvontajärjestelmät osana digitaalista resilienssiä

Digitaalista teknologiaa hyödynnetään kriittisen infrastruktuurin yrityksissä tämän lisäksi myös yleisen turvallisuuden valvonnassa. Tästä esimerkkejä ovat muun muassa palohälyttimet sekä erilaiset turvallisuutta lisäävät valvontajärjestelmät, kuten valvontakamerat ja muu turvallisuusteknologia. Koska tahallinen sabotaasi tunnistettiin kaikissa haastatteluissa mahdolliseksi häiriön aiheuttajaksi, ei näiden merkitystä tule väheksyä, vaan näitä teknologioita voidaan pitää yhtä lailla merkittävänä osana digitaalista resilienssiä.

5.2.2 Häiriöiden ehkäiseminen mittauksien ja IoT:n avulla

Toinen teema, joka korostui haastatteluissa häiriöiden ehkäisemiseen liittyen oli digitaalisten ratkaisujen, kuten erilaisten mittausten ja IoT-teknologian käyttäminen häiriöiden ennaltaehkäisemisessä. Erityisesti näitä hyödynnetään laitevikojen estämisessä ja kunnossapidon tukena, mutta myös muita soveltamismahdollisuuksia on. Laitteiden vioittumiset ja fyysisten komponenttien hajoamiset ovat merkittäviä uhkia ja mahdollisia häiriötilanteiden aiheuttajia kriittisen infrastruktuurin yrityksissä (Osei-Kyei ym. 2021), joten niiden estäminen on oleellista.

Digitaalisuutta ja erilaisia teknologioita voidaan haastateltavien mukaan hyödyntää erityisesti laitevikojen estämisessä erilaisilla mittauksilla. Tästä esimerkkinä on värinämittaus, jossa mitataan ja analysoidaan laitteiden värähtelyjä mekaanisten vikojen ennakoimiseksi. Myös muunlaisia mittauksia on, joiden avulla pyritään huomaamaan tulevia mahdollisia ongelmia. Trembaly ym. (2023) kertovatkin, että erilaiset mittausteknologiat ovat tärkeitä digitaaliselle resilienssille, ja haastatteluaineisto tukee tätä näkemystä. Todettuaan ensin laitosten ja laitteiden teknisten tai mekaanisten vikojen olevan mahdollisia häiriön aiheuttajia, haastateltava H7 kertoi, että digitaalisuutta voidaan hyödyntää niiden estämisessä online-mittausten avulla:

> ”Meillä kriittisistä laitteista järjestään tällaisia online-mittauksia. Seurataan niiden tilannetta, vaikka erilaisia lämpötiloja tai paineita tai muita tiloja -- jos siellä on jotakin poikkeavaa, niin pystytään ennakoimaan ja tekemään

> toimenpiteitä ennen kuin ne realisoituu, vaikka nyt laitoksen alasajoksi tai sen tyyppiseksi.”

Digitaalisten teknologioiden avulla voidaan siis suorittaa mittauksia, joissa kerätään laitteista eri muodoissa olevaa dataa, jota voidaan hyödyntää laitevikojen ehkäisemissä ja havaitsemissa. Energiasektorin yritysten toiminnassa erilaiset fyysiset laitokset ja laitteet ovat oleellinen osa toimintaa, joten niiden häiriöiden estäminen on tärkeää ja digitaalisuudella on tässä merkittävä rooli. Toinen konkreettinen esimerkki digitaalisuuden hyödyntämisestä laitteiden kunnossapidossa ja häiriöiden ehkäisemisessä on esineiden internetin eli IoT-teknologian hyödyntäminen tässä tarkoituksessa. IoT onkin Bohin ym. (2023) mukaan hyvä esimerkki digitaalisesta teknologiasta, jonka avulla voidaan kerätä ja tuottaa tietoa muun muassa häiriöiden estämiseen liittyen. Kysyttäessä miten digitaalisia keinoja voidaan käyttää häiriöiden ennakoimisessa ja estämisessä, H5 kertoi, että IoT-teknologiaa on alettu hyödyntämään erityisesti kunnossapitoon liittyen:

> ”Meillä tuolla kunnossapitopuolella, niin tätä iotti-tekniikkaa (IoT) esimerkiksi kovasti otetaan käyttöön ja mietitään kuinka se pystyy antamaan meille ennakoivia signaaleja siitä, että joku juttu on hajoamassa.”

IoT:n osalta on huomioitava myös se, että sille on myös paljon muita käyttötarkoituksia ennakoivan kunnossapidon lisäksi. Haastatteluissa ilmeni, että IoT-teknologiaa hyödynnetään kunnossapidon lisäksi myös esimerkiksi erilaisin sensorein varustetuissa palohälyttimissä ja muussa valvontateknologiassa.

Myös aikaisemmassa tutkimuksessa tiedon tuottaminen ja kerääminen mahdollisiin häiriöihin ja niitä aiheuttaviin tekijöihin on tunnistettu oleelliseksi osaksi digitaalista resilienssiä (Boh ym. 2023). Haastattelujen perusteella datan kerääminen erilaisin keinoin, kuten mittauksilla ja IoT-teknologian avulla on tärkeä osa häiriöiden ennakoimista ja estämistä erityisesti laitevikojen osalta. Häiriöiden ennakoimiseen ja ennaltaehkäisyyn liittyen muodostui teema IoT ja mittaukset häiriöiden ennakoinnissa, ja tähän teemaan liittyviä lainauksia ja koodeja on esitelty alla taulukossa 5.

Taulukko 5. Koodit ja teema: IoT ja mittaukset

Lainaus	Koodi	Teema
” Siellä on just tämmösiä erilaisia Iot-tyyppisiä ratkaisuja, meilläkin taitaa olla jossakin käytössä. Yritetään jonkin järjestelmän avulla vähän haistella, että prosessi toimii niin kuin pitääkin.” (H1)	IoT	IoT ja mittaukset häiriöiden ennakoimisessa

Lainaus	Koodi	Teema
”Lämpötila-anturit, lämmöt lähtevät nousemaan, jos joku rupeaa kuumenemaan siellä. Meillä tällainenkin kokeilu oli tässä, yleensä laitteet alkavat pitämään vähän epänormaalia ääntä ennen kuin ne hajoavat, niin tämmöiseenkin voi IoT:lla päästä kiinni ja muuta” (H5)	IoT	IoT ja mittaukset häiriöiden ennakoimisessa
”Sillä tavalla tämmöistä ennaltaehkäisevää, kunnossapitoon tarjoaa digitaalisuus mahdollisuuksia ilman muuta” (H5)	Digitaalisuus ennakoivassa kunnossapidossa	IoT ja mittaukset häiriöiden ennakoimisessa
”esimerkiksi on erilaisia värinämittauksia, joilla kerätään dataa jonkun vaikka moottorin pärinöistä. Ja sillä pystytään, sitä tietoa analysoimalla pystytään ennakoimaan mahdollisia tulevia mekaanisia vikoja.” (H3)	Värinämittaus	IoT ja mittaukset häiriöiden ennakoimisessa
”ja varmaan monessa muussakin paikassa tehdään tämmöistä ennakoivaa kunnossapitoa, että mitataan vaikka jonkun pumppujen värinää semmoisilla laitteilla, että sitten mitä ei silmällä tai korvalla välttämättä kuule, että sitten tavallaan siellä kun värinät rupee lisääntymään, niin sitten se ehkä indikoi sitä, että jos homma jatkuu näin, niin kuukauden päästä pumppu hajoaa, ja siinä ehkä se digitaalisuus luo ymmärrystä siitä tilannekuvasta.” (H4)	Digitaalisuus ennakoivassa kunnossapidossa	IoT ja mittaukset häiriöiden ennakoimisessa
Mutta sitten se miten tuotantoprosessi vaihtelee ja värisee ja missä on lähellä piti -tilanteita, näistä me keräämme dataa ja meillä on paljon laaturaportointia käytettävyydestä, paine-eroista, elinkaarista eli missä kohtaa infran elinkaarta mennään, niin täällä tilastolliset menetelmät auttavat paikantamaan niitä potentiaalisia häiriökohteita ennen kuin häiriö tapahtuu.	Datan hyödyntäminen häiriöiden ennakoimisessa	IoT ja mittaukset häiriöiden ennakoimisessa

5.3 Digitaalisuus häiriötilanteissa selviytymisessä ja palautumisessa

Resilienssille on olennaista se, ettei kaikkia ongelmia pystytä aina estämään, vaan niistä täytyy myös pystyä tarvittaessa selviytymään (Wied ym. 2019). Bohin ym. (2023) mukaan tämä selviytymis- ja palautumiskyky on tärkeä osa myös digitaalista resilienssiä. Haastatteluissa ilmenikin eri tapoja, miten digitaalisuutta ja digitaalisia keinoja voidaan käyttää energiasektorin yrityksissä tukena häiriötilanteista selviytymisessä ja niistä palautumisessa. Haastatteluaineistosta nousi esiin kolme

pääteemaa tähän liittyen: päätöksenteon tukeminen ja tilannekuvan ylläpitäminen, kriittisten järjestelmien turvaaminen sekä laitosten etäohjaus.

5.3.1 Päätöksenteon tuki ja tilannekuvan ylläpitäminen

Haastattelujen perusteella digitaalisuudella ja tietojärjestelmillä on häiriötilanteita kohdatessa tärkeä tehtävä tukea häiriön selvittämiseksi tapahtuvaa päätöksentekoa. Ne auttavat ylipäätään huomaamaan, että jokin on vialla esimerkiksi luvussa 5.2.1 esiteltyjen valvontajärjestelmien avulla, ja tämän lisäksi ne auttavat saamaan tietoa kyseisestä häiriöstä ja sen mahdollisesta aiheuttajasta. Käsiteltäessä sitä, miten digitaaliset teknologiat voivat auttaa minimoimaan häiriöiden vaikutuksia, H6 kuvasi tätä prosessia näin:

> ”Oikeastaan vähän niin kuin joka kerta, kun jotakin tapahtuu, niin siinä digitaalitekniikka on mukana. Nimenomaan indikaation saaminen siitä, että jotain on nyt pielessä ja että se saadaan mahdollisimman nopeasti siihen päätöksentekoon.”

Tutkimuksessaan vastaavan havainnon ovat tehneet myös Spagnoletti ja Za (2022), joiden mukaan digitaaliset teknologiat parantavat digitaalista resilienssiä erityisesti päätöksentekoa tukemalla. Digitaalisuuden ja tietojärjestelmien rooliin päätöksenteon tukemisessa on kiinnitetty huomiota siis myös muussa digitaalista resilienssiä käsittelevässä kirjallisuudessa. Haastattelujen ja aikaisemman tutkimuksen perusteella voidaan siis tehdä johtopäätös, että digitaalisuus ja digitaalinen resilienssi auttaa yrityksiä selviytymään häiriötilanteista esimerkiksi tukemalla päätöksentekoa.

Toinen tärkeä toiminto, jossa digitaalisuus auttaa energiasektorin yrityksiä selviytymään häiriötilanteista, ja joka liittyy myös osaltaan päätöksentekoon, on tilannekuvan ylläpitäminen. Häiriötilanteissa vallitseva tilannekuva voi olla epäselvä, mikä hankaloittaa päätöstentekoa. Tremblayn ym. (2023) mukaan digitaaliset teknologiat auttavat harkittujen päätösten tekemistä epävarmassa toimintaympäristössä. Haastatteluissa ilmeni, että digitaaliset teknologiat auttavat tilannetiedon välittämisessä ja ”digitaalitekniikan avulla luodaan pohjaa tilannekuvasta päätöksenteolle”, kuten H6 asian esitti.

Häiriötilanteesta palautumisessa oikean tilannekuvan ja oikeiden tietojen merkitys on hyvin suuri. Digitaaliset teknologiat ja tietojärjestelmät auttavat saamaan häiriötilanteesta ja sen aiheuttajasta mahdollisimman paljon tietoa, jonka avulla voidaan

ryhtyä tarvittaviin toimenpiteisiin. Käsiteltäessä digitaalisten menetelmien ja tietojärjestelmien roolia häiriötilanteista palautumisessa, H5 piti tietojärjestelmiä tärkeänä häiriön selvityksessä ja palautumiseen tarvittavien tietojen keräämisessä:

> ”Tietysti meillä tietojärjestelmät on tämän sähköjärjestelmän hoitamista varten, niin niissähän niiden rooli varsinkin sähköjärjestelmän häiriön selvityksessä on oleellinen. Niiden kautta saadaan sitä tietoa siitä järjestelmästä -- että osataan tehdä oikeita johtopäätöksiä ja ruveta sitten tätä varsinaista sähköjärjestelmää häiriötilanteesta palauttamaan perustuen oikeisiin oletuksiin ja tietoihin.”

H5 kertoi myös, että heillä on tässä tarkoituksessa käytössä myös erillinen tilannekuvajärjestelmä. Digitaalisuus auttaa siis kriittisen infrastruktuurin yrityksiä palautumaan häiriötilanteista tarjoamalla päätöksentekoon tarvittavaa tietoa, jotta tiedetään kuinka ja minkälaisin toimenpitein häiriöstä palautumista tulee lähteä edistämään. Pelkästään tämä oikean tiedon kerääminen tilannekuvan ylläpitämiseksi ja päätösten tekemiseksi ei kuitenkaan sellaisenaan riitä, vaan erityisesti vaikeammista häiriöstä selviytyminen ja palautuminen edellyttää usein monien eri toimijoiden yhteistyötä, jonka digitaalisuus mahdollistaa.

Digitaalisuuden avulla voidaan sekä tavoittaa nopeasti suuri määrä ihmisiä että mahdollistaa yhteistyö näiden henkilöiden fyysisestä sijainnista riippumatta. Ilman digitaalisuutta ja virtuaalisia keinoja tällainen ei olisi mahdollista tai ainakin huomattavasti hitaampaa ja työläämpää. Spagnolettin ja Zan (2022) mukaan digitaaliset teknologiat helpottavatkin yhteistyön tekemistä ja toiminnan koordinointia häiriötilanteissa. Käsiteltäessä häiriöstä palautumista ja normaalin toiminnan jatkamista H1 kuvaili IT:n roolia siinä näin:

> ”Yksi asia mikä nousee esiin on semmoinen että kun tarvitaan luultavasti hyvin paljon erilaisia osapuolia, niin että nämä eri osapuolet pystyvät keskenään tekemään yhteistyötä virtuaalisesti sen ongelman selvittämiseksi -- niin sitten tullaan siinä mielessä IT:hen, että niiden pitäisi pystyä etänä ja virtuaalisesti tekemään näitä toipumisjuttuja.”

Sen lisäksi, että digitaalisuuden avulla eri toimijat pystyvät tekemään yhteistyötä eri sijainneista käsin, digitaalisuus helpottaa myös ihmisten tavoittamista ja töihin kutsumista. Tämä voi olla erityisen tärkeää energiasektorin yritysten näkökulmasta esimerkiksi erilaisissa laitoksissa, joihin saatetaan tarvita pikaisesti lisää työvoimaa häiriöntilanteen syntyessä. Keskusteltaessa digitaalisuuden roolista häiriötilanteessa

selviytymisessä, H6 piti digitaalista teknologiaa hyödyllisenä juuri ihmisten tavoittamisessa:

> ”Tietysti yksi näkövinkkeli on se, että teknologiaa käytetään just ihmisen apuna -- sanotaan, että häiriötilanteessa ihan siitä lähtien, että kun tulee joku häiriötilanne, että miten me saadaan kutsuttua ihmiset selvittämään sitä häiriötilannetta.”

Digitaalisuuden avulla on siis mahdollista tavoittaa tarvittavat henkilöt nopeasti, jotta häiriöstä palautumisen edellyttämän toimenpiteet päästään aloittamaan nopeasti ja tehokkaasti. Spagnolettin ja Zan (2022) mukaan digitaaliset teknologiat parantavat digitaalista resilienssiä erityisesti tukemalla päätöksentekoa sekö edesauttamalla yhteistyötä ja toiminnan koordinointia. Tutkielman tulokset tukevat tätä näkemystä. Lainaukset ja koodit, joiden perusteella päätöksenteon tukemiseen ja tilannekuvan ylläpitämiseen liittyvä teema on muodostettu on esitelty alla taulukossa 6.

Taulukko 6. Koodit ja teema: Päätöksenteon tuki & tilannekuva

Lainaus	**Koodi**	**Teema**
”me puhutaan täällä paljon tilannekuvasta. Että nähdään missä tilanteessa se järjestelmä on, niin kyllähän siihen nämä kaikki järjestelmät, ohjelmistot ja itseasiassa meillä on ihan tilannekuvajärjestelmäkin nimeltään semmoinen, niin tuo sitä näkyvyyttä, että nähdään, siihen, että se järjestelmä on turvallisessa tilassa ja mitä mahdollisia poikkeamia siellä sitten on.” (H5)	Tilannekuvajärjestelmä	Päätöksenteon tuki ja tilannekuvan ylläpitäminen
”Ehkä siihen niin kuin johtamisen tukena ainakin on (digitaalisuudella) tärkeä rooli.” (H4)	Johtamisen tuki	Päätöksenteon tuki ja tilannekuvan ylläpitäminen
”digitaalitekniikan avulla luodaan pohjaa tilannekuvasta päätöksenteolle” (H6)	Digitaalisuus tilannekuvan luomisessa	Päätöksenteon tuki ja tilannekuvan ylläpitäminen
”Ja taas me pystytään monella tavalla tässä tiedon välityksessä, tilannetiedon välityksessä hyödyntämään digitaalitekniikkaa, jolloin tilannekuva siitä, että mitä on tapahtunut, niin se on parempi kuin se, että jotenkin manuaalisesti yritettäisiin pitää.” (H6)	Tiedonvälitys ja tilannekuvan ylläpitäminen	Päätöksenteon tuki ja tilannekuvan ylläpitäminen

5.3.2 Kriittisten järjestelmien toiminnan turvaaminen

Haastatteluissa ilmeni myös useita erilaisia digitaalisuuteen ja yritysten IT-järjestelyihin liittyviä toimenpiteitä ja ratkaisuja, joiden avulla voidaan vaikuttaa erityisesti kyberhyökkäysten aiheuttamiin häiriöihin estämällä niitä tapahtumasta, tukemalla häiriötilanteesta selviytymistä esimerkiksi varmistamalla toiminnan jatkuvuus niissä sekä myös nopeuttamalla häiriöstä toipumista. Ne olisi siis mahdollistaa sijoittaa digitaalisen resilienssin osa-alueista häiriöistä selviytymiseen ja palautumiseen sekä myös häiriöiden ennakointiin ja ennaltaehkäisyyn. Näistä muodostettiin yhdessä kriittisen järjestelmien turvaaminen -teema, joka kuvastaa kriittisten järjestelmien turvaamista ja sen roolia toiminnan jatkamisessa häiriötilanteessa, mikä on erittäin tärkeää kriittisen infrastruktuurin yrityksille. Tämän teeman muodostaneet haastattelulainaukset ja koodit on esitelty tarkemmin alla taulukossa 7.

Taulukko 7. Koodit ja teema: Kriittisten järjestelmien turvaaminen

Lainaus	Koodi	Teema
”Ja silloinhan nämä (tietojärjestelmät) on äärimmäisten tärkeitä, että meillä on perustietojärjestelmä ja sitten on olemassa joku varajärjestelmä. Sehän on sitä tietotekniikan hyödyntämistä tohon tarkoitukseen.” (H1)	Varajärjestelmä	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)
”Kyllä meillä on jonkin verran varajärjestelmiä myös, eli jos yksi kaatuu meillä -- me pystymme aika usein toisella järjestelmällä kompensoimaan toisen järjestelmän puutteita.” (H2)	Varajärjestelmä	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)
”varmasti tulee entistä tärkeämmäksi ja varsinkin se varmistaminen ettei olla yhden tai edes kahden (järjestelmän) varassa.” (H3)	Varajärjestelmä	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)
”Tärkeimpien järjestelmien pitää olla aina kahdennettuna, ja tällä tavalla, että on tärkeää tunnistaa mikä on sen tietojärjestelmän vaikutus mihinkin prosessiin.” (H5)	Järjestelmän kahdentaminen	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)
”Ja sitten lisäksi meillä on kaikki meidän serverit ja muut on kahdennettu tai kolmennettu, riippuen vähän kohteesta.” (H7)	Palvelinten kahdentaminen	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)
”meillä esimerkiksi verkkoratkaisut on siten, että meillä on kriittisyyden mukaan eriytetty verkkoja ” (H2)	Verkkojen eriyttäminen	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)

Lainaus	Koodi	Teema
”Mutta tosiaan nyt kun tällaiset huoltovarmuusverkot, kaikilla huoltovarmuuskriittisillä yhtiöillä on omat verkot, ja verkkoalueet on eriytetty.” (H2)	Verkkojen eriyttäminen	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)
”Tavallaan operatiiviset järjestelmät pidetään kokonaan irrallaan internet-maailmasta.” (H5)	Kyberuhilta suojautuminen	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)

Monissa haastatteluissa korostui erityisesti suuri tarve erilaisille varajärjestelmille, joiden merkitys on luonnollisesti sitä suurempi mitä kriittisempi järjestelmä on kyseessä. Digitaalisen resilienssissä onkin oleellista, että digitaalisuus tarjoaa tiettyä monipuolisuutta ja eri vaihtoehtoja toiminnan jatkuvuuden varmistamiseksi (Boh ym. 2023). Jos ensisijaisen järjestelmän toiminta jostain syystä estyy, täytyy pystyä siirtymään nopeasti toiseen järjestelmään. Kriittisen infrastruktuurin resilienssin kannalta tietojärjestelmien redundanssi ja sen lisääminen on tärkeää (Ouyang 2014), ja tätä korosti myös H1 käsiteltäessä tietojärjestelmien roolia toiminnan ylläpitämisessä ja häiriöstä selviytyessä:

> ”Esimerkiksi tietojärjestelmissä tällainen redundanttius on kauhean tärkeä kysymys. Jos sulla on joku komponentti tai osajärjestelmä ja se ei toimi, ja kyseessä on hyvin kriittinen prosessi, niin silloinhan sulla pitää olla joku varakomponentti tai varaprosessi, joka automaattisesti iskee päälle.”

Varajärjestelmiä voidaan siis pitää merkittävä osana toiminnan ylläpitämistä häiriötilanteissa. Näin ollen varajärjestelmät osat siis myös oleellinen osa digitaalista resilienssiä, ja erityisesti kriittisen infrastruktuurin yritysten on tärkeää varmistaa varajärjestelmien olemassaolo. Vastaavassa tarkoituksessa myös esimerkiksi palvelimien kahdentaminen ja verkkojen eristäminen toisistaan eli verkkojen eriyttäminen lisäävät järjestelmien turvallisuutta ja auttavat varmistamaan niiden jatkuvuuden myös häiriötilanteissa. Palvelimien kahdentamisen ja verkkojen eriyttämisen sijoittaminen tutkielman viitekehykseen on hieman haastavaa, sillä ne eivät itsessään ole varsinaisia digitaalisia teknologioita tai tietojärjestelmiä. Molempien niiden toteuttamiseksi kuitenkin hyödynnetään digitaalisia teknologioita, ja ne ovat haastattelujen perusteella oleellinen osa digitaalista resilienssiä, joten ne on tutkielman viitekehyksessä sijoitettu digitaalisten teknologioiden joukkoon.

Yksi merkittävä osa ainakin tiettyjen kriittisen infrastruktuurin energiayhtiöiden toimintaa on se, että ne pystyvät haastateltavien mukaan ylläpitämään vähintään kriittisen toimintansa tarvittaessa ilman internet-yhteyttä. Tästä kertoi esimerkiksi H2 kysyttäessä tietojärjestelmien tai digitaalisuuden roolista häiriöstä selviytymisessä:

> ”Meidän järjestelmä on suunniteltu siten, että me pystymme toimimaan myös ilman internettiä, eli pystytään täyttämään huoltovarmuusvaatimukset ilman internettiä.”

Tässä oli kuitenkin merkittävää myös se, että vaikka kriittisen toiminnan ylläpitäminen onnistuukin ilman internetiä, H2 kertoi järjestelmän ohjauskyvyn kuitenkin laskevan merkittävästi tällaisessa tilanteessa. Lisäksi haastatteluissa kävi ilmi, että kriittisen infrastruktuurin energiayhtiöiden prosessi- ja muille kriittisille järjestelmille on tyypillistä, etteivät ne ole yhteydessä internetiin. Tämän järjestelyn avulla pyritään minimoimaan erityisesti kyberuhkien riskiä vähentämällä ulkoisia yhteyksiä. Koska ennusteiden mukaan kyberhyökkäysten odotetaan lisääntyvän jatkossa (World Economic Forum 2023), voidaan näitä kyberuhkien minimoimiseksi tehtyjä ratkaisuja pitää tärkeänä osana kriittisen infrastruktuurin yritysten digitaalista resilienssiä.

5.3.3 Laitosten etäohjaus

Haastatteluissa selvisi myös, että etäohjattavat laitokset ovat tyypillisiä nykypäivän energiasektorin yrityksille ja digitaalisuus on niissä luonnollisesti keskeisessä roolissa. Vaikka tämä luo myös mahdollisia riskejä, voidaan etäohjausmahdollisuuden avulla nopeuttaa ja helpottaa tietyistä häiriötilanteista palautumista. Etäohjaus mahdollistaa esimerkiksi sen, että laitosten toiminta pystytään tarvittaessa pysäyttämään tai starttaamaan uudelleen häiriötilanteessakin ilman, että kenenkään tarvitsee fyysisesti mennä paikalle. Laitoksia siis ohjataan ja niiden tilaa ja toimintaa tarkkaillaan etäohjausyksiköstä tai keskusvalvomosta. Kysyttäessä siitä, miten digitaalisuus auttaa häiriötilanteista palautumisessa, H7 korosti juuri etäohjausmahdollisuuden merkitystä:

> ”Jokainen laitos on ajettavissa meidän keskusvalvomosta nappia painamalla käyntiin. Ja se tietysti nopeuttaa sitä toimintaa huomattavasti, kun paikan päälle ei ole pakko mennä.”

Mahdollisuus pysäyttää ja käynnistää laitokset uudelleen etäohjauksen avulla on siis yksi tapa, miten digitaalisuutta voidaan hyödyntää häiriöistä palautumisessa. Näin ollen sitä voidaan myös pitää digitaalista resilienssiä parantavana elementtinä, erityisesti

häiriöistä palautumisen nopeuttamisessa. Aikaisemmassa tutkimuksessa ei ole tunnistettu tätä etäohjausmahdollisuuden luomaa hyötyä häiriötilanteista palautumiseen liittyen. Esimerkkejä tämän teemaan muodostaneista lainauksista ja koodeista on alapuolella taulukossa 8.

Taulukko 8. Koodit ja teema: Laitosten etäohjaus

Lainaus	Koodi	Teema
”jos nyt on vaikka ollut häiriötilanne ja laitos on niin sanotusti alhaalla, niin meillä on eri laitostyypeillä vähän erilaisia järjestelmiä, mutta siellä on rakennettu start up -järjestelmä, eli periaatteessa se laitos, jos siellä mekaanisesti on kaikki oikeassa asennossa siellä laitoksella, niin se ohjelma pystyy starttaamaan itse itsensä.” (H3)	Laitoksen startup-järjestelmä	Laitosten etäohjaus häiriöstä palautumisessa
”me on panostettu siihen meidän keskusvalvomotoimintaan, että jokainen laitos, mitä meillä on, niin pystytään käynnistämään ja pysäyttämään sieltä meidän keskusvalvomosta.” (H7)	Etäohjaus keskusvalvomosta	Laitosten etäohjaus häiriöstä palautumisessa
”Kyllä se on elintärkeää nykypäivänä, että kaikki laitteet on etäohjattavissa ja ohjattavissa ja digitaalisesti hoidettavissa, ettei paikan päälle tarvitse mennä.” (H7)	Etäohjaus toiminnan jatkuvuuden nopeuttamisessa	Laitosten etäohjaus häiriöstä palautumisessa

5.4 Digitaalisuus häiriöistä oppimisessa ja toiminnan kehittämisessä

Yksi oleellinen resilienssin ominaisuus on, että häiriötilanteesta tai muusta haasteesta selvittyään organisaatiolla, järjestelmällä tai muulla vastaavalla toimijalla tulisi olla parempi valmius selvitä vastaavista haasteista jatkossa (Comfort ym. 2010). Tämä on myös yhtä lailla osa digitaalista resilienssiä, sillä myös sille on oleellista, että häiriön kohtaamisen ja siitä selviytymisen jälkeen tulisi olla aikaisempaa valmiimpi kohtaamaan tulevia vastaavia häiriöitä (Boh ym. 2023). Tämä vahvistui myös haastatteluissa, sillä tällaista oppimista ja jatkuvaa toiminnan kehittämistä pidetään energiasektorin yrityksissä todella tärkeänä, ja se on oleellinen osa näiden yritysten toimintaa. Jatkuvaan oppimiseen ja toiminnan kehittämiseen pyrkimistä kuvasi esimerkiksi H6 keskusteltaessa häiriötilanteista oppimista:

> ”aina kun tapahtuu jotakin, niin me pyritään ottamaan mahdollisimman tehokkaasti siitä opiksi. Eli miten me voidaan meidän toimintamenetelmiä kehittää, miten me voidaan ehkä meidän prosessia, järjestelmiä, laitteistoja kehittää.”

Voidaan siis yleisellä tasolla sanoa, että oppiminen on tärkeä osa kriittisen infrastruktuurin ja energiasektorin yritysten toimintaa ja niiden resilienssiä. Vaikka tätä oppimista voidaan toteuttaa eri tavoin, oli kuitenkin haastatteluiden perusteella selvää, että myös digitaalisuudella on oma merkittävä roolinsa tässä oppimisessa ja toiminnan kehittämisessä. Näihin liittyen nousi esiin erityisesti yksi pääteema, joka on nimetty datan keräämiseksi ja analysoimiseksi. Haastattelulainauksia ja koodeja, joiden pohjalta tämä teema muodostui on esitelty alla taulukossa 9.

Taulukko 9. Koodit ja teema: Datan kerääminen ja analysointi

Lainaus	Koodi	Teema
”Tämä kaikki (toiminnan kehittäminen) pohjautuu tuotantodataan ja kyllähän meidän pitää, me keräämme kaiken sen datan talteen. Sitten näistä meidän pitäisi löytää niitä anomalioita, se että mitkä syyt ovat johtaneet häiriötilanteeseen ja kuinka niitä voitaisiin ennakoida” (H2)	Anomalioiden etsiminen tuotantodatasta	Datan kerääminen ja analysointi
”Joo, ehdottomasti, ja varsinkin kun tuotantolaitoksillakin sitä dataa on todella paljon, niin sitten sieltä voidaan jollain louhinnan keinoin löytää semmoisia asioita, mitkä sitten indikoi (häiriöitä)” (H4)	Tuotantolaitosten datan käsittely	Datan kerääminen ja analysointi
”se on hyvin tyypillistä, että kun meillä tapahtuu jotakin, ja siinä syntyy sitä tapahtumadataa paljon, että sitä myös digitaalisesti myllätään sitä dataa” (H6)	Tapahtumadatan käsitteleminen	Datan kerääminen ja analysointi
”Kyllä mä sanoisin, että datan kerääminen ja käsittely. Niin se on ehkä sillä lailla, miten nyt ensimmäiseksi siinä voisi ajatella, että joka on ainakin hyvin keskeistä.” (H6)	Data tärkeä osa oppimista	Datan kerääminen ja analysointi
”Mutta monta kertaa tämmöisissä tapahtumissa, niin sitä tapahtumatietoa, sitä on valtavan paljon, aikatietoa, paikkatietoa. Niin digitaalitekniikkahan on ihan omaa luokkaansa sitten taas tämmöisen suuren, tavallaan bulkkitiedon käsittelyssä.” (H6)	Massadatan käsittely	Datan kerääminen ja analysointi

Haastatteluaineiston perusteella häiriöistä oppimisessa ja siten toiminnan kehittämisessä korostui erityisesti datan ja sen keräämisen merkitys. Datan keräämisen ja sen analysoimisen avulla voidaan pyrkiä esimerkiksi löytämään erilaisia indikaattoreita mahdollisista tulevista häiriöistä. Tämän osalta datan kerääminen ja sen analysoiminen voidaan sijoittaa digitaalisen resilienssin osa-alueista myös häiriöiden ennakoimiseen ja ennaltaehkäisemiseen.

Dataa kerätään ja pyritään analysoimaan erilaisin menetelmin kuten esimerkiksi tiedonlouhinnan avulla. Moni haastateltava myös korosti sitä, että erilaista dataa syntyy jatkuvasti ja sen määrä on valtava. Tämä vastaa myös Eisenbergin ym. (2019)

näkemystä, jonka mukaan kriittisen infrastruktuurin järjestelmät tuottavat koko ajan suuria datamääriä, jota voidaan sitten hyödyntää niiden resilienssin parantamisessa. Dataa syntyy ja kerätään suura määriä esimerkiksi laitoksilta ja osana tuotantoprosessia. Tästä suuresta datamäärästä voidaan käyttää käsitettä massadata (engl. big data). Barker ym. (2017) määrittelevät massadatan todella isoiksi datajoukoiksi, joita voidaan analysoida erilaisin laskennan ja tietojenkäsittelyn keinoin löytääkseen datasta trendejä, malleja ja yhteyksiä. Digitaalisten keinojen merkitys korostui erityisesti juuri massadataan liittyen, sillä sen analysoiminen tehokkaasti voi muuten olla haastavaa, kuten H6 kuvasi käsiteltäessä digitaalisten keinojen roolia osana oppimis- ja kehittymisprosessia:

> ”Niin digitaalitekniikkahan on ihan omaa luokkaansa sitten taas tämmöisen suuren, tavallaan bulkkitiedon käsittelyssä. Ei niin, että joku hakkaa Exceliin ja rupeaa ihmettelemään, vaan että pistetään koneeseen se mylläämään ja sitten se ihminen tekee sen pohdintaosuuden siinä.”

Koska dataa syntyy jatkuvasti ja niin paljon, vaaditaan sen tehokkaaseen käsittelyyn siis siihen tarkoitettua teknologiaa. Tätä havaintoa tukevat myös Jin ym. (2015), joiden mukaan massadatalle on ominaista se, että sitä syntyy nopeasti valtavia määriä eri lähteitä vaihtelevissa muodoissa, joten sen käsittely edellyttää kehittynyttä teknologiaa ja analyyttisiä malleja. Erilaisten digitaalisten datankäsittelykeinoja voidaan siis pitää osana digitaalista resilienssiä. Aikaisemman tutkimuksen mukaan massadataa voidaan hyödyntää kriittisen infrastruktuurin järjestelmien resilienssin parantamisessa esimerkiksi koneoppimisen avulla (Eisenberg ym. 2019). Koneoppimista ei kuitenkaan sellaisenaan mainittu tässä yhteydessä yhdenkään haastateltavan toimesta.

Massadataan ja datan käsittelyyn liittyen nousi esiin myös mahdollinen tulevaisuuden kehityskohde. Esimerkiksi H5 piti erittäin tärkeänä kehityskohtana sitä, että tästä valtavasta datamäärästä pystyttäisiin digitaalisuuden avulla löytämään niin sanottuja ”early warningeja” eli signaaleja siitä, että jokin on kehittymässä huonompaan suuntaan. Näiden signaalien avulla voitaisiin sitten ehtiä reagoimaan ja ryhtymään toimenpiteisiin ennen kuin se johtaa jonkinlaiseen häiriöön.

Vaikka datan keräämisen ja analysoimisen merkitys oppimiselle ja toiminnan kehittämiselle korostuikin erityisen paljon, H5 nosti esiin toisen mielenkiintoisen esimerkin miten teknologiaa hyödynnetään tähän hänen edustamassaan energiasektorin yrityksessä:

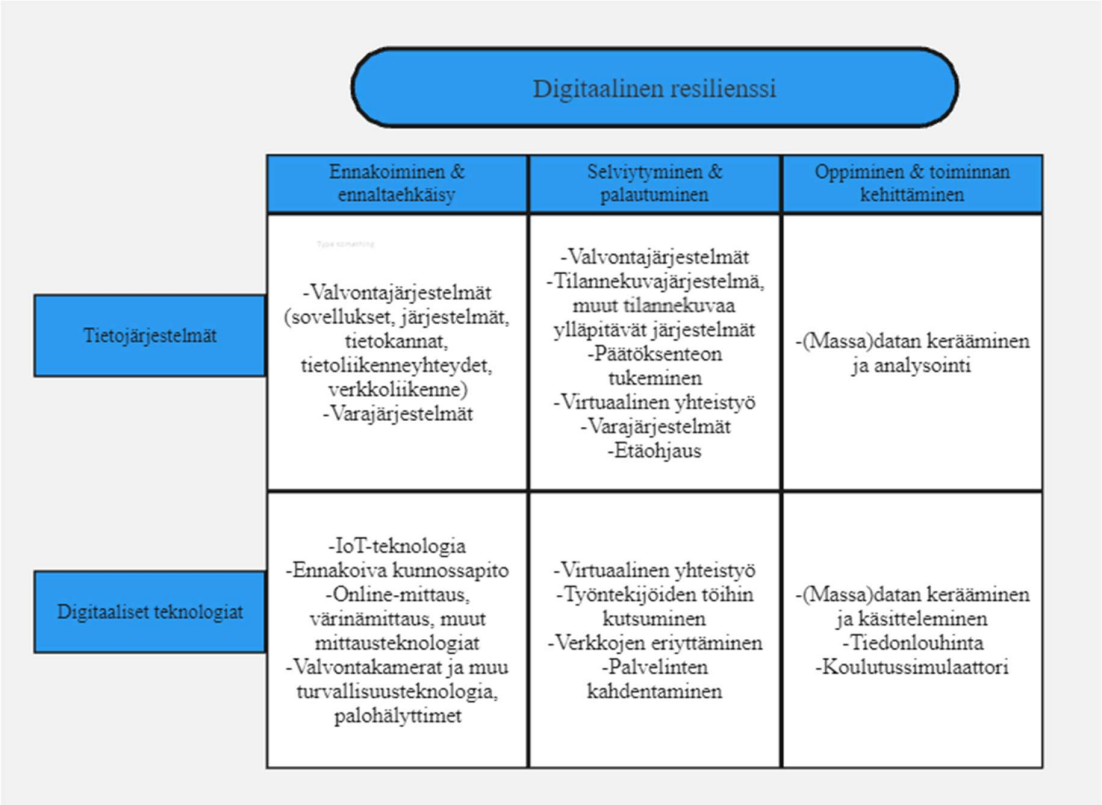
> ” Meillä on esimerkiksi tällainen koulutussimulaattori -- jossa me pystytään simuloimaan näitä erilaisia tapahtuneita häiriötilanteita ja käyttämään sitä apuna operaattorikoulutuksessa.”

Simulaattoria voidaan siis käyttää avuksi koulutettaessa työntekijöitä toimimaan häiriötilanteissa. Simuloimalla todellisia aikaisempia häiriötilanteita voidaan pyrkiä myös löytämään uusia ja tehokkaampia toimintatapoja niiden selvittämiseksi. Marcano ym. (2019) kertovat simulaattoriharjoittelun auttavan oppimaan ja kehittämään erilaisia taitoja käyttämällä tietokonepohjaisia malleja ja järjestelmää, jotka kuvaavat oikeita ilmiöitä ja prosesseja. Tässä tapauksessa kuvattava ilmiö voisi olla jonkinlainen häiriötilanne, kuten esimerkiksi kyberhyökkäys. Ravikanthin ym. (2018) mukaan simulaattoriharjoittelua voidaan hyödyntää esimerkiksi öljy- ja kaasualalla, ja sen avulla voidaan kehittää työntekijöiden kykyä tunnistaa ja reagoida häiriöihin ja ongelmiin ennen kuin ne pääsevät eskaloitumaan. Simulaattoreita voi siis olla mahdollista hyödyntää kriittisen infrastruktuurin ja energiasektorin yrityksissä, vaikkei se haastattelujen perusteella olekaan ainakaan vielä yleistä. Simulaattorit ovat kuitenkin konkreettinen esimerkki digitaalisesta teknologiasta, jonka avulla voidaan oppia aikaisemmista häiriötilanteista ja pyrkiä kehittämään toimintaa jatkoa ja tulevia häiriötä varten. Simulaattoria voidaan siis pitää digitaalista resilienssiä lisäävänä teknologiana, joka auttaa energiasektorin yrityksiä selviytymään tulevista häiriöistä paremmin, vaikkei tätä aikaisemmassa digitaalista resilienssiä käsittelevässä tutkimuksessa olekaan tunnistettu.

6 Johtopäätökset

Tutkielman empiirisen osuuden tavoitteena oli vastata tutkielman päätutkimuskysymykseen, joka on ”*Mistä digitaalinen resilienssi muodostuu kriittisen infrastruktuurin yrityksissä?”* Tämä toteutettiin käyttämällä temaattista analyysiä haastatteluilla kerätyn aineiston analysoimiseen. Tässä luvussa esitellään tutkielman keskeisimmät löydökset, jotka sisältävät sekä aikaisempaa tutkimusta tukevia tuloksia että täysin uutta tietoa.

Tutkielman tulosten perusteella on selvää, että kriittisen infrastruktuurin yritykset voivat kohdata monia eri häiriötilanteita, ja digitaalisilla teknologioilla ja tietojärjestelmillä on keskeinen rooli niiden selvittämisessä. Digitaalisen resilienssin eri vaiheet eli häiriöiden ennakoiminen ja ennaltaehkäisy, häiriöistä selviytyminen ja palautuminen sekä niistä oppiminen ja toiminnan kehittäminen ovat kaikki todella tärkeitä kriittisen infrastruktuurin yrityksille, eikä tutkielman perusteella voida varmuudella sanoa nousevatko digitaaliset teknologiat ja tietojärjestelmät jossain näistä vaiheista merkittävästi muita tärkeämmäksi. Sen sijaan voidaan todeta, että digitaalisuudella on oleellinen rooli kaikissa näistä vaiheista, ja erilaisia digitaalisia teknologioita ja tietojärjestelmiä hyödynnetään laajalti niistä jokaisessa. Osa tutkielmassa käsitellyistä teknologioista ja järjestelmistä voidaan myös sijoittaa useampaankin kuin yhteen digitaalisen resilienssin vaiheeseen. Aikaisemmin luvussa 4.3.2 esitelty tutkielman teoreettinen viitekehys on täydennetty digitaalisilla teknologioilla ja tietojärjestelmillä tutkielman tulosten perusteella alla olevassa kuvassa 4. Viitekehyksessä on kuitenkin huomioitava se, ettei se esimerkiksi haastattelujen rajallisen määrän takia ole täysin kattava, ja muitakin digitaalisia teknologioita ja tietojärjestelmiä voitaisiin varmasti lisätä siihen.



Kuva 4. Teoreettinen viitekehys täydennettynä

Kuten viitekehyksestä käy ilmi, häiriöiden ennakoimisessa ja ennaltaehkäisemisessä voidaan hyödyntää tietojärjestelmiä ja digitaalisia teknologioita varsin laajasti. Tietojärjestelmien rooli digitaalisen resilienssin tässä vaiheessa painottuu erityisesti erilaisiin valvontajärjestelmiin, joiden avulla voidaan valvoa ja seurata monia eri asioita, kuten esimerkiksi sovelluksien ja järjestelmien toimintaa, tietoliikenneyhteyksiä ja verkkoliikennettä. Tämän tärkeyttä korostaa erityisesti se, ettei tällaisen valvonnan suorittaminen luultavasti olisi mahdollista ilman näitä järjestelmiä. Digitaalisten teknologioiden osalta erityisen tärkeinä voidaan pitää erilaisia mittauksia, joiden avulla voidaan kerätä dataa eri käyttötarkoituksiin, kuten laitevikojen estämiseen. Myös Tremblay ym. (2023) korostavat mittausteknologioiden merkitystä, joten aikaisemman tutkimuksen ja tutkielman tulosten perusteella niitä voidaan pitää oleellisena osana digitaalista resilienssiä. IoT-teknologia on toinen esimerkki digitaalisesta teknologiasta, jonka rooli voidaan nähdä hyvin tärkeänä digitaalisen resilienssin kannalta. Aikaisemman tutkimuksen mukaan IoT:ta voidaan yleisesti pitää osana digitaalista resilienssiä (Boh ym. 2023). Tutkielman tulosten perusteella tätä voidaan kuitenkin vielä tarkentaa, sillä haastatteluaineistoon perustuen IoT vaikuttaa olevan erityisen

tärkeässä roolissa ennakoivassa kunnossapidossa, jota ei ole käsitelty aikaisemmassa kirjallisuudessa. IoT:ta voidaan hyödyntää tämän lisäksi esimerkiksi erilaisissa sensoreissa, kuten palohälyttimissä, joten sen käyttötarkoituksia on lukuisia ja sen tarjoamat mahdollisuudet ja potentiaali digitaalisen resilienssin kehittämiselle on tutkielman perusteella suuri.

Digitaalisilla teknologioilla ja tietojärjestelmillä on oma tärkeä roolinsa myös häiriötilanteista selviytymisessä ja palautumisessa. Niiden merkityksen arvioimista häiriötilanteissa kuitenkin vaikeuttaa osaltaan se, että erilaisissa häiriötilanteissa suoritettavat toiminnot vastaavat usein hyvin pitkälti normaalin tilanteen toimintoja. Energiasektorin yrityksissä erilaisia automaatio-ohjausjärjestelmiä ja muita digitaalisia järjestelmiä käytetään siis oikeastaan koko ajan, eikä ainoastaan häiriötilanteissa. Digitaalisilla teknologioilla ja tietojärjestelmillä on kuitenkin myös selkeitä käyttötarkoituksia nimenomaan häiriötilanteista selviytymiselle ja palautumiselle. Tutkielman tulosten perusteella niiden tärkeimpiä tehtäviä tässä digitaalisen resilienssin vaiheessa ovat tilannekuvan ylläpitäminen ja päätöksenteon tukeminen. Vastaavan havainnon ovat tehneet tutkimuksessaan myös Spagnoletti ja Za (2022). Toinen tapa, miten digitaalisuus voi helpottaa ja nopeuttaa häiriötilanteista palautumista energiasektorin yrityksissä on laitosten etäohjaus, joka tietysti edellyttää tietojärjestelmien ja digitaalisten teknologioiden käyttämistä. Näin ollen tämä digitaalisuuden avulla luotu etäohjausmahdollisuus voidaan katsoa osaksi digitaalista resilienssiä, vaikkei sitä aikaisemmassa tutkimuksessa olekaan käsitelty. Häiriötilanteista selviytymisen kannalta energiasektorin yrityksissä toteutetaan myös muita digitaalisuuteen liittyviä ratkaisuja, kuten verkkojen eriyttäminen ja palvelinten kahdentaminen, joiden avulla häiriötilanteet eivät pääse pahenemaan, vaan niistä voidaan selviytyä helpommin. Vaikka nämä eivät suoraan olekaan itsessään digitaalisia teknologioita, ovat ne digitaalisen resilienssin kannalta oleellisessa osassa ja siksi niitä voidaan pitää osana sitä.

Tutkielman haastattelujen ja tulosten perusteella voidaan sanoa, että aikaisemmista häiriötilanteista oppimista ja jatkuvaa toiminnan kehittämistä pidetään erityisen tärkeänä kriittiseen infrastruktuuriin kuuluvissa energiasektorin yrityksissä. Vaikka tätä oppimista ja kehittämistä voidaan toteuttaa myös ilman digitaalisuuttaa, luovat digitaaliset teknologiat ja tietojärjestelmät sille laajempia mahdollisuuksia. Merkittävimmän hyödyn digitaalisuus tuo tässä tarkoituksessa luomalla kyvyn datan

tehokkaaseen keräämiseen ja analysoimiseen suuressa mittakaavassa. Tutkielman perusteella digitaalisuuden luoma mahdollisuus suurienkin datamäärien keräämiseen ja analysoimiseen on erittäin tärkeää toiminnan kehittämisen kannalta. Koska energiasektorin yritysten toiminnassa syntyy jatkuvasti valtavia määriä dataa, ei sen kerääminen ja käsitteleminen onnistuisi tehokkaasti ilman tietojärjestelmien ja digitaalisten teknologioiden hyödyntämistä. Aikaisemmassa tutkimuksessa tällaisesta data-analytiikan hyödyntämisestä kriittisen infrastruktuurin resilienssin kehittämiseksi on käytetty termiä resilienssianalytiikka (Barker 2017, Eisenberg 2019). Tämä datan kerääminen ja analysoiminen ja siihen käytettävät teknologiat tulevat luultavasti jatkossa vain kehittymään entisestään ja niiden rooli kasvamaan kriittisen infrastruktuurin yrityksissä. Toinen tapa, miten digitaalista teknologiaa voidaan tutkielman tulosten perusteella käyttää tässä digitaalisen resilienssin vaiheessa on simulaattoriharjoittelun hyödyntäminen. Vaikkei tällainen teknologia välttämättä olekaan vielä laajemmassa käytössä, eikä sitä ole käsitelty aikaisemmassa tutkimuksessa, voidaan sitä pitää esimerkkinä digitaalisen resilienssin oppimis- ja kehittymisvaiheessa käytettävästä digitaalisesta teknologiasta.

Tutkielman haastatteluissa esiin nousseet digitaaliset teknologiat ja tietojärjestelmät olivat pitkälti samoja kuin mitä tutkielman teoriaosuudessa käsiteltiin. Tulokset olivat siis melko odotettuja, vaikkakin myös täysin uusia löydöksiä ilmeni, kuten esimerkiksi etäohjaus ja koulutussimulaattorit osana digitaalista resilienssiä. Aikaisemmassa digitaaliseen resilienssiin liittyvässä tutkimuksessa mainittiin kuitenkin myös tekoälyn ja koneoppimisen rooli organisaatioiden digitaalisen resilienssin vahvistamisessa. Esimerkiksi Vaddadin ym. (2023) mukaan tekoälyä ja koneoppimista voidaan hyödyntää kyberhyökkäysten havaitsemisessa ja torjumisessa, mutta tutkielman haastatteluissa tekoälyn ja koneoppimisen hyödyntämistä tällaisessa tarkoituksessa ei mainittu. Haastattelujen perusteella tekoäly ei siis ollut niin merkittävässä roolissa, vaikka sitä saatettiinkin hyödyntää esimerkiksi valvontateknologiassa ihmisen tukena. Vaddadin ym. (2023) mukaan tekoälyä ja koneoppimista hyödynnetään kuitenkin nimenomaan kyberturvallisuuteen liittyen, jota ei haastatteluissa voitu käsitellä kovinkaan tarkasti aiheen arkaluontoisuuden vuoksi, ja tämä saattaa siis selittää miksi nämä teknologiat eivät nousseet esiin tuloksissa.

7 Yhteenveto

Erilaisten häiriöiden ja kriisien lisääntyminen ovat korostaneet yhteiskunnan ja organisaatioiden tarvetta resilienssille eli kyvylle ennakoida, selvitä ja palautua näiden häiriöiden ja kriisien aiheuttamista haasteista. Digitalisaation myötä tietojärjestelmien ja digitaalisen teknologioiden roolia tällaisten haasteiden ja muiden häiriöiden selvittämisessä on korostunut. Digitaalisten teknologioiden ja tietojärjestelmien vuorovaikutusta resilienssin kanssa on alettu viime vuosina tutkimaan enemmän, ja on alettu puhua uudesta digitaalisen resilienssin käsitteestä, johon tutkielma keskittyi.

Muiden organisaatioiden ohella digitaalisuus on keskiössä myös kriittisen infrastruktuurin yritysten jokapäiväisessä toiminnassa. Kriittisen infrastruktuurin ja siitä vastaavien yritysten toiminta on yhteiskunnan kannalta elintärkeässä roolissa, joten niiden täytyy pystyä toimimaan myös erilaisissa häiriötilanteissa ja kriiseissä. Digitaalinen resilienssi on siis kriittisen infrastruktuurin yritysten kannalta hyvin oleellista, joten on tärkeää tutkia mitä digitaalinen resilienssi on kriittisen infrastruktuurin näkökulmasta, ja millaisista digitaalisista teknologioista ja tietojärjestelmistä se muodostuu. Tutkielmassa etsittiin vastausta tähän päätutkimuskysymyksen *mistä digitaalinen resilienssi muodostuu kriittisen infrastruktuurin yrityksissä* avulla. Aikaisempaa tutkimusta siitä, mitä digitaalinen resilienssi on ja miten sitä toteutetaan kriittisen infrastruktuurin yrityksissä on hyvin vähän. Tutkielman tarkoituksena oli siis selvittää mitä digitaalinen resilienssi on, ja mistä se koostuu kriittisen infrastruktuurin yrityksissä. Tutkielmassa selvisikin, että digitaalisilla teknologioilla ja tietojärjestelmillä on keskeinen merkitys kriittisen infrastruktuurin yritysten kyvylle ennakoida, selvitä, palautua ja oppia erilaisista häiriötilanteista. Digitaalinen resilienssi muodostuu niissä monista elementeistä, kuten esimerkiksi valvontajärjestelmistä, IoT-teknologiasta ja etäohjausteknologiasta. Tutkielman tulokset on esitelty tarkemmin edellä luvuissa 5 ja 6.

Digitaalinen resilienssi on käsitteenä melko uusi, joten merkittävä osa sitä käsittelevästä tutkimuksesta on keskittynyt sen määrittelyyn. Tämä näkyy useina hieman toisistaan poikkeavina määritelminä. Suuri osa aikaisemmasta tutkimuksesta on myös keskittynyt digitaaliseen resilienssiin erityisesti koronaviruspandemiaan liittyen ja käsittelee digitaalisen resilienssin merkitystä pandemiasta selviytymisen kannalta. Digitaalista resilienssiä on tutkittu kriittisen infrastruktuurin näkökulmasta vain vähän, eikä

aikaisempaa laadullista tutkimusta siitä ole aiheuttaen selkeän tutkimusaukon. Tutkielma on myös ensimmäinen pro gradu -tutkielma aiheeseen liittyen.

Tutkielma toteutettiin laadullisena tapaustutkimuksena, jonka tavoitteena oli löytää vastaukset tutkimuskysymyksiin ja täyttää tutkimusaukko. Tutkielmassa luotiin aikaisemman kirjallisuuden perusteella teoreettinen viitekehys, jota hyödynnettiin tutkielman empiriaosuudessa. Viitekehys on esitelty luvussa 4.3.2. Tutkielmassa keskityttiin energiasektorin yrityksiin, jotka ovat keskeinen osa Suomen kriittistä infrastruktuuria. Tutkielmassa aineistonkeruu suoritettiin yhteensä seitsemällä puolirakenteellisella haastattelulla. Haastateltavat toimivat vaihtelevissa työtehtävissä eri energiasektorin yrityksissä, joiden toimialat vaihtelivat kaasun, sähkön ja kaukolämmön välillä. Näin haastatteluissa saatiin kerättyä laajasti erilaisia kokemuksia ja näkemyksiä eri energiasektorin osista. Haastatteluilla kerätyn aineiston analysoimiseen käytettiin temaattista analyysiä, jossa aineistosta kehitetään koodeja ja laajempia teemoja, joiden avulla raportoidaan aineistosta tehtyjä havaintoja tutkimuskysymyksen johdattelemana.

Tutkielmaan ja sen tuloksiin liittyi tiettyjä rajoituksia, jotka tulee huomioida. Ensinnäkin on otettava huomioon se, että tutkielmassa ja haastatteluissa käsiteltiin arkaluontoisia aiheita, joten tarkkoihin yksityiskohtiin ei ollut aina mahdollista mennä. Kyseessä on julkinen tutkielma, joten esimerkiksi yritysten varautumiseen ja kyberturvallisuuteen liittyvä järjestelyjä ei voitu tietoturvasyistä käydä haastatteluissa läpi yksityiskohtaisesti. Toiseksi haastattelut poikkesivat myös hieman toisistaan sen osalta, kuinka yleisellä tasolla haastateltavat halusivat pysytellä, mikä loi tiettyjä haasteita niiden keskinäiseen vertailuun. Kolmas rajoittava tekijä tutkielmalle muodostui aikaisemman vastaavan tutkimuksen niukkuudesta. Tämä loi paikoitellen haasteita tutkielman tulosten vertailemiselle aikaisemman tutkimuksen kanssa.

Tutkielmassa tunnistettiin useita digitaalisia teknologioita ja tietojärjestelmiä, joista digitaalinen resilienssi muodostuu kriittisen infrastruktuurin kuuluvissa energiasektorin yrityksissä. Näille löytyi myös monia käyttötarkoituksia digitaalisen resilienssin eri vaiheissa. Koska kriittiseen infrastruktuuriin kuuluu energiasektorin yritysten lisäksi huomattava määrä muidenkin alojen toimijoita ja yrityksiä, voisi digitaalista resilienssiä tutkia jatkossa myös muilla kriittisen infrastruktuurin aloilla. Näin voitaisiin tutkia toteutuuko digitaalinen resilienssi merkittävästi eri tavalla muilla toimialoilla, vai

koostuuko se pitkälti samoista elementeistä. Jatkotutkimuksessa voitaisiin myös syventyä tarkemmin jonkin uuden nousevan digitaalisen teknologian, kuten esimerkiksi tekoälyn hyödyntämiseen osana digitaalista resilienssiä. Tässä tutkielmassa lähtökohtana oli pääasiassa se, että digitaalisuus ja tietojärjestelmien käyttäminen mahdollistavat resilienssin parantamisen kriittisen infrastruktuurin yrityksille. Digitaalisten teknologioiden ja tietojärjestelmien rooli näissä yrityksissä on kuitenkin niin suuri, että se luo varmasti myös tiettyjä haasteita ja riskejä. Tätä näkökulmaa ei tutkielmassa käsitelty juurikaan, joten myös tässä voisi olla paikka jatkotutkimukselle.

Tutkielmassa onnistuttiin sekä luomaan uutta tietoa että todentamaan aikaisemmassa tutkimuksessa tehtyjä havaintoja digitaaliseen resilienssiin liittyen. Tutkielman tuloksista voivatkin hyötyä monet eri tahot niin aiheen tutkijoiden, kriittisen infrastruktuurin kuin yhteiskunnankin osalta. Koska digitaalista resilienssiä on tutkittu kriittisen infrastruktuurin osalta vain vähän, eikä aikaisempaa laadullista tutkimusta ole juurikaan, tutkielma tarjosi uutta tietoa ja näkökulmia, joita aihealueen tutkijat voivat hyödyntää omassa tutkimuksessaan. Tutkielma voidaan käyttää perustana sille, mitä digitaalinen resilienssi voi käytännössä tarkoittaa kriittisen infrastruktuurin ja energiasektorin yritysten näkökulmasta, ja tätä tietoa voidaan käyttää vertailukohtana esimerkiksi muulla toimialalla tai toisessa maassa tehtävälle vastaavalle tutkimukselle. Kriittisen infrastruktuurin yritykset taas voivat hyödyntää tutkielman tuloksia kehittääkseen omaa resilienssiään ja miettiäkseen, kuinka ne voivat mahdollisimman hyvin hyödyntää olemassa olevia tai jopa uusia teknologioita ja tietojärjestelmiä häiriötilanteisiin liittyen. Tutkielman tuloksista voi olla hyötyä myös laajemmin yhteiskunnalle. Yhteiskunnan kannalta on ensisijaisen tärkeää varmistaa kriittisen infrastruktuurin häiriötön toiminta, ja tutkielma luo uutta tietoa siitä, miten digitaalisuutta voidaan hyödyntää tämän toimintavarmuuden parantamisessa entisestään.

Lähteet

Abidi, N. – El Herradi, M. – Sakha, S. (2023) Digitalization and resilience during the COVID-19 pandemic. *Telecomm Policy,* Vol. 47 (4), 102522 (doi: https://doi.org/ 10.1016/j.telpol.2023.102522).

Achillopoulou, D. – Mitoulis, S. – Argyroudis, S. – Wang, Y. (2020) Monitoring of transport infrastructure exposed to multiple hazards: a roadmap for building resilience. *Science of the total environment*, Vol. 746, 141001 (doi: https://doi.org/10.1016/j.scitotenv.2020.141001).

Agius, S. (2013) Qualitative research: its value and applicability. *The Psychiatrist,* Vol. 37, 204–206 (doi: https://doi.org/10.1192/pb.bp.113.042770).

Alcaraz, C. – Zeadally, S. (2014) Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection,* Vol. 8, 53–66 (doi: https://doi.org/10.1016/j.ijcip.2014.12.002).

Alkhaleel, B. (2024) Machine learning applications in the resilience of interdependent critical infrastructure systems—A systematic literature review. *International Journal of Critical Infrastructure Protection,* Vol. 44, 100646 (doi: https://doi.org/10.1016/j.ijcip.2023.100646).

Almaiah, M. – Al-Khasawneh, A. – Althunibat, A. (2020) Exploring the critical challenges and factors influencing the E-learning system usage during COVID-19 pandemic. *Education and Information Technologies*, Vol. 25, 5261–5280.

Argyroudis, S. – Mitoulis, S. – Chatzi, E. – Baker, J. – Brilakis, I. – Gkoumas, K. – Vousdoukas, M. – Hynes, W. – Carluccio, S. – Keou, O. – Frangopol, D. – Linkov, I. (2022) Digital technologies can enhance climate resilience of critical infrastructure. *Climate Risk Management,* Vol. 35, 100387 (doi: https://doi.org/10.1016/j.crm.2021.100387).

Aven, T. (2016) Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, Vol. 253 (1), 1–13 (doi: https://doi.org/10.1016/j.ejor.2015.12.023).

Barker, K. – Lambert, J. –Zobel, C. – Tapia, A. – Ramirez-Marquez, J. – Albert, L. – Nicholson, C. – Caragea, C. (2017) Defining resilience analytics for interdependent cyber-physical-social networks. *Sustainable and Resilient Infrastructure,* Vol 2 (2), 59–67 (doi: https://doi.org/10.1080/23789689.2017.1294859).

Bellini, E. – Gaitanidou, E. – Bekiaris, E. – Ferreira, P. (2020) The RESOLUTE project's European Resilience Management Guidelines for Critical Infrastructure: development, operationalisation and testing for the urban transport system. *Environment Systems and Decisions,* Vol. 40, 321–341 (doi: https://doi.org/10.1007/s10669-020-09765-0).

Boh, W. – Constantinides, P. – Padmanabhan, B. –Viswanathan, S. (2023) Building Digital Resilience Against Major Shocks. *MIS Quarterly*, Vol. 47 (1), 343–361.

Boh, W. – Constantinides, P. – Padmanabhan, B. –Viswanathan, S. (2020) Digital Resilience. Call for Papers. *MIS Quarterly*.

Brucherseifer, E. – Winter, H. – Mentges, A. – Mühlhäuser, M. – Hellmann, M. (2021) Digital Twin conceptual framework for improving critical infrastructure resilience, *Automatisierungstechnik*, Vol. 69 (12), 1062–1080 (doi: https://doi.org/10.1515/auto-2021-0104).

Carugati, A. – Mola, L. – Plé, L. – Lauwers, M. – Giangreco, A. (2020) Exploitation and exploration of IT in times of pandemic: from dealing with emergency to institutionalising crisis practices. *European Journal of Information Systems*, Vol. 29 (6), 762–777 (doi: https://doi.org/10.1080/0960085X.2020.1832868).

Choong-Hee, H. – Soon-Tai, P. – Sang-Joon, L. (2019) The enhanced security control model for critical infrastructures with the blocking prioritization process to cyber threats in power system. *International Journal of Critical Infrastructure Protection*, Vol. 26, 100312 (doi: https://doi.org/10.1016/j.ijcip.2019.100312).

Clarke, V. – Braun, V (2016) Thematic Analysis. *The Journal of Positive Psychology,* Vol. 12 (3), 297–298 (doi: https://doi.org/10.1080/17439760.2016.1262613).

Comfort, L. – Boin, A. – Demchak, C. (2010) *Designing resilience: Preparing for extreme events.* Pittsburgh Pennsylvania: University of Pittsburgh Press, 2010. Print.

Croope, S. – McNeil, S. (2011) Improving Resilience of Critical Infrastructure Systems Postdisaster: Recovery and Mitigation. *Transportation Research Record*, Vol. 2234 (1), 3–13 (doi: https://doi.org/10.3141/2234-01).

Cuel, R. – Ponte, D. – Virili, F. (2022*) Exploring Digital Resilience: Challenges for People and Organizations.* Springer Cham (doi: https://doi.org/10.1007/978-3-031-10902-7).

Curt, C. – Tacnet, J. (2018) Resilience of Critical Infrastructures: Review and Analysis of Current Approaches. *Risk Analysis,* Vol. 38 (11), 2441–2458 (doi: https://doi.org/10.1111/risa.13166).

Darkow, P. (2019). Beyond "bouncing back": Towards an integral, capability-based understanding of organizational resilience. *Journal of Contingencies and Crisis Management*, Vol. 27 (2), 145– 56 (doi: https://doi.org/10.1111/1468-5973.12246).

Duan, L. – Da Xu, L. (2021) Data Analytics in Industry 4.0: A Survey. *Information Systems Frontiers,* (2021), 1–17 (doi: https://doi.org/10.1007/s10796-021-10190-0).

Duchek, S. (2020). Organizational resilience: a capability-based conceptualization. *Business Research*, Vol. 13 (1), 215– 46 (doi: https://doi.org/10.1007/s40685-019-0085-7).

Dupin, J. – Pascal, A. – Godé, C. (2023) A Systematic Literature Review on Digital Resilience in Organizations: Towards a Conceptualization.

Eisenberg, D. – Seager, T. – Alderson, D. (2019) Rethinking Resilience Analytics. *Risk Analysis,* Vol. 39 (9), 1870–1884 (doi: https://doi.org/10.1111/risa.13328).

Eriksson, P. – Kovalainen, A. (2008). *Qualitative Methods in Business Research*. SAGE Publications Ltd. (doi: https://doi.org/10.4135/9780857028044).

Euroopan komissio (2012) Communication from the commission to the European Parliament and the Council. The EU approach to Resilience: Learning from food security crises. <https://ec.europa.eu/echo/files/policies/resilience/com_2012_586_resilience_en.pdf>, haettu 11.2.2024.

Fernandes, A. – Da Silva, M. M. – Pereira, R. (2023) Digital Resilience in Critical Infrastructures: A Systematic Literature Review. *31st International Conference on Information Systems Development.* Lisbon, Portugal.

Floetgen, R. – Strauss, J – Weking, J. – Hein, A. – Urmetzer, F. – Böhm, M. – Krcmar, H. (2021) Introducing platform ecosystem resilience: leveraging mobility platforms and their ecosystems for the new normal during COVID-19. *European Journal of Information Systems*, Vol. 30 (3), 304–321 (doi: https://doi.org/10.1080/0960085X.2021.1884009).

Fogli, D. – Greppi, C. – Guida, G. (2017). Design patterns for emergency management: An exercise in reflective practice. *Information & Management*, Vol. 54 (7), 971–986 (doi: https://doi.org/10.1016/j.im.2017.02.002).

Genge, B. – Kiss, I. – Haller, P. (2015) A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. *International Journal of Critical Infrastructure Protection*, Vol. 10, 3–17 (doi: https://doi.org/10.1016/j.ijcip.2015.04.001).

George, G. – Lakhani, K. – Puranam, P. (2020) What has changed? The Impact of Covid Pandemic on the Technology and Innovation Management Research Agenda. *Journal of Management Studies*, Vol. 57 (8), 1754–1758 (doi: https://doi.org/10.1111/joms.12634).

Gilpin, D. – Murphy, P. (2008) *Crisis Management in a Complex World*. Oxford University Press, Oxford.

Gkeredakis, M. – Lifshitz-Assaf, H. – Barrett, M. (2021) Crisis as opportunity, disruption and exposure: Exploring emergent responses to crisis through digital technology. *Information and Organization*, Vol. 31 (1), 100344 (doi: https://doi.org/10.1016/j.infoandorg.2021.100344).

Gunduz, M. – Das, R. (2020) Cyber-security on smart grid: Threats and potential solutions. *Computer Networks,* Vol. 169, 107094 (doi: https://doi.org/10.1016/j.comnet.2019.107094).

Heeks, R. – Ospina, A. (2018) Conceptualising the link between information systems and resilience: A developing country field study. *Information Systems Journal*, Vol. 29 (4), 1–27 (doi: https://doi.org/ 10.1111/isj.12177).

Holling, C. S. (1973) Resilience and stability of ecological systems. *Annual Review of Ecological Systematics,* Vol. 4 (1), 1–23.

Hollnagel, E. (2009) The four cornerstones of resilience engineering. *Preparation and restoration,* Vol. 2, 117–134.

Hollnagel, E. – Woods, D. – Leveson, N. (2006) *Resilience engineering: Concepts and precepts*. 1st ed. Abingdon: CRC Press, 2006. Web.

Huoltovarmuuskeskus A (2023) Ajankohtaisia kysymyksiä ja vastauksia kriittisestä infrastruktuurista ja varautumisesta. <https://www.huoltovarmuuskeskus.fi/a/ajankohtaisia-kysymyksia-ja-vastauksia-kriittisesta-infrastruktuurista-ja-varautumisesta>, haettu 3.11.2023.

Huoltovarmuuskeskus B (2024) Energiahuolto. <https://www.huoltovarmuuskeskus.fi/toimialat/energiahuolto>, haettu 26.5.2024.

Hurst, W. – Merabti, M. – Fergus, P. (2014) A Survey of Critical Infrastructure Security. *International Journal of Critical Infrastructure Protection,* Vol. 441, 127–138 (doi: (https://doi.org/10.1007/978-3-662-45355-1_9).

Iyamu, T. – Mutudi, M. (2022) Challenges and mitigation strategies in the use of the semi-structured interview technique. *15th IADIS International Conference Information Systems 2022.*

Jasiūnas, J. – Lund, P. – Mikkola, J. (2021) Energy system resilience – A review. *Renewable and Sustainable Energy Reviews,* Vol. 150, 111476 (doi: https://doi.org/10.1016/j.rser.2021.111476).

Jin, X. – Wah, B. W. – Cheng, X. – Wang, Y. (2015) Significance and Challenges of Big Data Research. *Big Data Research,* Vol. 2 (2), 59–64 (doi: https://doi.org/10.1016/j.bdr.2015.01.006).

Katina, P. – Pinto, C. – Bradley, J. – Hester, P. (2014) Interdependency-induced risk with applications to healthcare. *International Journal of Critical Infrastructure Protection,* Vol. 7 (1), 12–26 (doi: https://doi.org/10.1016/j.ijcip.2014.01.005).

Kotlarsky, J. – Van den Hooff, B. – Geerts, L. (2020). Under pressure: Understanding the dynamics of coordination in IT functions under business-as-usual and emergency conditions. *Journal of Information Technology*, Vol. 35(2), 94-122 (doi: https://doi.org/10.1177/0268396219881461).

Kumar, V. – Sindhwani, R. – Behl, A. – Kaur, A. – Pereira, V. (2023) Modelling and analysing the enablers of digital resilience for small and medium enterprises. *Journal of Enterprise Information Management*, Vol. ahead-of-print (doi: https://doi.org/10.1108/JEIM-01-2023-0002).

Kylili, A. – Afxentiou, N. – Ceorgiou, L. – Panteli, C. – Morsink-Georgalli, P. – Panayidou, A. – Papouis, C. – Fokaides, P. (2020) The role of Remote Working in smart cities: lessons learnt from COVID-19 pandemic. *Energy Sources, Part A: Recovery, Utilization and Environmental Effects* (doi: https://doi.org/10.1080/15567036.2020.1831108).

Labaka, L. – Hernantes, J. – Sarriegi, J. (2015) A holistic framework for building critical infrastructure resilience. *Technological Forecasting & Social Change,* Vol. 103, 21–33 (doi: https://doi.org/10.1016/j.techfore.2015.11.005).

Laugé, A – Hernantes, J. – Sarriegi, J. (2015) Critical infrastructure dependencies: A holistic, dynamic and quantitative approach. *International Journal of Critical Infrastructure Protection,* Vol. 8, 16–23 (doi: https://doi.org/10.1016/j.ijcip.2014.12.004).

Lee, J. – Chou, C. – Chang, H. – Hsu, C. (2023) Building digital resilience against crises: The case of Taiwan's COVID-19 pandemic management. *Information Systems Journal,* Vol. 34 (1), 39–79 (doi: https://doi.org/10.1111/isj.12471).

Li, Z. – Xu, Z. – Sukumar, A. (2023) Digital resilience and firm internationalization: a study of Chinese listed companies. *Journal of Enterprise Information Management*, (doi: https://doi.org/10.1108/JEIM-02-2023-0095).

Lichte, D. – Torres, F. – Engler, E. (2022) Framework for Operational Resilience Management of Critical Infrastructures and Organizations. *Infrastructures,* Vol. 7 (5), 70–97 (doi: https://doi.org/10.3390/infrastructures7050070).

Liu, Y. – Xu, X. – Jin, Y. – Deng, H. (2023). Understanding the digital resilience of physicians during the COVID-19 Pandemic: An Empirical Study. *MIS Quarterly*, Vol. 47 (1), 391–422 (doi: https://doi.org/10.25300/MISQ/2022/17248).

Mangalaraj, G. – Nerur, S. – Dwivedi, R. (2022) Digital Transformation for Agility and Resilience: An Exploratory Study. *Journal of Computer Information Systems,* Vol. 63 (1), 11–23 (doi: https://doi.org/10.1080/08874417.2021.2015726).

Marcano, L. – Haugen, F. – Sannerund, R. – Komulainen, T. (2019) Review of simulator training practices for industrial operators: How can individual simulator training be enabled? *Safety Science,* Vol. 115, 414–424 (doi: https://doi.org/10.1016/j.ssci.2019.02.019).

Mauro, C. – Bouchn, S. – Logtmeijer, C. – Pride, R. – Hartung, T. – Nordvik, J. (2010) A structured approach to identifying European critical infrastructures. *International Journal of Critical Infrastructures*, Vol. 6 (3), 277–292 (doi: https://doi.org/10.1504/IJCIS.2010.033340).

McAslan, A. (2010) The concept of resilience: Understanding its origins, meaning and utility. *Torrens Resilience Institute.*

McDaniels, T. – Chan, S. – Cole, D. – Mikawoz, J. – Longstaff, H. (2008) Fostering resilience to extreme events within infrastructure systems: Characterizing decision contexts for mitigation and adaptation. *Global Environmental Change*, Vol. 18 (2), 310–318 (doi: https://doi.org/10.1016/j.gloenvcha.2008.03.001).

Mehedintu, A. – Soava, G. (2022) A Structural Framework for Assessing the Digital Resilience of Enterprises in the Context of the Technological Revolution 4.0. *Electronics 2022*, Vol. 11 (15), 2439 (doi: https://doi.org/10.3390/electronics11152439).

Min-Allah, N. – Alahmed, B. – Albreek E. – Alghamdi, L – Alawad, D. – Alharbi, A. – Al-Akkas, N. – Musleh, D. – Alrashed, S. (2021) A survey of COVID-19 contact-tracing apps. *Computers in Biology and Medicine*, Vol. 137, 104787 (doi: https://doi.org/10.1016/j.compbiomed.2021.104787).

Nan, C. – Sansavini, G. (2017) A quantitative method for assessing resilience of interdependent infrastructures. *Reliability Engineering & System Safety*, Vol. 157, 35–53 (doi: https://doi.org/10.1016/j.ress.2016.08.013).

Nan, C. – Sansavini, G. (2015) Multilayer hybrid modeling framework for the performance assessment of interdependent critical infrastructures. *International Journal of Critical Infrastructure Protection,* Vol. 10, 18–33 (doi: https://doi.org/10.1016/j.ijcip.2015.04.003).

NIAC (2009) *Critial Infrastructure Resilience Final Report and Recommendations, National Infrastructure Advisory Council.* U.S. Department of Homeland Security. Washington, DC, USA.

Nieuwenhuijs, A. – Luijif, E. – Klaver, M. (2008) Modeling Dependencies In Critical Infrastructures. *International Conference on Critical Infrastructure Protection,* 205–213 (doi: https://doi.org/10.1007/978-0-387-88523-0_15).

Osei-Kyei, R. – Tam, V. – Ma, M. – Mashiri, F. (2021) Critical review of the threats affecting the building of critical infrastructure resilience. *International Journal of Disaster Risk Reduction,* Vol. 60, 102316 (doi: https://doi.org/10.1016/j.ijdrr.2021.102316).

Ouyang, M. (2014) Review on modeling and simulation of interdependent critical infrastructure systems. *Reliability Engineering & System Safety*, Vol. 121, 43–60 (doi: https://doi.org/10.1016/j.ress.2013.06.040).

Ouyang, M. – Dueñas-Osorio, L – Min, X. (2012) A three-stage resilience analysis framework for urban infrastructure systems. *Structural Safety,* Vol. 36–37, 23–31 (doi: https://doi.org/10.1016/j.strusafe.2011.12.004).

Ouyang, M. – Wang, Z. (2015) Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modeling and analysis. *Reliability*

Engineering and System Safety, Vol. 141, 74–82 (doi: https://doi.org/10.1016/j.ress.2015.03.011).

Pan, S. – Carter, L. – Tim, Y. – Sandeep, M. (2022). Digital sustainability, climate change, and information systems solutions: Opportunities for future research. *International Journal of Information Management*, Vol. 63 (2), 102444 (doi: https://doi.org/10.1016/j.ijinfomgt.2021.102444).

Park, J. – Son, Y. – Angst, C. (2023) The value of centralized it in building resilience during crises: evidence from us higher education's transition to emergency remote teaching. *MIS Quarterly*, Vol. 47 (1), 451–482 (doi: https://doi.org/10.25300/MISQ/2022/17265).

Petit, F. – Bassett, G. – Black, R. – Buehring, W. – Collins, M. – Dickinson, D. – Fisher, R. – Haffenden, R. – Huttenga, A. – Klett, M. – Phillips, J. – Thomas, M. – Veselka, S. – Wallace, K. – Whitfield, R. – Peerenboom, J. (2013) *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*. Argonne National Laboratory, Chicago, IL, USA.

Pursiainen, C. (2017) Critical infrastructure resilience: A Nordic model in the making? *International Journal of Disaster Risk Reduction,* Vol. 27, 632–641 (doi: http://dx.doi.org/10.1016/j.ijdrr.2017.08.006).

Ravikanth, K. – Bahuguna, P. – Glaser, D. – Shivalkar, S. (2018) Study of Effectiveness of Operator Training Simulators in the Oil and Gas Industry, *Proceedings of The 59th Conference on Simulation and Modelling (SIMS 59),* 79–86 (https://doi.org/10.3384/ecp1815379).

Rehak, D. – Senovsky, P. – Slivkova, S. (2018) Resilience of Critical Infrastructure Elements and Its Main Factors. *Systems,* Vol. 6 (2) (doi: https://doi.org/10.3390/systems6020021).

Rehak, D. – Senovsky, P. – Hromada, M. – Lovecek, T. (2019) Complex approach to assessing resilience of critical infrastructure elements. *International Journal of Critical Infrastructure Protection,* Vol. 25, 125–138 (doi: https://doi.org/10.1016/j.ijcip.2019.03.003).

Riger, S. – Sigurvinsdottir, R. (2015) *Handbook of Methodological Approaches to Community-Based Research: Qualitative, Quantitative, and Mixed Methods. Thematic Analysis*. New York, online edition, Oxford Academic. 33–42 (doi: https://doi.org/10.1093/med:psych/9780190243654.003.0004).

Rinaldi, S. – Peerenboom, J. – Kelly, T. (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine,* Vol. 21 (6), 11–25 (doi: https://doi.org/ 10.1109/37.969131).

Ryu, D. – Kim, H. – Um, K. (2009) Reducing security vulnerabilities for critical infrastructure. *Journal of Loss Prevention in the Process Industries*, Vol. 22 (6), 1020–1024 (doi: https://doi.org/10.1016/j.jlp.2009.07.015).

Schemmer, M. – Heinz, D. – Baier, L. – Vössing, M. – Kühl, N. (2021) Conceptualizing Digital Resilience for AI-based Information Systems. *29th European Conference on Information Systems (ECIS 2021).*

Shakou, L. – Wybo, J. – Reniers, G. – Boustras, G. (2019) Developing an innovative framework for enhancing the resilience of critical infrastructure to climate change. *Safety Science,* Vol. 118, 364–378 (doi: https://doi.org/10.1016/j.ssci.2019.05.019).

Spagnoletti, P. – Za, S. (2022) Digital Resilience to Normal Accidents in High-Reliability Organizations. Engineering the Transformation of the Enterprise, *Springer Cham*, 339–353 (doi: https://doi.org/10.1007/978-3-030-84655-8_21).

Stewart, M. (2010) Risk-informed decision support for assessing the costs and benefits of counter-terrorism protective measures for infrastructure. *International Journal of Critical Infrastructure Protection,* Vol. 3 (1) 29–40 (doi: https://doi.org/10.1016/j.ijcip.2009.09.001).

Tim, Y. – Chiew, T. – Lim, H. – Teo, C. – Ng, C. (2023) Design process knowledge for crisis-driven information systems solutions: Insights on building digital resilience from an action design research study. *Information Systems Journal*, Vol. 33 (6), 1343–1369 (doi: https://doi.org/10.1111/isj.12457).

Tim, Y. – Leidner, D. (2023) Digital Resilience: A Conceptual Framework for Information Systems Research. *Journal of the Association for Information Systems*, Vol. 24 (5), 1184–1198 (doi: https://doi.org/10.17705/1jais.00842).

Tremblay, M. – Kohli, R. – Rivero, C. (2023) Data is the New Protein: How the Commonwealth of Virginia Built Digital Resilience Muscle and Rebounded from Opioid and COVID Shocks. *MIS Quarterly*, Vol. 47 (1), 423–450 (doi: https://doi.org/10.25300/MISQ/2022/17260).

Tuomi, J. – Sarajärvi, A. (2018) *Laadullinen tutkimus ja sisällönanalyysi.* Uudistettu laitos. Helsinki. Kustannusosakeyhtiö Tammi, 2018. Print.

Tweneboah-Koduah, S. – Prasad, R. (2020) The Threats of Infrastructure Obsolescence to Smart Grid: A Case Study. *Wireless Presonal Communications,* Vol. 114, 1025–1043 (doi: https://doi.org/10.1007/s11277-020-07406-y).

Vaddadi, S. – Vallabhaneni, R. – Whig, P. (2023) Utilizing AI and Machine Learning in Cybersecurity for Sustainable Development through Enhanced Threat Detection and Mitigation. *International Journal of Sustainable Development Through AI, ML and IoT*, Vol. 2 (2), 1–8.

Valtioneuvosto (2023) National risk assessment 2023. <http://urn.fi/URN:ISBN:978-952-324-610-2>, haettu 15.12.2023.

Wied, M. – Oehmen, J. – Welo, T. (2019) Conceptualizing resilience in engineering systems: An analysis of the literature. *Systems Engineering,* Vol. 23 (1), 3–13 (doi: https://doi.org/10.1002/sys.21491).

Williamson, K. – Johanson, G. (2018*) Research Methods: Information, Systems, and Contexts*. Second edition. Cambridge, MA: Elsevier, Chandos Publishing.

Woods, D. (2015) Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering & System Safety*, Vol. 141, 5–9 (doi: https://doi.org/10.1016/j.ress.2015.03.018).

World Economic Forum (2023) The Global Risks Report 2023, 18th Edition.

Xu, D. – Tsang, I. – Chew, E. – Siclari, C. – Kaul, V. (2019) A Data-analytics Approach for Enterprise Resilience. *IEEE Intelligent Systems,* Vol. 34 (3), 6–18 (doi: https://doi.org/ 10.1109/MIS.2019.2918092).

Yin (2014) *Case Study Research Design and Methods*. 5th edition, Thousand Oaks, CA. Sage Publications.

Yle (2022) Suojelupoliisi: Suomen kriittiseen infrastruktuuriin kohdistuva uhka on noussut, seurasimme tiedotustilaisuuden keskeisen annin. <https://yle.fi/a/3-12642967/64-3-111024>, haettu 3.11.2023.

Yoo, Y. (2010) Computing in Everyday Life: A call for research on Experimental Computing. *MIS Quarterly*, Vol. 34 (2), 213–321 (doi: https://doi.org/10.2307/2072142).

Zio, E. (2016) Challenges in the vulnerability and risk analysis of critical infrastructures. *Reliability Engineering & System Safety,* Vol. 152, 137–150 (doi: https://doi.org/10.1016/j.ress.2016.02.009).

Zimmerman, R. – Restrepo, C. – Dooskin, N. – Fraissinet, J. – Hartwell, R. – Miller, J. – Remington, W. (2009) Diagnostic Tools to Estimate Consequences of

Terrorism Attacks Against Critical Infrastructure. *Institute for Civil Infrastructure Systems (ICIS).*

Liitteet

Liite 1. Haastattelurunko

Haastattelukysymykset

Taustaa haastateltavasta:

1) Voisitko alkuun kertoa hieman työtehtävästäsi, ja kuvailla millaisessa roolissa olet erilaisissa häiriötilanteissa?

Millaisia häiriötilanteita tai mitkä tapahtumat voisivat aiheuttaa häiriöitä energiasektoriin yrityksessä / Häiriöiden ennaltaehkäiseminen digitaalisuuden avulla:

2) Millaisia häiriöitä olette varautuneet kohtaamaan, ja mitä pidät todennäköisimpinä/merkittävimpinä häiriöinä nykyisessä toimintaympäristössänne?

3) Voisitko kertoa jostain tyypillisestä häiriötilanteesta, tai esimerkiksi viimeisimmästä kohtaamastanne häiriöstä?

4) Miten kuvailisit tietojärjestelmien/digitaalisten keinojen roolia tällaisten mahdollisten häiriöiden tunnistamisessa tai ennakoimisessa?

5) Onko joskus ollut tilanne, jossa digitaalisen teknologian avulla on onnistuttu estämään jokin häiriö? Voisitko kertoa tällaisesta tapauksesta enemmän?

Digitaalisuuden/tietojärjestelmien rooli häiriöistä selviytymisessä

6) Miten koet tietojärjestelmien tai digitaalisten teknologioiden merkityksen häiriötilanteista selviytymisessä kriittisen infrastruktuurin / energiasektorin yrityksissä?

7) Pystytkö kertomaan (yleisellä tasolla) millaisia digitaalisia teknologioita on, jotka auttavat ylläpitämään toimintaa häiriötilanteissa? (esim. tekoäly, IoT/monitorointijärjestelmät)

    a. Pystytkö kertomaan mihin teknologiaa x voidaan hyödyntää häiriötilanteissa?

8) Voisitko kertoa tapauksesta, jolloin digitaalisuus tai digitaaliset teknologiat ovat auttaneet häiriön vaikutusten minimoimisessa tai nopeuttaneet siihen reagointia?

Häiriöistä toipuminen / toiminnan kehittäminen

9) Miten kuvailisit tietojärjestelmien / digitaalisten menetelmien roolia häiriötilanteista palautumisessa ja normaalin toiminnan jatkamisessa?

10) Tuleeko mieleen jotain esimerkkiä, miten digitaalisuuden avulla on onnistuttu kehittämään toimintaa, jotta jatkossa vastaavista häiriöistä selvitään paremmin?

11) Miten kuvailisit omien kokemustesi perusteella digitaalisuuden merkitystä yrityksenne resilienssin parantamiselle?

Lopetus

12) Tuleeko sinulle vielä jotain mieleen tähän aihealueeseen liittyen, jota emme käsitelleet?

13) Tuleeko sinulle mieleen jotain toista henkilöä, ketä voisin mahdollisesti haastatella tutkimukseeni?

Liite 2. Haastattelusuostumuslomake

Haastattelusuostumuslomake

Digitaalinen resilienssi kriittisen infrastruktuurin yrityksissä

Pro gradu -tutkielma, Niilo Tulkki, Turun kauppakorkeakoulu

Ennen kuin aloitamme haastattelun, huomioi että:

a) Voit kieltäytyä vastaamasta kysymyksiin haastattelun aikana.

b) Voit päättää haastattelun, jos tahdot, milloin tahansa.

c) Nauhoitus ja sen litterointi säilytetään turvallisesti tutkielman tekijän henkilökohtaisella tietokoneella, kunnes yliopisto on hyväksynyt tutkielman.

Materiaalin käyttö

a) Materiaalia käytetään tutkimustarkoituksessa pro gradu -tutkielmassa.

b) Ainoastaan tutkielman tekijällä on pääsy materiaaliin.

c) Haastatteluiden tulokset esitellään pro gradu -tutkielmassa.

d) Tutkimuksessa voidaan käyttää tunnistamattomaksi muunnettuja lainauksia haastattelusta.

e) Sinun tai yrityksesi nimeä **ei** mainita tutkimusjulkaisussa tai esityksissä.

f) Voit olla yhteydessä niilo.p.tulkki@utu.fi jos haluat tiedustella tiedonsäilytyksestä tai jos haluat poistaa haastattelusi.

Suostutteko haastattelun nauhoittamiseen yllä olevin ehdoin?

__ Suostun

__ En suostu

HAASTATTELIJA: Niilo Tulkki *PÄIVÄMÄÄRÄ:* x.y.2024

HAASTATELTAVA: _____ *PAIKKA*____ZOOM_____

Haastateltavan allekirjoitus_____

Liite 3. Aineistonhallintasuunnitelma

Opiskelijan aineistonhallintasuunnitelma

Tämän dokumentin avulla voit suunnitella tutkimusaineistosi hallintaa. Yksityiskohtaisemmat ohjeet kuhunkin osioon löydät Opiskelijan aineistonhallintaoppaasta.

1. Tutkimusaineisto

Tutkimusaineistolla tarkoitetaan kaikkea sitä aineistoa, millä tutkimuksen analyysi ja tulokset voidaan todentaa ja toisintaa. Se voi olla esim. erilaisia mittaustuloksia, kyselyistä ja haastatteluista syntyvää dataa, äänitteitä ja videoita, muistiinpanoja, ohjelmistoja, lähdekoodeja, biologisia näytteitä, tekstinäytteitä ja keruuaineistoja.

Listaa alla olevaan taulukkoon kaikki tutkimuksessasi käyttämäsi tutkimusaineisto. Huomaa, että aineisto saattaa koostua useammasta eri aineistotyypistä, muista kirjata kaikki eri aineistotyypit. Listaa sekä digitaalinen että fyysinen tutkimusaineisto.

Aineistotyyppi	**Sisältää henkilötietoja***	**Tuotan aineiston itse**	**Joku muu on tuottanut aineiston**	**Muuta huomioitavaa**
Aineistotyyppi 1: *Haastattelutallenteet*		x		Tallenteet poistetaan haastatteluiden litteroinnin jälkeen.
Aineistotyyppi 2: *Haastattelujen litteroinnit*		x		Litteroinnit poistetaan, kun tutkielma on hyväksytty.
Aineistotyyppi 3: Analysoitu haastatteluaineisto		x		Analysoitu aineisto poistetaan, kun tutkielma on hyväksytty.

* Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Esimerkkejä henkilötiedoksi katsotuista tiedoista löydät Tietosuojavaltuutetun toimiston sivuilta

2. Henkilötietojen käsittely tutkimuksessa

Mikäli aineistosi sisältää henkilötietoja, olet velvoitettu noudattamaan EU:n tietosuoja-asetusta (GDPR) sekä Suomen tietosuojalakia. Henkilötietoja sisältävän aineiston osalta sinun tulee laatia tutkittavillesi tietosuojailmoitus sekä selvittää, kuka toimii aineiston osalta rekisterinpitäjänä.

Laadin tutkittavilleni tietosuojailmoituksen** ja toimitan sen heille ennen aineiston keruuta ☐

Henkilötietojen osalta rekisterinpitäjänä** toimii opiskelija ☐ yliopisto ☐

Aineistoni ei sisällä henkilötietoja ☒

**Lisätietoja yliopiston intranetin Tietosuojaohjeita opinnäytetyöhön -sivulta

3. Aineiston käyttöön liittyvät luvat ja oikeudet

Selvitä mitä lupia ja oikeuksia aineistojen käyttöön liittyy. Ole tarvittaessa yhteydessä opinnäytteesi ohjaajaan. Kuvaile jokaisen aineistotyypin osalta niiden käyttöön liittyvät luvat ja oikeudet, voit tarvittaessa lisätä aineistotyyppejä listaukseen.

3.1 Itse tuotettu aineisto

Saatat tarvita erillisiä lupia keräämäsi tai tuottamasi aineiston käyttöön sekä tutkimuksessa että tulosten julkaisemisessa. Mikäli olet arkistoimassa aineistoasi, pyydä tutkittavilta tarvittavat luvat aineiston arkistoimiseen ja jatkokäyttöön. Selvitä myös, vaatiiko valitsemasi arkisto kirjallisia lupia tutkittavilta.

Tarvittavat luvat ja niiden hankkiminen

Aineistotyyppi 1: Haastateltavilta pyydetään suostumus haastattelun äänittämiseen ennen haastattelun aloittamista.

Aineistotyyppi 2: Haastateltavilta pyydetään lupa hyödyntää haastattelusta saatuja tietoja tutkimustarkoituksessa ja käyttää tunnistamattomaksi muutettuja lainauksia haastatteluista.

3.2 Jonkun muun tuottama aineisto

Onko sinulla tarvittavat luvat aineiston käyttöön tutkimuksessa ja tulosten julkaisemiseen? Liittyykö aineistoon tekijänoikeuksia tai käyttölisenssejä? Huomioi, että esimerkiksi julkaisujen kuvien ja kaavioiden käyttö saattaa edellyttää lupaa.

Aineistoon liittyvät oikeudet ja lisenssit

Tuotan kaiken tutkimuksessa käytettävän aineiston itse. Muiden tuottamaa aineistoa ei käytetä tutkimuksessa.

4. Aineiston säilyttäminen tutkimuksen aikana

Missä säilytät aineistoasi tutkimuksen aikana?

Yliopiston verkkokansiossa ☒
Yliopiston tarjoamassa Seafile-pilvipalvelussa ☐
Jossakin muualla, missä? ☐

Yliopiston tallennuspalvelut huolehtivat automaattisesti tietoturvasta ja varmuuskopioinnista. Jos valitset tallentamisen muualle kuin yliopiston palveluihin, kuvaa, miten huolehdit tietoturvasta ja varmuuskopioinnista. Muista varmistaa, mihin tallennat aineiston aina sitä muokattuasi.

Jos käytät tallentamiseen puhelinta, tarkista etukäteen, minne ääni tai video tallentuu. Jos käytät tallentamiseen kaupallisia pilvipalveluita (iCloud, Dropbox, GoogleDrive jne.) ja aineistosi sisältää henkilötietoja, varmista, että tietosuojailmoituksessa antamasi tiedot tietojen siirtymisestä vastaavat laitteistosi asetuksia. Kaupallisten pilvipalveluiden käyttö merkitsee tietojen siirtoa kolmansiin maihin.

5. Aineiston dokumentointi ja metadata

Miten kuvailet aineistosi niin, että ulkopuolinenkin ymmärtää, millaista aineisto on? Miten itse tarpeen tullen palautat vuosien kuluttua mieleesi, mistä aineistosi koostuu?

5.1 Aineiston dokumentointi

Pystytkö kertomaan, mitä aineistollesi on tapahtunut tutkimuksen teon aikana? Aineiston dokumentointi on keskeisessä osassa aineistoon tehtyjen muutosten jäljittämisessä.

Käytän aineiston dokumentointiin

tutkimuspäiväkirjaa ☐
erillistä dokumenttia, johon kirjaan aineiston pääasiat, kuten tehdyt muutokset, analyysin vaiheet sekä esim. muuttujien merkitykset ☒
aineiston mukana kulkevaa readme-tiedostoa, jossa kuvataan aineiston pääasiat ☐
jotain muuta, mitä? ☐

5.2 Aineiston järjestys ja eheys

Miten pidät aineistosi järjestyksessä ja ehyenä, ja vältät sen tahattomat muutokset?

Säilytän alkuperäisen aineiston erillään tutkimuksenteon aikana käyttämästäni aineistosta, jotta voin palata alkuperäiseen, jos tarvetta ilmenee. ☒

Versionhallinta: mietin jo ennen tutkimuksenteon alkua, miten tulen nimeämään eri aineistoversiot ja noudan sitä systemaattisesti ☒

Tiedostan jo tutkimuksen alussa aineistoni elinkaaren, ja varaudun tilanteisiin, joissa data saattaa huomaamatta muuttua, kuten esim. nauhoitus, litterointi, konversio toiseen tiedostomuotoon, tallentaminen jne. ☒

5.3 Metadata

Metadata on kuvaus aineistostasi. Metadatan perusteella henkilö, joka ei tunne aineistoasi, ymmärtää, millaista aineistosi on. Metadataa voi olla mm. tiedoston nimi, sijainti, koko ja tieto aineiston tuottajasta. Tarvitsetko metadataa?

Tallennan aineistoni arkistoon tai tietopankkiin, joka huolehtii metadatasta puolestani. ☐

Minun pitää luoda metadata, koska arkisto, johon tallennan aineiston edellyttää sitä. ☐

En tallenna aineistoani julkiseen arkistoon, enkä tarvitse metadataa. ☒

6. Aineisto tutkimuksen valmistuttua

Olet vastuussa aineistostasi myös tutkimuksen valmistumisen jälkeen. Varmista, että käsittelet sitä tekemiesi sopimusten mukaisesti. Yliopiston suosittelema säilytysaika on viisi vuotta, poikkeuksena kuitenkin lääketieteen alan aineistot, joiden säilytysaika on 15 vuotta. Henkilötietoja voi säilyttää vain sen aikaa, kun tarve on. Jos olet sitoutunut tuhoamaan aineiston määräajan päätyttyä, sinun on huolehdittava siitä, vaikka et olisi enää opiskelija. Myös yliopiston tallennusratkaisuja käytettäessä aineiston tuhoaminen on sinun vastuullasi.

Mitä aineistollesi tapahtuu, kun tutkimus valmistuu?

Tuhoan koko datan heti, koska kun tutkielma on valmis ja hyväksytty, kerätylle aineistolle ei ole enää tarvetta. Lisäksi on huomioitavaa, että tutkielmassa on käsitelty osittain arkaluontoisia aiheita, joten aineistoa ei ole perustelua säilyttää pidempään. Tutkielmaan osallistuneille henkilöille on myös haastattelusuostumuslomakkeessa ilmoitettu, että aineisto poistetaan, kun tutkielma on hyväksytty.

Aineistonhallintasuunnitelma kannattaa pitää ajan tasalla läpi tutkimuksen.

Lisätietoja Turun yliopiston kirjaston laatimasta Opiskelijan aineistonhallintaoppaasta

Liite 4. Operationalisointitaulukko

Digitaalisen resilienssin osa-alue	Lähde	Haastatteluteema	Haastattelukysymykset (liite 1)	Varakysymykset
Ulkoisten tapahtumien aiheuttamien ongelmien ja häiriöiden ennakoiminen tietojärjestelmiä ja digitaalisia teknologioita hyödyntämällä.	Tim ym. 2023	Häiriöiden ennakointi ja ennaltaehkäiseminen digitaalisuuden avulla	Kysymykset 4–5 Miten kuvailisit tietojärjestelmien/digitaalisten keinojen roolia mahdollisten häiriöiden tunnistamisessa tai ennakoimisessa?	Miten digitaalisia keinoja voitaisiin hyödyntää häiriötilanteiden ennakoimisessa tai ennaltaehkäisemisessä?)
Ulkoisen tapahtuman aiheuttamasta haitasta ja häiriöstä selviytyminen.	Boh ym. 2023	Digitaalisuuden/tietojärjestelmien rooli häiriötilanteesta selviytymisessä	Kysymykset 6–8 Miten koet tietojärjestelmien tai digitaalisten teknologioiden merkityksen häiriötilanteista selviytymisessä kriittisen infrastruktuurin / energiasektorin yrityksissä?	Miten kuvailisit digitaalisuuden merkitystä (kriittisen) toiminnan ylläpitämiselle häiriötilanteissa? / Miten digitaalisuuden avulla voitaisiin pyrkiä minimoimaan häiriön aiheuttamat ongelmat?
Tietojärjestelmien ja digitaalisten keinojen suunnittelu ja käyttö tarkoituksena auttaa organisaatiota palautumaan nopeasti häiriöstä.	Cuel ym. 2022	Digitaalisuuden rooli häiriöstä palautumisessa	Kysymys 9 Miten kuvailisit tietojärjestelmien / digitaalisten menetelmien roolia häiriötilanteista palautumisessa ja normaalin toiminnan jatkamisessa?	Ovatko digitaaliset keinot merkittävässä roolissa häiriöistä palautumisessa ja normaaliin toimintaan palaamisessa?
Muuntautuminen ja toiminnan kehittäminen, jotta jatkossa ollaan paremmin varautuneita kohtaamaan vastaavia häiriöitä.	Boh ym. 2023	Digitaalisuuden rooli toiminnan kehittämisessä ja häiriöstä oppimisessa	Kysymys 10 Tuleeko mieleen jotain esimerkkiä, miten digitaalisuuden avulla on onnistuttu kehittämään toimintaa, jotta jatkossa vastaavista häiriöistä selvitään paremmin?	Voidaanko digitaalisia keinoja hyödyntää häiriöistä oppimisessa?

Liite 5. Koodaustaulukko

Lainaus	1. tason koodi	2. tason koodi	Teema
”Onhan meillä kaikenlaisia järjestelmiä, joiden ainoa tehtävä on monitoroida, että asiat toimii kuten niiden pitäisi toimia. Eli tietojärjestelmät toimii niin kuin niiden pitää toimia. Varmaan tämä on sellainen sektori, joka olisi täysin mahdotonta ilman tietojärjestelmiä.” (H1)	Tietojärjestelmien toiminnan valvominen	Tietojärjestelmien häiriöiden estäminen	Valvontajärjestelmät osana digitaalista resilienssiä
”Valvomojärjestelmät ovat meillä tosi iso IT-alue, joka nimenomaan on järjestelmä, joka on suunniteltu tähän. Jos oletettaisiin kaiken toimivan aina moitteitta, niin eihän meillä olisi koko valvomojärjestelmiä, emmehän me käyttäisi sellaisia mihinkään. Eli kyllä meillä käytetään paljon digitaalisia teknologioita tähän.” (H2)	Valvontajärjestelmät merkittävä IT-alue	Häiriöiden estäminen digiteknologian avulla	Valvontajärjestelmät osana digitaalista resilienssiä
”Kyllähän me koko ajan verkkoa monitoroidaan ja sitten poikkeamia löydetään, ja siten niihin päästään voisi sanoa jopa yleensä puuttumaan proaktiivisesti eli ennen kuin kriisi tapahtuu.” (H2)	Verkon monitorointi valvontajärjestelmillä	Kyberhäiriöiden estäminen	Valvontajärjestelmät osana digitaalista resilienssiä
”Ja siis kyllähän kaikkea, mitä aikaisemmin asiat havaitaan, ja jos joku hyökkäys tai häiriö kohdistuu johonkin järjestelmään, niin silloinhan se, joko se tai joku valvova järjestelmä sitten sen huomaa, ja sitten pystytään aloittamaan torjuntatoimet. Tai voi olla jotain automaattisia torjuntatoimia tai eristystoimintoja, mitkä toimii sitten itsenäisesti siinä tilanteessa.” (H4)	Valvontajärjestelmät häiriön havaitsemisessa	Järjestelmien häiriöiden estäminen	Valvontajärjestelmät osana digitaalista resilienssiä
”Että kyllähän ilman jotain digitaalista valvontaa, niin sitten tavallaan joku prosessihäiriö pääsee paljon isommaksi.” (H4)	Valvontajärjestelmä prosessihäiriön estämisessä	Häiriön eskaloitumisen estäminen	Valvontajärjestelmät osana digitaalista resilienssiä
” Ja kyllä se online-valvonta laitteille ja niiden seuranta, niiden kunnon seuranta ja tilanteen seuranta on kaiken a ja o” (H7)	Laitteiden seuranta valvontajärjestelmillä	Laitehäiriöiden estäminen	Valvontajärjestelmät osana digitaalista resilienssiä

Lainaus	1. tason koodi	2. tason koodi	Teema
”Seurataan erinäköisillä etävalvontajärjestelmillä erinäköisiä laitteita, että ne kaikki on kunnossa.”(H7)	Laitteiden seuranta valvontajärjestelmillä	Laitehäiriöiden estäminen	Valvontajärjestelmät osana digitaalista resilienssiä
” Siellä on just tämmösiä erilaisia Iot-tyyppisiä ratkaisuja -- Yritetään jonkin järjestelmän avulla vähän haistella, että prosessi toimii niin kuin pitääkin.” (H1)	IoT	Häiriöiden estäminen IoT:n avulla	IoT ja mittaukset häiriöiden ennakoimisessa
”Lämpötila-anturit, lämmöt lähtevät nousemaan, jos joku rupeaa kuumenemaan siellä. Meillä tällainenkin kokeilu oli tässä, yleensä laitteet alkavat pitämään vähän epänormaalia ääntä ennen kuin ne hajoavat, niin tämmöiseenkin voi IoT:lla päästä kiinni ja muuta” (H5)	IoT	Laitehäiriöiden estäminen IoT:n avulla	IoT ja mittaukset häiriöiden ennakoimisessa
”Sillä tavalla tämmöistä ennaltaehkäisevää, kunnossapitoon tarjoaa digitaalisuus mahdollisuuksia ilman muuta” (H5)	Digitaalisuus ennakoivassa kunnossapidossa	Laitehäiriöiden estäminen digitaalisuuden avulla	IoT ja mittaukset häiriöiden ennakoimisessa
”esimerkiksi on erilaisia värinämittauksia, joilla kerätään dataa jonkun vaikka moottorin pärinöistä. Ja sillä pystytään, sitä tietoa analysoimalla pystytään ennakoimaan mahdollisia tulevia mekaanisia vikoja.” (H3)	Värinämittaus	Värinämittaus häiriöiden ennakoimisessa	IoT ja mittaukset häiriöiden ennakoimisessa
”ja varmaan monessa muussakin paikassa tehdään tämmöistä ennakoivaa kunnossapitoa, että mitataan vaikka jonkun pumppujen värinää semmoisilla laitteilla, että sitten mitä ei silmällä tai korvalla välttämättä kuule, että sitten tavallaan siellä kun värinät rupee lisääntymään, niin sitten se ehkä indikoi sitä, että jos homma jatkuu näin, niin kuukauden päästä pumppu hajoaa, ja siinä ehkä se digitaalisuus luo ymmärrystä siitä tilannekuvasta.” (H4)	Digitaalisuus ennakoivassa kunnossapidossa	Laitehäiriöiden estäminen digitaalisuuden avulla	IoT ja mittaukset häiriöiden ennakoimisessa
”Se miten tuotantoprosessi vaihtelee ja värisee ja missä on lähellä piti -tilanteita, näistä me keräämme dataa ja meillä on paljon laaturaportointia käytettävyydestä, paine-eroista, elinkaarista eli missä kohtaa infran elinkaarta mennään, niin täällä tilastolliset menetelmät auttavat paikantamaan niitä potentiaalisia häiriökohteita ennen kuin häiriö tapahtuu. (H2)	Datan kerääminen häiriöiden ennakoimisessa	Häiriöiden ennakoiminen datan avulla	IoT ja mittaukset häiriöiden ennakoimisessa

Lainaus	1. tason koodi	2. tason koodi	Teema
”me puhutaan täällä paljon tilannekuvasta. Että nähdään missä tilanteessa se järjestelmä on, niin kyllähän siihen nämä kaikki järjestelmät, ohjelmistot ja itseasiassa meillä on ihan tilannekuvajärjestelmäkin nimeltään semmoinen, niin tuo sitä näkyvyyttä, että nähdään, siihen, että se järjestelmä on turvallisessa tilassa ja mitä mahdollisia poikkeamia siellä sitten on.” (H5)	Tilannekuvajärjestelmä	Tilannekuvan ylläpitäminen häiriötilanteessa	Päätöksenteon tuki ja tilannekuvan ylläpitäminen
”Ehkä siihen niin kuin johtamisen tukena ainakin on (digitaalisuudella) tärkeä rooli.” (H4)	Johtamisen tuki	Digitaalisuus tukemassa päätöksentekoa häiriötilanteessa	Päätöksenteon tuki ja tilannekuvan ylläpitäminen
”digitaalitekniikan avulla luodaan pohjaa tilannekuvasta päätöksenteolle” (H6)	Digitaalisuus tilannekuvan luomisessa	Digitaalisuus tukemassa päätöksentekoa häiriötilanteessa	Päätöksenteon tuki ja tilannekuvan ylläpitäminen
”Ja taas me pystytään monella tavalla tässä tiedon välityksessä, tilannetiedon välityksessä hyödyntämään digitaalitekniikkaa, jolloin tilannekuva siitä, että mitä on tapahtunut, niin se on parempi kuin se, että jotenkin manuaalisesti yritettäisiin pitää.” (H6)	Tiedonvälitys ja tilannekuvan ylläpitäminen	Tilannekuvan ylläpitäminen häiriötilanteessa	Päätöksenteon tuki ja tilannekuvan ylläpitäminen
”Ja silloinhan nämä (tietojärjestelmät) on äärimmäisten tärkeitä, että meillä on perustietojärjestelmä ja sitten on olemassa joku varajärjestelmä. Sehän on sitä tietotekniikan hyödyntämistä tohon tarkoitukseen.” (H1)	Varajärjestelmä	Toiminnan ylläpitäminen häiriötilanteessa varajärjestelmällä	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)
”Kyllä meillä on jonkin verran varajärjestelmiä myös, eli jos yksi kaatuu meillä -- me pystymme aika usein toisella järjestelmällä kompensoimaan toisen järjestelmän puutteita.” (H2)	Varajärjestelmä	Toiminnan ylläpitäminen häiriötilanteessa varajärjestelmällä	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)
”varmasti tulee entistä tärkeämmäksi ja varsinkin se varmistaminen ettei olla yhden tai edes kahden (järjestelmän) varassa.” (H3)	Varajärjestelmä	Toiminnan ylläpitäminen häiriötilanteessa varajärjestelmällä	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)

Lainaus	1. tason koodi	2. tason koodi	Teema
”Tärkeimpien järjestelmien pitää olla aina kahdennettuna, ja tällä tavalla, että on tärkeää tunnistaa mikä on sen tietojärjestelmän vaikutus mihinkin prosessiin.” (H5)	Järjestelmän kahdentaminen	Toiminnan ylläpitäminen häiriötilanteessa varajärjestelmällä	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)
”Ja sitten lisäksi meillä on kaikki meidän serverit ja muut on kahdennettu tai kolmennettu, riippuen vähän kohteesta.” (H7)	Palvelinten kahdentaminen	Toiminnan ylläpitäminen häiriötilanteessa	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)
”meillä esimerkiksi verkkoratkaisut on siten, että meillä on kriittisyyden mukaan eriytetty verkkoja ” (H2)	Verkkojen eriyttäminen	Häiriötilanteesta selviytyminen verkkoratkaisujen tukemana	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)
”Mutta tosiaan nyt kun tällaiset huoltovarmuusverkot, kaikilla huoltovarmuuskriittisillä yhtiöillä on omat verkot, ja verkkoalueet on eriytetty.” (H2)	Verkkojen eriyttäminen	Häiriötilanteesta selviytyminen verkkoratkaisujen tukemana	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)
”Tavallaan operatiiviset järjestelmät pidetään kokonaan irrallaan internet-maailmasta.” (H5)	Kyberuhilta suojautuminen	Digitaalisuus häiriöstä selviytymisessä	Kriittisten järjestelmien turvaaminen (ja jatkuvuudenhallinta)
”jos nyt on vaikka ollut häiriötilanne ja laitos on niin sanotusti alhaalla, niin meillä on eri laitostyypeillä vähän erilaisia järjestelmiä, mutta siellä on rakennettu start up -järjestelmä, eli periaatteessa se laitos, jos siellä mekaanisesti on kaikki oikeassa asennossa siellä laitoksella, niin se ohjelma pystyy starttaamaan itse itsensä.” (H3)	Laitoksen startup-järjestelmä	Digitaalisuus häiriöstä palautumisessa	Laitosten etäohjaus häiriöstä palautumisessa
”me on panostettu siihen meidän keskusvalvomotoimintaan, että jokainen laitos, mitä meillä on, niin pystytään käynnistämään ja pysäyttämään sieltä meidän keskusvalvomosta.” (H7)	Etäohjaus keskusvalvomosta	Digitaalisuus häiriöstä palautumisessa	Laitosten etäohjaus häiriöstä palautumisessa

Lainaus	1. tason koodi	2. tason koodi	Teema
”Kyllä se on elintärkeää nykypäivänä, että kaikki laitteet on etäohjattavissa ja ohjattavissa ja digitaalisesti hoidettavissa, ettei paikan päälle tarvitse mennä.” (H7)	Etäohjaus toiminnan jatkuvuuden nopeuttamisessa	Digitaalisuus häiriöstä palautumisessa	Laitosten etäohjaus häiriöstä palautumisessa
”Tämä kaikki (toiminnan kehittäminen) pohjautuu tuotantodataan ja kyllähän meidän pitää, me keräämme kaiken sen datan talteen. Sitten näistä meidän pitäisi löytää niitä anomalioita, se että mitkä syyt ovat johtaneet häiriötilanteeseen ja kuinka niitä voitaisiin ennakoida” (H2)	Anomalioiden etsiminen tuotantodatasta	Häiriöistä oppiminen datan avulla	Datan kerääminen ja analysointi
”Joo, ehdottomasti, ja varsinkin kun tuotantolaitoksillakin sitä dataa on todella paljon, niin sitten sieltä voidaan jollain louhinnan keinoin löytää semmoisia asioita, mitkä sitten indikoi (häiriöitä)” (H4)	Tuotantolaitosten datan käsittely	Oppiminen datan digitaalisen käsittelyn avulla	Datan kerääminen ja analysointi
”se on hyvin tyypillistä, että kun meillä tapahtuu jotakin, ja siinä syntyy sitä tapahtumadataa paljon, että sitä myös digitaalisesti myllätään sitä dataa” (H6)	Tapahtumadatan käsitteleminen	Oppiminen datan digitaalisen käsittelyn avulla	Datan kerääminen ja analysointi
”Kyllä mä sanoisin, että datan kerääminen ja käsittely. Niin se on ehkä sillä lailla, miten nyt ensimmäiseksi siinä voisi ajatella, että joka on ainakin hyvin keskeistä.” (H6)	Data tärkeä osa oppimista	Häiriöistä oppiminen datan avulla	Datan kerääminen ja analysointi
”Mutta monta kertaa tämmöisissä tapahtumissa, niin sitä tapahtumatietoa, sitä on valtavan paljon, aikatietoa, paikkatietoa. Niin digitaalitekniikkahan on ihan omaa luokkaansa sitten taas tämmöisen suuren, tavallaan bulkkitiedon käsittelyssä.” (H6)	Massadatan käsittely	Oppiminen datan digitaalisen käsittelyn avulla	Datan kerääminen ja analysointi