Tampereen yliopisto

Laura Karintaus

# KYBERHYÖKKÄYKSEEN VARAUTUMINEN TERVEYDENHUOLTO-ORGANISAATIOSSA

Tapaustutkimus

Johtamisen ja talouden tiedekunta
Diplomityö
Toukokuu 2022

# TIIVISTELMÄ

Laura Karintaus: Kyberhyökkäykseen varautuminen terveydenhuolto-organisaatiossa
Diplomityö
Tampereen yliopisto
Tietojohtaminen
Toukokuu 2022

---

Kyberrikollisuus kehittyy jatkuvasti ja eri toimialojen organisaatioilla on kova paine kehittää valmiuttaan jatkuvasti kasvavien kyberuhkien edessä. Terveydenhuolto on viime vuosina noussut yhdeksi kyberhyökkääjien keskeisimmistä kohteista ja esimerkkejä tapahtuneista hyökkäyksiä on lukuisia. Hyökkääjiä houkuttelee terveydenhuolto-organisaatioiden tärkeä rooli yhteiskunnan toimintakyvyn ja huoltovarmuuden toteuttamisessa ja se, että ne käsittelevät paljon luottamuksellista potilastietoa, jonka arvo pimeillä markkinoilla on suuri. Tietojärjestelmät ja teknologia näyttelevät merkittävää roolia terveydenhuolto-organisaatioiden toiminnassa ja potilaiden hoidossa ja niiden menettäminen voi pahimmillaan aiheuttaa vakaviakin riskejä. Organisaatioiden on siis varauduttava reagoimaan erilaisiin häiriötilanteisiin ja niiden aiheuttamiin moninaisiin haasteisiin.

Tässä diplomityössä tutkittiin suuren terveydenhuolto-organisaation varautumista toteutuvaan kyberhyökkäystilanteeseen ja sitä, miten organisaatioiden varautumista voidaan kehittää. Tutkimus rajattiin koskemaan sellaisen vakavuusasteen kyberhyökkäyksiä, joilla olisi hoitotoiminnassa näkyviä vaikutuksia. Tutkimusmenetelmänä käytettiin yhteen kohdeorganisaatioon keskittyvää tapaustutkimusta ja tiedonkeruu suoritettiin kohdeorganisaation henkilöstön haastatteluilla. Haastateltaviksi valittiin keskenään erilaisissa rooleissa työskenteleviä henkilöitä organisaation eri osista, jotta saatiin mahdollisimman kattava kuva koko organisaation toiminnasta.

Tutkimuksessa haluttiin selvittää, mitä organisaatiossa tapahtuu kyberhyökkäyksen aikana ja millaisilla keinoilla organisaatio voi varautua hyökkäyksen toteutumiseen. Haastattelujen perusteella muodostettiin kattava käsitys siitä, miten kohdeorganisaatio nykytilassaan toimisi hyökkäyksen aikana. Tietohallinnon ja sen kumppaneiden vastuulla olisi tilanteen koordinointi, hyökkääjän pysäyttäminen ja tietojärjestelmäinfrastruktuuriin liittyvä toiminta. Johdon avainhenkilöiden vastuulla on koko organisaation toiminnan johtaminen ja päätöksenteko, sidosryhmäyhteistyö sekä sisäinen ja ulkoinen viestintä. Hoitotoimintaa johtavat ja suorittavat tahot vastaavat korvaavien toimintatapojen käyttöönotosta sekä hoidon jatkuvuuden ja potilaiden turvallisuuden varmistamisesta. Henkilöstön toimintavalmiutta voidaan nostaa esimerkiksi harjoittelulla, koulutuksella ja selkeillä toimintaohjeilla. Tietojärjestelmäinfrastruktuurin reagointi- ja palautumiskykyyn voidaan vaikuttaa teknisillä varautumiskeinoilla. Varautumisen taso voi vaihdella samankin organisaation eri osissa paljon, joten koko organisaation kattava ja säännöllinen valmiuden mittaaminen kannattaa.

Tutkimus tuotti paljon uutta tietoa siitä, miten kyberhyökkäys voi vaikuttaa hoitotoiminnan toteuttamiseen suuressa terveydenhuolto-organisaatiossa. Nykytilan analyysin kautta tunnistettiin kohdeorganisaation toiminnasta neljä kybervarautumisen ongelmakohtaa: henkilöstön vaihteleva asenneilmapiiri ja puutteellinen kybertietoisuus, haasteet tilannekuvan ymmärtämisessä ja viestinnässä, käytössä olevien toimintaohjeiden puutteellinen soveltuvuus, saatavuus ja sisäistäminen sekä lääkintälaitteiden heikko tietoturva. Tutkimus täydensi aiempaa kirjallisuutta erityisesti ihmiskeskeisen näkökulmansa kautta. Sen avulla voitiin kuvata varautumista tehtävien sijaan niitä suorittavien ihmisten näkökulmasta ja siten tunnistaa myös haasteiden taustalla vaikuttavia juurisyitä. Lisäksi tutkimuksessa tunnistettiin kyberhyökkäysvarautumisen ”sokeita pisteitä”, joihin liittyvälle kehitystyölle voi olla tarvetta tulevaisuudessa. Tällaisia olivat esimerkiksi terveydenhuollolle spesifit harvinaisemmat kyberkriisiskenaariot, joita ei kirjallisuudessa vielä juuri käsitelty.

Tutkimuksessa todettiin, että kyberhyökkäykseen varautuminen on laaja kokonaisuus, joka vaatii toimia kaikkialla organisaatiossa, kaikilta sen toimijoilta. Tutkimuksessa tunnistettiin myös tarve kehittää toimialojen välistä yhteistyötä ja monialaista osaamista, jotta hoitotyö, kyberhyökkäysvarautuminen ja näiden toisilleen asettamat vaatimukset voidaan sovittaa paremmin yhteen. Varautuminen on jatkuvaa kilpajuoksua nopeasti muuttuvia haasteita vastaan, ja siksi siinä ei tulla koskaan valmiiksi. Tutkimusta ja kehitystyötä on siis tehtävä jatkuvasti.

Avainsanat: Kyberhyökkäys, varautuminen, kriisitilanteet, terveydenhuolto

# ABSTRACT

Laura Karintaus: Preparing for a cyber-attack in a healthcare organization
Master of Science Thesis
Tampere University
Information and Knowledge Management
May 2022

---

The cybercrime industry is constantly evolving and organizations in different industries are under pressure to develop their preparedness in the face of ever-increasing cyber threats. Healthcare has emerged as one of the key targets for cyber-attackers in recent years, with numerous examples of attacks taking place. Attackers are attracted by the important role of healthcare organizations in delivering societal resilience and security of supply, and by the fact that they handle a large amount of confidential patient data, which has a high value on the black market. Information systems and technology play an important role in the operation of healthcare organizations and the care of patients, and their loss can, at worst, pose serious risks. Organizations must therefore be prepared to respond to a variety of disruptive events and the multiple challenges they pose.

This thesis explored the preparedness of a large healthcare organization for a cyber-attack and how to improve preparedness. The study was limited to cyber-attacks of a severity that would have a visible impact on healthcare operations. The research methodology used was a case study focusing on a single target organization and data collection was carried out through interviews with staff in the target organization. The interviewees were selected from different parts of the organization, in different roles, to obtain as comprehensive a picture as possible of the whole organization.

The aim of the study was to find out what happens in an organization during a cyber-attack and how to prepare for a cyber-attack. The interviews provided a comprehensive picture of how the target organization would operate in its current state during an attack. IT and its partners would be responsible for coordinating the situation, stopping the attacker, and dealing with the IT infrastructure. Key management personnel would be responsible for the management and decision making of the whole organization, stakeholder cooperation, internal and external communication. Those who manage and deliver care are responsible for the implementation of substitute policies and for ensuring continuity of care and patient safety. Staff capacity can be enhanced through training, education, and clear guidelines, for example. Technical contingency measures can contribute to the responsiveness and resilience of the information system infrastructure. The level of preparedness can vary widely across different parts of the same organization, so it is worthwhile to measure preparedness across the whole organization on a regular basis.

The study provided a lot of new information on how a cyber-attack can affect the delivery of care in a large healthcare organization. Through the analysis of the current situation, four cyber preparedness problem areas were identified in the target organization: variable attitudes and lack of cyber awareness among staff; challenges in situational awareness and communication; inadequate suitability, availability, and internalization of existing operational guidelines; and poor security of medical equipment. The study complements previous literature, through its human-centered perspective. It allowed us to describe preparedness from the perspective of the people performing the tasks rather than the tasks themselves, and thus to identify the root causes of the challenges. The study also identified 'blind spots' in cyber-attack preparedness that may require further development in the future. These included, for example, the less common healthcare-specific cyber-crisis scenarios, which have not yet been widely addressed in the literature.

The study found that cyber-attack preparedness is a broad issue that requires action across the organization, by all its actors. The study also identified the need to develop cross-sectoral collaboration and multidisciplinary skills to better align care work, cyber preparedness, and the demands of each on the other. Preparedness is a constant race against rapidly changing challenges, and therefore it is never finished. Research and development must be continuous.

Keywords: Cyberattack, preparedness, crisis situations, healthcare

# ALKUSANAT

Aluksi haluan kiittää ja onnitella itseäni siitä, että selvisin tästä urakasta, vaikka se ei ollut aina helppoa. Olen ylpeä siitä, että sain työtä etenemään myös vaihto-opiskelujeni aikana, vaikka muutakin opiskeltavaa ja ohjelmaa todella riitti. Häiriötekijöiden keskellä eläminen olikin ehkä haastavinta koko hommassa, mutta opin vuoden aikana valtavasti itsestäni ja itselleni parhaista työskentelytavoista. Yliopistourani ei ennen tätä ollut vielä vaatinut minulta kovinkaan pitkäjänteistä työtä minkään asian eteen, joten tämä oli opettavainen kokemus siinäkin mielessä. Oli myös hienoa huomata, että sataprosenttisena tiimityöskentelijänä onnistuin saattamaan maaliin näinkin laajan itsenäisen projektin. Jatkossa taidan kuitenkin keskittää energiani mieluummin yhteisöllisempiin projekteihin.

Haluan kiittää ohjaajiani Samuli Pekkolaa ja Maija Ylistä hyvistä neuvoista ja arvokkaasta tuesta koko projektin ajan. Teidän avullanne pysyin kiinni tekemisessä ja työn punaisessa langassa silloinkin, kun muu elämä meinasi puhaltaa voimakkaasti vastatuuleen. Samulia haluan kiittää monista oivalluksista, sekä tiivistämisen tärkeydestä muistuttamisesta. Maijaa haluan kiittää sparrailuavusta ja turhan itsekriittisyyden ravistelusta pois niskastani. Kiitos kuuluu myös työn kohdeorganisaatiolle yhteistyöstä sekä haastateltavilleni hyvähenkisistä haastattelutilaisuuksista. Ilman avoimia ja syvällisiä vastauksianne ei lopputuloksesta olisi tullut näin mielenkiintoinen!

Ystäviäni (mm. BFI & BP & Q & SLC) haluan kiittää upeista vuosista, joita saimme viettää yhdessä yliopistolla. Monet elämäni rakkaimmista ystävyyksistä ja hienoimmista muistoista ovat syntyneet juuri teidän kanssanne. Kiitos kuuluu myös killalleni Tietojohtajakilta Man@gerille, josta löysin oman henkisen kotini yliopistolla. Oli ihanaa saada viettää aikaa, oppia uutta ja kehittää toimintaa (ja itseäni), yhdessä muiden huikeiden kiltalaisten kanssa. Kiitos myös PCT Flames ja muu cheerleading-yhteisöni siitä, että ette ole koskaan antaneet minun pudota akateemiseen kuplaan miettimään pelkkää opiskelua.

Lisäksi haluan kiittää sydämeni pohjasta rakasta perhettäni (mm. Äitiä, Isää, pikkuveli Mikkoa sekä koiria Niiloa, Nemoa, Inkaa ja Olgaa) koko elämäni jatkuneesta pohjattomasta tuesta ja uskosta minuun, ilman teitä en olisi tässä. Äitiäni haluan kiittää myös avusta työn oikolukemisessa ja monien hyödyllisten kirjojen lainasta, sekä Isääni etätyöangstien jakamisesta sekä vaihtelevien työskentelypaikkojen tarjoamisesta. Lopuksi haluan vielä kiittää poikaystävääni Henriä tuesta ja huolenpidosta, ja siitä että ruokit minut silloin, kun en itse meinannut stressin keskellä muistaa syödä. Olet paras!

Tampereella, 23.5.2022,

Laura Karintaus

# SISÄLLYSLUETTELO

1. JOHDANTO ..... 1
1.1 Työn motivaatio ja tausta ..... 1
1.2 Tutkimusongelma ja rajaus ..... 3
1.3 Tutkimuksen rakenne ..... 4
2. TUTKIMUSASETELMA JA –METODOLOGIA ..... 5
2.1 Tutkittava organisaatio ..... 5
2.2 Tutkimusasetelma ..... 6
Tutkimusfilosofia: Interpretivismi ..... 6
Lähestymistapa: Induktio ..... 7
Tutkimusmetodologia: Laadullinen tutkimus ..... 7
Aikahorisontti: Poikittaistutkimus ..... 8
2.3 Tutkimusstrategia: Tapaustutkimus ..... 8
2.3.1 Tapaustutkimuksen laatukriteerit ..... 9
2.3.2 Puolistrukturoitu haastattelututkimus ..... 10
2.3.3 Tiedonkeruu ..... 11
2.3.4 Aineiston analyysi ..... 14
3. TERVEYDENHUOLTO-ORGANISAATIO KYBERHYÖKKÄYKSEN KOHTEENA 16
3.1 Terveydenhuolto toimintaympäristönä ..... 16
3.1.1 Tietojärjestelmien rooli terveydenhuollossa ..... 18
3.1.2 Terveydenhuollon kyberturvallisuus ..... 19
3.2 Terveydenhuolto-organisaatioihin kohdistuvat kyberuhat ..... 21
3.2.1 Kyberuhista yleisesti ..... 21
3.2.2 Kyberhyökkäystyyppejä ..... 23
4. VARAUTUMINEN KYBERHYÖKKÄYSTILANTEESTA SELVIÄMISEEN ..... 26
4.1 Kyberhyökkäykseen varautuminen ..... 26
4.1.1 Uhan tunnistaminen ..... 29
4.1.2 Suojauksen rakentaminen ..... 30
4.1.3 Hyökkäyksen havaitseminen ..... 31
4.1.4 Reagointi hyökkäykseen ..... 32
4.1.5 Palautuminen ..... 33
4.2 Kyberhyökkäykseen varautuminen terveydenhuolto-organisaatiossa ..... 34
4.2.1 Tekninen varautuminen terveydenhuollossa ..... 35
4.2.2 Hallinnollinen varautuminen ..... 38
4.2.3 Koko henkilöstön varautuminen ..... 40
4.3 Kyberhyökkäysvalmiuden mittaaminen ..... 41
5. TAPAUSTUTKIMUS: KOHDEORGANISAATION TOIMINTA KYBERHYÖKKÄYSTILANTEESSA ..... 44
5.1 Erilaiset kyberhyökkäysskenaariot ja niiden mahdolliset seuraukset kohdeorganisaatiossa ..... 44
5.2 Toiminta kyberhyökkäystilanteessa ..... 48
5.2.1 Hyökkäyksen havaitseminen ..... 48
5.2.2 Häiriötilanteen koordinointiryhmä ja tietohallinnon toiminta ..... 50

5.2.3 Hyökkäykseen reagointi....52
5.2.4 Johtaminen ja viestintä....53
5.2.5 Hoitotoiminnan jatkuvuuden varmistaminen....55
5.2.6 Hyökkäyksestä palautuminen....58
5.3 Kyberhyökkäyksessä toimimiseen valmistavat käytännöt....61
5.3.1 Koulutus....61
5.3.2 Toimintaohjeet ja niiden saatavuudesta huolehtiminen....62
5.3.3 Harjoittelu....63
5.3.4 Tietojärjestelmien suojaaminen....64
5.3.5 Valmiuden mittaaminen....65
6. TAPAUSTUTKIMUS: VARAUTUMISEN HAASTEET KOHDEORGANISAATIOSSA 67
6.1 Asenneilmapiiri ja tietämyskuilu....67
6.2 Haasteet tilannekuvan viestinnässä....70
6.3 Toimintaohjeiden puutteellisuus ja sisäistämisongelmat....72
6.4 Lääketieteellisten laitteiden heikko tietoturva....74
7. TAPAUSTUTKIMUS SUHTEESSA AIEMPAAN KIRJALLISUUTEEN....76
7.1 Ongelmakohdat ja niiden ratkaiseminen kirjallisuuden pohjalta....76
7.2 Tapaustutkimuksen ja kirjallisuuden yhteys....80
7.3 Pohdintaa....83
7.4 Synteesi – terveydenhuolto-organisaation kyberhyökkäysvarautuminen nyt ja tulevaisuudessa....85
8. JOHTOPÄÄTÖKSET JA YHTEENVETO....88
8.1 Johtopäätökset....88
8.2 Tutkimuksen arviointi....92
8.3 Tutkimustulosten merkitys ja hyödyntäminen....96
8.4 Jatkotutkimustarpeet tulevaisuuteen....97
LÄHTEET....99
LIITTEET....105

# KUVALUETTELO

***Kuva 1.*** *Metodologiset valinnat perustuen Saunders et al. (2009, s. 138.)* ..... *6*
***Kuva 2.*** *Hyökkäyksen havaitsemismenetelmät* ..... *49*
***Kuva 3.*** *Häiriötilanteen koordinointiryhmä kyberhyökkäystilanteessa* ..... *50*
***Kuva 4.*** *Johtoryhmän toiminta kyberhyökkäystilanteessa* ..... *53*
***Kuva 5.*** *Hoitotoiminnan vastuut kyberhyökkäystilanteessa* ..... *55*
***Kuva 6.*** *Hyökkäyksestä palautumisen työvaiheet* ..... *59*
***Kuva 7.*** *Organisaation kyberhyökkäysvalmiutta lisäävät käytännöt* ..... *61*
***Kuva 8.*** *Kybervarautuminen ja sen kehittäminen terveydenhuolto-organisaatioissa – nyt ja tulevaisuudessa* ..... *86*
***Kuva 9.*** *Terveydenhuolto-organisaatio kyberhyökkäystilanteessa: varautuminen ja toiminta eri toimijoiden vastuiden näkökulmasta* ..... *91*

# TAULUKKOLUETTELO

*Taulukko 1. Tutkimuksen laatukriteerit ja niiden kannalta olennaiset tutkimusvaiheet (Perustuen Yin 2014 s. 45) …….....…….……...…….9*

*Taulukko 2. Tutkimuksen haastateltavat asiantuntemusalueineen……....12*

*Taulukko 3. Haastatteluissa käytetty kysymysrunko……...……13*

*Taulukko 4. Haastatteluissa tehtyjen havaintojen analyysi……..14*

*Taulukko 5. Kyberturvallisuussuositukset terveydenhuolto-organisaatioille (Perustuen Norri-Sederholm et al. 2019)…….……...20*

*Taulukko 6. Kyberhyökkäysskenaarioita ja niiden mahdollisia seurauksia……...23*

*Taulukko 7. Kyberturvallisuuden osafunktiot (Perustuen NIST 2018)……...27*

*Taulukko 8. Haastatteluissa tunnistetut kyberhyökkäystilanteet……45*

*Taulukko 9. Kohdeorganisaatiolle esitettävät jatkosuositukset……..….77*

*Taulukko 10. Tutkimuksen laatukriteerit ja niiden kannalta olennaiset tutkimusvaiheet (Perustuen Yin 2014 s. 45)……..….92*

# 1. JOHDANTO

Johdantoluvussa esitellään tämän diplomityötutkimuksen lähtökohdat. Aluksi esitellään tutkimuksen motivaatio, aiheeseen liittyvää taustatietoa ja sen liittymäpintoja ajankohtaisiin yhteiskunnallisiin aiheisiin. Sitten esitellään tutkimuskysymykset, joihin tutkimus pyrkii vastaamaan sekä tutkimuksen rajaus. Lopuksi kerrotaan kirjallisen työn rakenteesta.

## 1.1 Työn motivaatio ja tausta

Digitaaliset palvelut ja järjestelmät auttavat ihmisiä ja yhteiskuntaa tekemään monia asioita tehokkaammin ja helpommin. Monet organisaatiot ovat hyvin riippuvaisia käyttämistään palveluista ja järjestelmistä, minkä vuoksi myös kyberturvallisuus kasvattaa jatkuvasti merkitystään. (Kyberturvallisuuskeskus 2021) Kyberhyökkäyksiä vastaan taistelemisesta onkin tullut viime vuosina tärkeä aihe erityisesti sellaisilla aloilla, joiden toiminta nojaa vahvasti tietoteknologiaan (Huang et al. 2018). Myös terveydenhuoltoalan organisaatiot ja asiantuntijat toimivat nykyisin jatkuvasti enemmän tietojärjestelmien varassa. Järjestelmät sisältävät tietoa, joka on usein hyvin henkilökohtaista ja luottamuksellista, mutta toisaalta myös äärimmäisen tärkeää potilaiden oikean hoidon kannalta. Lisäksi tietojärjestelmiä tarvitaan erilaisten hoitotoimenpiteiden suorittamisessa. Näihin järjestelmiin kohdistuvat uhat voivat olla vakavia ja ongelmat järjestelmien toiminnassa saattavat aiheuttaa uhkaa jopa ihmishengille. (Lovis 2014)

Tässä tutkimuksessa tutkitaan julkisiin terveydenhuolto-organisaatioihin kohdistuvia kyberhyökkäystilanteita ja sitä, miten organisaatiot selviäisivät sellaisen osuessa kohdalle. Varautumista tutkitaan etenkin päätöksenteon, ihmisten ja prosessien näkökulmista. Tutkimus on osa laajempaa kriisivalmiutta käsittelevää RECPHEALS-tutkimushanketta, jonka tavoitteena on hahmottaa terveydenhuoltojärjestelmään kohdistuvia uhkia. Hankkeessa tutkitaan muutosjoustavuutta, kriisivalmiutta ja huoltovarmuutta suomalaisessa terveydenhuoltojärjestelmässä. Tutkimushankkeen projekteissa arvioidaan terveydenhuoltojärjestelmän valmiutta toimia erilaisissa kriisitilanteissa sekä kehittää järjestelmän kykyä varautua niihin, hallita niitä ja oppia niistä. (Terveyden ja hyvinvoinnin laitos 2020)

**Julkisen terveydenhuolto-organisaation** tehtävänä on edistää, suojella ja ylläpitää vaikutuspiiriinsä kuuluvien ryhmien ja yksilöiden terveyttä, sekä ehkäistä tautien leviämistä. Sen tavoitteena on taata jokaiselle yhteisöön kuuluvalle henkilölle oikeus terveyden ylläpitoon tarvittaviin palveluihin ja sen tehtäviin kuuluu muun muassa ennaltaehkäi-

sevää työtä, diagnosointia ja hoitoa. Julkinen terveydenhuolto on organisoitu alueen yhteisenä ponnistuksena, esimerkiksi verovaroin. (Sharma et al. 2014) Suomessa julkisen terveydenhuollon vastuulle kuuluu huolehtia kaikista alueensa potilaista, heidän laadukkaasta hoidostaan ja potilasturvallisuudestaan, sekä siitä, että hoito on saatavilla kaikille yhdenvertaisesti. (Terveydenhuoltolaki 1326/2010, 2§)

**Kyberhyökkäys** tarkoittaa ”tekoa tai toimintaa, jolla pyritään tietoverkon, tietojärjestelmän, laitteen tai datan vahingoittamiseen tai oikeudettomaan käyttöön”. (Sanastokeskus 2018) Se on rikollista toimintaa, jolla pyritään aiheuttamaan vahinkoa ja joka voidaan luokitella esimerkiksi kiristykseksi, terrorismiksi tai sodankäynniksi. (Watters et al. 2012) Hyökkäyksiä on monenlaisia ja niihin kuuluvat esimerkiksi kiristyshaittaohjelmat, palvelunestohyökkäykset, tietomurrot ja verkkovakoilu (Kyberturvallisuuskeskus 2021).

**Varautumisella** tarkoitetaan toimintaa, jolla pyritään varmistamaan organisaation tehtävien mahdollisimman sujuva hoitaminen sekä mahdollisesti tarvittavat normaalista poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa. Varautumistoimenpiteisiin kuuluvat esimerkiksi valmiussuunnittelu, jatkuvuudenhallinta, etukäteisvalmistelut, koulutus ja valmiusharjoitukset. (Turvallisuuskomitea 2021)

Kyberhyökkäyksien uhka terveydenhuolto-organisaatioille on ollut paljon esillä mediassa. Esimerkiksi suomalaisen psykoterapiakeskus Vastaamon tietomurrossa suuri määrä asiakkaiden luottamuksellisia terveystietoja vuoti järjestelmästä rikolliselle, joka pyrki kiristämään yksittäisiä asiakkaita tiedoilla (Hakkarainen 2020). Erityisesti sairaaloihin kohdistuvista kyberhyökkäyksistä on tulossa jopa globaali trendi, ja monet terveydenhuollon organisaatiot ovat jo kärsineet vakavista seurauksista hyökkäystilanteissa (Pulliainen 2020). Esimerkiksi Saksassa vuoden 2020 syksyllä nainen kuoli ambulanssiin kyberhyökkäyksen sekoitettua sairaalan järjestelmät niin pahasti, ettei häntä kyetty ottamaan sairaalaan hoidettavaksi. Mikäli Saksan poliisin suorittama rikostutkimus johtaa syytteeseen, kyseessä on ensimmäinen kerta, kun kuolematapaus on yhdistetty suoraa kyberhyökkäykseen. (Heikkilä 2020) Irlannissa puolestaan kohdattiin suuria ongelmia, kun rahaa tavoittelevien rikollisten kiristysohjelma sulki koko Irlannin viranomaisten yhteisen potilastietojärjestelmän toukokuussa 2021. Maan hallinto pitää tapausta Irlannin historian vakavimpana kyberhyökkäyksenä. (STT 2021)

Suomalainen Vastaamon tapaus, sekä Saksan ja Irlannin tapaukset osoittavat, että yhteiskunnassa voidaan nähdä merkkejä siitä, miten kyberhyökkäykset aiheuttavat merkittävää haittaa terveydenhuolto-organisaatioille. Tähän tutkimukseen valikoitunut tutkimusaihe on ajankohtainen ja mielenkiintoinen, sillä tutkimuksen kautta voidaan selvittää, mitä alan organisaatiot voivat tehdä varautuakseen näihin vääjäämättä kasvaviin uhkiin.

## 1.2 Tutkimusongelma ja rajaus

Tässä diplomityössä tutkitaan julkisen terveydenhuolto-organisaation valmistautumista kyberhyökkäystilanteisiin. Tavoitteena on tutkia organisaatioita kyberhyökkäysten kohteina ja selvittää, millaisia asioita niiden tulisi ottaa huomioon kyberhyökkäyksiin varautumisessa. Tavoitteena on myös selvittää, mitä haasteita varautumiseen voi liittyä ja millaisilla toimilla organisaatioiden kriisivalmiutta voidaan parantaa niin, että kyberhyökkäyksestä selvittäisiin mahdollisimman tehokkaasti ja turvallisesti. Tutkimuksen tavoitteiden pohjalta on muodostettu päätutkimuskysymys, johon tutkimus pyrkii vastaamaan. Päätutkimuskysymykseen vastaamista helpottamaan on muotoiltu myös alatutkimuskysymyksiä. Kysymyksiin pyritään vastaamaan kirjallisuuden ja tapaustutkimuksen kautta.

**Päätutkimuskysymys:**

**P: Miten terveydenhuolto-organisaatio varautuu kyberhyökkäystilanteesta selviämiseen ja miten varautumista voitaisiin kehittää?**

Alatutkimuskysymykset ja luvut, joissa niihin osaltaan vastataan:

A1: Millaisia ovat terveydenhuolto-organisaatioihin kohdistuvat kyberhyökkäysuhat? (luvut 3 ja 5)

A2: Mitä terveydenhuolto-organisaatiossa tapahtuu toteutuvan hyökkäyksen aikana ja sen jälkeen?
(luvut 4, 5 ja 7)

A3: Miten terveydenhuolto-organisaatiot edistävät hyökkäyksestä selviämistä? (luvut 4, 5 ja 7)

A4: Mitkä ovat mahdollisia kehittymiskohteita?
(luvut 5, 6 ja 7)

Tutkimuksessa keskitytään vastaamaan tutkimuskysymyksiin erityisesti prosessien, johtamisen ja ihmisten toiminnan näkökulmasta. Tietojärjestelmiä käsitellään osana prosesseja, mutta yksityiskohtaisiin teknologioihin tai niiden valintaan ei tarkemmin perehdytä. Tutkimus käsittelee terveydenhuolto-organisaation valmiutta toimia kyberhyökkäystilanteissa silloin, kun hyökkäystilanne todella tapahtuu. Näin ollen esimerkiksi kyberhyökkäyksiä ennaltaehkäisevä toiminta rajautuu tutkimusaiheen ulkopuolelle. Tutkimusaiheen piiriin kuuluvat kuitenkin sellaiset ennen hyökkäystä tehtävät toimet, jotka pyrkivät valmistamaan organisaatiota, sen tietojärjestelmäinfrastruktuuria ja sen henkilöstöä toimintaan hyökkäystilanteen tapahtuessa. Kyberhyökkäyksistä tutkitaan erityisesti sellaisia, joilla voi olla selkeitä vaikutuksia organisaation toimintaan tai potilasturvallisuuteen.

Vähemmän vakavat ja pelkkään tietohallinnon toimintaan vähäisesti vaikuttavat häiriötilanteet rajautuvat siis tutkimuksen ulkopuolelle. Tutkimuksen kirjallisuusosio tutkii aihetta kaikissa julkisen sektorin terveydenhuoltoalan organisaatioissa, kun taas empiirinen osa rajautuu yhdestä organisaatiosta tapaustutkimuksessa saatavaan tietoon.

## 1.3 Tutkimuksen rakenne

Tämä diplomityö koostuu kirjallisuusosiosta ja empiirisestä tapaustutkimuksesta, joista molemmat pyrkivät osaltaan vastaamaan tutkimuksen tutkimuskysymyksiin. Kirjallisuusosiossa ja tapaustutkimuksessa tehtyjä havaintoja vertaamalla pyritään yhdistämään teoriatietoa käytännön tutkimukseen ja siten muodostamaan tutkimusaiheesta mahdollisimman kokonaisvaltainen käsitys. Tutkimuksen lopulliset päätelmät muodostetaan molemmissa osioissa tehtyjen löydösten perusteella.

Kirjallinen työ koostuu kahdeksasta luvusta. Johdannon jälkeen toisessa luvussa esitellään tutkimusasetelma sekä tutkimuksessa käytetyt menetelmät. Myös empiirisessä osassa tutkittava kohdeorganisaatio esitellään toisessa luvussa. Kolmas ja neljäs luku käsittävät tutkimuksen kirjallisuusosuuden. Kolmas luku perehtyy terveydenhuolto-organisaatioon kyberhyökkäyksen kohteena. Siinä esitellään terveydenhuolto-organisaatiota toimintaympäristönä sekä siihen kohdistuvia kyberuhkia. Neljännessä luvussa tutkitaan varautumista kyberhyökkäyksen toteutumiseen. Aluksi varautumista käsitellään yleisellä tasolla ja sitten erityisesti terveydenhuollon kontekstissa. Viides ja kuudes luku esittelevät tutkimuksen empiirisenä osana tehdyn tapaustutkimuksen. Viidennessä luvussa esitellään tutkimuksen perusteella muodostettu kuvaus tutkittavan organisaation nykytilasta kyberhyökkäysvarautumisessa. Luvussa kuvataan myös, mitä organisaatiossa tapahtuisi kyberhyökkäyksen aikana. Kuudennessa luvussa esitellään tutkimuksessa havaittuja haasteita tapausorganisaation kyberhyökkäysvalmiudessa.

Seitsemännessä luvussa annetaan kirjallisuuden avulla kohdeorganisaatiolle ehdotuksia jatkotoimista liittyen havaittuihin ongelmakohtiin. Lisäksi luvussa tutkitaan tapaustutkimuksen ja kirjallisuuden välistä yhteyttä, pohditaan tutkimuksessa tehtyjen havaintojen merkitystä kyberhyökkäysvarautumiselle ja sen tulevaisuudelle sekä muodostetaan synteesi terveydenhuolto-organisaation kyberhyökkäysvarautumisesta tapaustutkimuksen ja kirjallisuuden löydösten perusteella. Kahdeksas luku on yhteenvetoluku, jossa esitellään vielä tutkimuksen päätelmät ja vastaukset tutkimuskysymyksiin. Sen jälkeen arvioidaan tulosten paikkansapitävyyttä, tutkimuksen onnistumista ja siihen vaikuttaneita haasteita ja rajoitteita. Yhteenvedossa pohditaan myös tutkimuksen merkitystä ja sitä, miten siinä tehtyjä päätelmiä voidaan hyödyntää tulevaisuudessa. Luvun lopuksi esitetään vielä muutamia tämän tutkimuksen perusteella tunnistettuja jatkotutkimusaiheita.

# 2. TUTKIMUSASETELMA JA –METODOLOGIA

Tässä luvussa esitellään tutkimuksen tutkimusasetelma sekä metodologiset valinnat, joita tutkimusta suunniteltaessa ja sen edetessä on tehty. Aluksi esitellään tapaustutkimuksessa tutkittava organisaatio ja sen tutkimuksen kannalta olennaiset toimijat ja yhteistyökumppanit. Sen jälkeen esitellään tutkimusmetodologiaa ja tutkimuksessa käytettävät menetelmät.

## 2.1 Tutkittava organisaatio

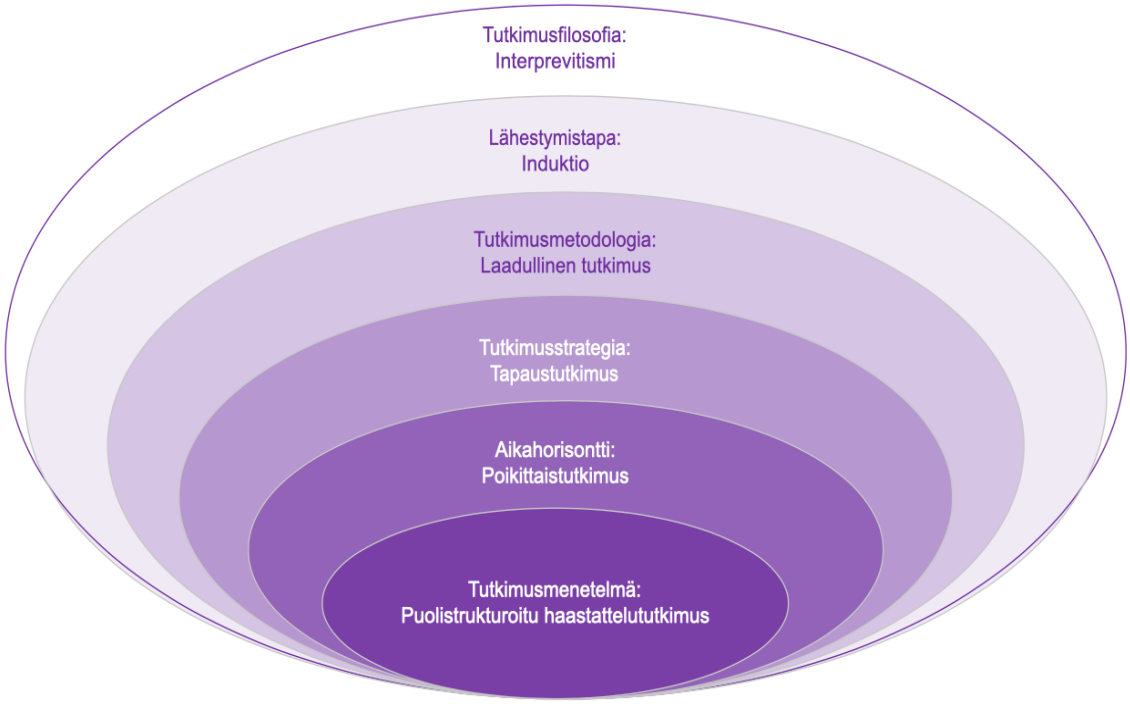
Tutkimuksen empiirisessä osassa tutkitaan valmistautumista kyberhyökkäystilanteessa selviämiseen erityisesti yhden terveydenhuolto-organisaation tapauksessa. Organisaatio on suuri suomalainen terveydenhuolto-organisaatio, jolla on toimintaa useilla terveydenhuollon eri osa-alueilla. Toiminta kattaa sekä kiireellistä akuuttihoitoa että kiireetöntä ajanvarauksiin perustuvaa hoitoa. Organisaation toiminta jakautuu useille eri toimialueille, joita johdetaan erillisinä yksiköinä. Kullakin toimialueella on oma johto, toimintamallit ja paljon omia käytäntöjä erilaisissa tilanteissa toimimiseen. Tämän tutkimuksen kannalta olennaista on erityisesti organisaation tietohallinnon ja johdon toiminta ja yhteistyö muiden toimijoiden kanssa, sekä se, miten organisaation toiminnan ytimessä oleva hoitotoiminta toteutetaan poikkeustilanteessa.

Organisaation tietohallinto vastaa monista kyberhyökkäyksiin varautumiseen ja reagointiin liittyvistä tehtävistä ja moni poikkeustilanteissa tarvittavista avainhenkilöistä työskentelee tietohallinnossa. Kyberhyökkäyksiin valmistautumisen kannalta merkittävä toimija on myös terveydenhuolto-organisaation IT-alan kumppaniyritys, jolle on ulkoistettu suuri osa organisaation tietojärjestelmiin ja tietoturvaan liittyvistä tehtävistä. Yrityksellä on merkittävä rooli kyberhyökkäysten tunnistamisessa, niihin reagoinnissa ja niistä palautumisessa. Kumppaniyritys tuntee terveydenhuolto-organisaation IT-infrastruktuurin erittäin hyvin ja yhteistyö ja tiedonvaihto organisaatioiden välillä on päivittäistä. Kumppaniyrityksen toimintatapoja kartoitettiin kohdeorganisaation henkilöstöä haastattelemalla.

Kyberhyökkäyksen kannalta olennaisia toimijoita ovat myös muun muassa organisaation yleisjohto, operatiivisen hoitotoiminnan johto ja hoitohenkilökunta. Hoidon toimialoista keskitytään tässä tutkimuksessa erityisesti sellaisiin, joiden toimintaan kuuluu kiireellistä hoitoa, joka ei aina voi odottaa poikkeustilanteen, kuten kyberhyökkäyksen, päättymistä. Nämä toimialat valikoituivat tutkittaviksi myös siksi, että organisaation ensimmäiset haastateltavat suosittelivat näiden alueiden henkilöstön pyytämistä haastatteluihin.

## 2.2 Tutkimusasetelma

Tutkimusasetelmalla kuvataan tutkimuksen suunnittelussa käytettävää tieteellistä viitekehystä ja siinä tehtyjä valintoja, jotka ohjaavat tutkimuksen tekemistä ja siinä kerättävän tiedon tulkintaa. Tutkimusasetelma pitää sisällään metodologian ja menetelmät, joita on valittu käyttää tutkimuksen suorittamisessa. Tutkimuksen lähtökohtien kuvaamiseen voidaan käyttää esimerkiksi Saunders et al. (2009) kirjassa esiteltyä sipulimallia, jossa kukin tutkimuksen suunnittelussa tehty valinta muodostaa yhden sipulin kerroksista. Tämän tutkimuksen metodologiset valinnat esitetään sipulimallin muodossa kuvassa 1.




***Kuva 1.*** *Metodologiset valinnat perustuen Saunders et al. (2009, s. 138.)*

**Tutkimusfilosofia: Interpretivismi**

Saundersin et al. (2019) mukaan tutkimusfilosofialla tarkoitetaan tutkimuksen taustalla vaikuttavaa ajattelua siitä, millaista tieto on, miten sitä luodaan sekä millainen on olemassa olevan ja tutkimuksessa luotavan tiedon suhde. Tutkimusfilosofia onkin eräänlainen tutkimuksen maailmankuva, jolla määritellään, millaista tietoa tutkimuksessa etsitään ja millaisia oletuksia voidaan tehdä. Tutkimusfilosofioita on monenlaisia ja ne eroavat keskenään esimerkiksi siinä, millä tavoilla kerättyä tietoa voidaan pitää hyväksyttävänä ja siinä, millainen on tutkijan rooli suhteessa tutkimukseen. (Saunders et al. 2019, s. 107)

Tässä tutkimuksessa tutkimusfilosofia on interpretivistinen. Interpretivistisessä tutkimusfilosofiassa todellisuus muodostuu sosiaalisten toimijoiden toimesta jatkuvasti muuttuvista sosiaalisista konstruktioista ja todellisuuksia voi olla useita erilaisia eri henkilöillä. Tutkija pitää yksilöiden subjektiivisia kokemuksia ja motiiveja tutkimuksen kannalta merkittävinä sosiaalisina ilmiöinä, jotka muodostavat yhdessä kuvan tutkittavasta ilmiöstä. (Saunders et al. 2019, s. 119, 116) Tässä tutkimuksessa käsitys organisaation kriisivarautumisen nykytilasta muodostetaan tutkimalla eri puolilla organisaatiota työskentelevien yksilöiden käsityksiä siitä, mitä tapahtuisi hyökkäyksen sattuessa. Interpretivistisessä tutkimuksessa on käytännössä mahdotonta välttää sitä, että tutkija vaikuttaa itse tutkimustuloksiin. Tutkija toimii tutkittavien subjektiivisten kokemusten tulkitsijana ja antaa heidän kokemuksilleen merkityksiä omien oletustensa ja maailmankuvansa kautta sekä toisaalta saattaa vaikuttaa tilanteisiin, joissa tutkittavat kertovat ajatuksiaan. (Saunders et al. 2019, s. 119)

**Lähestymistapa: Induktio**

Saunders et al. (2009) jakaa tutkimusten lähestymistavat kahteen päätapaan, induktioon ja deduktioon. Lisäksi lähestymistapoja voi muodostua näiden kahden yhdistelmänä. Deduktiossa tutkimusta tehdään siten, että tutkimus pyrkii testaamaan olemassa olevia teorioita ja siten joko vahvistamaan tai hylkäämään ne. Induktiossa, jota tämä tutkimus edustaa, puolestaan teoria muodostuu empiirisen tutkimuksen tuloksena ja tutkimustuloksiin pyritään suhtautumaan mahdollisimman avoimesti ilman ennakko-oletuksia. (Saunders et al. 2009, s. 590, 593, 600) Tämän tutkimuksen kontekstissa induktiivisella lähestymistavalla tarkoitetaan käytännössä sitä, että käsitys tutkittavasta ilmiöstä, eli tutkittavan organisaation toiminnasta kyberhyökkäystilanteessa, syntyy empiirisen aineiston tutkimuksen tuloksena.

**Tutkimusmetodologia: Laadullinen tutkimus**

Tutkimuksia voidaan yleisesti jaotella kvantitatiiviseen ja kvalitatiiviseen tutkimukseen, joista tämä tutkimus edustaa jälkimmäistä. Kvantitatiivisen tutkimuksen keräämä tieto on laskennallista, kuten mittausarvoja tai muita määrällisiä ja tilastointikelpoisia arvoja. (Saunders et al. 2009, s. 151) Kvalitatiivinen tutkimus puolestaan kerää laadullista tietoa, jota saadaan esimerkiksi avoimista haastattelukysymyksistä. Laadullisen tutkimuksen tavoitteena on ymmärtää ja kuvailla jotakin tilannetta, ilmiötä tai toimintaa ja tunnistaa asioiden välisiä suhteita. (Saunders et al. 2009, s. 516) Tutkimuskysymys määrittelee

pitkälti sen, kumman tyyppistä tietoa tutkimuksessa halutaan kerätä. Tässä tutkimuksessa etsitään vastauksia tutkimuskysymyksiin, joissa esiintyvät esimerkiksi kysymyssanat *”Millaisilla” ja ”Miten”*. On luontevaa, että tällaisiin kysymyksiin vastataan tiedolla, joka pyrkii mahdollisimman kattavasti ja syvällisesti kuvailemaan tutkittavaa tilannetta ja auttamaan sen ymmärtämisessä.

**Aikahorisontti: Poikittaistutkimus**

Tutkimuksen aikahorisontin valinnassa päätetään, kuinka pitkällä aikavälillä tutkittavaa ilmiötä halutaan tutkia. Tutkimusta voidaan suorittaa pidemmällä aikavälillä, jolloin voidaan seurata esimerkiksi tiettyjen toimien aiheuttamia muutoksia. Toinen vaihtoehto on poikittaistutkimus, jossa keskitytään yhteen ajanhetkeen ja muodostetaan siitä mahdollisimman kattava kuva. (Saunders et al. 2009, s. 155) Tässä tutkimuksessa aikahorisontiksi on valittu poikittaistutkimus, sillä tarkoitus on tutkia erityisesti organisaation kyberhyökkäysvalmistautumisen nykytilaa ja sitä, miten sitä voitaisiin kehittää. Organisaatio on myös todella suuri ja jo pelkästään nykyhetken tilanteen ymmärtäminen vaatii paljon tutkimusta, joten pidemmän aikavälin seuranta ei tutkimuksen resurssien ja aikataulun puitteissa ole mahdollista.

## 2.3 Tutkimusstrategia: Tapaustutkimus

Tutkimuksessa käytetään tutkimusstrategiana tapaustutkimusta, joka Robert Yinin (2014) määritelmän mukaan on empiirinen tutkimus, joka tutkii jotakin nykyaikaista ilmiötä syvällisesti sen tosielämän kontekstissa (Yin 2014, s. 237). Tapaustutkimuksen keskiössä on halu ymmärtää ihmisten toimintaa ja päätöksentekoa tutkittavissa tilanteissa ja selittää, miksi ne tehdään, miten ne toimeenpannaan ja millaisia tuloksia ne tuottavat (Schramm 1971).

Tapaustutkimuksessa tutkittavaa ilmiötä tutkitaan monien eri tietolähteiden avulla (Saunders 2009, s. 588) Tutkittavina on usein organisaatioita, prosesseja, instituutioita, ohjelmia, yksilöitä ja tapahtumia. Tutkittava ilmiö ja sen konteksti ovat vahvasti sidoksissa toisiinsa. (Yin 2014, s 16) Tämä tapaustutkimus vastaa edellä esitettyjä määritelmiä hyvin, sillä sen tavoitteena on kuvata tarkasti kohdeorganisaation toimintaa, prosesseja, yksilöiden toimintaa ja päätöksentekoa tietyn tapahtuman, eli tässä tapauksessa kyberhyökkäyksen, sattuessa.

### 2.3.1 Tapaustutkimuksen laatukriteerit

Tapaustutkimukselle voidaan asettaa tiettyjä laatukriteereitä, joiden täyttymiseen tutkimusmenetelmien valinnassa ja toteutuksessa pyritään. Samoja kriteerejä hyödynnetään myös tutkimuksen ja sen tulosten laadun arvioinnissa tutkimuksen jälkeen. Ihmisten käyttäytymistä koskevassa tutkimuksessa käytetään yleisesti neljää kriteeriä: rakenteellista –, ulkoista – ja sisäistä validiteettia, sekä reliabiliteettia. (Yin 2014, s.45) Laatukriteerit ja niiden kannalta olennaiset tutkimuksen vaiheet ovat esitettynä taulukossa 1.

Taulukko 1. *Tutkimuksen laatukriteerit ja niiden kannalta olennaiset tutkimusvaiheet (Perustuen Yin 2014, s. 45)*

| **Laatukriteeri** | **Tutkimuksen vaihe** |
|---|---|
| Rakenteellinen validiteetti | Tutkimusmenetelmien valinta, tiedonkeruu, otannan valinta |
| Ulkoinen validiteetti | Teorian käyttö, kirjallisuuden ja empirian tutkimustulosten vertailu ja synteesi |
| Sisäinen validiteetti | Ongelmakohtien taustasyiden analyysi, hypoteesien rakennus |
| Reliabiliteetti | Tutkimusmenetelmien valinta, tiedonkeruun toteutus ja dokumentointi |

Tutkimuksen rakenteellisella validiteetilla pyritään siihen, että valittavat tutkimusmenetelmät ja tutkimuskohteet soveltuvat mahdollisimman hyvin tutkimuskohteena olevan ilmiön tutkimiseen (Yin 2014, s. 46). Rakenteellisen validiteetin varmistaminen liittyy erityisesti tutkimusmenetelmien valintaan ja toteutukseen. Tässä tutkimuksessa tutkimusmenetelmiksi on valittu mahdollisimman monipuolisen haastateltavajoukon haastattelut, joilla uskotaan saatavan kattavin ja syvällisin mahdollinen käsitys siitä, mitä eri puolella organisaatiota tapahtuu. Alustavia tutkimustuloksia pyritään katsastamaan tutkimuksen aikana organisaation avainhenkilöillä palautteen saamiseksi.

Ulkoinen validiteetti taas tutkii sitä, miten hyvin tutkimuksesta saatavia tuloksia voidaan yleistää koskemaan muita kuin tutkittavina olevia tilanteita tai organisaatioita (Yin 2014, s. 234). Tämän tutkimuksen empiirisessä osassa tutkitaan vain yhtä organisaatiota, joten empirian tuloksia ei voida suoraa yleistää kuvaamaan kaikkia terveydenhuolto-organisaatioita. Yleistettävyyttä voidaan kuitenkin hakea vertailemalla empiirisessä osuudessa

tehtyjen havaintoja kirjallisuudesta löydettävään teoriatietoon ja hakemalla näistä yhtäläisyyksiä ja eroavaisuuksia tutkimuksen synteesiosiossa.

Tutkimuksen sisäinen validiteetti arvioi sitä, miten hyvin tutkimuksen perusteella pystytään hahmottamaan syy-seuraus-suhteita. Tämä laatukriteeri on merkittävä tutkimuksissa, jotka pyrkivät selittämään tutkittavaa ilmiötä ja sitä, miksi jotkin asiat tapahtuvat. (Yin 2014, s. 47) Tässä tutkimuksessa pääpaino on tutkittavan organisaation toiminnan kuvailemisella, mutta erityisesti organisaation kehityskohteiden tutkimisessa kuudennessa luvussa käytetään paikoin myös selittävämpää otetta. Sisäiseen validiteettiin pyritään etsimällä toistuvia kaavoja haastateltavien vastauksista ja rakentamalla näistä mahdollisia selityksiä ilmiöille. Muodostettavien hypoteesien taustana pyritään käyttämään mahdollisimman kattavasti erilaisia kommentteja.

Tapaustutkimuksen reliabiliteetilla tarkoitetaan puolestaan tutkimuksessa käytettävien tutkimusmenetelmien johdonmukaisuutta ja toistettavuutta (Yin 2014, s. 240). Tässä tutkimuksessa reliabiliteetin varmistamiseen pyritään objektiivisen tutkimusotteen ja hyvän tieteellisen käytännön noudattamisella esimerkiksi haastattelutilanteissa, ja sillä, että tutkimuksen suorittaminen ja tiedonkeruussa käytetyt menetelmät dokumentoidaan tarkasti osaksi tätä tutkimusraporttia.

### 2.3.2 Puolistrukturoitu haastattelututkimus

Tapaustutkimuksessa voidaan hyödyntää monia erilaisia tiedonkeruutapoja, joista tässä tutkimuksessa päädyttiin haastatteluihin. Haastattelujen etuna on Robert Yinin (2014) mukaan se, että niissä voidaan keskittyä suoraan tapaustutkimuksen aiheeseen. Tämän tutkimuksen toteuttaminen esimerkiksi tarkkailumenetelmällä tai arkistotutkimuksella olisi todennäköisesti ollut suhteellisen vaikeaa järjestää, sillä se olisi vaatinut todellisen tai simuloidun tilanteen järjestämistä. Haastattelujen etuna on myös se, että niiden aikana saadaan tietoa hyvin monipuolisesti, sillä niissä voidaan haastateltavien suorien vastauksien ja näkemyksien lisäksi havainnoida myös heidän asenteitaan ja oletuksiaan tutkittavista aiheista. Haastattelujen haasteena puolestaan ovat potentiaaliset tutkijan omat ennakkoasenteet ja biakset kysymysten ajattelussa ja vastausten tulkinnassa. Näitä pyrittiin välttämään tutkimuksessa palautteen kysymisellä ja aktiivisella keskustelulla tarkastajien kanssa. Haasteita voi aiheutua myös, jos haastateltava yrittää vastata kysymyksiin siten, kun olettaa tutkijan tai oman organisaationsa haluavan. (Yin 2014, s. 106) Tätä haastetta pyrittiin välttämään avoimen ilmapiirin luomisella haastattelutilanteisiin.

Tieteellisissä tutkimuksissa käytettäviä haastattelutyylejä on olemassa monen tyyppisiä, joista tämän tutkimuksen haastattelut edustavat puolistrukturoituja haastatteluja. Puolistrukturoidussa haastattelussa haastattelija tuo haastattelutilanteeseen rungon, joka sisältää kysymyksiä erilaisista teemoista, joista haastattelussa on tarkoitus kysyä. Haastattelija ei kuitenkaan pitäydy orjallisesti haastattelurungon mukaisissa kysymyksissä tai sen järjestyksessä, vaan reagoi haastateltavan kommentteihin esimerkiksi kysymällä tarkentavia tai kokonaan uusia tutkimusaiheeseen liittyviä kysymyksiä. (Saunders et al. 2019, s. 601) Seuraavissa alaluvuissa kuvataan vielä tarkemmin tämän puolistrukturoidun haastattelututkimuksen tiedonkeruun menetelmiä sekä sitä, miten haastatteluissa saatuja tuloksia analysoidaan.

### 2.3.3 Tiedonkeruu

Tietoa tutkimusta varten kerättiin kohdeorganisaation henkilöstöä haastattelemalla. Haastateltavien henkilöiden valinta suoritettiin lumipallomenetelmällä siten, että haastattelut aloitettiin organisaation tutkimuksen kannalta keskeisimmistä avainhenkilöistä, jonka jälkeen jokaiselta haastateltavalta kysyttiin, keitä hänen mielestään olisi myös tarpeen haastatella. Kyberhyökkäyksiin varautuminen oli osa ensimmäisten haastateltavien tärkeimpiä työtehtäviä, kun taas loppupään haastateltaville niiden riski oli kaukaisempi aihe, mutta heidän tulee silti osata toimia sellaisen tapahtuessa. Haastattelut aloitettiin organisaation tietohallinnosta, josta siirryttiin vähitellen kohti yrityksen johtoa. Johdon jälkeen siirryttiin vähitellen kohti operatiivista hoitotoimintaa, aloittaen osastojen vastaavista henkilöistä ja päätyen lopulta varsinaista hoitotoimintaa suorittaviin henkilöihin. Haastateltavia oli lopulta 14 ja heidän joukossaan oli hallinnon henkilökuntaa, sairaanhoitajia, sekä lääkäreitä. Haastateltavat ja heidän asiantuntemusalueensa ovat esiteltyinä taulukossa 2.

Taulukko 2. *Tutkimuksen haastateltavat asiantuntemusalueineen*

| Haastateltava | Asiantuntemus |
|---|---|
| **Tietohallinto A** | Tietohallinnon toiminta, tietoturva, koordinaatioryhmän toiminta |
| **Tietohallinto B** | Tietohallinnon toiminta, tietoturva, IT-kokonaisuudet, yhteys hoitotoimintaan, koordinaatioryhmän toiminta |
| **Tietohallinto C** | Tietohallinnon toimintamallit ja johtaminen, tietohallinto osana koko organisaatiota, yleisjohdon toiminta |
| **Tietohallinto D** | Tietohallinnon toimintamallit ja johtaminen, tietohallinto osana koko organisaatiota, yleisjohdon toiminta |
| **Johto A** | Yleisjohdon toiminta ja vastuut kriisitilanteissa |
| **Johto B** | Yleisjohdon toiminta ja vastuut kriisitilanteissa |
| **Hoitohenkilökunta A** | Hoitotoiminta, turvallisuuskouluttaminen |
| **Hoitohenkilökunta B** | Akuutin hoitotoiminnan koordinointi ja toteuttaminen |
| **Hoitohenkilökunta C** | Akuutin hoitotoiminnan koordinointi ja toteuttaminen, hoitotoiminnan tietojärjestelmät |
| **Hoitohenkilökunta D** | Lääkäreiden toiminnan johtaminen, akuutin toimialueen hoitotyö |
| **Hoitohenkilökunta E** | Akuutin hoitotoiminnan koordinointi ja toteuttaminen |
| **Hoitohenkilökunta F** | Akuutin hoitotoiminnan koordinointi ja toteuttaminen |
| **Hoitohenkilökunta G** | Akuutin toimialueen hoitotyö |
| **Tekniikka A** | Lääkintätekniikan käyttö ja toiminta, hoitotoiminnan tietojärjestelmät |

Haastattelukysymysten muodostamisessa hyödynnettiin Robert Yinin (2014) esittelemiä tapaustutkimuksen suunnitteluohjeita. Haastattelut toteutettiin Teams-alustalla ja ne nauhoitettiin myöhempää tarkastelua varten. Haastattelija teki haastattelujen aikana myös muistiinpanoja tekstin ja käsitekartan muodossa. Haastattelutilanteissa käytettiin reaktiivista strategiaa, jossa etukäteen valmistellut haastattelukysymykset olivat avoimia ja haastattelija reagoi haastateltavien antamiin vastauksiin kysymällä uusia kysymyksiä. Tällaiseen menettelyyn päädyttiin, sillä haastattelijalla oli varsinkin työskentelyn alkupuolella melko vähän tietoa organisaatiosta ja sen käytännöistä. Haastateltavien taustat ja osaamisalueet olivat myös keskenään hyvin erilaisia, joten olisi ollut vaikeaa etukäteen arvioida, minkä asioiden kysyminen keneltäkin olisi tutkimuksen kannalta olennaista.

Koska haastateltavista varsin pieni osa oli työnsä puolesta perehtynyt kyberuhkiin ja hyökkäystilanteiden tyypillisiin piirteisiin, oli haastattelijan autettava haastateltavia ymmärtämään niitä haastattelujen edetessä. Tämä aiheutti paikoitellen haasteita, sillä haastattelijan oli pysyttävä objektiivisena, mutta tarjottava myös asiaan perehtymättömille haastateltaville jotakin, mihin tarttua. Hoitohenkilökunnan haastattelutilanteet vaativat melko paljon objektiivisuuden ja ohjaamisen välillä tasapainoilua, jotta haastateltavat osasivat kertoa tutkimuksen kannalta olennaisista asioista tulematta kuitenkaan ohjailluksi. Haastateltaville kerrottiin tarvittaessa kyberhyökkäyksien olevan tilanteita, joissa hyökkääjä jollakin tavalla vaikuttaa käytössä olevien tietojärjestelmien toimintaan, esimerkiksi poistamalla ne käytöstä häiritsemällä niiden toimintaa jollakin tavalla. Suurin osa haastateltavista tunnisti tietovuodon mahdollisena kyberhyökkäysskenaariona, mutta sekin mainittiin joillekin haastateltaville haastattelijan toimesta.

Haastattelutilanteiden runkona toimivat taulukossa 3 esitetyt kysymykset. Kysymysten teemoja laajennettiin kussakin haastattelussa haastateltavan rooliin liittyvillä täydentävillä kysymyksillä.

Taulukko 3. *Haastatteluissa käytetty kysymysrunko*

| |
|---|
| Henkilö esittelee itsensä ja aiheeseen liittyvät tehtäväkuvaukset |
| Miten hyökkäys havaitaan? / Mistä saat tiedon hyökkäyksestä? |
| Kun havaitaan, että kyberhyökkäys tapahtuu, mitä tapahtuu? Miksi? |
| Kuka tekee ja mitä? Miksi? |
| Mitä hyökkäyksestä voi seurata? |
| Mitä haasteita kriisitilanteessa todennäköisesti kohdataan?<br>Mitä ongelmia voi syntyä? |
| Miten arvioit, tietävätkö kaikki, mitä heidän pitää tehdä?<br>Onko kaikilla riittävästi tietoa? Miten he kokevat tehtävänsä? |
| Mitataanko kyberhyökkäysvalmiuttanne jotenkin? |
| Miten toiminta palautuu normaaliksi hyökkäyksen jälkeen? |
| + Ketä muita henkilöitä kannattaa vielä haastatella? Mistä aiheista? |

Haastattelutilanteiden lisäksi organisaatioon liittyvää tietoa saatiin sen edustajien kanssa ennen varsinaista tutkimusta ja sen aikana pidetyissä palavereissa.

### 2.3.4 Aineiston analyysi

Kerätty tutkimusaineisto koostui haastattelujen nauhoitteista, haastattelujen aikana koostetuista käsitekartoista sekä haastattelujen aikana tehdyistä muistiinpanoista. Suuri osa tiedosta kerättiin jo haastattelujen aikana, mutta haastattelunauhoitukset kuunneltiin uudestaan muistiinpanojen täydentämiseksi ja niiden oikeellisuuden varmistamiseksi. Myös sitaatteja varten palattiin äänitteisiin, jotta ne saatiin muotoiltua täsmällisesti.

Haastattelujen muistiinpanot taulukoitiin haastattelukysymysten mukaan ja eri haastateltavien vastauksista etsittiin yhteisiä teemoja, joita ryhmittelemällä muodostettiin havaintoja. Vaikka haastateltavat edustivat hyvin erilaisia osaamisalueita, löytyi yhteisiä teemoja hyvin ja niistä saatiin koostettua tutkimuksen keskeisimmät havainnot. Havaintojen analysointia ja vertailua kuvataan taulukossa 4.

Taulukko 4. *Haastatteluissa tehtyjen havaintojen analyysi*

| **Lainaus haastattelusta** | **Lainauksesta tehdyt huomiot** | **Ryhmitellyt havainnot** |
|---|---|---|
| *”Kyberhyökkäyksen toimintavalmiutta ole arvioitu ulkopuolelta, eikä harjoiteltukaan. On tiedossa, että tällaisia on ja että tällaisia voi tulla. Voisi olla hyvä varautua konkreettisten tilanteiden harjoittelemisella. Muita kriisitilanteita ja vaaratilanteita on harjoiteltu kyllä.”*<br><br>*(Hoitohenkilökunta G)* | Valmiutta kyberhyökkäyksessä toimimiseen ei olla arvioitu<br><br>Ei ole päässyt harjoittelemaan kyberhyökkäystilanteita<br><br>Tunnistaa riskin kyberhyökkäyksestä<br><br>On harjoitellut muita poikkeustilanteita | Kaikkien yksiköiden valmiutta toimia kyberhyökkäyksessä ei ole arvioitu<br><br>Kaikki eivät ole harjoitelleet kyberhyökkäystilanteita<br><br>Kyberhyökkäysriski tunnetaan organisaatiossa<br><br>Muita poikkeustilanteita harjoitellaan organisaatiossa enemmän kuin kyberhyökkäystilanteita |
| *”Vaihtoehtoiset toimintatavat pitäisi olla sisäistettyinä, eikä saisi luottaa liikaa tietojärjestelmiin. Jokaisessa yksikössä pitäisi olla selvä suunnitelma siitä, mitä tehdä, kun jotain tapahtuu. Olen erittäin ylpeä siitä, että meillä on nämä asiat hyvin. Kaikki prosessit on mietitty alusta asti. Varauduttu on paljon! Muilla ei ehkä ole asiat yhtä hyvin.”*<br><br>*(Hoitohenkilökunta E)* | Tärkeää, että kattavat poikkeustilanteen toimintatavat on sisäistetty ennen tilannetta, jotta kaikki tietävät miten toimia<br><br>Kyseisessä yksikössä tehtyyn varautumissuunnitelmaan luotetaan vahvasti<br><br>Ei varmuutta siitä, onko muut organisaation osat yhtä varautuneita | Poikkeustilanteiden toimintasuunnitelmat ovat yksikkökohtaisia<br><br>Pitkälle mietittyjä ja hyvin sisäistettyjä varautumismalleja on käytössä<br><br>Epävarmuutta siitä, onko varautuminen järjestetty koko organisaatiossa yhtä hyvin ja tietävätkö kaikki, kuinka toimia poikkeustilanteessa |

Sen lisäksi, että haastatteluvastauksista etsittiin ryhmittelemällä tekijöitä, joita useampi henkilö nosti esiin, kiinnitettiin erityistä huomiota myös haastateltavien omiin osaamisalueisiin. Mikäli haastateltava oli jonkin alueen erityisosaaja, voitiin hänen kommenttejaan tämän alueen osalta pitää merkittävinä, vaikka ne eivät olisikaan nousseet esiin muissa haastatteluissa. Esimerkiksi lääkintälaitteet parhaiten tunteva haastateltava oli ainoa, joka tunnisti tiettyjä laitteisiin liittyviä riskejä, mutta ne nostettiin esiin tuloksissa, sillä hänen asiantuntemustaan niistä pidettiin luotettavana.

Tehtyjen havaintojen perusteella muodostettiin kaksi erilaista esitystä nykytilan analyysista: prosessikuvaajat ja sanallinen selostus. Prosessikuvaajissa eriteltiin olennaisimmat kyberhyökkäystilanteen toimijat ja kuvattiin, millaisia tehtäviä he suorittavat tilanteen aikana. Muitakin mahdollisia kuvaustapoja olisi ollut mahdollista käyttää, mutta tätä kuvaustapaa pidettiin tutkimuksen tarkoituksiin parhaana, sillä tarkoituksena oli havainnollistaa ihmisten ja organisaation osien välisiä prosesseja. Kaavioilla pyrittiin kuvaamaan erityisesti päätöksentekoa, toimintaa ja tiedonkulkua organisaatiossa. Sanallinen selostus valmisteltiin täydentämään, selittämään ja tukemaan prosessikuvaajaa ja sen tulkintaa. Nykytilan analyysiluvussa kuvataan sanallisesti myös kyberhyökkäyksen mahdollisia seurauksia organisaatiolle ja erilaisia tapoja, joilla organisaatio pyrkii kehittämään kykyään toimia hyökkäystilanteessa ja mittaamaan kriisivalmiuttaan.

# 3. TERVEYDENHUOLTO-ORGANISAATIO KYBERHYÖKKÄYKSEN KOHTEENA

Terveydenhuolto-organisaatio on monimuotoinen ja kompleksinen yksikkö, jossa suuri määrä henkilöitä tekee aikakriittistä ja tietointensiivistä työtä tietojärjestelmät apunaan. Potilastietoja käsitellään useissa eri järjestelmissä, ja hoidossa käytettävät laitteet hyödyntävät ja tuottavat paljon tietoa. (Maryati 2015). Sosiaali- ja terveysministeriön (2019) mukaan käsiteltävä tieto on kuitenkin usein erittäin luottamuksellista ja siten arvokasta, ja siksi se voi herättää myös rikollisten huomion. Terveydenhuolto-organisaatiot ovat toiminnallaan joka päivä vastuussa ihmisten terveydestä ja turvallisuudesta. Niiden toiminnan jatkuvuus on myös yhteiskunnan kriisivalmiuden ja turvallisuuden kannalta erittäin kriittistä. Tämän tietävät valitettavasti myös kyberrikolliset. Terveydenhuolto-organisaatioiden toimintaa lamauttamalla ja ihmisten terveystietoja varastamalla kyberhyökkääjät pyrkivät häiritsemään yhteiskunnan toimintaa ja kiristämään organisaatioita. (Sosiaali- ja terveysministeriö 2019)

Tässä luvussa perehdytään terveydenhuolto-organisaatioihin kyberhyökkäysten kohteina. Tarkoituksena on muodostaa yleiskuva terveydenhuollon toimintaympäristöstä, johon tietojärjestelmät olennaisena osana kuuluvat, sekä siitä, millaisia erityispiirteitä kyberturvallisuuteen ja -hyökkäyksiin liittyy juuri terveydenhuollon alalla toimittaessa.

## 3.1 Terveydenhuolto toimintaympäristönä

Terveydenhuolto-organisaatiot ovat kompleksisia ja jatkuvasti muuttuvia toimintaympäristöjä, jotka kokoavat yhteen monien alojen ammattilaisia (Kvist et al. 2013). Esimerkiksi sairaalassa työtehtäviä on lääkäreille ja sairaanhoitajille, mutta myös lukuisille logistiikka-alan henkilöille, insinööreille ja IT-ammattilaisille, tutkijoille, laboranteille, johtajille, kiinteistöhuoltajille, asiakaspalvelijoille ja ravintolatyöntekijöille. Vaikka modernit digitaaliset työkalut ja laitteet mahdollistavat nykyään monia terveydenhuollon tehtäviä, on työskentelystä merkittävä osa silti hyvin ihmiskeskeistä paikkaan sidottua ja manuaalista käsillä tehtävää työtä. Työntekijöitä on paljon ja heidän väliseen yhteistyöhönsä liittyvät tekijät ovat terveydenhuolto-organisaatioiden toiminnan kannalta hyvin merkityksellisiä. (Donchin & Gopher 2014)

Hoitotoiminnan keskiössä on aina potilaat ja heidän terveytensä ja turvallisuutensa (Turunen et al. 2015) Pienetkin virheet voivat johtaa potilaiden vaarantumiseen. Potilastur-

vallisuuden muodostumisen kannalta on hyvin tärkeää, että kaikki organisaation eri rooleissa työskentelevät työntekijät ovat tietoisia tehtävänsä merkityksestä potilasturvallisuuskulttuurin muodostumisessa, ja sitoutuneita siihen. (Feng et al. 2011; Groves et al. 2011).

Organisaatioiden asiakasjoukko voi koostua pienemmistä ihmisryhmistä ja yhteisöistä tai vaihtoehtoisesti jopa kokonaisisten valtioiden tai niiden alueiden asukkaista. Hoito- ja diagnostiikkatoiminta ovat terveydenhuolto-organisaatioiden ydintehtäviä. Suuret alan organisaatiot tarjoavat hyvin monen tyyppisiä palveluita, esimerkiksi päivystystä, kuvantamista ja laboratoriokokeita, vuodehoitoa ja leikkaustoimintaa. (Sharma et al. 2014) Akuutilla hoidolla tarkoitetaan hätätilojen kiireellistä diagnostiikkaa ja hoitoa, joka on toteutettava heti ja jonka tekemättä jättäminen voisi vaarantaa potilaan turvallisuuden (Finto 2021). Suomessa julkisen terveydenhuollon on pystyttävä tarjoamaan kiireellinen hoito kaikille hoitoon saapuville heidän asuinpaikastaan riippumatta (Terveydenhuoltolaki 1326/2010, 2§). Elektiivisellä toiminnalla puolestaan tarkoitetaan sellaisia hoitotoimia, jotka voidaan jättää tekemättä tai tehdä myöhemmin ilman, että siitä koituu potilaalle vaaraa (Finto 2021). Tällaista toimintaa voi olla esimerkiksi ajanvarauksella tehtävät hoitotoimenpiteet.

Terveydenhuollon toimintaympäristöön liittyvät ajoittain myös haastavat työskentelyolosuhteet ja -ajat. Hoidon tarve ei aina katso kelloa tai loma-aikoja. Monesti laadukasta hoitoa on voitava toteuttaa ympäri vuorokauden jokaisena vuoden päivänä. (Witkoski & Dickson 2010) Kiire ja stressi ovatkin usein läsnä hoitotyössä, etenkin sellaisilla osastoilla, joilla hoidetaan kiireellisiä potilaita. Gopher (2014) ajattelee, että jos terveydenhuollossa tehdään hoitovirheitä, ne eivät yleensä johdu henkilöstön motivaationpuutteesta tai huolimattomuudesta, vaan pikemminkin vaikeista työskentelyolosuhteista. Tällaisia haasteita voi aiheuttaa esimerkiksi yllättävät tilanteet ja puutteellinen parhaiden työskentelytapojen suunnittelu, työnjako ja johtaminen. (Donchin & Gopher 2014, Kiviluoma et al. 2020) Varsinkin hoitajien kokemasta stressistä, uupumuksesta ja sitä kautta myös työtyytymättömyydestä, löytyy paljon tieteellistä näyttöä ympäri maailmaa. (Kshetrimayum et al. 2019; Kvist et al 2013; Leineweber et al. 2016; Zhang et al. 2014)

Suuret julkiset terveydenhuolto-organisaatiot ovat varsin monimutkaisia systeemejä, joiden pyörittäminen voi ajoittain olla sekä haastavaa että kallista. Monet modernit valtiot käyttävätkin merkittävän prosenttiosuuden bruttokansantuotteestaan juuri terveydenhuolto-organisaatioiden rahoittamiseen. (Donchin & Gopher 2014) Koska valtio rahoittaa julkista terveydenhuoltoa, myös poliittiset päätökset voivat vaikuttaa niiden toimintaan, esimerkiksi valtion määräämien rakenneuudistusten tai kustannusleikkausten muo-

dossa. Julkisesta ohjauksesta seuraa myös se, että julkisten terveydenhuolto-organisaatioiden tulee usein olla tarkkoja rahankäytöstään, eikä kaikkiin asioihin välttämättä ole mahdollista investoida. (Hacker 2004) Julkisen terveydenhuollon toteuttamiseen liittyykin usein haastava tasapainottelu tehokkaan ja laadukkaan hoidon tarjoamisen ja poliittisten tekijöiden mukanaan tuomien vaatimusten ja epävarmuuden välillä (Opedal & Rommetvedt 2010).

### 3.1.1 Tietojärjestelmien rooli terveydenhuollossa

Gopherin (2014) ja Lovisin (2014) mukaan hoitohenkilökunnan lisäksi myös tietojärjestelmät ja muu teknologia näyttelevät jatkuvasti suurempaa roolia terveydenhuollossa. Tietotekniikkaa käytetään niin diagnostiikassa, hoitotoimenpiteissä, hoidon seurannassa kuin toiminnan organisoinnissakin. (Donchin & Gopher 2014; Lovis 2014) Parhaimmillaan tietojärjestelmät tukevat hoitotyöhön liittyvää yhteistyötä ja tiedonkulkua sekä tuottavat hyötyjä asiakkaiden ja potilaiden hoitoprosessille (Kyytsönen 2020). Tietotekniikka on mullistanut koko terveydenhuoltojärjestelmän ja sen toimintakulttuurin ja kehityksen seurauksena terveydenhuollon piiriin kehitetään jatkuvasti uusia laitteita, tietolähteitä ja työrooleja kaikille terveydenhuollon toimijoille (Krexner & Duftschmid 2014; Lovis 2014). Tietotekniset innovaatiot, kuten robotiikka, mahdollistavat entistä tarkempaa ja tehokkaampaa hoitotyötä ja uudet lähes vallankumouksellisina pidettävät modernit analytiikka- ja IoT-ratkaisut antavat hoidon ammattilaisille enemmän tietoa potilaista. Jopa sellaisia sairauksia, joiden hoitoa pidettiin aiemmin mahdottomana, voidaan nyt hoitaa tietotekniikan avulla. (Donchin & Gopher 2014)

Krexnerin ja Duftschmidin (2014) mukaan terveydenhuolto-organisaatioiden tietojärjestelmäinfrastruktuurille on tyypillistä, että ne muodostuvat suuresta verkostosta eri toimittajien itsenäisesti toimivia, mutta keskenään viestiviä järjestelmiä. Tästä seuraa, että esimerkiksi potilastietoa sijaitsee hajautetusti eri järjestelmissä. Laadukkaan ja tehokkaan hoitotoiminnan takaamiseksi on tärkeää, että nämä järjestelmät vaihtavat tietoa keskenään sujuvasti. Järjestelmien välisessä viestinnässä tärkeä rooli on tiedon standardoinnilla ja järjestelmien välisillä integraatioilla. (Krexner & Duftschmid 2014) Tietojärjestelmien sisältämän datan merkitys hoitotyössä on suuri ja joissain hoitotoiminnan tehtävissä data onkin kaikkein keskeisin työkalu. Datan kerääminen ja analysointi on tärkeä osa potilaille tehtävää diagnostiikkaa ja monitorointia ja parhaimmillaan analytiikka tarjoaa hoitohenkilökunnalle kokonaisvaltaisen näkyvyyden potilaan tilanteeseen. (Donchin & Gopher 2014)

Toimintaympäristöt ja työtehtävät, joiden osana teknologia toimii, voivat olla hyvin monimutkaisia ja laajoja (Misser et al. 2020). Järjestelmät toimivat tärkeinä tiedonlähteinä, työkaluina, sekä kommunikaatioväylinä eri yksiköiden välillä. Tietojärjestelmiä käyttävät käytännössä kaikki hoitotyötä tekevät, mutta järjestelmillä on myös lukuisia muita käyttäjiä, jotka muodostavat keskenään monimutkaisen sidosryhmien verkoston. Terveydenhuollon tietojärjestelmiä käyttävät arjessaan lääkärien ja hoitajien lisäksi muun muassa hoidon koordinoinnista vastaavat työntekijät, viranomaiset, organisaatioiden sidosryhmät, kuten yksityiset hoitolaitokset ja apteekit, organisaatioiden omat tukitoiminnot, kuten johto ja IT, sekä usein myös potilaat itse. Järjestelmien kautta pyörii hoitotyön lisäksi siis myös suuri osa terveydenhoito-organisaation kommunikaatiosta ja yhteistyöstä muiden tahojen kanssa. (Virkanen & Mykkänen 2014)

Terveydenhuollon kompleksisen toimintaympäristön ja tietojärjestelmien yhteensovittaminen on toisinaan haastavaa. Vaikka tietojärjestelmien tehtävänä on ensisijaisesti tukea hoitotyöskentelyä, on yleistä, että järjestelmien toimivuudessa koetaan haasteita. Tietojärjestelmähaasteisiin yleisimpänä syynä koetaan usein käytettävyysongelmat ja se, että järjestelmät eivät aidosti helpota työskentelyä. (Saranto et al. 2021; Kyytsönen et al. 2020; Scandurra et al. 2013) Haasteita koetaan aiheutuvan myös automaation puutteesta ja siitä, ettei tieto siirry organisaatioilta tai niiden osilta toiseen riittävän sujuvasti. Terveydenhuollossa käytetään myös useissa tehtävissä yhä faksia ja paperisia lomakkeita, jotka eivät monilla muilla aloilla ole enää kovin yleisiä. (Kyytsönen et al. 2020) Terveydenhuolto-organisaatioissa tietointensiivistä työtä tekevät ihmiset, joiden ydinosaaminen on hoitotyössä, ei teknologiassa. Tästä johtuen tietojärjestelmien oikeaan käyttöön liittyvän kouluttamisen merkitys on suuri. (Saranto et al. 2021)

### 3.1.2 Terveydenhuollon kyberturvallisuus

Terveydenhuolto on osa yhteiskunnan kriittistä infrastruktuuria, joten sen luotettavasta toimivuudesta kaikissa tilanteissa on huolehdittava. Kyberturvallisuuden tavoitteena on tehdä infrastruktuureista ja järjestelmistä turvallisia ja parantaa niiden resilienssiä häiriötilanteiden varalta. (Tikanmäki & Ruoslahti 2021) Kyberturvallisuudesta huolehtiminen on tärkeä osa terveydenhuollon organisaatioiden päivittäistä toimintaa ja jatkuvuudenhallintaa (Coronado & Wong 2014; Sosiaali- ja terveysministeriö 2019). Suomalainen terveydenhuollon kyberturvallisuustyöryhmä (Health Care Industry Cybersecurity Task Force, HCIC) on määritellyt suomalaisille terveydenhuolto-organisaatoille kuusi kyberturvallisuussuositusta, joita esitellään taulukossa 5. (Norri-Sederholm et al. 2019)

Taulukko 5. *Kyberturvallisuussuositukset terveydenhuolto-organisaatioille (Perustuen Norri-Sederholm et al. 2019)*

| |
|---|
| 1. Tehosta johtajuutta ja hallintotapaa, sekä määritä selkeitä tavoitteita terveydenhuollon kyberturvallisuudelle. |
| 2. Lisää lääkinnällisten laitteiden ja terveydenhuollon tietoturvaa ja organisaation häiriötilanteiden sietokykyä. |
| 3. Kehitä terveydenhuollon henkilöstön osaamisalueita, jotka ovat tarpeen kyberturvallisuustietoisuuden ja teknisten valmiuksien priorisoimiseksi ja varmistamiseksi. |
| 4. Kasvata terveydenhuollon sektorin toimintavalmiutta parantamalla kyberturvallisuustietoisuutta ja -koulutusta. |
| 5. Tunnista mekanismit tutkimus- ja kehitystoiminnan sekä tiedollisen omaisuuden suojelemiseksi. |
| 6. Paranna tiedonvaihtoa alan kyberturvallisuuden uhista, riskeistä ja suojaustoimenpiteistä. |

Suositusten tarkoituksena on lisätä organisaatioiden tietoisuutta, hallita uhkia, vähentää riskejä ja haavoittuvuuksia sekä toteuttaa suojauksia, joita tällä hetkellä ei vielä ole käytössä suurimmassa osassa organisaatioita. Terveydenhuolto-organisaatioiden kyberturvallisuudesta huolehtiminen on monimutkaisten systeemien hallintaa. Koska organisaatioiden tietojärjestelmäinfrastruktuuri muodostuu useiden sidosryhmien, järjestelmien ja käyttäjien verkostosta, tarvitaan myös kyberturvallisuuteen paljon yhteistyötä ja kokonaiskuvan ajattelua. (Norri-Söderholm et al. 2019) Myös valtion julkisen infrastruktuurin tasolla kyberturvallisuuden lähtökohtana on, että kukin taho huolehtii oman toimintansa kyberturvallisuudesta ja tekee yhteistyötä muiden tahojen kanssa uhkien tunnistamisessa ja torjumisessa (Candolin 2020). Sidosryhmien välisen yhteistyön tavoitteena on myös huolehtia siitä, että toiminnan jokaisella alueella on riittävästi osaamista toimia uhkia vastaan. (Norri-Söderholm et al. 2019; Hubbard et al. 2017) Jatkuvalla ja järjestelmällisellä uhkien seurannalla voidaan huolehtia kyberturvallisuuden ajantasaisuudesta. (Ayala 2016)

Kyberturvallisuuden tärkeimpinä tavoitteina on huolehtia terveydenhuolto-organisaation toimintakyvystä, varmistaa organisaatioiden henkilöstön riittävä osaaminen ja suojella potilaisiin ja toimintaan liittyvää tietoa. (Ayala 2016) Tietoa on suojeltava asianmukaisilla tavoilla huomioiden siihen liittyvät erityispiirteet. Joskus tiedon tärkein ominaisuus on sen nopea saatavuus (esim. potilaan tunnisteranneke), kun taas toisinaan tärkeämpää on

varmistaa tiedon luottamuksellisuus ja yksityisyys (esim. potilaan yksityiset terveystiedot). Joskus taas kaikkein merkittävintä on tiedon eheys, eli paikkansapitävyys (esim. lääkeaineallergiat). (Coronado & Wong 2014)

Suositukset keskittyvät monilta osin kyberhyökkäyksiltä suojautumiseen ja hyökkäysten tapahtumisen ehkäisemiseen. Niissä on vahvasti läsnä myös kyberhäiriötilanteiden toteutumiseen varautuminen terveydenhuollossa, jota käsitellään syvällisemmin seuraavassa luvussa.

## 3.2 Terveydenhuolto-organisaatioihin kohdistuvat kyberuhat

Tässä alaluvussa käsitellään terveydenhuoltoalaan kohdistuvia kyberuhkia ja niiden seurauksia. Aluksi käsitellään kirjallisuudesta löydettyjä kyberuhkia ja niiden mahdollisia vaikutuksia yleisellä tasolla ja sitten tarkastellaan muutamia esimerkkiskenaarioita.

### 3.2.1 Kyberuhista yleisesti

Norri-Sederholm et al. (2019) mukaan kyberuhkalla tarkoitetaan ”mahdollisesti toteutuvaa haitallista tapahtumaa tai kehityskulkua, joka kohdistuu kybertoimintaympäristöön ja joka toteutuessaan vaarantaa siitä riippuvaisen toiminnon”. Uhka voidaan myös määritellä jonkun tahon haluksi ja kyvyksi toimia tavalla, joka voisi vahingoittaa organisaation tai muun tahon kriittisiä toimintoja (Casson-Moreno et al. 2018). Terveydenhuollon toimiala on tällä hetkellä kyberrikollisten ja –hyökkäysten keskeisin kohde ja alan organisaatioihin kohdistuneita hyökkäyksiä on raportoitu jo hyvin monenlaisia. Kyberhyökkäysten motivaationa on potilastiedon ja muun luottamuksellisen tiedon korkea arvo pimeillä markkinoilla ja terveydenhuollon kriittinen rooli osana yhteiskunnan huoltovarmuutta, ja täten myös mahdollisuus lunnasvaatimusten onnistumiseen toiminnan kriittisyyden vuoksi. (Willing et al. 2021; Norri-Sederholm et al. 2019; Huang et al. 2018; Coronado & Wong 2014)

Tietojärjestelmäinfrastruktuureista voi löytyä monenlaisia kyberhyökkäyksille altistavia heikkouksia. Hyökkääjä hyödyntää heikkouksia saavuttaakseen pääsyn johonkin organisaation kriittiseen järjestelmään tai tietoon. (Casson-Moreno et al. 2018) Heikkoudet voivat aiheutua esimerkiksi teknisistä puutteista käytettävissä järjestelmissä ja laitteissa, tai laitteiden fyysisen sijainnin turvallisuuden puutteesta. Heikkouksia voi syntyä myös tietoturvakäytäntöjen tai koulutuksen puutteesta, joka johtaa siihen, että henkilöstö ei osaa käyttää järjestelmiä tietoturvallisesti. (Norri-Sederholm et al. 2019; Casson-Moreno et al. 2018) Myös teknologian kehitys luo jatkuvasti uusia kyberuhkia, kun esimerkiksi

aiemmin vain paikallisessa käytössä olleet laitteet ottavat nyt verkon kautta yhteyttä muihin järjestelmiin ja vaihtavat siellä potilaisiin liittyvää tietoa keskenään. Kyberturvallisuudelle tämä aiheuttaa jatkuvasti uusia haasteita ja sen pitäminen kehityksen tahdissa onkin hyvin haastavaa. (Coronado & Wong 2014)

Kyberturvallisuus rakentuu siis toisaalta teknisten suojausmekanismien, mutta toisaalta myös kaikkien terveydenhuolto-organisaation tietojärjestelmien käyttäjien tietoturvaosaamisen varaan. Ayalan (2016) ja Willing et al. (2021) mukaan monien terveydenhuolto-organisaatioiden kybersuojaus on usein muihin toimialoihin verrattuna merkittävästi heikompi. Tähän syinä he nostavat esiin hoitoon käytettävien laitteiden kehnon tietoturvan ja niille annettavien komentojen heikon tunnistamiskäytännön sekä muutoin vajaan tietoturvan, kokeneen tietotekniikkahenkilöstön puutteen ja haastavan toimintaympäristön. (Willing et al. 2021; Ayala 2016) Owens (2020) puolestaan toteaa, että suurin osa terveydenhuoltoalaan kohdistuvista hyökkäyksistä alkaa inhimillisestä virheestä ja terveydenhuoltoala vaikuttaisi olevan niille monia muita aloja alttiimpi (Owens 2020).

Kyberhyökkäyksen vaikutukset terveydenhuolto-organisaatioon voivat olla moninaisia. Vaikutuksia voi seurata esimerkiksi liittyen turvallisuuteen, hoitotoiminnan jatkuvuuteen, potilaiden ja työntekijöiden tietojen yksityisyyteen, terveydenhuolto-organisaation toimintakykyyn, talouteen tai maineeseen. (Owens 2020) Yhteistä erilaisille terveydenhuolto-organisaatioon kohdistuville häiriötilanteille on, että ne voivat aiheuttaa riskejä potilasturvallisuudelle. Erityisesti kriittisten potilaiden hoito, kuten leikkaussalit, ensiapuosastot ja tehohoito, ovat potilaan hyvinvoinnille hyvin kriittisiä. Esimerkiksi tietojärjestelmän väärä toiminta voi aiheuttaa potilaille vahinkoa tai pahimmassa tapauksessa jopa kuoleman. Tietoverkkoon kytkettyjen lääkinnällisten laitteiden nopean yleistymisen vuoksi näissä järjestelmissä on myös useita teknisiä hyökkäyskohteita. Potilaat ovat monesti hyvin riippuvaisia siitä, että lääketieteelliset laitteet toimivat oikein ja hoitohenkilökunta käyttää niitä oikein. (Willing et al. 2021; Coronado & Wong 2014) Kyberhyökkäyksessä voidaan myös menettää hoidon kannalta tärkeää tietoa, jolloin se pitää kerätä jollakin keinolla uudelleen. Potilastiedon menetyksessä vakavimmat haitat voivat kuitenkin syntyä tietovuotojen tai -varkauksien kohteena oleville potilaille, joiden henkilökohtaiset tiedot ovat vaarantuneet. Asiakas voi joutua jopa kiristyksen kohteeksi. (Norri-Sederholm et al. 2019)

Kyberhyökkäystilanteet voivat aiheuttaa organisaatioille myös taloudellisia haittoja, esimerkiksi menetettyjen tai tuhoutuneiden kalliiden laitteiden muodossa. Äärimmäisissä tapauksissa on mahdollista menettää rahaa jopa lunnaiden muodossa, kun rikollinen kiristää hyökkäyksen kohteena olevaa organisaatiota esimerkiksi tietojen tai järjestelmien toiminnan palauttamisella. Potilaiden yksityisen tiedon käsittelyyn liittyy myös useita

säännöksiä ja jos näitä rikotaan ja tärkeitä tietoja vuodetaan tai menetetään, organisaatio saattaa syyllistyä jopa rikokseen. Tällöin taloudellisia seurauksia seuraa siitä, että organisaation katsotaan laiminlyöneen laillisia velvollisuuksiaan potilaiden ja heidän yksityisten tietojensa suojelussa. (Norri-Sederholm et al. 2019) Potilastietojen menetys tai muut hoitovirheet voivat tuottaa organisaatiolle merkittäviä sanktiota esimerkiksi oikeusjuttujen tai sakkojen muodossa. (Ayala 2016; Coronado & Wong 2014) Potilaiden hoidossa ja tietojen käsittelyssä epäonnistuminen voi aiheuttaa haittoja myös organisaation maineelle, jos sen asiakkaat ja sidosryhmät eivät enää tiedä, voiko sen toimintaan luottaa (Norri-Sederholm et al. 2019). Kyberhyökkäyksistä seuraavat poikkeustilanteet voivat aiheuttaa organisaatiolle muitakin hankaluuksia, kuten toiminnan koordinoinnin ja kommunikoinnin haasteita, stressiä ja kiirettä sekä hoidon ruuhkautumista. (Willing et al. 2021)

### 3.2.2 Kyberhyökkäystyyppejä

Seuraavaksi taulukossa 6 tarkastellaan muutamia esimerkkejä erilaisista kyberhyökkäysskenaarioista, joita terveydenhuolto-organisaatioon voi kohdistua. Jokaisesta skenaariosta esitellään niiden yleiset piirteet ja mahdolliset seuraukset, sekä niille altistavat tekijät organisaation omissa toimintatavoissa. Erilaisia kyberhyökkäystyyppejä on olemassa enemmänkin, mutta tähän on valittu muutamia terveydenhuolto-organisaatioiden kannalta keskeisimpiä.

Taulukko 6. *Kyberhyökkäysskenaarioita ja niiden mahdollisia seurauksia*

| **Kyberhyökkäys** | **Piirteet ja seuraukset** | **Altistavat tekijät** |
|---|---|---|
| Järjestelmien käytön estäminen<br><br>(Norri-Sederholm et al. 2019; Huang et al. 2018; Ayala 2016; Kwon & Hwang 2016) | • Hyökkääjä estää järjestelmän käytön osittain tai kokonaan.<br>• Kohteena esim. potilastietojärjestelmä<br>• Esim. palvelunestohyökkäykset.<br>• Seurauksina hoitotyön ja toiminnan koordinoinnin häiriintyminen, mahdolliset lunnasvaatimukset toiminnan palauttamiseksi | • Ylläpitoon ja suojaukseen liittyvä osaaminen ja vastuut liian hajautuneet → valheellinen käsitys todellisuutta paremmasta hallinnasta ja suojauksesta<br>• Johtamishaasteet<br>• Vaillinainen valvonta<br>• Puutteelliset tekniset tietoturvallisuuskäytännöt<br>• Inhimilliset virheet |

| | | |
|---|---|---|
| | • Terveydenhuolto-organisaatiot yleisin kohde (88 % vuoden 2016 palvelunestohyökkäyksistä, Huang et al. 2018) | |
| Tietovuoto tai -varkaus<br>(Norri-Sederholm et al. 2019; Huang et al. 2018; Ayala 2016; Coronado & Wong 2014) | • Rikollisille ja mahdollisesti myös julkisuuteen päätyy tietoa, jota ei pitäisi.<br>• Tieto esim. luottamuksellista potilastietoa.<br>• Seurauksia tietonsa menettäneille potilaille ja organisaatiolle. (yksityisyyden menetys, sanktiot) | • Luottamukselliset tiedot puutteellisesti suojattu tietojärjestelmissä<br>• Inhimilliset virheet, esim. väärät tallennustavat, heikko salasanakäyttäytyminen<br>• Tietojen täydellinen menetys: puutteet varmuuskopiointikäytännöissä. |
| Tiedon muokkaaminen salaa<br>(Willing et al. 2021; Huang et al. 2018; Kwon & Hwang 2016; Coronado & Wong 2014) | • Tietojärjestelmissä olevaa tietoa muutellaan siten, ettei se pidä paikkaansa.<br>• Järjestelmissä olevan tiedon eheys vaarantuu.<br>• Seurauksena hoitoa annetaan väärän tiedon varassa tai hoitohenkilökunta ei voi luottaa tietoon, jota heillä on käytettävissään → vaaratilanteet | • Puutteellinen tietosuojaus<br>• Heikko varmuuskopiointi<br>• Huono ohjelmistosuunnittelu<br>• Puutteellinen käyttäjän tunnistaminen<br>• Ohjelmistovirheet<br>• Heikko verkko- ja etäyhteyden suojaaminen |
| Laitteisiin kohdistuva hyökkäys<br>(Willing et al. 2021; Norri-Sederholm et al. 2019; Ayala | • Tavoitteena laitteen täydellinen tuhoaminen tai sen haltuunotto ja etäohjaaminen.<br>• Kohteena esim. röntgenlaite, lääkeannostelija, nukutuslaitteisto, leikkauksia tekevä robotti… | • Verkkoon yhdistettyjen IoT-tyyppisten laitteiden määrän räjähdysmäinen lisääntyminen → yhdistettävyys kehittynyt nopeammin kuin tietoturva<br>• Laitteiden tai laitetilojen puutteellinen fyysinen suojaus |

| | | |
|---|---|---|
| 2016; Coronado & Wong 2014) | • Muut kriittiset laitteet: kulunvalvonta, vedenjakelu...<br>• Seurauksia vaaratilanteet, häiriöt hoidossa, kalliiden laitteiden tuhoutuminen | • Puutteet verkkoyhteyksien ja etäkäytön suojauksessa<br>• Heikko salasana- ja käyttäjän tunnistamiskäytäntö<br>• USB-tikut ja muistikortit |

Erilaiset kyberhyökkäysuhat asettavat organisaatioille erilaisia kyberturvallisuusvaatimuksia ja työtä on tehtävä samanaikaisesti useilla rintamilla. Kyberturvallisuusala kehittyy, mutta samaan aikaan vähintään yhtä nopeasti kehittyy myös rikollisten toiminta. (Kyberhyökkäyksiltä suojautumista voidaankin verrata myös jatkuvassa muutoksessa olevaan peliin, jossa vastakkain ovat hyökkääjä ja infrastruktuurin suojelija. Molemmat haluavat olla jatkuvasti vastustajaa askeleen edellä. (Ahn et al. 2020; Kwon & Hwang 2016) Seuraavassa luvussa käsitellään sitä, miten organisaatiot voivat valmistaa itseään toimimaan kyberhyökkäyksen tapahtuessa.

# 4. VARAUTUMINEN KYBERHYÖKKÄYSTILANTEESTA SELVIÄMISEEN

Kyberhyökkäyksien uhka voimistuu jatkuvasti, hyökkäykset kehittyvät ja muuttuvat vaarallisemmiksi ja vaarallisemmiksi. Ne voivat yllättää organisaation juuri silloin, kun se sitä vähiten odottaa. (Hubbard et al. 2017) Kriisivalmistautumisella pyritään luomaan järjestelmä, jolla organisaatio voi kestää yllättävät ja vakavat tilanteet joutumatta määrittämään tai korjaamaan järjestelmää uudelleen kiireen keskellä (Hellenberg et al. 2011). Tässä luvussa esitellään kirjallisuuden pohjalta toimia, joilla organisaatiot voivat parantaa valmiuttaan toimia kyberhyökkäystilanteessa. Tieteellisen kirjallisuuden lisäksi tässä luvussa käytetään lähdemateriaalina yhdysvaltalaisen standardointilaitoksen ”National Institute of Standards and Technology:n”, eli NIST:in (2018) tuottamaa ”Framework for Improving Critical Infrastructure Cybersecurity” -kyberturvallisuusohjeistusta. NIST:in luomien standardien ja viitekehysten avulla organisaatiot voivat mitata ja arvioida toimintansa onnistumista sekä kehittää sitä. Valittu viitekehys kokoaa yhteen kyberturvallisuuden kannalta tärkeitä käytäntöjä. (NIST 2018)

Luvun ensimmäisessä alaluvussa keskitytään kyberhyökkäykseen varautumisen eri osa-alueisiin yleisellä tasolla. Toisessa alaluvussa varautuminen tuodaan terveydenhuolto-organisaation toimintaympäristöön ja sitä käsitellään teknisestä, hallinnollisesta ja koko organisaation henkilöstön näkökulmasta. Kolmas alaluku käsittelee kybervalmiuden arviointia ja antaa esimerkkejä siitä, miten organisaatio voi mitata oman kyberhyökkäysvarautumisensa tasoa.

## 4.1 Kyberhyökkäykseen varautuminen

Kyberuhkat voivat varautumisesta huolimatta myös toteutua, minkä vuoksi organisaatioiden tulee kyberturvallisuuden osana kehittää resilienssiään, eli sietokykyään häiriötilanteille (Norri-Sederholm et al. 2019). Jokaisen julkisen ja yksityisen organisaation tulisi hyväksyä se tosiasia, että heidän toimintansa tulee jossakin vaiheessa olemaan kyberhyökkäyksen kohteena. Organisaatioiden kannalta ratkaisevaa näissä tilanteissa on se, miten hyvin niihin on varauduttu, sillä vahinkojen laajuus riippuu usein reagoinnin nopeudesta ja tehokkuudesta. (Owens 2020; Hubbard et al. 2017; Ayala 2016) Candolin (2020) puolestaan toteaa, että kyberhyökkäyksiä pidetään usein liikaa pelkästään teknologiaan liittyvänä ongelmana. Hänen mielestään on tärkeää tunnistaa myös ihmisten, vastuunjaon ja johtamisen rooli sekä kyberhyökkäyksiin varautumisessa että niistä selviämisessä. (Candolin 2020)

Hellenbergin (2011) mukaan kriisitilanteessa, kuten kyberhyökkäyksessä, organisaation toiminta tapahtuu jo valmiiksi olemassa olevia resursseja ja toimintamalleja käyttäen, sillä kriisin aikana organisaatiolla ei todennäköisesti ole aikaa eikä voimavaroja järjestelmän merkittäviin korjauksiin. Tarve tehdä jotakin nopeasti häiriötilanteen hallitsemiseksi on yleistä kriisitilanteille ja siksi kriisipäätöksenteolta vaaditaan usein poikkeuksellista nopeutta ja suoraviivaisuutta. (Hellenberg et al. 2011) Kyberhyökkäystilanteeseen valmistautumiseen kuuluu muun muassa tarvittavien reagointitoimenpiteiden suunnittelua, niihin tarvittavien resurssien tunnistamista, vastuuhenkilöiden määrittämistä, kriittisen tiedon ja infrastruktuurin tunnistamista ja suojaamista sekä teknisten kontrollimenetelmien pitämistä ajan tasalla. Varautumiseen kuuluu myös valittujen toimintatapojen ohjeistamista ja kouluttamista henkilöstölle, niiden testaamista käytännössä, kyberturvallisuustietoisuuden levittämistä sekä valmiuden säännöllistä mittaamista. (Bahuguna et al. 2019; Ayala 2016)

NIST:in (2018) viitekehyksen mukaisesti kyberturvallisuuden kokonaisuudesta huolehtimiseen kuuluu viisi osa-aluetta: uhan tunnistaminen, suojauksen rakentaminen, hyökkäysten tunnistaminen, hyökkäykseen reagoiminen, sekä hyökkäyksistä palautuminen. Toteutuvan kyberhyökkäystilanteen kannalta on olennaista tutkia NIST:in mallista erityisesti kahta viimeistä vaihetta, mutta kaikkien vaiheiden onnistunut toteutus vaikuttaa osaltaan kyberhyökkäystilanteessa toimimiseen. Esimerkiksi monet suojauksen rakentamisessa tehdyt valinnat ratkaisevat, kuinka nopeasti hyökkäyksestä voidaan toipua ja kuinka pahasti hyökkäys pystyy vahingoittamaan organisaatiota. NIST:in kyberturvallisuusviitekehyksen hyökkäystilanteen kannalta oleellisia osa-alueita esitellään taulukossa 7. (NIST 2018)

Taulukko 7. *Kyberturvallisuuden osafunktiot (Perustuen NIST 2018)*

| **Funktio** | **Kuvaus ja tavoitteet** | **Esimerkkejä tehtävistä** |
|---|---|---|
| Uhan tunnistaminen | - kyberuhkiin liittyvän osaamisen ja ymmärryksen kehittäminen<br>- liiketoiminnan kontekstin ja tarpeiden ymmärtäminen<br>- kyberturvallisuuden strateginen johtaminen (kehitystoimien kohdistaminen, resursointi, priorisointi) | Riskiarvioinnit, kehityskohdat, riskienhallinta, riskienhallintastrategia. auditointi |

| | | |
|---|---|---|
| Suojauksen rakentaminen | - kriittisen infrastruktuurin suojaaminen<br>- eri tietotyyppien oikeanlainen suojaaminen<br>- suojaavien toimintatapojen ja teknologioiden suunnittelu ja käyttöönotto<br>- häiriötilanteen vaikutusten minimointi ja rajaus | Pääsynhallinta, tietoturva, suojausteknologiat, tietoturvalliset prosessit, teknologian huolto ja päivitykset, tietoisuuden lisääminen ja koulutus |
| Hyökkäyksen havaitseminen | - kyberuhkatilanteen nopea havaitseminen<br>- kyberuhkatilanteen ja sen vaikutusalueen tunnistaminen | Jatkuva monitorointi, poikkeamien havaitsemisteknologiat |
| Reagointi hyökkäykseen | - toimintasuunnittelu uhkaskenaarion toteutumiseen<br>- hyökkäystilanteen koordinointi<br>- hyökkäyksen pysäyttäminen<br>- hyökkäyksen vaikutusten minimointi ja rajaus | Reagointisuunnittelu, tilanneanalyysi, vaikutusten minimointi, parannukset, johtaminen ja kommunikaatio |
| Palautuminen | - resilienssin tukeminen<br>- vahingoittuneiden resurssien palauttaminen<br>- nopean normaaliin paluun mahdollistaminen<br>- kyberhyökkäyksen vaikutusten minimointi | Palautumissuunnittelu, jatkuvuussuunnittelu, kommunikaatio, parannukset ja kehityskohdat, varmuuskopiointi |

Seuraavissa alaluvuissa perehdytään syvällisemmin kyberturvallisuusmallin eri vaiheisiin. Vaiheita käsitellään erityisesti toteutuvaan kyberhyökkäykseen varautumisen näkökulmasta. Mukaan tarkasteluun tuodaan myös tieteellistä kirjallisuutta.

### 4.1.1 Uhan tunnistaminen

Uhan tunnistusvaiheen tavoitteena on kehittää organisaation ymmärrystä ja osaamista sen tietoon, järjestelmiin ja toimintaan kohdistuvien kyberuhkien hallinnassa. Uhkien tunnistamista varten on olennaista ymmärtää organisaation toimintakonteksti ja sen erityispiirteet. Toiminnan kontekstin ymmärtäminen ja toimintaan kohdistuvien uhkien tunnistaminen on perusta kaikelle kyberturvallisuustyölle. (NIST 2018) Tällaista kontekstin määrittelyä ja uhkien tunnistamista tehtiin jo terveydenhuolto-organisaatioiden kohdalla edellisessä luvussa.

Uhkien tunnistamisvaiheeseen kuuluu myös kyberturvallisuuden strateginen johtaminen organisaatiossa. Tämä tarkoittaa käytännössä kyberturvallisuuteen käytettävissä olevien resurssien järkevää jakamista ja priorisointia erilaisten tarpeiden ja hankintojen välillä, sillä harvalla organisaatiolla on käytössään rajattomasti resursseja kyberturvallisuuden rakentamiseen. (NIST 2018; Hubbard et al. 2017; Coronado & Wong 2014) Myös resurssien ja kehitystoimien kohdistamisessa on olennaista ymmärtää organisaation toimintaa ja sen kyberturvallisuudelle asettamia tarpeita. Uhan tunnistamisvaiheen tärkeitä työkaluja ovat muun muassa organisaation riskienhallintastrategia ja riskiarvioinnit, joiden avulla voidaan varautua erilaisilta uhkilta suojautumiseen ja niiden toteutumiseen. (NIST 2018) Tikanmäen ja Ruoslahden (2021) mukaan myös yleisen kyberturvallisuusilmapiirin ja uhkien kehityksen seuraaminen on tärkeä kulmakivi organisaation kyberturvallisuuden onnistumiselle. Osa tätä on myös avoin keskusteluyhteys muiden alan toimijoiden ja viranomaisten kanssa. (Tikanmäki & Ruoslahti 2021)

Uhkien tunnistaminen, arvioiminen ja niiden realisoitumiseen varautuminen on kriisivarautumisen perusta. (NIST 2018) Monet uhkaskenaariot voidaan tunnistaa etukäteen, jolloin niiden todennäköisyyttä voidaan arvioida ja niiden toteutumiseen voidaan varautua. On kuitenkin olemassa sellaisiakin uhkia, joiden tunnistaminen ja ennustaminen voi olla hyvin vaikeaa. Syitä haasteisiin voivat olla esimerkiksi se, uhkaskenaariot ovat hyvin harvinaisia, niitä ei ole tapahtunut koskaan ennen tai kenelläkään organisaatiossa ei ole sellaisista kokemusta tai osaamista. Erityisen hankala tilanne syntyy, jos tällaiseen joskus ”epäuskottavaltakin” vaikuttavaan uhkaan liittyy riski todella vakavista seurauksista. Tällöin voidaan puhua ”musta joutsen” -uhasta, joita esimerkiksi Taleb (2007) tutkii. Mustalla joutsenella tarkoitetaan epätodennäköisestä tapahtumaa, joka on ennustettavuudeltaan huono ja jonka seuraukset ovat mittavia. Mustia joutsenia voivat olla esimerkiksi tsunamit tai terrori-iskut. Kyberhyökkäykset ovat moniin muihin turvallisuusuhkiin verrattuna melko tuore ilmiö, ja organisaatioille voi olla haastavaa tunnistaa, miten niiden uhka

koskettaa heitä. Myös kyberhyökkäyksen seuraukset voivat olla hyvin mittavia, joten niiden kohdalla voi olla perusteltua puhua mustasta joutsenesta. Mustiin joutseniin varautuminen voi olla todella haastavaa, mutta jo niiden mahdollisuuden tiedostaminen on hyödyksi. (Taleb 2007) Niiden tapahtuessa ratkaisevaan rooliin nousevat yleiset kriisitilanteisiin varautumisen kyvykkyydet, kuten kriisijohtaminen ja -viestintä. (Hellenberg et al. 2011)

### 4.1.2 Suojauksen rakentaminen

Tiedon ja tietoa sisältävien järjestelmien kanssa toimittaessa on tärkeää tunnistaa minkälaisia suojaukseen, paikkansapitävyyteen ja jakamiseen liittyviä vaatimuksia tietyn tyyppiseen tietoon kohdistuu. Kybermaailmassa toimittaessa voidaan ajatella, että tiedon maksimaalisen suojaamisen vastapuolella on sujuva jakaminen järjestelmästä toiseen. Suojauksen rakentaminen on strategista tasapainoilua näiden välillä. Joidenkin tietojen kohdalla olennaisinta on saada ne helposti järjestelmien välillä jaettavaan muotoon ja kaikkien tarvitsijoiden saataville. Joskus taas tärkeintä on se, että esimerkiksi erittäin luottamuksellinen potilastietojen pidetään tarkasti turvassa väärältä käytöltä, vaikka tiedon tiukempi kontrolli tapahtuisi sen sujuvan saatavuuden kustannuksella. (Hubbard et al. 2017) Kolmas tietoon kohdistuva vaatimus on sen eheys, joka tarkoittaa sen paikkansapitävyyttä. Vaatimuksissa mielenkiintoista on erityisesti se, että kyberhyökkääjän tavoitteenakin on usein vaikuttaa juuri johonkin näistä kolmesta tekijästä. Hyökkäyksellä saatetaan pyrkiä poistamaan tieto organisaation saatavilta, rikkomaan sen luottamuksellisuus tai vaihtoehtoisesti muuttamaan se paikkansapitämättömäksi. (Huang et al. 2018; Coronado & Wang 2014) Tiedon ja järjestelmien erilaisten vaatimusten tunnistaminen ja sen perusteella suunnitelmallisesti asetetut kontrollit edistävät tiedon luottamuksellisuutta, eheyttä ja saatavuutta siellä, missä sille on tarvetta. Kun kriittinen suojattava toiminta erotetaan vähemmän kriittisestä, myös suojauksen rakentamiseen käytössä olevat resurssit, kuten henkilöstö- ja raharesurssit, voidaan hyödyntää siellä missä niitä eniten tarvitaan. (Tipton & Krause 2004)

Olennainen osa kybersuojauksen rakentamista on siis tunnistaa ja suojata ne tiedot ja järjestelmät, jotka ovat kriittisiä toiminnan kannalta (NIST 2018). Suojauksen rakentamisvaiheessa organisaatio kehittää ja ottaa käyttöön sen kriittistä infrastruktuuria suojaavat käytännöt. Näihin kuuluu toisaalta teknisiä suojausmekanismeja ja tietoturvateknologioita, mutta toisaalta myös ihmisten toimintaa ohjaavia tietoturvallisia käytäntöjä,

jotka koskettavat organisaation kaikkia työntekijöitä. Suojauksen rakentamisessa tärkeitä työkaluja ovat esimerkiksi pääsynhallinta, laitteiden fyysinen suojaus, verkko- ja -etäyhteyksien suojaus sekä käyttäjien tunnistaminen. (NIST 2018)

Tapahtuvan kyberhyökkäyksen kannalta keskeistä tiedon suojaamisessa on se, että siihen kuuluu myös teknisiä toimenpiteitä, joilla voidaan ehkäistä tiedon tai toimintojen menettämistä ja edistää niiden palauttamista, mikäli ne vaarantuvat kriisitilanteessa. Tällaisia toimenpiteitä ovat muun muassa infrastruktuurin osien kahdentaminen, verkkoliikenteen suojaus ja henkilöstön tietoturvakouluttaminen. (Norri-Sederholm et al. 2019). Hyvä suojaus ehkäisee siis toisaalta kyberhyökkäyksien onnistumista, mutta toisaalta rajaa ja minimoi mahdollisen tapahtuvan kyberhyökkäyksen vaikutuksia (NIST 2018).

### 4.1.3 Hyökkäyksen havaitseminen

Hyökkäystilanteessa olennaista on myös se, että organisaatiolla on kyvykkyys havaita, kun jokin ei ole kunnossa. Havainto pitää tehdä nopeasti, sillä tilanteen havaitsemisen pitkittyminen voi vakavoittaa hyökkäyksen vaikutuksia. (Hubbard et al. 2017) Havaitsemisvaiheessa organisaatio kehittää ja ottaa käyttöön toimintatavat, joilla voidaan nopeasti havaita ja tunnistaa kyberuhkatilanne, kuten kyberhyökkäys. Hyökkäyksen havaitseminen vaatii jatkuvaa infrastruktuurin monitorointia ja sitä, että mahdolliset poikkeamat ja niiden syyt osataan tunnistaa ja paikantaa nopeasti. Olennaista on myös se, että erilaisten häiriöiden mahdolliset vaikutukset toimintaan ymmärretään. Näissä tehtävissä kyberturvallisuusteknologioilla on merkittävä rooli. Havaitsemisvaiheen suunnitteluun kuuluu myös hälytysmenettelystä päättäminen. Tämä tarkoittaa käytännössä sitä, että luodaan selkeä suunnitelma siitä, keille kaikille havainnosta ilmoitetaan ja millä viestintämenetelmillä hälyttäminen tehdään. (NIST 2018)

Hyökkäyksien havaitsemiseen varautumiseen kuuluu myös kybertilannetietoisuuden jatkuva ylläpito tietoturvatiedotteita seuraamalla ja haavoittuvuuksia havainnoimalla sekä havaittuihin haavoittuvuuksiin reagoimalla (Norri-Sederholm et al. 2019). Kyberhyökkäykset voivat olla osa suurempaa hyökkäyskokonaisuutta, kohdistua useamman organisaation käytössä oleviin järjestelmiin, tai sitten ne voivat johtua haavoittuvuudesta, joka huomataan ensin muualla. Omaa organisaatiota laajempien kyberhyökkäystilanteiden havaitsemisessa olennaista on aktiivinen ja avoin keskusteluyhteys muiden alan toimijoiden ja viranomaisten kanssa. (Tikanmäki & Ruoslahti 2021)

### 4.1.4 Reagointi hyökkäykseen

Tietoturvaloukkauksia tapahtuu organisaatioille väistämättä, minkä vuoksi myös niiden infrastruktuurin häiriönsietokykyä ja henkilöstön reagointikykyä pitää jatkuvasti kehittää ja ylläpitää. Häiriönsietokykyään kehittävät organisaatiot ovat vähemmän alttiita turvallisuusloukkauksille, ja tällöin myös toteutuneet kyberhyökkäykset aiheuttavat yleensä lievempiä seurauksia. (Norri-Sederholm et al. 2019) NIST:in (2018) mallin reagointivaihe kattaa toiminnan häiriötilanteen, kuten kyberhyökkäyksen, aikana. Varautumisen tämän vaiheen tavoitteena on valita, suunnitella ja toteuttaa toimenpiteet, jotka toteutetaan kyberhyökkäysskenaarion toteutuessa. Reagointitavoilla pyritään pysäyttämään hyökkäys sekä minimoimaan ja rajaamaan sen vaikutuksia kriisin laajenemisen ehkäisemiseksi. Tämä vaatii kyberhyökkääjän toiminnan ja tavoitteiden ymmärtämistä ja kattavaa käsitystä siitä, mitä tapahtuu. (Ahn et al. 2020; Libicki 2012). Hyökkäystilanteessa toimimisen työkaluja ovat myös muun muassa tilanneanalyysit, kriisijohtamismallit sekä toimintasuunnitelmat ja -ohjeet. (NIST 2018)

Hyökkäystilanteen aikana toimittaessa on keskeistä hahmottaa ja säilyttää jatkuva käsitys siitä, mitä tapahtuu ja miten hyökkäystilanne vaikuttaa eri puolilla organisaatiota. Tätä varten organisaation reagoinnista vastuussa olevilla henkilöillä tulee olla ajantasainen ja kokonaisvaltainen käsitys kaikista sen käytössä olevista järjestelmistä ja ohjelmistoista, ja niiden arvioiduista keskinäisistä riippuvuuksista. Heidän on tunnettava myös liiketoimintaprosessit, joissa niitä käytetään. Tämä auttaa organisaatiota ymmärtämään hyökkäyksen kokonaisvaikutukset heti. Tilannetiedon perusteella organisaatio voi pyrkiä korjaamaan tai sulkemaan sellaiset tietojärjestelmäinfrastruktuurin osat, jotka mahdollistavat hyökkäyksen. (Tikanmäki & Ruoslahti 2021; Libicki 2012; Norri-Sederholm et al. 2019) Tilannekuvan muodostaminen tilanteen aikana voi kuitenkin olla hyvin hankalaa ja vaatia paljon kehitystyötä suuressa organisaatiossa, jossa toiminta jakautuu useampiin osafunktioihin ja eri järjestelmiä ja niiden käyttöä hallinnoi täysin eri tahot, jotkut jopa oman organisaation ulkopuolella. Reaaliaikaisen tilannekuvan avulla voidaan kuitenkin tukea päätöksentekoa myös lukuisissa muissa tilanteissa, kuin kyberhyökkäyksiin reagoimisessa, joten siihen tehtävät panostukset kannattaa tehdä. (Tikanmäki & Ruoslahti 2021) Kyberhyökkäystilanteissa tilannekuvaa voidaan hyödyntää esimerkiksi sopivien vastatoimien valinnassa, muuhun toimintaan liittyvässä päätöksenteossa ja viranomaisyhteistyössä. (Tikanmäki & Ruoslahti 2021; Hellenberg et al 2021; Mykkänen et al. 2019).

Kyberhyökkäyksien kaltaiset kriisitilanteet tulevat eteen yllättäen ja niiden aikana ei usein ole aikaa uusien toimintamallien muodostamiselle, kun suora toiminta on aloitettava heti.

Organisaatioilla on siis oltava selkeä toimintasuunnitelma kyberhyökkäystilanteiden toteutumisen varalle. Toimintasuunnitelma sisältää toisaalta teknisiä toimenpiteitä ja suojausmekanismeja, mutta myös tilanteen aikaiseen päätöksentekoon ja kommunikointiin sekä vastuun- ja resurssien jakoon liittyviä tekijöitä. (Norri-Sederholm et al. 2019; Hellenberg et al. 2011) Kyberhyökkäyksen tapahtuessa organisaation on hyvin nopeasti päätettävä, miten se toimii vastatakseen hyökkäykseen ja pysäyttääkseen sen etenemisen. Toimintasuunnitelman tavoitteena on tehdä hyökkäystilanteessa toimimisesta suunnitelmallista ja tehokasta. Kyberhyökkäyksen toteutuessa organisaation täytyy jo tietää, miten se saa tarvittavat prosessit käyntiin heti, jolloin aikaa ei tarvitse tuhlata hitaaseen päätöksentekoon. (Ayala 2016)

### 4.1.5 Palautuminen

Organisaation haasteet eivät pääty siihen, kun hyökkäyksen akuutti vaihe on selvitetty ja hyökkääjä on saatu pysäytettyä. Tilanteen pysäyttämiseksi on saatettu joutua tekemään monia toimintaa haitanneita toimenpiteitä, ja hyökkäyksestä on saattanut aiheutua suuriakin menetyksiä. Palautumisvarautumisessa on kyse jatkuvuudenhallinnasta ja organisaation resilienssin tukemisesta. Resilienssillä tarkoitetaan organisaation kykyä palauttaa toiminta vakaaseen tilaan häiriötilanteen jälkeen (Bhamra et al. 2011). Palautumisvaihe alkaa, kun kyberhyökkäystilanteen akuutti vaihe on ohi ja organisaatio toimii palauttaakseen häiriintyneet prosessit ja teknologiat takaisin normaaliksi (Weber et al. 2021). Tavoitteena on saada organisaation kriittiseen infrastruktuuriin kuuluvat hyökkäystilanteessa vahingoittuneet resurssit käyttöön mahdollisimman tehokkaasti, mahdollistaa nopea paluu normaaliin toimintaan sekä minimoida kyberhyökkäyksen vaikutuksia ja niiden kestoa. Palautumisvaihe koostuu korjaustoimenpiteiden tekemisestä ja tulevaisuuden kehitystarpeiden tunnistamisesta. (NIST 2018)

Ayalan (2016) mukaan toiminnan palautumisessa käytettävät keinot ja toimintatavat tulee ottaa huomioon jo niiden rakentamista ja ylläpitoa suunniteltaessa. Palautumissuunnitelmaan tulee dokumentoida yksityiskohtaisesti ohjeet siihen, miten organisaation kukin toiminto palautetaan normaaliksi häiriön jälkeen. Osa suunnittelua on myös palautumistoimiin kuluvan ajan määrittäminen ja arviointi, sekä tarvittaessa palautumiskyvyn nopeuttaminen, mikäli kriittisen toiminnon palautuminen vie liian kauan. Elementit onnistuvan, tehokkaan ja toistettavan palautumiskyvyn rakentamiseen muodostuvat muun muassa vaihtoehtoisten manuaalisten kontrollikeinojen rakentamisesta muulloin automaattisesti toimiviin järjestelmiin, tiedon turvallisesta varastoinnista organisaation sisällä ja

sen ulkopuolella, huolellisesta varmuuskopioinnista, sekä sen varmistamisesta, että tiedot saadaan palautettua varmuuskopioista helposti. Palautumissuunnitteluun kuuluu myös palautumisvaiheen vastuiden määrittelyä, kommunikaatiojärjestelmien turvaamista ja vaihtoehtoisten kommunikaatiojärjestelmien kehittämisestä. (Hubbard et al. 2017; Ayala 2016; Norri-Sederholm et al. 2019).

Hyökkäystilanteen ja korjausten jälkeen organisaation täytyy myös pohtia, mistä johtui, että hyökkäys pääsi tapahtumaan ja olisiko se ollut mahdollista estää. Kriisitilanteen jälkeen tärkeä vaihe onkin myös tapahtuneen tarkka raportointi, tilanteen kriittinen arviointi sekä siitä oppiminen, jolloin tapahtuneella voi olla positiivisiakin seurauksia. Parhaimmillaan tapahtunut kriisitilanne voi vauhdittaa tarvittavaa kehitystyötä ja saada sellaisiakin tahoja kiinnostumaan kyberturvallisuuteen panostamisesta, jotka eivät ole aiemmin nähneet sitä tärkeäksi. (Gkeredakis et al. 2021) Palautumisvaiheen jälkeen voidaan esimerkiksi ohjata lisäpanostuksia henkilöstön uudelleen kouluttamiseen ja osaamisen harjoitteluun tai kehittää olemassa olevia kyberstrategioita, toimintaohjeita ja käytäntöjä tilanteen aikana tehtyjen huomioiden perusteella (Ayala 2016).

## 4.2 Kyberhyökkäykseen varautuminen terveydenhuolto-organisaatiossa

Suomessa terveydenhuolto-organisaatioilla on valmiuslaissa asetettu velvollisuus varautua toimintaan häiriötilanteissa, sillä terveydenhuollon kriittiset palvelut on voitava tuottaa myös poikkeustilanteiden aikana. (Valmiuslaki 1552/2011, 12§) Kyberhyökkäys on esimerkki häiriötilanteesta, joka terveydenhuolto-organisaatioon voi kohdistua. Coronadon ja Wongin (2014) mukaan kybervarautuminen on organisaatioille suuri vastuu ja kaikkien terveydenhuollon toimijoiden tulee se mielessään. Toimivan yhteistyön avulla voidaan suojella terveydenhuollon tärkeää infrastruktuuria ja mahdollistaa potilaille paras mahdollinen hoito myös häiriötilanteiden aikana. (Coronado & Wong 2014) Päävastuu hyökkäyksiltä suojautumisessa ja hyökkäystilanteiden ratkaisemisessa on organisaatiolla itsellään. Tämä erottaa kyberhyökkäykset monista muista yhteiskunnan kriittiseen infrastruktuuriin kohdistuvista kriisitilanteista, joissa päävastuu on esimerkiksi puolustusvoimilla tai poliisilla. (Candolin 2020) Kyberhyökkäystilanteet vaativat organisaatiolta kuitenkin myös paljon organisaatiorajat ylittävää sidosryhmäyhteistyötä, jossa yhteistä vihollista vastaan taistellaan yhdessä kaikilla mahdollisilla keinoilla (Candolin 2020; Hubbard et al. 2017).

Sosiaali- ja terveysministeriön (2019) mukaan julkisen sektorin toimijoiden tulee ottaa kyberturvallisuus huomioon organisaation kaikessa resursoinnissa ja osana palveluiden tuottamista. Tällä voi olla vaikutuksia esimerkiksi järjestelmien ja palveluiden hankintaan.

Kyberturvallisuuden lisääminen ja häiriötilanteisiin ennalta varautuminen lisää kustannuksia, mutta kriittisen toiminnan osalta resursseja on kuitenkin varattava siten, että tilanteista voidaan selvitä. Varautuminen perustuu erityisesti laadukkaaseen toimintaan normaalioloissa ja siihen, että potentiaalisia häiriötilanteita ennakoidaan. Organisaation kyky toimia häiriötilanteissa edellyttää organisaatiolta ja sen toimijoilta vahvaa sitoutumista varautumisen ja toiminnan jatkuvuuden kehittämiseen. Varautumissuunnitteluun kuuluvia osa-alueita ovat esimerkiksi toimijoiden välinen vastuunjako, häiriötilanteen hallinta ja johtaminen, sekä häiriötilanteesta toipuminen. (Sosiaali- ja terveysministeriö 2019)

KPMG:n vuonna 2015 teettämässä kyberturvallisuuskyselyssä kävi ilmi, että jopa 81 prosenttia terveydenhuollon organisaatioista oli kahden edellisen vuoden aikana joutunut kyberhyökkäyksen kohteeksi ja niistä vain puolien varautuminen oli ollut riittävällä tasolla. Johtuen toteutuneista hyökkäyksistä ja valtion tasolla lisääntyneestä strategisesta ohjauksesta Suomen terveydenhuollossa on ryhdytty viime vuosina varautumistoimenpiteisiin. (Norri-Sederholm et al. 2019) Varautumisen ja jatkuvuudenhallinnan tarkoituksena on turvata yhteiskunnalle elintärkeät toiminnot ja tärkeänä osana varautumistoimintaa on myös yhteistyö eri toimijoiden ja viranomaisten välillä. Tässä tärkeä rooli on Kyberturvallisuuskeskuksella, joka kerää ja jakaa tietoa tietoturvauhkista ja ohjeistaa yhteistyötahojaan. (Kyberturvallisuuskeskus 2021a, Norri-Sederholm et al. 2019).

Tässä alaluvussa kyberhyökkäystilanteeseen varautumista tarkastellaan erityisesti terveydenhuolto-organisaation kontekstissa. Tavoitteena on löytää ja kuvata edellisessä alaluvussa kuvattujen yleisten kyberhyökkäykseen varautumistoimenpiteiden lisäksi sellaisia varautumistoimenpiteitä, jotka liittyvät terveydenhuollon toimintaympäristöön ja ovat erityisen tärkeitä alan organisaatioissa toimittaessa. Hubbard et al. (2017) jakaa organisaatioiden kybervarautumisen kolmeen osa-alueeseen: tekniikkaan, hallinnollisiin prosesseihin ja ihmisiin (Hubbard et al. (2017). Tätä samaa jakoa noudatetaan myös tässä alaluvussa.

### 4.2.1 Tekninen varautuminen terveydenhuollossa

Organisaation tietoturvasta vastaavalla taholla tulee olla riittävästi osaamista erilaisten teknisten suojausmenetelmien toteuttamiseksi, sillä vaikka täydellisen suojauksen saavuttaminen on mahdotonta, suurimman osan hyökkäyksistä vaikutuksia voidaan minimoida tai ne voidaan jopa estää kokonaan. Kyberuhkat voivat toteutua myös varautumisesta huolimatta, minkä vuoksi terveydenhuolto-organisaatioiden tulee kehittää myös sietokykyään ja toimintavalmiuttaan niiden tapahtuessa (Norri-Sederholm et al. 2019;

Ayala 2016) Sosiaali- ja terveysministeriön (2019) mukaan terveydenhuolto-organisaation on määritettävä varautumisessaan organisaation kriittiset toiminnot, palvelut, tieto sekä niihin liittyvät kriittiset tietojärjestelmät. Kun kriittiset järjestelmät on tunnistettu, on niiden toiminta ja kapasiteetti turvattava siten, että häiriötilanteista pystytään selviämään. Kriittisiä järjestelmiä on ylläpidettävä täsmällisesti ohjeiden mukaan ja esimerkiksi tarvittavista ohjelmistopäivityksistä on huolehdittava ilman katkoksia. Häiriönsietokykyyn pitää panostaa sitä enemmän, mitä vähemmän toiminta, johon järjestelmä liittyy, sietää keskeytyksiä. (Sosiaali- ja terveysministeriö 2019)

Aiemmin tunnistetut järjestelmien ja niiden sisältämän tiedon luottamuksellisuus-, eheys- ja saatavuusvaatimukset ovat tärkeitä myös terveydenhuoltoon kohdistuvien kyberhyökkäyksiin varautumisessa. Kyberhyökkäykset pyrkivät vaikuttamaan terveydenhuolto-organisaatioiden hallussa olevan tiedon eheyteen, luottamuksellisuuteen tai saatavuuteen, ja siksi organisaatioiden on ymmärrettävä minkälaisia vaatimuksia mihinkin järjestelmään ja toimintaan liittyy. (Huang et al. 2018; Coronado & Wong 2014) Terveydenhuollon kontekstissa saatavuus ja toimivuus voi olla prioriteettina esimerkiksi potilaiden henkeä ylläpitävien laitteiden toiminnassa tai potilaiden tunnisterannekkeissa. Salaukseltaan kriittisiä elementtejä voivat olla esimerkiksi potilaiden luottamukselliset hoitotiedot. Tiedon eheys voi olla prioriteettina esimerkiksi lääkintätiedon kohdalla. Terveydenhuollon tietojärjestelmäinfrastruktuurin arviointi juuri tästä näkökulmasta auttaa organisaatiota kohdistamaan suojaustoimet ja niihin käytössä olevat resurssit oikein (Coronado & Wong 2014; Tipton & Krause 2004).

Terveydenhuolto-organisaatioiden tietojärjestelmäinfrastruktuureille on ominaista, että suuren joukon järjestelmiä avulla luodaan kokonaisvaltaisia palveluita useille eri käyttäjätyypeille. Tietojärjestelmät toimivat harvoin irrallaan toisistaan. (Candolin 2008) Jo infrastruktuurin suunnitteluvaiheessa on tärkeää ymmärtää, että laitteiden ja järjestelmien korkea integraatio ja yhdistettävyys lisää riskiä kyberhäiriöihin (Willing et al. 2021; Coronado & Wong 2014). Palveluorientoitunut infrastruktuuri haastaa kyberturvallisuuden toteuttamista, kun myös järjestelmien välisiä yhteyksiä ja kommunikaatiota on suojattava ja kontrolloitava tarkkaan. (Candolin 2008) Terveydenhuolto-organisaation teknisen kyberturvallisuuden rakentaminen on erityisesti järjestelmien ja laitteiden muodostaman systeemin hallintaa, jossa tulee keskittyä järjestelmien kokonaisuuteen yksittäisten laitteiden sijaan. Potilastietojen lisäksi myös kansallisten sosiaali- ja terveydenhuollon tietovarantojen, erilaisten digitaalisten diagnostisten palveluiden sekä verkkoihin kytkettyjen laitteiden kyberturvallisuus on varmistettava. (Norri-Sederholm et al. 2019) Esimerkkejä organisaation resilienssiä kehittävistä teknisen varautumisen toimenpiteistä ovat

esimerkiksi kriittisten tietojärjestelmien ja prosessien monistaminen, hoitotietojen varmuuskopiointi ja koko organisaation tietojärjestelmäinfrastruktuuriin näkyvyyden antavan valvontajärjestelmän rakentaminen. Myös suojaukseen käytettävien teknologioiden ja niiden päivitysten pitäminen ajan tasalla on tärkeä osa teknistä varautumista. (Norri-Sederholm et al 2019; Ayala 2016; Coronado & Wong 2014; Bhamra et al. 2011)

Terveydenhuollon alalla toimittaessa teknisen varautumisen tulee rakentua hoitotoiminnan jatkuvuuden varmistamisen ympärille ja kybervarautuminen vaatii samanaikaista vahvaa ymmärrystä sekä kyberturvallisuudesta että terveydenhuollon toimintatavoista. Osatakseen suojata organisaatioiden kriittistä toimintaa mahdollisimman hyvin on teknistä varautumista suunnittelevien tietoteknisten asiantuntijoiden tunnettava myös hoitotoimintaa sen verran, että ymmärtävät sen kriittisimpiä tietoja ja prosesseja. (Norri-Sederholm et al. 2019) Organisaation on tunnistettava, minkä tietojen tai järjestelmien hajoaminen tai menetys aiheuttaisi toiminnalle ja yhteiskunnalle suurimpia ihmisten turvallisuuteen, terveyteen tai tietosuojaan aiheutuvia uhkia. (NIST 2018)

Terveydenhuolto-organisaation tietoturvahenkilöstön vastuulle kuuluu todennäköisesti myös hyökkäystilanteeseen reagointi. Tekniseen varautumiseen kuuluukin myös toimintasuunnitelman valmistelu kyberhyökkäystilanteen varalta. Suunnitelmaan tulee sisältyä muun muassa ajantasainen lista kaikista käytössä olevista järjestelmistä ja ohjelmistoista, ja niiden arvioiduista keskinäisistä riippuvuuksista. Tämä auttaa organisaatiota ymmärtämään hyökkäyksen kokonaisvaikutukset heti ja saavuttamaan tilannetietoisuuden tilannekuvan muodostamiseksi. (Norri-Sederholm et al. 2019) Hyökkäyksiin vastaamisessa olennaista on pyrkiä korjaamaan tai sulkemaan sellaiset tietojärjestelmäinfrastruktuurin osat, jotka mahdollistavat hyökkäyksen (Libicki 2012). Tilannekuvan hahmottaminen auttaa organisaatiota valitsemaan oikeat toimintatavat ja hahmottamaan hyökkäyksen vaikutuksia laajasti (Tikanmäki & Ruoslahti 2021; Norri-Sederholm et al. 2019). Mykkänen et al. (2019) tutkivat teknisen tilannekuvan mallintamista terveydenhuollon tietojärjestelmäinfrastruktuurissa. Heidän mukaansa kokonaisuuden reaaliaikainen mallintaminen on mahdollista, mutta tietojärjestelmien ja niiden rajapintojen pitää tällöin olla sellaisia, että ne palvelevat samanaikaisesti sekä tiedon ensisijaista, että toisiokäyttöä. Kokonaisuutta tulkitsemalla voidaan saavuttaa tilanneymmärrys, jonka avulla voidaan tukea toimintaprosesseja, eri tahojen päätöksentekoa ja tulevaisuuden kehitystyötä. (Mykkänen et al. 2019)

Terveydenhuollossa toimittaessa kuitenkin myös hyökkäykseen reagointiin käytettäviä teknisten ratkaisuiden vaikutuksia on arvioitava hoitotoiminnan näkökulmasta. Joillakin muilla aloilla toiminta ja työskentely voidaan pysäyttää, kunnes järjestelmät toimivat jäl-

leen, mutta terveydenhuollossa se ei todennäköisesti ole mahdollista. Kyberhyökkäyksen vastaukseksi ei todennäköisesti ole kannattavaa eikä mahdollistakaan suorittaa yhtäkkistä maksimaalista kaikkien organisaation palveluiden alasajoa (Libicki 2012). Hoitotoiminnan tuntemus korostuu etenkin hyökkäystilanteen aikana, jolloin ei välttämättä ole enää aikaa selvittää sitä, mitä mikäkin järjestelmä hoidon näkökulmasta tekee. On siis tiedettävä jo etukäteen, miten erilaiset ratkaisutoimet vaikuttavat toimintaan. Toiminnan jatkuvuuden kannalta kriittiset järjestelmät pyritään pitämään käytössä niin hyvin kuin mahdollista ja joitakin järjestelmiä ei saa koskaan sammuttaa, kun taas joitakin järjestelmiä tai niiden välisiä yhteyksiä voidaan sulkea varotoimenpiteenäkin (Willing et al. 2021). Hyökkäys pitää saada pysäytetyksi, mutta hoitoa häiritään mahdollisimman vähän.

### 4.2.2 Hallinnollinen varautuminen

Kyberhyökkäystilanteen kannalta keskeisimpiä terveydenhuolto-organisaation johdon tehtäviä on kyberhyökkäykseen varautumisen mahdollistaminen. Olennainen osa varautumisen onnistumista riittävien käytettävissä olevien resurssien varmistaminen, sillä turvallisuuteen ja häiriötilanteisiin varautuminen lisää väistämättä kustannuksia. Erityisesti kriittiseen toimintaan on varattava resursseja. Kyberhyökkäyksiin varautuminen ja sen vaatimat resurssit tulee ottaa huomioon jo järjestelmiä ja palveluita hankittaessa. (Coronado & Wong 2014; Sosiaali- ja terveysministeriö 2019)

Kyberhyökkäyksen kaltaisessa kriisitilanteessa tarve tehdä jotakin nopeasti syntyy tyypillisesti hyvin nopeasti. Samaan aikaan tilanteen kehittymiseen liittyy paljon epävarmuutta. Kyberhyökkäyksen tapahtuessa eri tasoisissa johtotehtävissä toimivien henkilöiden tärkeimmäksi tehtäväksi muodostuu kriisipäätöksenteko. Se eroaa tavallisesta päätöksenteosta erityisesti suoraviivaisuudessaan ja nopeudessaan, sillä aikaa voi olla hyvin vähän. Kriisitilanteiden johtamiseen voidaan varautua luomalla ennalta järjestelmä, joka tukee päätöksentekoa yllättävissä ja vakavissa tilanteissa. Johtamisen ja tilanteen koordinoinnin tarvittava taso määräytyy tilanteen vakavuuden ja laajuuden mukaan. Kriisipäätöksen teossa suurimmat haasteet liittyvät usein viiveisiin ja epäjatkuvuuskohtiin, jotka voivat vaikeuttaa ja hidastaa tilannetiedon välittämistä kaikille sitä tarvitseville tahoille. (Burnard & Bhamra 2019; Hellenberg 2011) Nopea ja tehokas toiminta kyberhyökkäystilanteessa on tarpeen myös siksi, että se vähentää hyökkäystilanteen ja sen vaikutusten eskaloitumisen mahdollisuutta (Libicki 2012).

Terveydenhuolto-organisaation kyberhyökkäystilanteen johtamisessa tulee ottaa huomioon myös se, että mahdollisen kriisin vaikutukset eivät kohdistu vaan omaan organisaatioon vaan pahimmillaan jopa koko valtion kriittisen infrastruktuurin huoltovarmuuteen.

Tämä on yksittäiselle organisaatiolle ja sen henkilöstölle valtava vastuu. Tästä johtuen yhteistyön toimivuuden varmistaminen myös erilaisten ulkoisten sidosryhmien, kuten viranomaisten kanssa on hyvin tärkeää. (Candolin 2020; Hubbard et al. 2017) Suomalaisten julkisten tahojen on kyberhyökkäyksen aikana otettava yhteyttä muun muassa kyberturvallisuuskeskukseen (Sosiaali- ja terveysministeriö 2019). Kriisitilanteen käynnistyessä olennaista on saada kaikki tarvittavat tahot hälytettyä paikalle. Sen jälkeen tilanne on analysoitava nopeasti ja tehtävä päätökset siitä, miten toimintaa jatketaan. Tässä olennainen merkitys on jälleen kattavan ja selkeän tilannekuvan hahmottamisella. Tilannekuvaa tarvitaan myös viestinnässä kriittisen infrastruktuurin eri toimijoiden välillä. (Norri-Sederholm et al. 2019) Myös ulkoisilla tahoilla voi olla merkittäviä vastuita tilanteen selvittämisessä. Keskeistä tilanteessa pärjäämisessä on toimiva yhteistyö, vastuunjako ja johtamisjärjestelmä, ja se, että kaikki tuntevat oman roolinsa siinä. (Norri-Sederholm et al 2019; Hubbard et al. 2017; Tikanmäki & Ruoslahti 2021; Candolin 2020)

Organisaation johdon on viestittävä kriisitilanteessa myös muiden tahojen, esimerkiksi median ja oman henkilöstön kanssa. (Hellenberg et al. 2011) Suureen terveydenhuolto-organisaatioon kohdistuva kyberhyökkäys herättää hyvin todennäköisesti myös median ja yleisön huomion, joten johdon on koordinoitava myös sitä, mitä medialle kerrotaan. On tärkeää, että organisaatio johtaa itse sitä, mitä media kertoo, sillä hallitsematon kohu voi osaltaan kasvattaa kriisitilanteen negatiivisia vaikutuksia. (Libicki 2012) Ulkoisen yhteistyön lisäksi on johdettava myös organisaation operatiivista toimintaa, joka terveydenhuolto-organisaation tapauksessa tarkoittaa hoitotoimintaa. Toiminnan mukauttaminen voi vaatia nopeita ratkaisuita, sekä joskus yllättävissä tilanteissa myös hieman luovuutta (Burnard & Bhamra 2019). Viestintä kyberhyökkäystilanteessa on suunniteltava niin tarkkaan, että kriisitilanteen tapahtuessa organisaation kaikki henkilöt tietävät, kenen vastuulla kommunikaatio minkäkin ryhmän kanssa on ja toisaalta mistä itse saa tietoa. (NIST 2018)

Terveydenhuolto-organisaation johtamisen näkökulmasta kyberhyökkäystilanteessa toimimisessa on paljon yhteistä muunlaisten kriisitilanteiden kanssa ja koetuista kriiseistä voidaan saada vauhtia kaikkeen kriisivalmistautumiseen (Gkeredakis et al. 2021). Terveydenhuolto-organisaatiossa samat henkilöt vastaavat ylimmän tason päätöksenteosta, viestinnästä ja viranomaisyhteistyöstä kaikissa poikkeustilanteissa. Hellenberg et al. (2011) ja Somersin (2009) mukaan kaikkiin kriisitilanteisiin varaudutaan osittain samoilla periaatteilla, koska kriisitilanteet sisältävät aina yllätyksiä ja ne vastaavat harvoin täydellisesti ennalta määriteltyjä riskiskenaarioita. Tästä syystä kriisivarautumisessa kannattaa keskittyä yleisen resilienssin ja toimintavalmiuden luomiseen, reagointikyvyn

parantamiseen ja äkillisten tilanteiden prosessien ja johtamisen peruskäytäntöjen luomiseen. (Burnard & Bhamra 2019; Hellenberg et al. 2011; Somers 2009)

### 4.2.3 Koko henkilöstön varautuminen

Willing et al. (2021) toteavat, henkilöstön kriisikäyttäytymisellä on erityisen tärkeä rooli toimittaessa lääketieteellisissä ympäristöissä, sillä elintärkeän hoitotoiminnan on aina jatkuttava. Monet terveydenhuollon työntekijät tekevät työtään korkean kysynnän keskellä ja joskus heikosti kontrolloitavissa olevassa suuren riskin ympäristössä. Näin ollen heidän osaamisensa ja käyttäytymisensä on ratkaisevan tärkeää potilasturvallisuuden varmistamisessa. Koska aika on kriittinen tekijä kriittisissä tilanteissa, heidän toimintansa epävarmoissakin tilanteissa on oltava nopeaa ja tehokasta. Vaikka kyberhyökkäystilanteen ratkomiseen liittyvät päätökset tekee monesti tietohallinnon ja lääketieteen ammattihenkilöstö, jokainen hoitohenkilöstön jäsen voi joutua tekemään nopeita päätöksiä. (Willing et al. 2021) Kyberturvallisuuskeskuksen mukaan henkilöstön kybertietoisuus on kriittisessä avainroolissa kyberhyökkäystilanteissa ja niiltä suojautumisessa (Kyberturvallisuuskeskus 2021a). Henkilöstön riittävän osaamisen varmistaminen on tärkeä osa kyberhyökkäyksiin varautumista ja koko henkilöstön käyttäytyminen on aina otettava huomioon kyberhyökkäystilanteita käsiteltäessä (Willing et al. 2021; Norri-Sederholm et al. 2019)

Coronadon ja Wongin (2014) mukaan henkilöstön kouluttaminen on yksi terveydenhuolto-organisaation tärkeimmistä tavoista varautua kyberuhkiin, sillä sen avulla organisaation kaikki toimijat voidaan saada työskentelemään yhteistyössä niitä vastaan (Coronado & Wong 2014). Koulutus on tarpeen, koska tietotekniikka ja kyberhyökkäykset eivät ole tietojärjestelmiä käyttävien hoitoalan henkilöiden ydinosaamisalueita, jolloin heidän osaamistansa on kehitettävä ja varmistettava säännöllisesti organisaation toimesta (Saranto et al. 2021). Organisaatioiden henkilöstön tulee tunnistaa häiriötilanteita ja ymmärtää, miten heidän tulee itse reagoida niitä havaitessaan (NIST 2018). Merkittävä määrä kyberuhista saapuu esimerkiksi henkilöstön sähköpostilaatikoihin ja siksi kaikilla työntekijöillä on oltava perusymmärrys kyberturvallisuudesta ja -uhista. (Ayala 2016) NIST:in (2018) mukaan henkilöstön koulutuksessa ja tietoisuuden lisäämisessä on kyse siitä, että organisaation koko henkilöstölle ja kumppaniverkostolle tarjotaan sellainen määrä opetusta, joka takaa sen, että he pystyvät suoriutumaan omiin työtehtäviinsä liittyvistä kyberturvallisuuteen liittyvistä vastuista ja velvollisuuksista erilaisissa tilanteissa. Jokaisen toimijan tulee tietää, miten tehdä omat työtehtävänsä ja vastuunsa siten, että

ne ovat linjassa organisaation ohjeistuksien kanssa. (NIST 2018) Myös Sosiaali- ja terveysministeriön (2019) mukaan tietoturva- ja tietosuojaosaaminen ovat tärkeitä osia sosiaali- ja terveydenhuollon henkilöstön tarvitsemaa ammattitaitoa ja siten jokaisen toimijan vastuulla. Ministeriö ohjeistaa terveydenhuollon toimijoita vahvistamaan henkilöstön osaamista jatkuvasti. (Sosiaali- ja terveysministeriö 2019).

Terveydenhuollon alalla toimittaessa esimerkiksi kriittisen hoidon on jatkuttava häiriötilanteesta huolimatta (Willing et al. 2021). Tätä varten organisaatioiden on suunniteltava kyberhyökkäystilanteita varten myös varajärjestelmä toiminnan suorittamiseen ja korvaavat toimintatavat, joihin voidaan siirtyä välittömästi ongelmatilanteen ilmettyä. Owensin (2020) mukaan terveydenhuolto-organisaatioiden, kuten sairaaloiden, tulisi tehdä kyberturvallisuudesta osa sen koko henkilöstön yhdessä ylläpitämää turvallisuuskulttuuria, samaten kuin esimerkiksi paloturvallisuuden kohdalla. Tällöin organisaatio valmistelee sellaiset prosessit ja toimintatavat, joilla hoitotoimintaan kohdistuva häiriö minimoidaan kyberhäiriötilanteessa. Tämä tarkoittaa esimerkiksi sitä, että nuoremmankin henkilöstön on osattava käyttää paperikirjausmenetelmiä, vaikka heidän työuransa aikana niitä ei olisikaan koskaan arjessa käytetty. (Owens 2020)

Myös Sosiaali- ja terveysministeriön (2019) mukaan koko henkilöstön on oltava aktiivisesti mukana varautumisen toteuttamisessa. Kaikkien organisaatioiden työntekijöiden tulee tietää, miten toimia, jos tietojärjestelmät eivät ole normaalisti käytössä ja mikä on heidän vastuunsa tilanteessa. Tällöin jokainen tietää, mitä tehdä, heti tilanteen käynnistyessä. (Sosiaali- ja terveysministeriö 2019) Jotta korvaaviin toimintamalleihin voidaan siirtyä tehokkaasti ja sujuvasti, eri tahojen välillä häiriötilanteen aikana tehtävän yhteistyön tulee olla etukäteen sovittua ja koordinoitua, sekä mielellään myös harjoiteltua. (NIST 2018; Norri-Sederholm et al. 2019; Sosiaali- ja terveysministeriö 2019) Harjoituksiin tulee osallistua sellaisia tahoja, joilla keskeinen rooli todellisissakin tilanteissa. Näin voidaan varmistaa, että harjoittelulla saavutetut tulokset jalkautuvat tehokkaasti käytännön toimintaan. (Sosiaali- ja terveysministeriö 2019) Harjoittelun avulla voidaan myös kehittää sidosryhmäyhteistyötä, esimerkiksi muiden organisaatioiden ja viranomaisten kanssa (Norri-Sederholm et al. 2019).

## 4.3 Kyberhyökkäysvalmiuden mittaaminen

Kriisivarautumiseen kuuluu olennaisena osana myös käytössä olevien varautumistoimien kriittinen arviointi. Arvioinnin avulla voidaan löytää sokeita pisteitä ja kehityskohteita ja siten jälleen kehittää organisaation valmiutta. Varautumisen tulee olla jatkuva iteratiivinen ja syklinen prosessi, jossa organisaation toimintakykyä ja olemassa olevia varau-

tumiskeinoja arvioidaan, sitten kehitetään, testataan uudelleen ja kehitetään jälleen lisää. (NIST 2018) Varautuminen jaettiin aiemmassa alaluvussa mukaisesti tekniseen, hallinnolliseen ja henkilöstön varautumiseen, joten seuraavaksi esitetään muutamia esimerkkejä siitä, miten kullakin osa-alueella onnistumista voidaan mitata organisaatioissa.

Organisaation teknistä valmiutta kyberhyökkäyksiin voidaan mitata esimerkiksi erilaisilla auditoinneilla, jossa käytössä olevia teknisiä varautumismekanismeja verrataan haluttuun tavoitetilaan tai ulkopuolisten tahon määrittämään standarditasoon. (Coronado & Wong 2014) Auditointeja voi toteuttaa joko oman organisaation sisäiset tai ulkoiset tahot. Infrastruktuurin teknistä varautumistasoa voidaan arvioida erilaisilla penetraatiotestauksilla ja testihyökkäyksillä, jossa pyritään luomaan kyberhyökkäystilanne keinotekoisesti. Testaamisella voidaan myös löytää infrastruktuurista uusia kehityskohtia, joita ei välttämättä muuten olisi huomattu. (Bahuguna et al. 2019)

Kybervalmiuden hallinnon ja johtamisen kannalta merkittäviä mittauskohteita ovat kyberturvallisuustoiminnan tavoitteet, toiminnassa tehdyt priorisoinnit, kybervarautumiseen käytössä olevien taloudellisten ja -henkilöresurssien määrä, tehtävän yhteistyön ja tiedonjaon laatu sekä varautumisen lainmukaisuus. Myös organisaation rakenne ja toimintaprosessien sujuvuus voivat vaikuttaa kyberhyökkäyksessä toimimiseen ja niitä tutkimalla voidaan löytää. (Bahuguna et al. 2019)

Vaikka varautumiseen liittyvät vastuut ja päätoimiset tehtävät kuuluvat usein teknisille osaajille ja organisaation johdolle, kybervarautumisen kokonaisuuteen osallistuu koko organisaatio, kuten aiemmin todettiin. Tästä syystä myös muun henkilöstön ajankohtaisen osaamisen ja tietoisuuden riittävää tasoa tulee mitata jatkuvasti. (Bahuguna et al. 2019; Sosiaali- ja terveysministeriö 2019) Tässä toimivia keinoja voivat olla esimerkiksi Willing et al. (2021) tutkimuksessaan käyttämän kaltaiset testitilanteet. Tutkimuksessa teho-osaston henkilöstö laitettiin toimimaan simuloidussa hoitotilanteessa ja heidän tietämättään monitorien näyttämää tietoa alettiin vääristää. Hoitohenkilökunnan tehtävänä oli havaita virhetilanne ja mukauttaa toimintaansa sen mukaisesti. Tutkimuksesta saatiin mielenkiintoisia tuloksia, nimittäin vain 40 % heistä onnistui havaitsemaan poikkeavuuden monitorin toiminnassa. Tutkimuksen tulokset tarjosivat tietoa siitä, kuinka valmiita henkilökunnan jäsenet olivat toimimaan tällaisessa tilanteessa. (Willing et al. 2021) Harjoittelutilanteilla on mahdollista mitata oman organisaation toiminnan lisäksi myös laajemman sidosryhmäverkoston yhteistyötä (Norri-Sederholm et al. 2019). Suomessa julkishallinnon piirissä olevien organisaatioiden on mahdollista osallistua Digi- ja väestötietoviraston järjestämiin TAISTO-harjoituksiin, joissa häiriötilanteissa toimimista harjoitel-

laan kuvitteellisten tilanteiden kautta (Digi- ja väestötietovirasto 2021). Yksinkertaisempia keinoja henkilöstön varautumisen mittaamiseen voivat olla esimerkiksi säännölliset kriisitilanteiden toimintaohjeiden osaamiskartoitukset.

Kybervalmiuden mittaamisessa on tärkeää huomioida myös se, että joillekin valmiuden mittausmenetelmille, kuten auditoinneille, saattaa riittää se, että organisaatiolla on olemassa dokumentoitu suunnitelma, jolloin katsotaan varautumisen olevan kunnossa. Ayalan (2016) mukaan tämä ei kuitenkaan riitä, mikäli halutaan, että organisaatiolla on aina aito kyky toimia, vastata, toipua ja palautua kriisitilanteen aikana. Varautuminen ei myöskään ole toimintaa, jolla on alku ja päätepiste, jonka jälleen se on kunnossa ja se voidaan unohtaa. Varautumiseen liittyy jatkuvaa ylläpitoa ja harjoittelua ja sille ja sen mittaamiselle syntyy uusia tarpeita esimerkiksi joka kerta, kun organisaatioon liittyy uusi henkilö tai käyttöön otetaan uusi järjestelmä. (Ayala 2016)

Monilla julkisilla toimialoilla, kuten myös terveydenhuoltoalalla, on käytössä myös erilaisia virallisia ohjeistuksia ja tarkistuslistoja, jotka alan julkisten organisaatioiden kriisivarautumisen tulee täyttää. Organisaatiot voivat mitata varautumistaan vertaamalla oman toimintansa nykytilaa tarkistuslistoihin. Suomessa terveydenhuollon organisaatioiden kyberhyökkäysvarautumista voi verrata esimerkiksi Sosiaali- ja terveysministeriön (2019) kyberturvallisuusohjeeseen terveydenhuollon toimijoille tai Kyberturvallisuuskeskuksen kybermittariin. Kybermittarin avulla organisaatio voi mitata kypsyystasonsa kyberturvallisuuden hallinnan eri osa-alueilla. Kybermittari kertoo organisaation nykytilasta ja esittää seuraavalle tasolle vaadittavia kehitysalueita. Mittarin antamat tulokset ovat keskenään vertailukelpoisia ja halutessaan organisaatio voi myös verrata niitä anonyymiin vertailutietoon toimialalta. Julkisen sektorin toimijat voivat myös pyytää kyberturvallisuuskeskukselta tukea ja apua kyberturvallisuusvalmiutensa kehittämiseen, tai esimerkiksi harjoitusten toteuttamiseen. (Kyberturvallisuuskeskus 2021a; Kyberturvallisuuskeskus 2021b; Sosiaali- ja terveysministeriö 2019)

# 5. TAPAUSTUTKIMUS: KOHDEORGANISAATION TOIMINTA KYBERHYÖKKÄYSTILANTEESSA

Tässä luvussa esitellään tapaustutkimuksessa haastattelujen kautta kerätyt havainnot kohdeorganisaation nykytilan mukaisesta toiminnasta kyberhyökkäystilanteessa ja siihen varautumisessa. Prosessin tapahtumia kuvataan sekä kuvien muodossa että sanallisesti. Sanallisissa osioissa nostetaan esiin keskeisimpiä tutkimuksessa organisaation toiminnasta tehtyjä havaintoja. Tehtyjä havaintoja analysoidaan erityisesti organisaation eri toimijoiden näkökulmasta. Tutkimusaiheen kannalta olennaisimpia toimijoita ovat organisaation tietohallinto ja sen kanssa läheisessä yhteistyössä toimiva IT-toimittajayritys, yleisjohto, hoitotoimintaa koordinoivat henkilöt ja hoitohenkilökunta.

Ensin esitellään haastateltavien käsitystä mahdollisista kyberhyökkäysskenaarioista ja niiden mahdollisista seurauksista. Sen jälkeen esitellään organisaation toimintaa kyberhyökkäyksen aikana sekä sellaisia toimia, joita organisaatio tekee toimintasuunnittelun lisäksi nostaakseen valmiuttaan toimia kriisitilanteissa. Teemojen käsittelyjärjestys valikoitui tällaiseksi, sillä kun halutaan ymmärtää varautumista ja toimintaa kriisitilanteessa, on hyvä tuntea riskit ja seuraukset, joita niillä pyritään välttämään. Samaten on hyvä ymmärtää kriisitilanteen aikana tarvittavia toimintamalleja, jotta voidaan tunnistaa keinoja, joilla voidaan kehittää organisaation valmiutta toteuttaa ne.

## 5.1 Erilaiset kyberhyökkäysskenaariot ja niiden mahdolliset seuraukset kohdeorganisaatiossa

Jotta voidaan ymmärtää ja tutkia organisaation toimintaa kyberhyökkäystilanteessa, on ymmärrettävä, millaisten hyökkäyksien välttämiseen ja minimoimiseen organisaation toiminnalla pyritään. Haastateltavien tuntemus kyberhyökkäysaiheesta vaihteli paljon. Osa haastateltavista tiesi hyökkäyksistä paljonkin, mutta osalle aihe oli varsin tuntematon. Haastateltavat tunnistivat kuitenkin monen tyyppisiä mahdollisia organisaatioon kohdistuvia kyberhyökkäysskenaarioita. Hyökkäysskenaarioita ja niihin liittyviä mahdollisia seurauksia esitellään taulukossa 8.

Taulukko 8. *Haastatteluissa tunnistetut kyberhyökkäystilanteet*

| Hyökkäystyyppi | Mahdolliset seuraukset |
|---|---|
| Palvelunestohyökkäys | - **kiire, ruuhkautuminen**<br>- potilasturvallisuusriskit<br>- mainehaitat, taloudelliset haitat |
| Tietovuoto/-varkaus | - **potilaisiin kohdistuvat henkilökohtaiset haitat**<br>- **mainehaitat, taloudelliset haitat** |
| Tietojen muuttaminen salaa | - **merkittävät potilasturvallisuusriskit**<br>- kiire, ruuhkautuminen<br>- mainehaitat, taloudelliset haitat |
| Lääkintälaitteisiin kohdistuva hyökkäys | - **merkittävät potilasturvallisuusriskit**<br>- mainehaitat, taloudelliset haitat |
| Yhdistelmähäiriö (esim. kyberhyökkäys + suuronnettomuus TAI yhtäaikaisesti kyber- ja fyysiseen maailmaan kohdistuva hyökkäys) | - **potilasturvallisuusriskit**<br>- **kiire ja ruuhkautuminen**<br>- mainehaitat, taloudelliset haitat<br>- **seuraukset vakavampia kuin yhden häiriön aikana** |

Terveydenhuolto-organisaatiossa hyökkäysten riskit ulottuvat tulonmenetyksiä ja liiketoiminnan epäjatkuvuuksia kauemmas, sillä häiriöt toiminnassa aiheuttavat usein uhkia jopa ihmishengille. Kaikkein keskeisimmäksi riskiskenaarioksi haastatteluissa nousikin potilasturvallisuuden vaarantuminen, joka voi liittyä monenlaisiin hyökkäysskenaarioihin ja jonka myös jokainen haastateltava mainitsi. Potilaiden terveys ja turvallisuus ovat organisaation kaiken toiminnan keskiössä, ja vaikka riskejä pyritäänkin kaikin tavoin minimoimaan, on potilasturvallisuusriskit usein läsnä. (Tietohallinto A-D, Johto A-B, Hoitohenkilökunta A-G, Hoitotekniikka A) Potilasturvallisuus voi vaarantua monin tavoin ja joidenkin haastateltavien mukaan voidaan myös ajatella, että jokainen häiriö toiminnassa on aina potilasturvallisuusriski (Johto A, Hoitohenkilökunta A, B).

Vastaajien tunnistamiin mahdollisiin kyberhyökkäystilanteisiin lukeutuvat muun muassa palvelunestohyökkäykset ja muut hyökkäykset, jotka estävät organisaation tietojärjestelmien tai laitteiden käyttöä. Skenaario hyökkäyksestä, jossa järjestelmät eivät toimi, oli yleisin haastatteluissa esiin noussut skenaario ja sitä käsiteltiin jokaisessa haastattelussa. (Tietohallinto A-C, Johto A-B, Hoitohenkilökunta A-G, Hoitotekniikka A) Erityisen kriittisiä potilasturvallisuuteen liittyviä seurauksia voi syntyä esimerkiksi toimivien potilaiden hoitoon käytettävien laitteiden puutteesta, mikäli kyberhyökkäys onnistuisi sekoittamaan tai hajottamaan laitteita käyttökelvottomiksi. Osa laitteista ovat niin sanottuja elämää ylläpitäviä laitteita, joten pienikin katkos niiden toiminnassa voisi olla kohtalokas. (Hoitohenkilökunta D, Hoitotekniikka A) Eräs haastateltava nosti esiin tietämänsä tapauksen sydämentahdistimen hakkeroinnista (Hoitotekniikka A). Mikäli tällainen tapaus

ilmenisi laajemmin jopa koko organisaation toiminta-alueella, voisi siitä seurata merkittäviä ja aivan uudenlaisia haasteita. (Hoitohenkilökunta D, Hoitotekniikka A) Esimerkiksi organisaation sähköisen kulunvalvontajärjestelmän lamauttaminen voisi olla pelottava skenaario, kun kukaan ei pääsisi liikkumaan paikasta toiseen (Hoitohenkilökunta B).

Mikäli organisaation tietojärjestelmät olisivat kyberhyökkäyksen takia poissa käytöstä, syntyisi monessa hoitotilanteessa myös uusia tietotarpeita. Normaalisti hoitohenkilökunta näkee hoidettaviensa pohjatiedot tietokoneelta ja esimerkiksi hoitoketjun aiemmissa vaiheissa tehdyt diagnoosit ovat nähtävissä. Mikäli järjestelmät eivät kuitenkaan olisi käytössä, olisi kaikki tiedot hankittava muuten, esimerkiksi potilailta kysyen. Tämä teettää hoitohenkilökunnan haastateltavien mukaan paljon lisätyötä ja joissain tilanteissa voi olla myös tarpeen toimia heikomman tiedon varassa. (Tietohallinto B, Hoitohenkilökunta A-G, Hoitotekniikka A) Jos kaikkea hoitoon tarvittavaa tietoa ei ole käytettävissä, myös potilasturvallisuus voi olla uhattuna. Kiireellisen hoidon parissa toimivien haastateltavien mukaan vakavia seurauksia voisi olla vaikkapa sillä, että akuutisti operoitavan ihmisen lääkitystä tai lääkeaineallergioita ei olisi tiedossa. (Hoitohenkilökunta A, D, G, Hoitotekniikka A)

Yksi kaikissa haastatteluissa todennäköisenä pidetty kyberhyökkäyksen seuraus oli kiire ja toiminnan ruuhkautuminen. Tietojärjestelmien toimimattomuus vaatii korvaavia toimintatapoja, jotka eivät ole yhtä tehokkaita kuin normaalit toimintatavat. (Tietohallinto A-D, Johto A-B, Hoitohenkilökunta A-G, Hoitotekniikka A) Kiirettä syntyy myös silloin, jos viestintäyhteydet eivät toimi normaalisti, vaan tietoa on siirrettävä jalkaisin. (Tietohallinto A, Hoitohenkilökunta A, B, D, G) Hoitohenkilökunnan haastateltavien mukaan kiire, ruuhkautuminen ja epävarma tilanne kasvattavat myös henkilöstön ja potilaiden kokemaa stressiä ja mahdollisesti pelkoakin. (Hoitohenkilökunta A, B, D, F) Pahimmillaan ruuhkatilanteet ja toiminnan merkittävä hidastuminen voivat aiheuttaa myös potilasturvallisuusriskejä, jos tarvittavaa hoitoa ei saada annettua riittävän nopeasti tai kiireestä aiheutuu virheitä. (Hoitohenkilökunta A, E) Haastateltavien mukaan kiireen ja ruuhkautumisen aiheuttamat seuraukset pahenevat sitä mukaa, mitä kauemmin hyökkäys kestää. Mikäli hyökkäys kestää vain tunteja, voidaan kiireetöntä hoitoa ajaa alas jonkin verran, jolloin vain akuuteimmat tapaukset hoidetaan. Tilanteen pitkittyessä jonoa alkaa kuitenkin kertyä ja myös kiireetöntä hoitoa vaativat tapaukset voivat muuttua kiireellisemmiksi. (Hoitohenkilökunta B, G, Hoitotekniikka A) Erään haastateltavan mukaan organisaatiolla on käytännössä aina hoidossaan useita potilaita, jotka vaativat kiireellistä hoitoa (Hoitohenkilökunta D).

”*Kyllä se Vastaamo-case herätti meidät ja muut laajasti, se oli niin iso varoitus, että nyt todella täytyy varmistaa, että sellaista ei pääse käymään*” – Tietohallinto D

Myös Vastaamo-tapauksen kaltaiset tietovuodot ja -varkaudet nousivat esiin useissa haastatteluissa, ja tapaus onkin herättänyt organisaatiossa keskustelua laajemminkin (Hakkarainen 2020) (Hoitohenkilökunta A, B, E). Tietovuoto- tai tietovarkaustyyppisiin kyberhyökkäyksiin liittyy uhka potilastietojen joutumisesta vääriin käsiin. Vääriin käsiin joutuneita potilastietoja voidaan käyttää esimerkiksi potilaiden tai organisaation kiristyksessä tai uhkailussa. Varkauden kohteeksi joutuneelle henkilölle voi aiheutua tilanteesta paljon huolta ja hankaluuksia. (Tietohallinto A, Hoitohenkilökunta E) Vaikka henkilökohtaisten potilastietojen leviämisen seuraukset kohdistuvatkin erityisesti organisaation potilaisiin ja heidän yksityisyyteensä, on organisaatio vastuussa potilaistaan ja siten myös heidän tietojensa turvallisuudesta. Epäonnistumisesta potilaiden luottamuksellisten tietojen suojelemisessa voi seurata organisaatiolle esimerkiksi sanktioita ja mainehaittoja. (Tietohallinto A-D, Johto A-B, Hoitohenkilökunta A, B, Hoitotekniikka A)

Kyberhyökkäyksestä seuraavat mainehaitat nousivat esiin erityisesti johtavissa asemissa työskentelevien henkilöiden haastatteluissa. Riskinä olisi, ettei organisaation palveluihin enää luotettaisi kuten ennen. Mainehaittoja voisi syntyä edellä mainitun tietovarkaustilanteen lisäksi esimerkiksi silloin, jos kyberhyökkäystilanteessa tapahtuu hoitovirheitä tai hoidon saanti vaikeutuu. Kohdeorganisaatiolle on tärkeää, että ihmiset luottavat organisaation tarjoamaan hoitoon ja siihen, että apua saa hädän tullen. Mikäli organisaation asiakkaat kokisivat, etteivät he tai heidän tietonsa olisi turvassa organisaation käsissä, voisi se haitata sekä organisaation toimintaa että sen palvelemien ihmisten kokemaa turvallisuudentunnetta. (Tietohallinto A-D, Johto A-B, Hoitohenkilökunta A, B, Hoitotekniikka A)

”*Se on ehkä vakavin ja vaikein tilanne, jos potilastietoa on taustalla muokattu eikä mikään tuo herätettä, sitä ei huomata ja toiminta jatkuu normaalisti.”* – Tietohallinto B

Erittäin haastavana skenaariona haastateltavat pitivät tilannetta, jossa kyberhyökkäystä ei huomattaisi, mutta vahinkoa tapahtuisi koko ajan. Tällainen tilanne voisi olla esimerkiksi sellainen, jossa hyökkääjä muuttaisi potilaiden hoidolle tärkeää tietoa, kuten veriryhmätietoja tai lääkeaineallergioita. Muuttuneiden tietojen havaitseminen muutoin normaalisti toimivassa järjestelmässä olisi äärimmäisen haastavaa, mutta kriittisten tietojen muuttumisella voisi olla erittäin vakavia, potilaiden henkiäkin uhkaavia seurauksia. Lisäksi vaarallisia seurauksia olisi sillä, jos hyökkääjä onnistuisi etäohjaamaan lääketieteellisiä laitteita. (Tietohallinto B, Hoitohenkilökunta B, D, E, Hoitotekniikka A) Erittäin pahoja seurauksia saatettaisiin kohdata myös silloin, jos hyökkäys tapahtuisi samanaikaisesti toisen kriisin, esimerkiksi suuronnettomuuden tai kanssa. Tällöin kiireellistä toimintaa olisi jo valmiiksi paljon suhteessa organisaation hoitokapasiteettiin. (Hoitohenkilökunta B, D)

Muutamassa haastatteluissa nousi kyberhyökkäyksen mahdollisena seurauksena esiin myös siitä aiheutuvat ylimääräiset kustannukset, joita voi aiheutua esimerkiksi lisähenkilöstön tarpeesta, hajonneiden järjestelmien tai laitteiden korvauskustannuksista tai tietosuojarikkomuksista seuraavista sakoista. Taloudelliset haitat ovat luonteeltaan hitaampia ja niitä pohditaankin todennäköisesti vasta akuutin tilanteen ollessa jo ohi. (Tietohallinto A-B, Hoitohenkilökunta A, Hoitotekniikka A)

## 5.2 Toiminta kyberhyökkäystilanteessa

Tässä alaluvussa esitellään haastattelujen perusteella muodostettua kuvaa organisaation toiminnasta kyberhyökkäyksen aikana. Sanallisen selityksen tukena käytetään prosessikaaviota, joilla kuvataan eri toimijoiden toimintaa tilanteen aikana. Prosessikaavio on pilkottu alalukujen aiheiden mukaisesti osiin tekstin joukkoon. Kaikista prosessikaaviokuvista muodostuvaa kokonaiskuvaa voi tarkastella liitteessä 1.

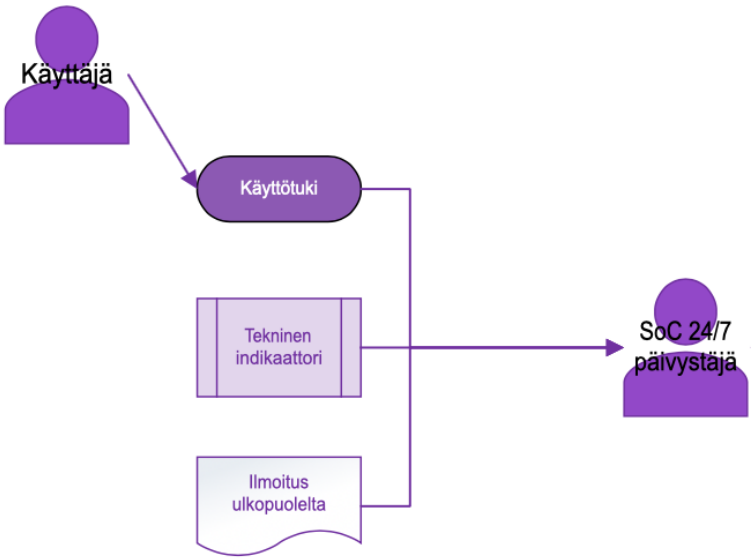
Vaikka haastateltavat tunnistivat edellisessä alaluvussa useita erilaisia harvinaisempiakin hyökkäysskenaarioita, perustuivat heidän vastauksensa varautumiseen liittyviin kysymyksiin pääasiassa yleisimpiin skenaarioihin, kuten siihen, ettei järjestelmiä tai laitteita voisi käyttää. Harvinaisempiin skenaarioihin liittyviä varautumistoimia ei juurikaan noussut esiin. Tarvetta varautua myös harvinaisempiin hyökkäysskenaarioihin käsitellään tarkemmin luvussa 7.

### 5.2.1 Hyökkäyksen havaitseminen

Reagointi kyberhyökkäykseen alkaa hyökkäyksen havaitsemisesta. Kaikki havaitsemistapaukset johtavat lopulta siihen, että kohdeorganisaation IT-palveluntarjoajalla työvuorossa kyseisellä ajanhetkellä oleva päivystysvastaava saa tiedon hyökkäyksestä. Päivystysvuorossa on aina joku, ympäri vuorokauden. Hyökkäyksen havaitseminen voi tapahtua muutamalla erilaisella tavalla. Joskus havainto tehdään tietojärjestelmiin rakennettujen teknisten indikaattorien, eli herätteiden, tai esimerkiksi palomuurin avulla. Näissä tapauksissa indikaation huomaa ensimmäisenä IT-kumppanin päivystysvuorolainen, joka käynnistää tarvittavat toimet hyökkäykseen reagoimiseksi. (Tietohallinto A-D) Tieto voi tulla myös kokonaan organisaation ulkopuolelta, esimerkiksi kyberturvallisuuskeskukselta tai muilta viranomaisilta, jotka ovat havainneet jotakin epäilyttävää, kuten internetiin vuodettuja tietoja. Tieto voi tulla esimerkiksi toisilta samalla alalla toimivilta organisaatioilta, joihin on kohdistunut hyökkäys samanaikaisesti. (Tietohallinto A, D)

Kyberhyökkäys voidaan havaita myös organisaation omien työntekijöiden ja tietotekniikan käyttäjien toimesta. Käyttäjä voi tällöin esimerkiksi havaita käyttämänsä tietokoneen

hidastuvan, hajoavan tai toimivan muuten epänormaalisti. Hän ottaa yhteyttä organisaation IT-kumppanin hallinnoimaan käyttötukeen, jossa vuorossa olevalla valvojalla on selkeä prosessi siihen, mitä seuraavaksi tehdään. (Tietohallinto A-D) Hän myös viestii asiasta eteenpäin tietohallinnolle. Käyttötukimenettelyn pitäisi olla tiedossa kaikilla työntekijöillä (Tietohallinto B, C). Käyttäjä ei tällöin kuitenkaan välttämättä ymmärrä havainneensa kyberhyökkäystä, joten tilanteen luonteen selvittäminen voi viedä aikaa (Tietohallinto C). Erilaiset kyberhyökkäyksen havaitsemismenetelmät kuvataan kuvassa 2.

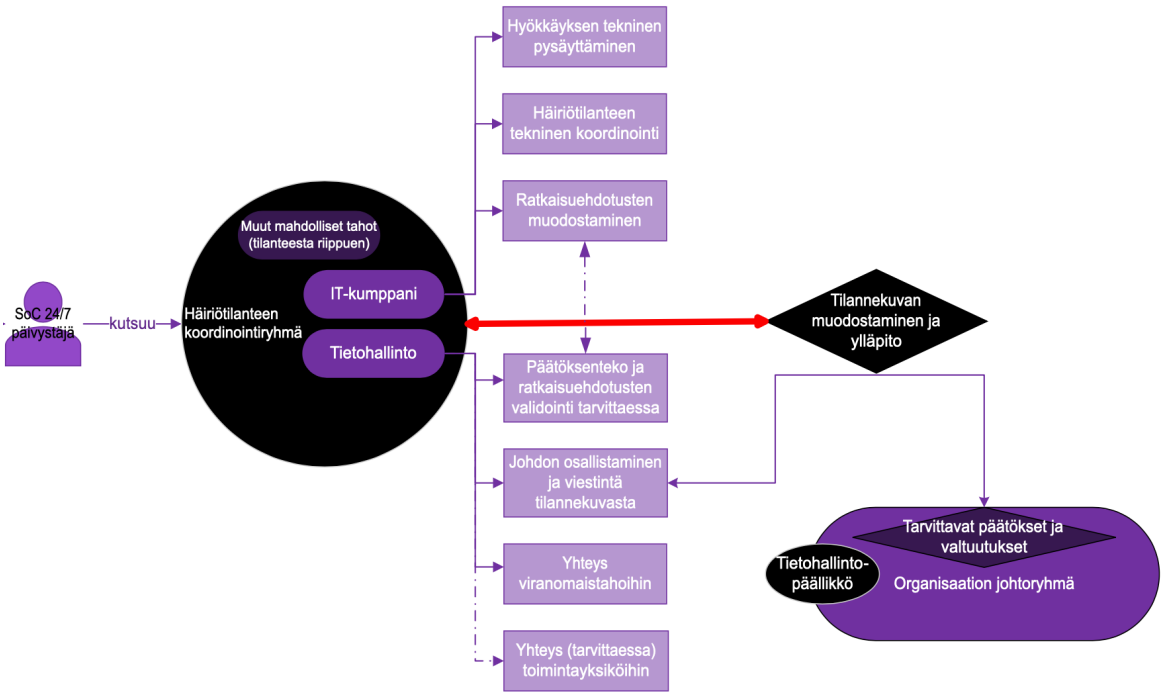



***Kuva 2.*** *Hyökkäyksen havaitsemismenetelmät*

Tietohallinnon haastateltavan mukaan kyberhyökkäyksen havaitseminen voi olla paljon haastavampaa, mikäli hyökkääjän tarkoituksena on pysyä huomaamattomana esimerkiksi tietoja muutellakseen. Tällaisissa tilanteissa hyökkäyksen havaitseminen voi olla huomattavasti hankalampaa. Teknisiä indikaattoreita on pyritty rakentamaan siten, että tunkeutuminen huomataan aina, mutta havaitsemisen kannalta pahimpana skenaariona haastatteluissa tunnistettiin tilanne, jossa hyökkäys havaittaisiin vasta, kun virheellisen tiedon perusteella on jo toimittu. (Tietohallinto B) Tällöin ensimmäisenä havaittaisiin virhe hoidossa, jonka jälkeen ehkä ymmärrettäisiin järjestelmästä löytyneen virheellistä tietoa. Vielä tässäkin vaiheessa voi olla pitkä matka siihen, että ymmärretään, että tietoa on muuteltu rikollisen toiminnan seurauksena. Havainnon tekeminen vaatii havaitsijalta pohjaymmärrystä siitä, että tällaisen rikoksen mahdollisuus on olemassa.

### 5.2.2 Häiriötilanteen koordinointiryhmä ja tietohallinnon toiminta

Kohdeorganisaatiolla ja sen IT-palveluntarjoajalla on käytössään yleinen hallintamalli ja -prosessit kaikkiin organisaation tietojärjestelmiä koskeviin häiriötilanteisiin. Kun on havaittu, että tietojärjestelmiin kohdistuu mikä tahansa laajempi häiriötilanne, kuten järjestelmän yllättävä hajoaminen tai kyberhyökkäys, kutsutaan koolle häiriötilanteen koordinointiryhmä, jonka toimintaa kuvataan kuvassa 3. Ryhmän koordinoinnista vastaa kohdeorganisaation IT-palveluntarjoajan vuorossa oleva päivystysvastaava, joka kutsuu ryhmän koolle saatuaan tiedon hyökkäyksestä. Koordinointiryhmään kutsutaan vastuuhenkilöitä ja asiantuntijoita sekä palveluntarjoajalta ja terveydenhuolto-organisaation tietohallinnosta. Ryhmään kuuluu muutamia vakiohenkilöitä, mutta jokaisen häiriötilanteen alussa arvioidaan myös sitä, onko myös joitakin muita erityisasiantuntijoita syytä kutsua mukaan. Mikäli häiriö kohdistuu esimerkiksi HR-järjestelmään, kutsutaan tällöin mukaan asiantuntijoita, joilla on asiantuntemusta tältä alueelta. (Tietohallinto B) Koordinointiryhmä toimii keskeisenä komentokeskuksena koko häiriötilanteen ajan, sen havaitsemisesta siihen asti, kun toiminta on palautunut kokonaan normaaliksi. (Tietohallinto A-D)




***Kuva 3.*** *Häiriötilanteen koordinointiryhmä kyberhyökkäystilanteessa*

Koordinointiryhmässä olevat IT-kumppanin henkilöt vastaavat häiriötilanteen teknisestä koordinoimisesta sekä ratkaisuehdotusten valmistelusta ja välittämisestä terveydenhuolto-organisaatiolle. Terveydenhuolto-organisaation tietohallinnon edustajat vastaavat viestinnästä ja päätöksenteon koordinoinnista organisaation johdon kanssa. Tietohallinto

voi myös tehdä matalamman tason päätöksiä, mutta kun tietohallinto tunnistaa, että tilanne alkaa vaikuttaa hoitotoimintaan ja potilasturvallisuuteen, johtoryhmä otetaan mukaan vastaamaan päätöksenteosta. Tietohallinto viestii johdolta tulevia ohjeita jälleen koordinointiryhmälle. Tietohallinnon johtaja toimii tärkeänä linkkinä tietohallinnon ja johtoryhmän välillä. (Tietohallinto A-D) Joskus koordinointiryhmän jäsenet viestivät myös suoraa yksittäisille toimintayksiköille, mikäli hyökkäystilanne vaatii juuri heiltä joitakin tiettyjä toimenpiteitä. Koordinointiryhmän vastuulle kuuluu myös viestintä muutamille viranomaistahoille: tietosuojavaltuutetulle, Valviralle ja kyberturvallisuuskeskukseen, joista viimeisin voi myös tukea kohdeorganisaatiota hyökkäykseen vastaamisessa (Tietohallinto A).

Selvän, reaaliaikaisen ja kattavan tilannekuvan muodostaminen, ylläpitäminen ja sen viestintä eteenpäin on yksi koordinaatioryhmän keskeisimmistä tehtävistä häiriötilanteen hallinnassa (Tietohallinto A-D). Tilannekuvan muodostamisessa hyödynnetään automatiikkaa ja teknologiaa, mutta se voi vaatia myös manuaalista soittelua ja selvitystä siitä, miltä tilanne näyttää eri puolilla organisaatiota (Tietohallinto D). Organisaatio on suuri, järjestelmiä ja laitteita on valtavasti ja monet niistä ovat kriittisiä hoidon jatkumisen kannalta. Tästä syystä tietohallinnon on tunnistettava juuri ne toiminnot, jotka ovat häiriintyneet, jotta korjaavat toimet saadaan kohdistettua oikein. (Tietohallinto A-D) Erityisesti johtavissa asemissa toimivat henkilöt sekä tietohallinnossa, hoitotoiminnassa, että koko organisaation johdossa korostivat sitä, miten tärkeää päätöksenteon kannalta on, että he saavat selkeän kuvauksen siitä, missä, mihin ja miten hyökkäys vaikuttaa (Tietohallinto A-D, Johto B, Hoitohenkilökunta B, C, E). Tietohallinto ja johto tarvitsevat tilannekuvaa, jotta he ymmärtävät mitä kaikkia organisaation osia tilanne koskee ja mitä erilaisia päätöksiä heidän on tehtävä. Hoitohenkilökunnan taas on tiedettävä nopeasti, mitä tehtäviään he eivät voi suorittaa normaalisti, jotta he voivat ottaa juuri oikeat korvaavat toimintatavat käyttöön. (Tietohallinto A, D, Johto A-B, Hoitohenkilökunta B, C, E, F, Hoitotekniikka A)

Haastateltavien mukaan koordinointiryhmän toiminta on sujuvaa ja kokemuksen kautta toimivaksi hioutunutta. Toimintaa on harjoiteltu useita kertoja sekä tositilanteissa että kriisitilanneharjoituksissa. Useamman haastateltavan mukaan on etu, että erilaisissa ongelmatilanteissa käytetään samaa toimintatapaa, sillä niissä vaaditaan nopeita päätöksiä ja toimivaa yhteistyötä. Haasteita koordinointiryhmän toiminnalle voisi aiheutua esimerkiksi silloin, jos ryhmän normaaliin toimintatapaan käytettävät viestintäteknologiat eivät olisi käytettävissä, mutta haastateltavat luottivat siihen, että asiat saataisiin hoidettua tarvittaessa myös puhelimitse tai viranomaisverkkoyhteyttä käyttäen. (Tietohallinto A-D)

### 5.2.3 Hyökkäykseen reagointi

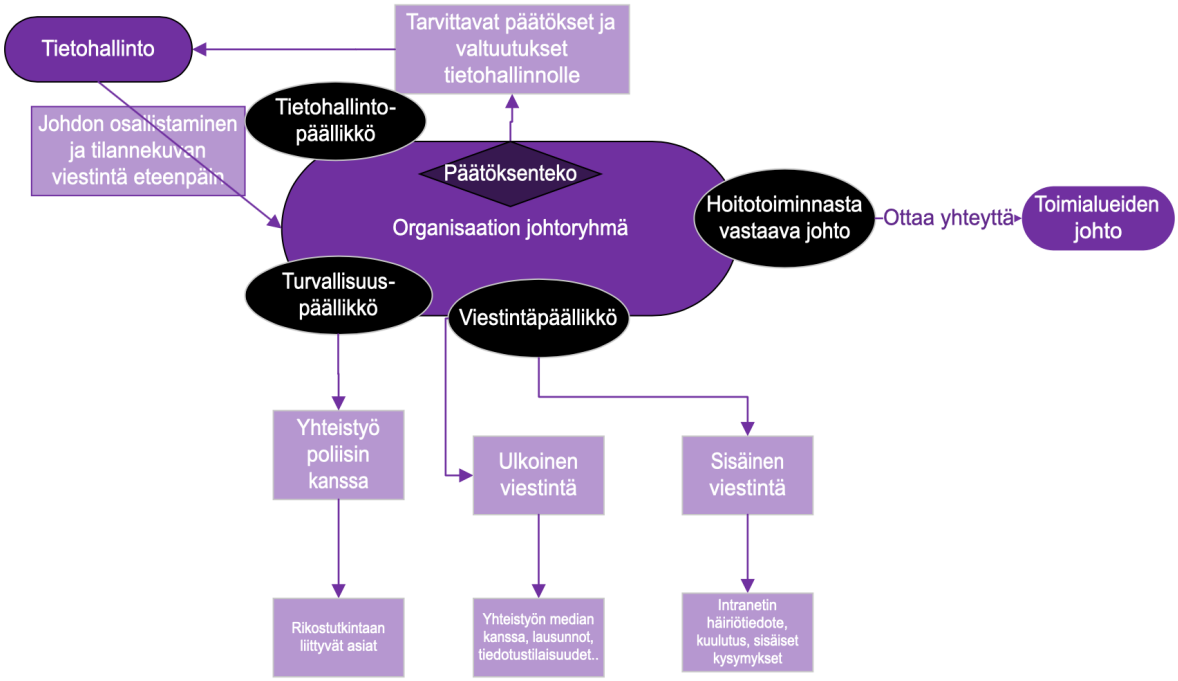
Kun hyökkäys organisaatiota kohtaan on käynnissä, on tietenkin huolehdittava siitä, että se saadaan mahdollisimman nopeasti keskeytettyä ja hyökkääjä pysäytettyä. Kyberhyökkäykseen reagoinnin suunnittelusta vastaa organisaation IT-yhteistyökumppani, kuten edellisen alaluvun kuvassa 3 kuvattiin. IT-kumppani tuntee organisaation infrastruktuurin todella hyvin. Päivystysvuorossa oleva henkilö kokoaa IT-kumppanin organisaatiosta nopeasti yhteen ihmiset, jotka tuntevat hyökkäyksen kohteena olevan teknologian parhaiten. He valmistelevat teknisen asiantuntijuutensa avulla ratkaisuehdotukset, jotka he esittelevät kohdeorganisaation tietohallinnolle. Mahdollisia ratkaisumalleja voivat olla esimerkiksi tiettyjen järjestelmien tai laitteiden sulkeminen tai poistaminen verkkoyhteydestä. Mikäli ratkaisumallit vaikuttavat potilashoitoon, tietohallinto välittää IT-kumppanin esittämät ratkaisuehdotukset johdolle, joka viime kädessä päättää niiden käyttöönotosta. (Tietohallinto A-D)

”*It-kumppani esimerkiksi ehdottaa, että eristetään joku kone kokonaan käytöstä, mutta se tarkoittaa sitten, että tämä ja tämä asia lakkaa toimimasta hoitotoiminnassa. Jos se vaikuttaa potilasturvallisuuteen, niin johto tekee siitä päätöksen, että otetaanko tällainen varautumiskeino käyttöön vai ei.”* – Tietohallinto A

Haastateltavien mukaan ratkaisuiden valmistelussa on erittäin olennaista ymmärtää, miten ratkaisut vaikuttavat toisaalta käynnissä olevaan kyberhyökkäykseen, mutta toisaalta myös hoitotoiminnan jatkumiseen. Tilanne vaatii tasapainottelua kyberhyökkäyksen tehokkaan pysäyttämisen ja hoitotoiminnan varmistamisen välillä. Jo aiemmin käsiteltyyn hyökkäystilanteen tilannekuvan ja hyökkäyksen kokonaisvaikutusten ymmärtämiseen yhdistyy siis myös ratkaisuehdotusten vaikutusten kokonaisvaltainen ymmärtäminen. (Tietohallinto A, B, D) Organisaatio on valtava, laitteita ja järjestelmiä on valtavasti ja jokainen käytöstä poistettava elementti voi aiheuttaa haasteita potilaiden hoidossa ja sitä kautta jopa potilasturvallisuusriskejä, joten vaikutukset on arvioitava tarkkaan. Usein ei ole järkevää poistaa käytöstä varmuuden vuoksi liikaa järjestelmiä tai laitteita, joten on tärkeää kohdistaa korjaavat toimenpiteet sinne, missä niitä todella tarvitaan. (Tietohallinto A-D, Johto B) Jotkut hoitohenkilökunnan haastateltavat nostivat kuitenkin haasteeksi sen, että vaikka IT-kumppani tuntee organisaation infrastruktuurin hyvin, eivät he tai välttämättä tietohallinto tai johtokaan tunne hoitotoimintaa niin hyvin, että ymmärtäisivät aina mahdollisten ratkaisuiden todelliset vaikutukset hoitotoimintaan. (Hoitohenkilökunta B, C, Hoitotekniikka A) On esimerkiksi täysin mahdoton ajatus, että potilaissa kiinni olevia laitteita lähdettäisiin sulkemaan varotoimenpiteenä, sillä varalaitteita ei yleensä ole (Hoitotekniikka A).

### 5.2.4 Johtaminen ja viestintä

Kun organisaation johto on saanut häiriötilanteen koordinointiryhmän ja tietohallinnon kautta tiedon kyberhyökkäyksestä ja sen vaikutuksista, on sen tehtävänä ottaa haltuun organisaation toiminnan kokonaiskuva sekä huolehtia koko organisaation laajuisesta päätöksenteosta ja viestinnästä. Kyberhyökkäyksen vaikutukset voivat ulottua kaikkialle organisaatioon ja johdon tehtävänä on huolehtia edellytyksistä sille, että toiminta voi jatkua niin sujuvasti kuin mahdollista. Johdon tehtävänä on myös varmistaa, että kaikilla organisaatiossa on tarvittavat ohjeet toiminnan tueksi. (Tietohallinto C-D, Johto A-B) Johdon keskeisimmät vastuut kyberhyökkäystilanteen aikana on esitettynä kuvassa 4.




***Kuva 4.*** *Johtoryhmän toiminta kyberhyökkäystilanteessa*

Johtoryhmän toimintaa ohjataan samaan tapaan kuin tietohallinnon ja IT-kumppanin koordinaatioryhmää. Johtoryhmän jäsenet kutsutaan nopeasti tilannepalaveriin, jossa käydään läpi tietohallinnolta saatavia tilannetietoja, päätetään jatkotoimista ja jaetaan vastuita. (Tietohallinto C-D, Johto A-B) Toiminnan onnistumisen kannalta on hyvin tärkeää, että tietohallinto toimittaa tilannekuvatietoa johdolle riittävän nopeasti ja johdon henkilöille ymmärrettävässä muodossa, sillä heidän on viestittävä tilanteesta heti eteenpäin. (Johto A) Tässä tehtävässä tärkeä rooli on tietohallintopäälliköllä, joka toimii tietohallinnon ja johtoryhmän välisenä linkkinä.

”*Ruvettaisiin heti miettimään sen asian viestintää ja vaikutuksia. Tällaisessa tilanteessa tulee nopeasti vaikutuksia, jotka vaikuttavat potilaiden hoitoon ja se on ykkösasia joka johtaa ulkoiseen viestintään ja myös henkilöstöviestintään*” – Johto A

Kuten kuvasta 4 nähdään, johdon vastuut sisältävät paljon viestintää eri suuntiin ja kommunikaation merkitys kriisitilanteessa korostuu. Tärkeä osa kyberhyökkäystilanteen hallintaa on muun muassa organisaation sisäinen viestintä tilanteesta ja toimista, joita se mahdollisesti vaatii henkilöstöltä. Viestinnän suunnittelusta ja toteutuksesta vastaa viestintäosasto viestintäpäällikön johdolla. Organisaation henkilöstöä voidaan ensikädessä informoida hyökkäyksestä eri tavoilla. Viestintään käytettäviä väyliä ovat esimerkiksi intranet, sähköposti, hätäilmoitukset, viranomaisverkkoyhteys ja suurimman osan organisaation hoitotyöskentelytiloista saavuttava keskusradio. (Johto A) Toimintatavoista eri toimialueilla ja hoitoyksiköissä vastaavat ja viestivät ensisijaisesti näiden yksiköiden johto ja henkilöstön esimiehet. (Johto A, Hoitohenkilökunta A-G, Hoitotekniikka A)

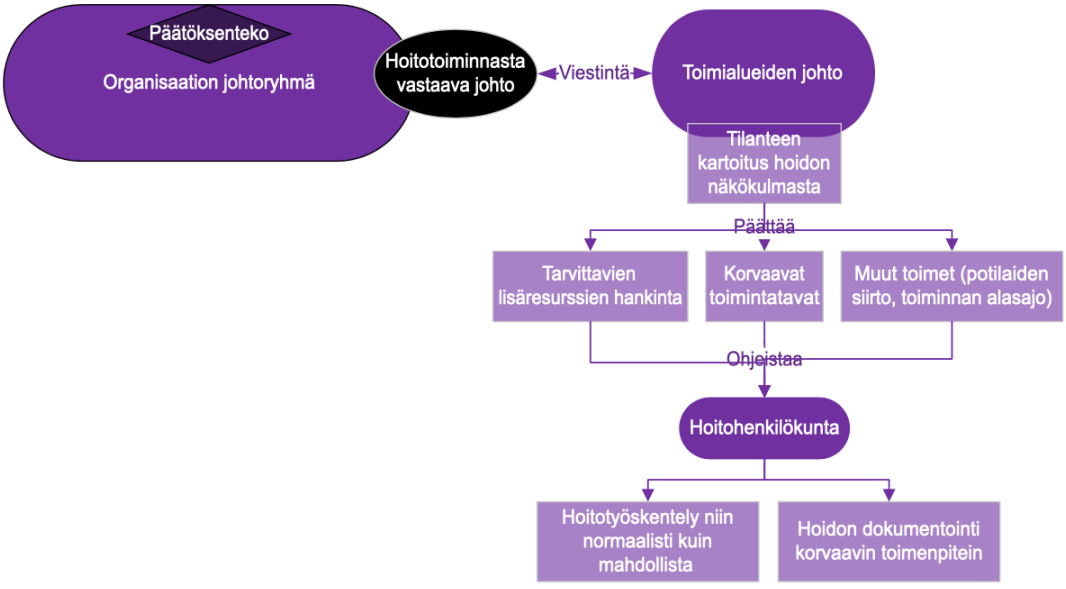
Koska kyseessä on julkinen organisaatio, joka vastaa merkittävästä osasta oman alueensa terveyspalveluita ja kyseessä on rikostilanne, on olennainen osa viestintää myös viestiminen ulospäin, esimerkiksi poliisille ja medialle. Poliisin kanssa viestimisestä vastaa organisaation turvallisuuspäällikkö ja turvallisuusosasto. Kyberhyökkäystilanteet ovat aina rikoksia, joten niihin liittyy rikostutkinta, jossa turvallisuusosasto toimii johdon ja poliisin välisenä linkkinä. (Johto B) Median kanssa viestinnästä vastaa puolestaan organisaation viestintäosasto viestintäpäällikön johdolla. Medialle puhuvat henkilöt on määritelty tarkasti. Yksi hyväksi koettu tapa toteuttaa viestintää kriisitilanteen aikana on tiedotustilaisuudet, sillä ilmoittamalla etukäteen tiedotustilanteen ajankohdasta saadaan toisaalta rauhoitettua yleisö tiedolla siitä, että lisätietoa saadaan pian, ja toisaalta saadaan itselle aikaa valmistella hyvin jäsennelty tiedonanto. (Johto A) Haastateltavien mukaan on erittäin tärkeää, että viestimisvastuu eri suuntiin on määritelty tarkasti, jolloin tilanteen ollessa käynnissä ei anneta ulospäin harkitsemattomia, puutteellisia tai keskenään ristiriitaisia lausuntoja. Median kanssa yhteistyössä tehtävästä kriisiviestinnästä saatiin paljon harjoitusta Covid19-tilanteen aikana. (Johto A-B)

Haastattelujen perusteella vaikutti siltä, että viestintävastuut olivat suhteellisen selviä kaikille ja esimerkiksi hoitohenkilökunta tiesi, ettei heidän kuulu kommentoida asioita ulospäin. Pieniä epäselvyyksiä vaikutti kuitenkin olevan siinä, kuka vastaa henkilöstöltä tilanteen aikana tuleviin kysymyksiin. Tietohallinnon mukaan kysymyksiin vastaa viestintäosasto, kun taas johdossa ajateltiin, että niihin vastaa tietohallinto itse. (Tietohallinto C, Johto A-B) Tämä haaste näkyi myös siinä, että jotkut haastateltavat hoitohenkilöstöstä kokivat, että heidän voi olla todella vaikeaa saada vastauksia kysymyksiinsä häiriötilanteiden aikana (Hoitohenkilökunta A-B). Tätä haastetta käsitellään tarkemmin alaluvussa

6.3. Toisena kriisitilanteen johtamisen ja viestinnän haasteena tunnistettiin se, että eri puolilla organisaatiota johtohenkilöstö on pääsääntöisesti poissa viikonloppuisin ja toimistoaikojen ulkopuolella. Jokaisen työntekijän pitäisi aina tietää, kuka johtaa heitä missäkin tilanteessa, mutta myös miten toimia, jos he ovat yksin paikalla kriisitilanteen käynnistyessä. Virka-ajan ulkopuolella tässä saattaa olla puutteita. (Hoitohenkilökunta A)

### 5.2.5 Hoitotoiminnan jatkuvuuden varmistaminen

Kaikkein aikakriittisimmät kyberhyökkäyksen mahdolliset seuraukset liittyvät potilasturvallisuuteen ja hoidon jatkuvuuteen. Tutkittava terveydenhuolto-organisaatio on jatkuvasti vastuussa ihmishengistä, joten toiminnan on voitava jatkua tilanteesta riippumatta. Hoitotoiminta ei aina voi odottaa järjestelmien tai laitteiden heräämistä, vaan esimerkiksi leikkauspöydällä tai synnytyssalissa hoidon on jatkuttava kyberhyökkäyksestä riippumatta. Siksi on tärkeää, että organisaatiolla on jokaista poikkeustilannetta varten toimintatavat, joiden mukaisesti jatkaa hoitotoimintaa. Seuraavaksi kuvataan korvaavia toimintamalleja, jotka käynnistyisivät organisaatiossa kyberhyökkäyksen tapahtuessa haastateltavien tämänhetkisen tietämyksen mukaisesti. Käytössä olevista ohjeistuksista kerrotaan lisää luvussa 5.3. Hoitotoiminnan keskeisimmät vastuut on kuvattu kuvassa 5. On kuitenkin tärkeää ymmärtää, että hoitotoimintaa on monenlaista ja eri yksiköiden toiminnassa on omat erityispiirteensä. Näin ollen hyökkäystilanteessa käyttöönotettavat toimenpiteet voivat vaihdella yksiköiden välillä hyvin paljon, eikä kaikista yksiköistä haastateltu ihmisiä. Tässä alaluvussa keskitytään erityisesti sellaisiin hyökkäystilanteisiin, jotka vaativat hoitotoiminnan mukauttamista tietojärjestelmien epänormaaliin toimintaan.




***Kuva 5.*** *Hoitotoiminnan vastuut kyberhyökkäystilanteessa*

Hoitotoiminnan hyökkäystilanteen toiminnassa on olennaista ymmärtää, että hoitohenkilökunta ei pyri korjaamaan kyberhyökkäystilannetta, vaan he keskittyvät vain ja ainoastaan potilaiden hoitoon. Haastateltavat korostivat sitä, että hoitohenkilökunta luottaa tietohallintoon ja siihen, että näillä on tilanteen ratkominen hallussa (Hoitohenkilökunta D, Hoitotekniikka A). Hoidon toiminnan kannalta olennaista on tietää, mitkä osat hoitoprosesseista ei toimi normaalilla tavalla, jolloin näiden toimintojen kohdalla siirrytään suunnitelman mukaisiin korvaaviin toimintatapoihin. Muutoin hoitoa jatketaan niin normaalisti kuin suinkin mahdollista. Suuri osa hoidosta on myös manuaalisesti käsillä tehtävää työtä, johon kyberhyökkäys ei vaikuta. (Hoitohenkilökunta A-G, Hoitotekniikka A) Hoitohenkilökunta voi huomata käynnissä olevan hyökkäyksen monin tavoin. Kaikki eivät välttämättä saa tietoa ensin, vaan ensimmäinen asia, jonka he havaitsevat on toimimattomat järjestelmät. (Hoitotoiminta F) Tämän jälkeen heitä informoi heidän omassa yksikössään toimivat esimiehet, jotka saavat tiedon organisaation johdolta, intranetistä tai muiden hoitotoiminnan johtajien kautta. Hoitotoimintaa koordinoivat johtajat kommunikoivat tietohallinnon ja johdon kanssa, sekä päättävät korvaavien toimintatapojen käyttöönotosta ja siitä, miten hoitotoimintaa jatketaan. (Johto A-B, Hoitohenkilökunta B, C, D, E, F) Mikäli hyökkäyksestä saadaan jonkinlainen varoitus etukäteen, silloin tulostetaan kaikki tieto paikalla olevista potilaista, jos mahdollista (Hoitohenkilökunta B).

Merkittävin kyberhyökkäyksen vaikutus hoitotoiminnan toteuttamiseen seuraa siitä, kun hoitoon tarvittavia tietojärjestelmiä ei voida käyttää normaalisti. Tietojärjestelmät ovat läsnä lähes kaikessa hoitotoiminnassa ja niihin kirjataan kaikki mitä potilaille tehdään ja mitä heidän kanssaan puhutaan. Kaikki tämä on tehtävä toisin, kun järjestelmät eivät toimi. Suurin tapahtuva muutos onkin paperikirjaukseen siirtyminen, jolloin kaikki, mikä normaalisti kirjataan tietokoneelle, kirjataan paperille. Haastateltavien mukaan kaikilla osastoilla on olemassa prosessit siihen, mitkä tiedot kirjataan ja miten. Paperikirjaukseen siirrytään nopeasti ja kaikkien pitäisi osata käyttää sitä. Samaa menettelyä käytetään myös käyttökatkojen aikana. Joillakin osastoilla tarvittavat paperipohjat ovat jopa valmiiksi tulostettuina ja pakattuina sellaisten tilanteiden varalta, joissa tietojärjestelmät ovat poissa pelistä. Hyökkäyksen tapahtuessa toiminta siirtyy siis kokonaan paperin ja kynän varaan, ja toiminnan koordinoinnissa hyödynnetään esimerkiksi tussitauluja. Koska tieto potilaista ei nyt siirry automaattisesti osastolta ja henkilöltä toiselle, paperit siirtyvät hoidettavien potilaiden mukana. (Hoitohenkilökunta A-G, Hoitotekniikka A) On myös tärkeää, että hoitohenkilöstö vaihtaa keskenään tietoa suullisesti, kun kaikkea ei näe suoraan järjestelmistä. Tämä on erityisen tärkeää työvuorojen vaihtuessa, jolloin saapuvalla henkilöstöllä on normaalia huonompi näkyvyys siihen, ketä talossa on ja ketkä vaativat välitöntä huomiota. (Hoitohenkilökunta D) Osa hoidossa kerättävästä tiedosta kerätään

lääkintälaitteiden avulla suoraan sähköiseen muotoon. Tämä on mahdollista myös ilman verkkoyhteyksiä ja tietojärjestelmiä, niin kauan kuin laitteet itsessään toimivat. Tieto voidaan kerätä laitteista esimerkiksi laitteiden muistiin tai DVD-levyille. Tällöin tietoa tarvitsevat lääkärit tulkitsevat niitä suoraa laitteiden näytöltä tai DVD-levyiltä. (Hoitohenkilökunta C, Hoitotekniikka A)

Paperikirjausjärjestelmä on hyvin hallussa oleva prosessi, mutta sen suurin ongelma on, että se on tietojärjestelmien käyttöä huomattavasti työläämpi vaihtoehto. Papereiden täyttäminen on hidasta, mikä voi aiheuttaa kiirettä ja toiminnan ruuhkautumista, ja myös virheiden riski kasvaa. (Hoitohenkilökunta A-G, Hoitotekniikka A) Kiirettä aiheuttaa myös monien tietojärjestelmien avulla suoritettavien työvaiheiden puuttuminen. Joillakin osastoilla kaikkiin potilaisiin on kiinnitetty automaattisia valvontalaitteita, joita hoitohenkilö voi keskitetysti seurata valvomohuoneesta. Mikäli nämä järjestelmät eivät toimi, näitä tietoja ei saada näkyville. Tämä taas tarkoittaa, että hoitohenkilökunnan on käytävä jokaisessa huoneessa tasaisin väliajoin tarkastamassa kunkin potilaan tilanne. (Hoitohenkilökunta F-G) Samankaltaisia haasteita aiheutuu myös siitä, että hoitotoiminnan eri vaiheista vastaavat osastot eivät voi jakaa verkon välityksellä tietoa, kuten esimerkiksi tutkimustuloksia tai lausuntoja. Molemmista tilanteista seuraa haastateltavien mukaan paljon kiirettä ja juoksevia ihmisiä rakennusten käytävillä. (Johto A-B, Hoitohenkilökunta A-G, Hoitotekniikka A)

Useampi haastateltava mainitsi, että kriisitilanteen käynnistyessä koko hoitotoimintayksikön hoitokapasiteetti voi laskea, muun muassa yllä mainittujen lisätöiden takia. Tällöin joidenkin yksiköiden on mahdollista ajaa alas joitakin toimintoja, esimerkiksi ajanvarauksilla tapahtuvaa elektiivistä toimintaa. Tällöin töissä oleva henkilöstö siirtyy hoitotoiminnan kriittisiin pisteisiin ja keskittyy hoitamaan niitä potilaita, jotka on hoidettava heti. (Tietohallinto C, Johto A-B, Hoitohenkilökunta C, E) Kaikilla hoitoa tekevillä yksilöillä ei kuitenkaan ole ollenkaan elektiivistä toimintaa ja kaikki yksikön hoitoon saapuvat potilaat on hoidettava kiireellisesti. Tästä voi aiheutua merkittävää kiirettä ja ruuhkautumista. (Hoitohenkilökunta F) Tilanteen pitkittyessä myös elektiivisen toiminnan siirtämisestä voi aiheutua potilasturvallisuusriskejä hoidon viivästyessä ja ei-kiireellisten tilanteiden muuttuessa kiireellisiksi (Johto A, Hoitohenkilökunta E).

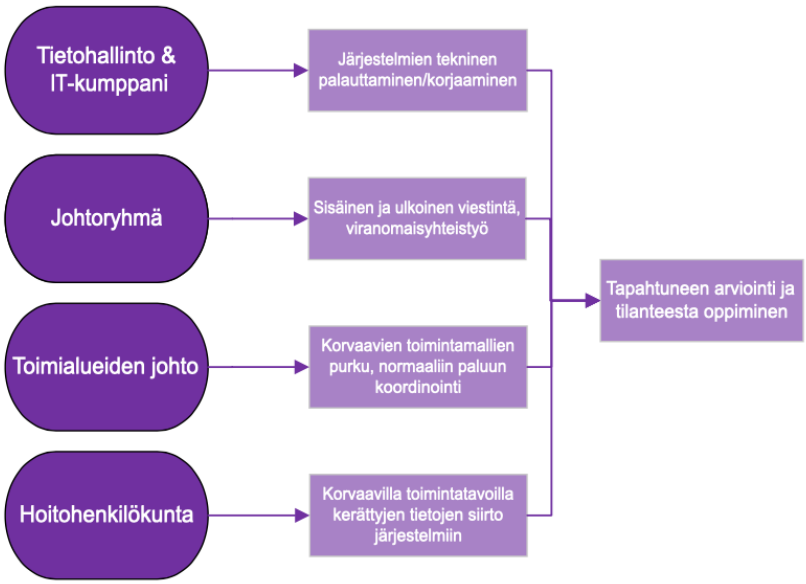
Yhtenä keinona kiireen helpottamiseen nousi haastatteluissa esiin lisähenkilöstön kutsuminen töihin. Joissain yksiköissä tätä pidettiin tarpeellisena, sillä esimerkiksi kasvanut kirjauskuorma tai automaattisen valvonnan puute voi aiheuttaa tarvetta lisäkäsille. Lisähenkilöstön kutsuminen tulisi suorittaa vuorossa olevan esimiehen toimesta heti, joskin se voisi olla hieman haastavaa, mikäli siihen tarvittavat tietojärjestelmät eivät jostakin

syystä olisi toiminnassa. (Tietohallinto C, Johto A-B, Hoitohenkilökunta A, C, D, F) Toinen useamman haastateltavan esiin nostama mahdollinen keino kiireen purkamiseen ja potilaiden hoidon varmistamiseen on myös potilaiden siirto toisiin hoitopaikkoihin. Tällöin potilaat vietäisiin sairaskuljetuksen avulla esimerkiksi toisen paikkakunnan sairaalaan, jossa heidän hoitonsa pystyttäisiin järjestämään paremmin. (Tietohallinto A-B, Johto A, Hoitohenkilökunta B, F) Akuuttien potilaiden siirtämiseen liittyy kuitenkin monesti myös riskejä, joten siirtäminen ei välttämättä aina ole mahdollista (Hoitohenkilökunta F)

Eräs hoitohenkilökunnan haastattelujen aikana tehty havainto korvaavista toimenpiteistä oli se, että korvaavat toimenpiteet ovat usein paluuta aikaan ennen tietojärjestelmiä. Moni pidempään työskennellyt haastateltava kertoi, että he ovat työskennelleet uransa aikana vuosia juuri sillä tavalla, jolla kyberhyökkäystilanteessakin toimittaisiin. Vastauksissa korostui, että potilaita on hoidettu jo pitkään ennen tietojärjestelmiäkin, joten hoitotoimet osataan kyllä hoitaa. (Hoitohenkilökunta A-B, E-G, Hoitotekniikka A) Korvaavat toimintatavat ovat siis erityisen hyvin hallussa erityisesti kokeneemmalla hoitohenkilökunnalla, mutta haastatteluissa ei noussut esiin viitteitä siitäkään, että nuoremman henkilöstön taidoissa olisi puutteita kokemuksen takia. Koulutustoiminnan tunteva haastateltava kuitenkin totesi, että on silti mahdollista, että organisaatiossa on sellaista henkilöstöä, joka ei ole koskaan käyttänyt paperikirjausta käytännössä tai harjoitustilanteissa (Hoitohenkilökunta A).

### 5.2.6 Hyökkäyksestä palautuminen

Kun hyökkäyksen akuutein vaihe on ohi ja hyökkääjä on saatu pysäytettyä, on organisaatiolla vielä paljon tehtävää ennen paluuta normaaliin työskentelyyn. Järjestelmiä ja laitteita on saatettu poistaa käytöstä ja hoitotoiminta pyörii tilapäisillä toimintatavoilla. Palautumisen onnistumiseen ja suoraviivaisuuteen vaikuttavat esimerkiksi hyökkäyksen tyyppi, sen aikana menetetyt tiedot ja toiminta, aiemmin tehty varmuuskopiointi ja hyökkäyksen aikainen toiminta. Haastateltavien mukaan myös hyökkäyksen kesto vaikuttaa palautumiseen. Mitä kauemmin hyökkäys on kestänyt, sitä hankalampaa ja hitaampaa palautuminen on. (Tietohallinto A-B, Hoitohenkilökunta B, C, E, F, Hoitotekniikka A) Palautumisen työvaiheita esitetään kuvassa 6.




***Kuva 6.*** *Hyökkäyksestä palautumisen työvaiheet*

Tietojärjestelmäinfrastruktuurin näkökulmasta palautuminen tarkoittaa sitä, että eristettyjä, vaihdettuja ja sammutettuja järjestelmiä sekä laitteita aletaan käydä läpi ja niitä aletaan palauttaa toimintaan. (Tietohallinto A-B, Hoitotekniikka A) Osa laitteista saattaa myös vaatia korjausta, mikäli ne ovat hajonneet hyökkäyksen aikana. Erään haastateltavan mukaan tämä vaatii paljon yhteistyötä organisaation ja laitteiden toimittajien välillä. Myös järjestelmien välisiä yhteyksiä ja integraatioita voidaan joutua korjaamaan, sillä niitä on saatettu kiertää tai poistaa käytöstä hyökkäyksen aikana. (Hoitotekniikka A) Myös aiemmin otettuja varmuuskopioita saatetaan tarvita palautumisvaiheessa, mikäli laitteet tai järjestelmät on jouduttu hyökkäyksen aikana tyhjentämään. (Tietohallinto B, Hoitohenkilökunta C, Hoitotekniikka A) Pahimmassa tapauksessa myös varmuuskopiot voisivat olla saastuneita hyökkäyksen seurauksena. On siis pohdittava tarkkaan, onko hyökkäyksen kohteena olleiden laitteiden palauttaminen turvallista, vaikka näyttäisikin siltä, että hyökkäys on ohi. (Hoitotekniikka A) Myös toipumisessa on siis tehtävä huolelliset arviot siitä, millaisia vaikutuksia toipumismenetelmillä, kuten laitteiden ja järjestelmien palauttamisella verkkoyhteyteen, voi olla.

Häiriötilanteen koordinointiryhmän vastuut ulottuvat siihen asti, että toiminta on palautettu ennalleen. Yksi tietohallinnon haastateltavista nosti kuitenkin esiin, että ei ole varma onko suuresta häiriöstä palautumisen prosesseja suunniteltu yhtä yksityiskohtaisesti kuin toimintaa hyökkäyksen aikana. Esimerkiksi harjoitustilanteet eivät ulotu niin pitkälle.

Organisaatiolla on olemassa ylätason ohjeistukset liiketoiminnan jatkuvuudesta ja kriisitoipumisesta, mutta järjestelmiä ja laitteita on todella paljon erilaisia, ja niiden varmuuskopiot ja toipumismenetelmät voivat erota toisistaan todella paljon. (Tietohallinto A)

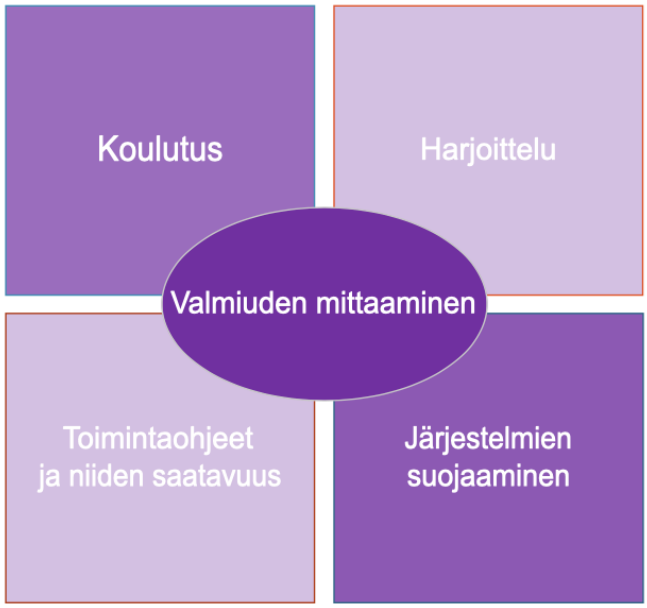
Mikäli hyökkäyksen takia on jouduttu luopumaan normaaleista potilastietojen kirjausmenetelmistä, on tilanteen aikana kerättyjen tietojen käsittely yksi merkittävä palautumisvaiheen työtehtävä. Hoitotietoja voi olla esimerkiksi papereilla ja DVD-levyillä. Mitä kauemmin hyökkäys on kestänyt, sitä suurempi määrä eri tavoin kerättyä tietoa on käytävä läpi ja siirrettävä tietojärjestelmiin. (Hoitohenkilökunta B-G, Hoitotekniikka A) Usein tietojen siirtäminen digitaaliseen muotoon tapahtuu käsin. Osa tiedoista voidaan ehkä siirtää järjestelmiin suoraa lääkintälaitteiden muistista ja jotkut tiedot siirtyvät laitteista järjestelmiin automaattisesti niiden palattua verkkoyhteyteen. Automaattinen tiedonsiirto sisältää kuitenkin paljon standardimuotoista dataa, jolloin manuaalista lähettämistä ja esimerkiksi henkilötietojen korjaamista on joka tapauksessa paljon. (Hoitotekniikka A) Erään haastateltavan mukaan pidemmän paperikirjausjakson jälkeen papereita voi pahimmillaan olla niin paljon, että niiden vieminen järjestelmiin vie kokonaisia työpäiviä. (Hoitohenkilökunta B)

Mikäli siirrettävää tietoa on paljon, saatetaan päättää, ettei kaikkea kirjata järjestelmiin, sillä tiedoissa voi olla myös hoitojakson jälkeen epäolennaista tietoa. Tähän on haastateltavien mukaan olemassa ohjeistukset, joita seurataan myös muun muassa käyttökatkotilanteissa. (Hoitohenkilökunta B, D) On myös mahdollista, että jotakin tietoa jää kyberhyökkäyksen seurauksena puuttumaan pysyvästi, esimerkiksi tietovarkauden tai laitteen hajoamisen seurauksena. Osa näistä saatetaan pystyä palauttamaan varmuuskopioista, uusilla tutkimuksilla tai kysymällä niitä hoitohenkilökunnalta ja potilailta, mutta mikäli paljon olennaista tietoa katoaa, se voi vaikeutta potilaan hoitoa jatkossa. (Hoitohenkilökunta B)

Olennainen osa palautumisvaihetta on myös pyrkimys tilanteesta oppimiseen. Oppiminen voi olla sen varmistamista, ettei vastaavaa pääsisi tapahtumaan tai esimerkiksi toimintatapojen selventämistä, jotta ne seuraavalla kerralla sujuvat paremmin. Olennaista on tapahtuneen tilanteen huolellinen läpikäynti ja arviointi yhdessä erilaisten tiimien kesken. Oppimisen kannalta tärkeää on myös tilanteessa asiakkailta ja henkilöstöltä saadun palautteen läpikäyminen. (Tietohallinto A-B, Johto A, Hoitohenkilökunta B-C, E)

## 5.3 Kyberhyökkäyksessä toimimiseen valmistavat käytännöt

Tähän asti on keskitytty kohdeorganisaation toimintaan hyökkäyksen ollessa käynnissä. Kohdeorganisaatiossa on kuitenkin käytössä toimintasuunnittelun lisäksi muitakin toimia, joilla pyritään varautumaan kyberhyökkäystilanteisiin ja lisäämään henkilöstön valmiutta toimia niiden aikana. Näitä toimia esitellään kuvassa 7.




***Kuva 7.*** *Organisaation kyberhyökkäysvalmiutta lisäävät käytännöt*

Yllä olevilla toimilla pyritään toisaalta kehittämään ja perehdyttämään henkilöstöä oikeisiin toimintatapoihin ja toisaalta helpottamaan organisaation hyökkäyksen jälkeistä paluuta normaaliin. Seuraavissa alaluvuissa avataan tarkemmin jokaista kuvan kohtaa.

### 5.3.1 Koulutus

Lähes kaikki haastateltavat mainitsivat organisaation järjestämät koulutukset yhtenä mahdollisena tapana lisätä henkilöstön kykyä toimia kyberhyökkäystilanteessa. Eri aiheisiin liittyviä koulutuksia järjestetään organisaatiossa keskitetysti ja koulutusyksiköllä on käytettävissään tieto kaikkien henkilöiden käymistä koulutuksista. Henkilöstön koulutusten osallistumisen seurannasta vastaa näiden omat esimiehet. (Tietohallinto B-D, Johto B, Hoitohenkilökunta A-B, D-G, Hoitotekniikka A)

Kohdeorganisaation koko henkilökunta suorittaa tietoturvakoulutuksen. Haastateltavien mukaan tietoturvakoulutuksissa opetetaan muun muassa hälytysmerkkejä, joista voi päätellä jotakin epäilyttävää tapahtuvan omalla tietokoneella. Koulutuksissa kerrotaan myös, miten epäilyttävistä tilanteista voidaan ilmoittaa käyttötukeen. (Tietohallinto B-D)

Kyberhyökkäystilanteessa toimimisesta ei koulutuksissa kuitenkaan olla tarkemmin kerrottu. Niissä on keskitytty ennaltaehkäisevään toimintaan ongelmatilanteiden välttämiseksi. (Johto B) Hoitohenkilökunnan haastateltavat toivoivat yleisesti lisää tietoa kyberturvallisuusasioista ja siitä, miten se liittyy heidän omaan toimintaansa. (Hoitohenkilökunta A, C, F, G) Eräs haastateltava osasikin kertoa, että lähitulevaisuuden turvallisuuskoulutuksiin on mahdollisesti tulossa sisältöä kyberturvallisuudesta. (Johto B)

Yhtenä haasteena organisaation koulutuskäytännöissä on se, että kaikki koulutukset eivät ole pakollisia, vaan henkilöstö saa ilmoittautua heitä itseään erityisesti kiinnostaviin koulutuksiin. Joihinkin koulutuksiin tuleekin paikalle vain erityisen turvallisuusorientoituneet henkilöt. (Hoitohenkilökunta A)

### 5.3.2 Toimintaohjeet ja niiden saatavuudesta huolehtiminen

Toinen varautumisen kannalta tärkeä ennakkovalmistautumisen keino on häiriötilanteiden toimintaohjeet ja niiden saatavuuden varmistaminen joka tilanteessa. Organisaatiolla on olemassa prosessit häiriötilanteen hallintaan, mutta häiriön käynnistyessä ei välttämättä ole aikaa etsiä ohjeita eikä niiden löytäminen esimerkiksi intranetistä ole kyberhyökkäystilanteessa välttämättä mahdollistakaan. Ohjeiden olisi siitä huolimatta oltava helposti käsillä heti häiriötilanteen käynnistyessä.

Ohjeiden olemassaoloon ja niiden löytämiseen liittyen organisaatiossa oli monia erilaisia käytäntöjä. Osalle haastateltavista oli hyvin selvää, mistä ohjeet tilanteessa toimimiseen löytyy ja osa taas ei löytänyt sellaisia, vaikka yritti etsiä niitä haastattelua varten. Ohjeiden etsiminen intranetistä nousi esiin monessa haastattelussa, mutta kysyttäessä tilanteesta, jossa tietojärjestelmät ei toimisi, kävi ilmi, etteivät kaikki tietäisi mistä etsiä seuraavaksi. (Hoitohenkilökunta A, C, D) Organisaatiossa vaikuttaisi kuitenkin olevan myös sellaisia yksiköitä, jossa varautuminen on viety askelta pidemmälle.

Kaksi hoitohenkilökunnan parissa työskentelevää haastateltavaa nostivat kriisivalmiutta nostavana tekijänä esiin erilaisia poikkeustilanteita varten koostetut fyysiset toimintakortit. (Hoitohenkilökunta D, E) Niiden tarkoituksena on sujuvoittaa ja selkiyttää toimintaa kriisitilanteessa siinäkin tapauksessa, että kaikki eivät ole sisäistäneet toimintaohjeita etukäteen tai osaavimmat henkilöt eivät ole työvuorossa. Valmiiksi painettuja toimintakortteja säilytetään toimintayksikön keskeisessä tilassa ja niihin on kirjattu jokaista tunnistettua poikkeustilannetta varten toimintaohjeet jokaiselle erilaisille hoitohenkilökunnan roolille. Näin ollen kriisin tapahtuessa henkilöstön jäsen voi kävellä huoneeseen, ottaa kortin käteensä ja seurata sen yksityiskohtaisia ohjeita. Henkilöstö vaihtuu hoito-osas-

toilla usein ja esimerkiksi keskellä yötä ja viikonloppuisin ei välttämättä ole paikalla ihmistä, joka tuntee kaikkien poikkeustilanteiden toimintaohjeet läpikotaisin. Toimintakortin hyödyt voivat korostua entisestään kyberhyökkäystilanteissa, sillä hyökkäyksen aikana esimerkiksi pääsy intranetiin voi olla estynyt. Toimintakorteilla varmistetaan siis myös, että olennaiset tiedot kriisitilanteissa toimimisesta ovat kaikkien saatavilla aina oikealla hetkellä. (Hoitohenkilökunta E)

”*Vaihtoehtoiset toimintatavat pitäisi olla sisäistettyinä, eikä saisi luottaa liikaa tietojärjestelmiin. Jokaisessa yksikössä pitäisi olla selvä suunnitelma siitä, mitä tehdä, kun jotain tapahtuu. Olen erittäin ylpeä siitä, että meillä on nämä asiat hyvin ja on varauduttu paljon. Kaikki prosessit on mietitty alusta asti. Muilla ei ehkä ole asiat yhtä hyvin.”* - Hoitohenkilökunta E

Toimintakortit oli koettu niitä käyttävillä osastoilla erittäin hyödyllisiksi, mutta haastatteluissa kävi ilmi, että niiden olemassaolo ei kuitenkaan ole standardi. Toimintakorttikäytäntö on käytössä sellaisilla osastoilla, jotka ovat itse halunneet ottaa sen käyttöön ja haastatteluissa saadun tiedon mukaan se on systemaattisesti käytössä vain yhdellä osastolla. Toimintakorttien kanssa paljon toiminut hoitohenkilökunnan jäsen kertoi kuitenkin, että heidän toimintamalliaan on pyritty viestimään myös muualle organisaatioon. Käytäntö on esitelty muun muassa turvallisuustyöryhmässä, jossa sen hyötyjä on pyritty viestimään, jotta muutkin ottaisivat sen käyttöön. (Hoitohenkilökunta E)

Organisaatiolla ei ole olemassa omaa spesifiä toimintakorttia kyberhyökkäystilanteeseen, vaan silloin käytetään tietojärjestelmähäiriön toimintamallia, joka soveltuu siihen melko hyvin, muttei täydellisesti. Tätä haastetta käsitellään tarkemmin luvussa 6.3.

### 5.3.3 Harjoittelu

Kriisitilanteissa toimimisen harjoittelu korostui jokaisessa pidetyssä haastattelussa. Haastateltavat pitivät harjoittelua erittäin kriittisenä vaatimuksena sille, että tositilanteen sattuessa pystytään toimimaan tehokkaasti. Harjoittelulla voidaan myös tutkia, miten paperille kirjatut ohjeet, käytännöt ja prosessit toimivat ja on sisäistetty organisaatiossa. Harjoittelu kuuluu organisaation toimintakulttuuriin, ja se pitääkin usein harjoituksia erilaisista poikkeustilanteista, kuten tulipaloista ja suuronnettomuuksista. Kaikki työntekijät eivät ole päässeet harjoittelemaan toimintaa juuri kyberhyökkäystilanteessa. Sellaista oli harjoiteltu vain tietohallinnon ja johdon keskuudessa (Tietohallinto A-D, Johto A-B).

Tietohallinnon ja johdon haastateltavat kertoivat osallistuneensa kattavaan kyberhyökkäysharjoitukseen. Harjoituksessa organisaation avainhenkilöt oli kutsuttu harjoituksen

järjestäjän toimesta virtuaaliselle alustalle, jossa simuloitiin kyberhyökkäystilannetta ja heidän piti toimia ja tehdä yhteistyötä kuten aidossa tilanteessa. Harjoituksesta oli saatu paljon positiivista palautetta, mutta myös hyödyllisiä oppeja tulevaan. Harjoituksessa oli onnistuttu erityisen hyvin toimijoiden välisessä yhteistyössä ja kommunikaatiossa. Kyseiseen harjoitukseen osallistuneet haastateltavat kokivat, että heidän oma kykynsä toimia hyökkäystilanteessa olisi harjoituksen ansiosta parempi kuin ilman sitä. (Tietohallinto A-D, Johto A-B)

*”Paperilla asiat pitäisi olla mietitty ja yleisessä jaossa, mutta osataanko tilanteessa sitten kuitenkaan toimia, kun se iskee. Siinä mielessä harjoittelu olisi tärkeää kaikille*” – Tietohallinto B

Myös aiemmissa erilaisissa tositilanteissa saatu harjoitus katsottiin eduksi kyberhyökkäystilanteessa toimimiseen. Muutama haastateltava koki saaneensa paljon erikoistilanneharjoitusta erityisesti Covid19-tilanteen aikana, jolloin tilanteet ja ohjeistukset muuttuivat nopeasti ja organisaatiolta vaadittiin paljon nopeita päätöksiä ja kriisiviestintää. (Johto A-B) Tietojärjestelmien toimimattomuudesta puolestaan saadaan usein harjoitusta erilaisten käyttökatkojen aikaan. Hoitohenkilökunnan haastateltavat sanoivat, että käyttökatkoja on sen verran usein, että ilman tietojärjestelmiä toimiminen on suurimmalle osalle tuttua. Näin ollen myös esimerkiksi kyberhyökkäyksen aikana käyttöön tulevat paperikirjausmenetelmät saavat ajoittain harjoitusta. (Hoitohenkilökunta B, D, E, Hoitotekniikka A)

”*Voisi olla sellainen harjoitus, että nyt teillä ei toimi mikään, mitä teette? Tulisi käytyä toimintamallit läpi ja löydettäisiin kohdat, jotka vaativat huomiota”* – Hoitohenkilökunta E

Jotkut hoitohenkilökunnan haastateltavat olivat sitä mieltä, että juuri kyberhyökkäystilanteessa toimimista voisi harjoitella enemmänkin. Nämä henkilöt työskentelivät operatiivisen hoitotoiminnan parissa, eivätkä olleet osallisina edellisen vuoden kyberhyökkäysharjoituksessa. (Hoitohenkilökunta A, D, F, G, Hoitotekniikka A) Myös tietohallinnon ja johdon haastateltavat pohtivat, olisiko hoitohenkilökunnalla tarvetta kyberhyökkäysharjoitukselle. Koko organisaation laajuiset harjoitukset ovat kuitenkin varsin hankalia järjestää. (Tietohallinto A-B, Johto A) Toimintaohjeiden sisäistämishaasteita tarkastellaan lisää alaluvussa 6.3.

### 5.3.4 Tietojärjestelmien suojaaminen

Tietojärjestelmät ja laitteet ovat kyberhyökkäyksissä usein hyökkäyksen kohteena, joten niiden sisältämän tiedon suojaaminen ja järjestelmien palautumiskyvyn varmistaminen

on tärkeä osa kyberhyökkäykseen valmistautumista. Haastateltavat nostivat esiin useita varautumistoimia, joita järjestelmien osalta on tehty ja joita voisi vielä tehdä.

Tietohallinnon haastateltavien mukaan suurin osa organisaation toiminnalle kriittisestä IT-infrastruktuurista on kahdennettu, jotta jonkin laitteen vaurioituessa se voidaan eristää ulos toiminnasta ja korvata toisella. Tällä pyritään lisäämään infrastruktuurin vikasietoa ja turvaamaan toiminnan jatkuvuutta. Haastateltavien mukaan on kahdentaminen ja laitteiden eristämismahdollisuus tärkeää, sillä jos kyberhyökkäyksen aikana jokin laite saastuu, se on voitava eristää systeemistä nopeasti ilman kaiken toiminnan lakkaamista. (Tietohallinto A-D) Toisena tietoteknisenä varautumiskeinona haastatteluissa nousi esiin osan toiminnoista siirtäminen kokonaan organisaation IT-infrastruktuurin ulkopuolelle. Näin onkin toimittu organisaatiossa esimerkiksi joidenkin viestintätoimintojen kanssa. Osa viestinnästä käyttää organisaation ulkopuolisia palvelimia juuri siksi, että se ei häiriinny, jos organisaation IT-infrastruktuuriin kohdistuu jokin häiriötilanne. (Johto A) Myös lääkintälaitteiden tietoturvasta on huolehdittava, jotta ne pysyvät toiminnassa, niiden sisältämät tiedot ovat mahdollisimman turvassa ja toisaalta helposti palautettavissa kyberhyökkäyksen aikana. Laitteiden tietoturva on kuitenkin suurilta osin puutteellista. Tämä aiheuttaa haasteita, sillä puutteet aiheuttavat organisaatioihin kohdistuvia riskejä, mutta kehitystoimet ovat vahvasti laitteiden valmistajien varassa. (Hoitotekniikka A) Laitteiden tietoturvaan liittyviä haasteita käsitellään tarkemmin alaluvussa 6.4.

Ennaltaehkäisevässä hyökkäystilanteisiin varautumisessa on haastateltavien mukaan myös tärkeää seurata jatkuvasti kehittyvää kyberrikollisuutta ja ymmärtää rikollisten toimintatapoja, jotta voidaan kerätä oppeja mahdollisten omalle kohdalle osuvien tilanteiden varalle. Organisaation tietohallinto ja IT-kumppani seuraavatkin jatkuvasti maailmalla tapahtuvia kyberhyökkäyksiä. Useampi haastateltava osasi nimetä muihin terveydenhuolto-organisaatioihin kohdistuneita hyökkäystilanteita. Tapahtuneiden hyökkäysten perusteella voidaan tunnistaa oman organisaation toimintaympäristössä riskejä, joihin tulee varautua tai jotka tulee tunnistaa kyberhyökkäyksen sattuessa omalle kohdalle. Muita haastatteluissa esiin nousseita tapoja suojata organisaation tietojärjestelmäinfrastruktuuria kyberhyökkäystilanteissa olivat jatkuva tietoturvavalvonta, kyberturvahankkeet sekä tietoturvapolitiikan ja riskienhallinnan kehittäminen. (Tietohallinto A, B, D)

### 5.3.5 Valmiuden mittaaminen

Haastateltavilta kysyttiin, tietävätkö he keinoja, joilla organisaation kyberhyökkäys- tai yleistä kriisivalmiutta mitattaisiin. Kaikki haastateltavat mainitsivat harjoituksen sekä har-

joitustilanteista saatavan palautteen ja havainnot erittäin hyvänä tapana mitata henkilöstön valmiuden ja varautumisen tasoa. Myös koetut oikeasti tapahtuneet häiriötilanteet antavat osviittaa organisaation kyvystä toimia yllättävissä poikkeustilanteissa. (Tietohallinto A-D, Johto A-B, Hoitohenkilökunta A-G, Hoitotekniikka A) Harjoittelulla voidaan mitata hyvin sitä, miten ylös kirjatut ohjeet toimivat ja osataan käytännössä, ja myös kehityskohteet tulevat niissä usein esiin. Myös kyberhyökkäystilanteen aikana ja sen jälkeen saatu palaute on tärkeä väline valmiuden tason mittaamiseen. Haastateltavien mukaan poikkeustilanteiden aikana asiakkailta ja henkilöstöltä saatu palaute käydään useimmiten hyvin systemaattisesti läpi, jotta ymmärretään, mitä ongelmia tilanteen aikana syntyi. (Tietohallinto A-B, Johto A, Hoitohenkilökunta B-C, E)

Muita juuri kyberhyökkäysvalmiuden arvioimiseen käytettäviä mittareita ei harjoitusten lisäksi kuitenkaan haastatteluissa juuri mainittu. Useampi haastateltava pohtikin, saattaisiko organisaatiolla olla tarvetta valmiuden objektiivisempaan ja systemaattisempaan arviointiin. Tällaisia formaalimpia mittareita voisivat olla esimerkiksi kyberhyökkäysvalmiutta tutkivat auditoinnit, GAP-analyysit ja riskiarvioinnit. Organisaation tämänhetkisen sisäisen auditoinnin piiriin kyberhyökkäysvalmiuden tutkiminen ei kuulu, mutta muita tietoturvaan liittyviä muita auditointeja tehdään. (Tietohallinto A-D)

Mittareita pohdittaessa haastatteluissa nousi esiin myös hyökkäystestaaminen, jota ei olla organisaatiolla säännönmukaisesti vielä tehty. Hyökkäystestaamisella tarkoitettiin tässä yhteydessä ”white hat -hacker” –tyyppistä penetraatiotestaamista, jossa organisaation tietojärjestelmäinfrastruktuuriin yritetään murtautua rikollisten suosimilla keinoilla. Tämän tyyppisellä testaamisella voitaisiin löytää potentiaalisia heikkouksia ja sokeita pisteitä organisaation kyberhyökkäysvarautumisessa, sillä testauksessa organisaation infrastruktuuria katsotaan erityisesti potentiaalisten hyökkääjien näkökulmasta. On kuitenkin hieman epäselvää, voisiko tällaista testausta teettää organisaation tyyppisessä toimintaympäristössä. (Tietohallinto A, B, D)

Haastatteluissa nousi esiin myös toive hoitohenkilöstön tietotaidon systemaattisesta mittaamisesta. Jotkut haastateltavat sanoivat, etteivät itsekään ole varmoja siitä, onko heillä ja heidän kanssaan työskentelevillä henkilöillä tarvittava ajantasainen osaaminen toimia kyberhyökkäystilanteessa, sillä he eivät ole olleet osallisina kyberhyökkäysharjoituksissa. (Hoitohenkilökunta A, B, D, Hoitotekniikka A) Organisaation koulutuksesta vastaavalla yksiköllä hallussaan tieto siitä, kuka on käynyt mitäkin koulutuksia, mutta on epäselvää, käytetäänkö sitä henkilöstön riittävän osaamistason seurantaan. (Hoitohenkilökunta A)

# 6. TAPAUSTUTKIMUS: VARAUTUMISEN HAASTEET KOHDEORGANISAATIOSSA

*”Eikö IT-maailma voisi keksiä jotain, ettei me jouduttaisi pelkäämään koko ajan, töissä ja kotona.”* – Johto B

Tässä luvussa tarkastellaan vielä syvällisemmin tapaustutkimuksen aikana tehtyjä löydöksiä tutkittavan kohdeorganisaation haasteista kyberhyökkäystilanteeseen varautumisessa. Tunnistetuista ongelmakohdista pureudutaan neljään merkittävimpään: asenneilmapiiriin ja kybertietämyksen puutteeseen, hyökkäystilanteen tilannekuvan ymmärtämiseen ja viestintään, toimintaohjeiden puutteeseen ja haasteisiin niiden sisäistämisessä sekä laitteiden puutteelliseen tietoturvaan. Alaluvuissa hyödynnetään useita haastattelusitaatteja, jotta haasteita saataisiin kuvattua mahdollisimman tarkasti.

## 6.1 Asenneilmapiiri ja tietämyskuilu

Haastattelujen perusteella oli mahdollista havaita kohdeorganisaatiossa paljon vaihtelua ja ristiriitoja eri haastateltavien asenteissa, tuntemuksissa ja käsityksissä, jotka liittyivät kyberturvallisuuteen ja siihen liittyviin työtehtäviin, sekä mahdolliseen kyberhyökkäystilanteeseen. Tässä alaluvussa tuodaan esiin erilaisia näkökulmia, joita haastatteluissa nousi esiin.

*”Kun tehdään esimerkiksi tietoturvapäivityksiä, mikään ei käy! Ihminen ajattelee, että ettekö te tajua, että olen niin kiireinen, ettei mulla ole koskaan hyvä hetki. Ihmisten pitäisi ymmärtää, miksi näitä tehdään. Näitä tehdään siksi, että niitä pahiksia on niin paljon ja niiden toiminta kehittyy koko ajan… Siksi tämä on tätä kilpajuoksua. Tämä yritetään tehdä henkilöstölle helpoksi, mutta joskus jokaisen on vain ajettava se päivitys, ei voi ylenkatsoa.”* – Tietohallinto D

Tietohallinnon ja johdon haastateltavien käsityksissä välittyi paikoin turhautumista siihen, ettei kaikki organisaatiossa tunnu ottavan kyberturvallisuutta yhtä vakavasti. Esimerkiksi tietoturvaan liittyvien työasemapäivitysten tekemisessä on havaittavissa usein laiminlyöntejä ja välinpitämättömyyttä. (Tietohallinto D, Johto B, Hoitohenkilökunta B) Useamman henkilön mielestä organisaatiossa ei osata suhtautua tarvittavalla vakavuudella siihen, miten vakavaa olisi, jos jotain tällaista tapahtuisi. Heidän mielestään kaikkien tietämys kybermaailman vaaroista ei ole sillä tasolla, millä pitäisi ja siitä syystä myös ymmärrys omista tietoturvavastuista on puutteellinen. (Tietohallinto D, Johto A-B, Hoitohenkilökunta A-C, Hoitotekniikka A)

*”Minkälaisen ongelmavyyhdin se tarvitsee, että tietoturvan tärkeys osataan ottaa huomioon ajoissa. Toivottavasti sellaista ei tule, mutta aina mennään vähän kantapään kautta*.” – Hoitohenkilökunta C

Yhtenä huolenaiheena riskin jo tuntevien joukossa olikin, että pitääkö todella tapahtua jotakin pahaa, ennen kuin kaikki hahmottavat sen, miten vakavasta asiasta on kyse (Hoitohenkilökunta C). Johdon haastateltavan mukaan olisi tärkeää, että kaikki ymmärtäisivät, että näin voi tapahtua, ennen kuin niin todella käy. On ymmärrettävä, miten rankka esimerkiksi puutteellisesta tietoturvakäyttäytymisestä johtuva kyberhyökkäys olisi organisaatiolle. Näissä tilanteissa pieni inhimillinen virhe voisi aiheuttaa järkyttäviä seurauksia ja jonkun pitäisi mennä median eteen selittämään niitä. (Johto A) Kyberhyökkäysuhkaan tulee suhtautua potilasturvallisuusriskinä (Tietohallinto D, Johto A, Hoitohenkilökunta B).

*”Siinä on tietotarve, tarvitaan tietoa siitä, että näitä ihan oikeasti tapahtuu, ei ole vain IT-nörttien puuhailua*. ” – Hoitohenkilökunta C

*"Ei sitä jotenkin usko, että sellaista voisi joku tehdä tai että sellainen tulisi, mutta kuitenkin niitä tapahtuu. Mitä se sitten aiheuttaa, kuinka paljon voi varautua ja millä tavoin, ne olisivat sellaisia asioita, joista tarvittaisiin koulutusta.* " – Hoitohenkilökunta F

Vastaavasti hoitohenkilökunnan haastateltavien vastauksissa nousi puolestaan esiin epäusko ja yleinen skeptisyys siihen, että kyberhyökkäys voisi kohdistua omaan organisaatioon. Useampi haastateltava piti kyberhyökkäystilannetta niin kaukaisena tilanteena, että sitä on vaikea kuvitella omalle kohdalle. (Hoitohenkilökunta F, G) Haastattelun aikana kyberhyökkäysskenaarioiden pohtiminen tuntui erään haastateltavan mukaan hieman hämmentävältä ja jopa pelottavalta (Hoitohenkilökunta G). Muutama hoitohenkilökunnan haastateltava koki, että samaisen ”lintukoto”-ajattelun takia kyberturvallisuusasioita on vaikeaa edistää hoitotoimijoiden keskuudessa, koska niiden vakavuutta ja oman toiminnan merkitystä niihin varautumisessa ei tunnisteta. (Hoitohenkilökunta A, B, Hoitotekniikka A) Erityisesti lääkäreiden haluttomuus varautumistoimintaan ja tietoturvatehtäviin nousi esiin useissa vastauksissa. Haastateltavien mukaan lääkärit saattavat kokea, että tietoturva-asiat eivät kuulu heille. (Tietohallinto D, Hoitohenkilökunta B, E)

”*Valveutuneisuus tällaisten uhkien olemassaolosta on sellainen osaamistarve, mikä tulisi olla kaikilla, jotka kriittisiä järjestelmiä käyttää. Että osaisi varoa ja vähän pelätäkin*.” - Hoitohenkilökunta B

*”Ehkä sellainen kaikkien sivistäminen ja tiedottaminen skenaarioista voisi olla ihan hyvä… Yleensä niistä tehdään liian järeitä, hirveitä oppaita, eikä niitä lue kuin viisi ihmistä, jotka ovat asiantuntijoita siinä tietoturva-alalla… Kuinka monta sairaanhoitajaa*

*luulet, että sen lukee? Ei varmaan kukaan. Jos olisi edes yksi yhden sivun sarjakuva, että tällainen se tilanne on… Ihmiset saataisiin tietoisiksi, että tällaisia tilanteita voi tulla, ne voi eskaloitua näin vakaviksi ja näin ne voidaan hoitaa*." – Hoitotekniikka A

Välinpitämättömyys ja vaihtelu asenteissa liittyy läheisesti eroihin ja puutteisiin tietämyksessä. Moni haastateltava kokikin organisaation yleisen tietämystason kyberaiheesta olevan liian alhainen, mikä vaikeuttaa kyberhyökkäyksiin varautumista ja siihen liittyviä tehtäviä merkittävästi. Tarve ymmärryksen ja osaamisen kehittämiseen nostettiinkin esiin jokaisessa johdon ja hoitohenkilökunnan haastattelussa (Johto A-B, Hoitohenkilökunta A-G, Hoitotekniikka A). Moni haastateltava toivoi, että kyberturvallisuusasiat saisivat organisaatiossa enemmänkin näkyvyyttä ja painoarvoa etenkin hoitohenkilöstön kouluttamisessa. (Johto A-B, Hoitohenkilökunta A, C, F, G, Hoitotekniikka A) Tässä voisivat erään haastateltavan mukaan auttaa tarinan tai sarjakuvan muotoon puetut helposti lähestyttävät tietoiskut, jotka toisivat esimerkiksi kyberhyökkäystilanteessa vaadittavaa toimintaa näkyväksi koko organisaatiolle. Pitkät tekstimuotoiset ja teknispainotteiset ohjeistukset ovat hänen mielestään tehottomia laajan tietoisuuden levittämisessä, sillä niitä lukee hyvin harva. (Hoitotekniikka A)

*"Ennen ajateltiin, että nörtit ne siellä keskenään leikkii, nykyään tajutaan että nämä on vakavimman luokan asioita."* - Johto B

Vastauksista kävi kuitenkin ilmi myös se, että aiheeseen on jo havahduttu organisaatiossa. Esimerkiksi Vastaamo-tapauksen kerrottiin havahduttaneen henkilöstöä kaikkialla organisaatiossa. Erään haastateltavan mukaan sitä olisi voitu puida enemmänkin, jotta olisi vielä paremmin ymmärretty, mitä sellainen tilanne organisaatiolta vaatii. (Johto A) Myös koulutuksiin on tarkoitus tuoda tulevaisuudessa lisää sisältöä kyberaiheista (Johto B). Havainnot liittyen ongelmiin asenteissa ovat mielenkiintoisia myös siksi, että haastatteluissa kävi ilmi, että organisaatiossa vallitsee muuten varsin vahva turvallisuus- ja varautumiskulttuuri. Monet muut tutummat turvallisuusriskit otetaan paljon vakavammin ja niihin liittyvien varautumistoimien tarpeellisuus ymmärretään. On mahdollista, että haasteet kyberasioiden eteenpäin viemisessä liittyvät juuri tietämättömyyteen. Tästä syystä olisikin tärkeää lisätä henkilöstön tietoisuutta ja saada koko henkilöstö ymmärtämään, mitä tietoturvan laiminlyönti voi aiheuttaa (Tietohallinto D, Johto A-B, Hoitohenkilökunta A, B, F, G).

## 6.2 Haasteet tilannekuvan viestinnässä

Yhdeksi keskeisimmäksi tekijäksi kriisitilanteen toiminnan onnistumisen kannalta nostettiin haastatteluissa selvän, reaaliaikaisen ja kattavan tilannekuvan muodostaminen, ylläpitäminen ja viestintä. Samaan aikaan haasteet tilannekuvan viestinnässä ja ymmärtämisessä nousivat monissa haastatteluissa yhdeksi organisaation merkittävimmistä kehityskohdista. Syinä tähän pidetiin esimerkiksi rakenteeltaan ja kooltaan haastavaa organisaatiota, tiedonkulun ja viestinnän haasteita sekä sitä, että kyberasioita ymmärtävältä tietohallinnon henkilöstöltä ja hoitohenkilökunnalta puuttuu monesti yhteinen kieli. (Tietohallinto A-D, Johto A-B, Hoitohenkilökunta B, C, E)

*”Jos ei sitä kukaan osaa piirtää yhdelle A4-paperille niin ei sitä kukaan sitten hallitsekaan.”* - Johto B

Useampi haastateltava toivoi tilannekuvan viestintään tehokkaampia ja etenkin ymmärrettävämpiä keinoja. Jotkut haastateltavat kokivat esimerkiksi tietohallinnon ja johtoryhmän välisen kommunikaation tilanteiden aikana hieman hankalaksi, sillä tietohallinnolta saatava tieto sisältää usein hieman liian teknistä kieltä, eikä johto siten heti ymmärrä tilanteen merkitystä. Kyberhyökkäystilanteeseen liittyy monia teknisiä yksityiskohtia, mutta johdolle merkityksellisempää on ymmärtää hyökkäyksen vaikutukset. (Tietohallinto A, Johto A-B) Johdon haastateltava toivoikin tietohallinnolta selkeää ja visuaalista, esimerkiksi kuvien tai grafiikan muodossa toimitettavaa esitystä siitä, miten hyökkäys vaikuttaa. Koska johdon pitää joskus myös päättää käyttöönotettavista ratkaisuista, toivottiin, että myös niiden vaikutukset voitaisiin tulkata johdolle selkeästi tiiviin esityksen muodossa. Aiemmin ongelmia oli kohdattu ongelmia esimerkiksi siinä, että johdon piti päättää jonkun tietyn verkon osan sulkemisesta, vaikkeivat he kunnolla ymmärtäneet, mitä se käytännössä tarkoittaa toiminnan kannalta. (Johto B) Sama haaste oli jo havaittu myös tietohallinnon puolella. Tietohallinnon edustaja toivoikin, että tilannekuvan muodostamiseen ja kommunikointiin löytyisi visuaalinen menetelmä tai työkalu, jolla näitä haasteita saataisiin ratkaistua. (Tietohallinto A)

*”Meidän pitäisi pystyä paremmin esittämään asiat johdolle. Johtoa ei kiinnosta, että jokin serveri on alhaalla, ei se kerro heille mitään. Meidän pitäisi itse ymmärtää, että kun tämä ja tämä serveri on alhaalla, niin miten se vaikuttaa potilastyössä. Sitten johtajat pystyvät tekemään niitä päätöksiä, että onko tämä korjaava toimi liian vakava vai ei. Tilannekuvan selkeä muodostaminen on mielestäni sellainen haaste, jota on kehitettävä*.” - Tietohallinto A

Kehityskohteita havaittiin myös häiriötilanteiden aikaisessa kommunikaatiossa ja tiedonkulussa erilaisten toimijoiden välillä ja siinä, miten hyökkäykseen liittyvät tekniset tiedot

käännetään yleistajuiseksi ymmärrykseksi siitä, miten hyökkäys vaikuttaa mihinkin toiminnan osa-alueeseen. Myös hoitohenkilökunnan on tiedettävä, mitä tehtäviään he eivät voi suorittaa normaalisti, jotta he voivat ottaa juuri oikeat korvaavat toimintatavat käyttöön nopeasti. Hoitotyön ja tietohallinnon välisen kommunikaation koettiin kuitenkin olevan ongelmatilanteiden aikana välillä liian hidasta, etenkin silloin, kun tietohallinnolle kohdistuvia kysymyksiä tulee joka puolelta organisaatiota. (Tietohallinto A, D, Johto A, B, Hoitohenkilökunta B, C, E, F, Hoitotekniikka A) Jotkut hoitohenkilökunnan haastateltavat kokivat, että joskus tilanteissa ei meinaa löytyä ketään, jolta saisi tietoa, vaikka heidän mielestään olisi tärkeää, että joku olisi koko ajan kuulolla hoitotoimintaan päin (Hoitohenkilökunta A-C). Tämä haaste näkyi myös siinä, että tietohallinnon henkilöiltä saatiin kommentteja, joiden mukaan viestintäosasto hoitaisi kysymykset, kun taas viestintäosastolla ajateltiin, että tietohallinto vastaa kyselyihin itse, kun heillä on riittävästi tietoa. Molemmilla puolilla painotettiin omien asiantuntijoiden työrauhan säilyttämistä muihin tehtäviin, joten hieman kysymysmerkiksi jäikin, kuka muualta organisaatiosta tuleviin kysymyksiin vastaa. (Tietohallinto C, Johto A, B) Eräs haastateltava koki hoitohenkilökunnalle aiheutuvan tiedonsaannin hankaluuksia erityisesti silloin, mikäli ongelmatilanteet tapahtuvat toimistoajan ulkopuolella. Tällöin esimerkiksi suuri osa tietohallinnon ja johdon henkilöstöstä ovat normaalisti poissa työpaikalta, ja kommunikaatiorajapinta näiden suuntaan toimii tällöin liian hitaasti. Haastateltavan mukaan yhteistyön tulisi olla saumattomampaa kellon ympäri (Hoitohenkilökunta A).

*”Kaipaisin enemmän yhteistyötä tietohallinnon ja käytännön toiminnon kanssa. Saataisiin muodostettua kuva siitä, mitkä toiminnot on kriittisiä. Jos esimerkiksi mietitään järjestystä, mitä lähdetään pelastamaan ensin ja mitkä pitää saada ensin käyttöön, että pystytään hoitamaan potilaat ja pitää tietää, mihin mitäkin järjestelmää käytetään. Sellaista vuoropuhelua olisi hyvä käydä ennen kuin mitään isompaa tapahtuu*”. – Hoitohenkilökunta C

Erityisesti hoitotoiminnan johtavissa asemissa toimivat henkilöt korostivat, miten tärkeää hoitotyön päätöksenteon kannalta on saada mahdollisimman nopeasti tietoa siitä, missä, mihin ja miten hyökkäys vaikuttaa. (Hoitohenkilökunta B, C, E) Sekä hoitohenkilökunnan että tietohallinnon haastateltavat kuitenkin arvelivat, ettei tietohallinnolla ole välttämättä riittävän kattavaa käsitystä hoitotoiminnasta (Tietohallinto A, Hoitohenkilökunta C). Organisaatio on suuri, järjestelmiä ja laitteita on valtavasti ja monet niistä ovat kriittisiä hoidon jatkumisen kannalta. Tästä syystä on selvää, ettei tietohallinto voi sulkea kaikkea pois käytöstä, vaan on tärkeää tunnistaa juuri ne toiminnot, jotka ovat häiriintyneet, jotta korjaavat toimet saadaan kohdistettua oikein. Tietohallinnolla on kuitenkin haastateltavan mukaan hyvin vähän näkyvyyttä hoitotoiminnan yksityiskohtiin (Tietohallinto A).

## 6.3 Toimintaohjeiden puutteellisuus ja sisäistämisongelmat

Alaluvussa 5.3.2 todettiin, että organisaation sisällä voidaan havaita paljon eroavaisuuksia siinä, miten tarkkoja ohjeistuksia kyberhyökkäystilanteiden varalle on olemassa ja miten hyvin ohjeet tunnetaan henkilöstön keskuudessa. Alaluvussa 5.3.3 kävi ilmi, että johto ja tietohallinto ovat päässeet harjoittelemaan toimintaa kyberhyökkäystilanteessa, mutta hoitohenkilökunta ei. Alaluvussa 6.1 puolestaan todettiin, että kyberhyökkäys on aiheena varsin tuntematon etenkin hoitohenkilökunnalle, minkä takia edes sen uhkaa ei ole sisäistetty kaikkialla. Näitä havaintoja yhdistelemällä voidaan arvioida, että ainakaan kaikki organisaation henkilöt eivät ehkä osaisi toimia tilanteessa ohjeiden mukaan.

*"Tätä haastattelua varten vähän kävin katsomassa, sen tiedän, että meidän yksiköllämme ei ole mitään ohjeistusta, mutta en löytänyt intrastakaan ohjeistusta kyberhyökkäystä varten... ... Jos tulisi tällainen ja pitäisi äkkiä intrasta katsoa ohjeet niin en löytäisi"* – Hoitohenkilökunta F

Haastattelujen perusteella voidaan arvioida, että joissain organisaation osissa ohjeistus kyberhyökkäyksissä toimimiseen saattaa olla osittain puutteellinen, tai vähintäänkin sen saavutettavuudessa on kehitettävää. Sen lisäksi, että toimintaohjeita ei välttämättä ole, niitä ei tunneta ennalta tai niitä ei löydetä helposti, haasteita kyberhyökkäystilanteessa aiheuttaa myös se, ettei olemassa oleviakaan ohjeita ole välttämättä saatavilla hyökkäyksen aikana. Mikäli ohjeita ei tunneta ennalta, eikä niitä ole tulostettuna missään, eivät intranetissä olevat ohjeet auta tilanteen aikana, jos niihin ei pääse käsiksi. Useampi haastateltava arveli, että etsisi tilanteen aikana ohjeita intranetistä, mutta mikäli sitä ei voisi käyttää, olisi vaikeaa tietää, mistä etsiä seuraavaksi. (Hoitohenkilökunta A, C, D, F)

"*Jos tämä tulee ilman varoitusta ja me menetetään kaikki tiedot siitä, ketä meillä on sisällä ja meillä on yli 100 potilasta sisällä… Suunniteltuja katkoja on useita vuodessa, tiedetään koska alkaa ja koska päättyy. Se on rutiinia ja sen mukaan osataan toimia. Mutta yllättävät tilanteet ovat kyllä vaikeita, jos ei me osata sitä ennakoida."* – Hoitohenkilökunta D

*"Jos se häiriö kestäisi pitkään, siitä se malli puuttuu… Toimintamallit on luotu lyhytaikaisempaan toimintaan."*- Hoitohenkilökunta B

Toinen ohjeistuksiin liittyvä puute on niiden mahdollinen puutteellinen soveltuvuus juuri kyberhyökkäystilanteeseen. Hoitohenkilökunnan haastateltavat kertoivat, että käyttökatkojen aikainen toimintaohje soveltuu hyvin melko hyvin myös hyökkäystilanteeseen, vaikkei hyökkäykseen itsessään olekaan spesifiä ohjetta. (Hoitohenkilökunta A-G, Hoitotekniikka A) Yksi haastateltava kuitenkin oli sitä mieltä, että käyttökatko-ohjeistus ei ole

riittävä kyberhyökkäystilanteessa, sillä käyttökatkot ovat usein suunniteltuja ja niihin voidaan jollain tavalla vähintään henkisesti varautua. Kyberhyökkäystilanne tapahtuisi kuitenkin hyvin yllättäen, mikä voisi lisätä riskiä epäjatkuvuuskohdille ja kommunikaatiohaasteille nykyisillä ohjeilla. (Hoitohenkilökunta D) Suurena haasteena pidettiin sitäkin, että käyttökatkojen toimintaohjeet on rakennettu melko lyhytkestoisia tilanteita varten. Käyttökatkoissa tiedetään yleensä ennalta, kauanko ne kestävät, kun taas kyberhyökkäyksen kestosta ei sen alkaessa välttämättä ole mitään tietoa. Tilanteen pitkittyessä ja jonojen kasvaessa toimintaohjeet eivät kuitenkaan enää välttämättä riitä, eikä pitkittyneeseen, esimerkiksi päiviä kestävään tilanteeseen ole olemassa ohjeistusta. (Hoitohenkilökunta B)

"*Paloturvallisuuteen ja henkilöturvallisuuteen meillä panostetaan ehkä eniten kuukausittaisissa turvallisuuskävelyissä, mutta tietoturva ja järjestelmäturvallisuus on vähän lapsenkengissä, meidän yksikössä ainakin.*" – Hoitohenkilökunta F

Ohjeiden puutteellisuuden lisäksi ongelmaksi koettiin myös haasteet ohjeiden sisäistämisessä. Erään haastateltavan mukaan kaikki hyvätkin suunnitelmat ovat vain hyödyttömiä papereita, jos niitä ei ole harjoiteltu ja koeponnistettu käytännössä (Hoitohenkilökunta A). Hoitohenkilökunnan haastateltavista lähes kaikki toivoivatkin kyberhyökkäystilanteiden harjoittelua. Moni lisää harjoittelua kaivanneista nosti esiin, että monia muita ongelmatilanteita harjoitellaan todella usein, mutta harjoitusta kyberhyökkäystilanteessa toimimiseen ei ole koskaan tullut vastaan. Käytännön harjoituksen puuttuessa he eivät ole ihan varmoja, kuinka heidän pitäisi toimia, vaikka kirjallinen ohjeistus jostakin ehkä löytyykin. Monet haastateltavat olivat sitä mieltä, että kaikki ohjeistukset tulee kunnolla sisäistettyä vasta, kun niitä on kokeiltu joko harjoituksessa tai tositilanteessa. (Tietohallinto B, Johto B, Hoitohenkilökunta A, B, D, F, G)

*”Totta kai voin itse arvioida olemassa olevia ohjeita ja niiden ajantasaisuutta ja voin sanoa, että varautuminen on tietyllä tasolla. Se, mitä en voi kuin arvata, on se, että mikä se työntekijöiden oma ajatus valmiudesta on, osasiko he toimia... Tällaiset tulee yleensä mitatuksi siinä, kun häiriötilanne on ollut.”* – Hoitohenkilökunta B

”*Kyberhyökkäyksen toimintavalmiutta ole arvioitu ulkopuolelta, eikä harjoiteltukaan. On tiedossa, että tällaisia on ja että tällaisia voi tulla. Voisi olla hyvä varautua konkreettisten tilanteiden harjoittelemisella. Muita kriisitilanteita ja vaaratilanteita on harjoiteltu kyllä.”* - Hoitohenkilökunta G

Huomionarvoista toimintaohjeiden ja niiden sisäistämisen kohdalla oli myös se, että kyberhyökkäyksen kohdalla toimintaohjeiden osaamistasoa ei ole mitattu koko organisaation mittakaavassa. Näkyvyys osaamisen riittävyyteen olisi kuitenkin hyvä saavuttaa.

Suuri osa haastateltavista ei osannut arvioida, miten hyvin ohjeet on sisäistetty työyhteisössä. (Tietohallinto A, B, D, Johto B, Hoitohenkilökunta A-G, Hoitotekniikka A) Organisaatiolle ominainen tapa mitata henkilöstön osaamista eri asioissa vaikuttaisi olevan käytännön harjoitukset, jotka eivät tällä alueella ylety koko organisaatioon. Useampi haastateltava toivoikin jotakin keinoa saada näkyvyyttä siihen, kuinka hyvin henkilöstö todellisuudessa ymmärtää kyberturvallisuuteen liittyviä uhkia ja kuinka valmiita he olisivat toimimaan kriisitilanteessa. (Tietohallinto A-B, Hoitotekniikka A). Haasteeksi tunnistettiin sekin, että kriisivalmiuden ja henkilöstön riittävän osaamisen mittaaminen ja arviointi suuressa organisaatiossa on vaikeaa ja vie paljon aikaa ja resursseja. Mikäli harjoittelu ei koko organisaation mittakaavassa onnistu, olisi heidän mielestään mittaamiseen tarpeellista löytää muita keinoja, esimerkiksi yksiköiden sisäisiä harjoituksia (Tietohallinto A-B, Hoitotekniikka A).

## 6.4 Lääketieteellisten laitteiden heikko tietoturva

Neljäntenä ongelmakohtana haastatteluissa tunnistettiin hoitotoimintaan käytettävien lääketieteellisten laitteiden heikko tietoturva, joka voi luoda uhkia esimerkiksi laitteisiin kohdistuvista tahallisista väärinkäytöksistä. Tämän nosti esiin haastateltava, joka tunsi organisaation käyttämät lääkintälaitteet erityisen hyvin (Hoitotekniikka A).

*”Niissä medikaalipuolen laitteissa se toimintakyky edes vastata näihin tiettyihin minimivaatimuksiin on heikko… Se potilaan hoito kuitenkin vaatii tietyn laitteen, ja pakko on hankkia joku laite. Sitten siinä tulee vähän sellainen dilemma, kun niiden se kyky torjua tai olla tarpeeksi tietoturvallisia nykypäivän mittapuulla… Se on laitepuolen ongelma ollut.”* – Hoitotekniikka A

Kaikki lääkintälaitteet eivät täytä organisaation käytössä olevia tietojärjestelmille ja laitteille määriteltyjä tietoturvavaatimuksia. Monia laitteita saattaa valmistaa kuitenkin vain yksi valmistaja, joten valmistajien ei ole pakko tehdä niiden asiakkaiden vaatimuksille mitään, kun heillä on joka tapauksessa markkinajohtajan asema. Jotkut laitteet ovat hoitotoiminnan kannalta niin välttämättömiä, että ne on hankittava joka tapauksessa. Tällöin terveydenhuolto-organisaatioiden on joustettava tietoturvallisuusvaatimuksista ja hankittava laitteet puutteista huolimatta, jotta hoidon tarjoaminen potilaille on mahdollista. (Hoitotekniikka A)

”*Tehtiin huoltovarmuuskeskuksen kanssa yhteistyössä semmoista hankintojen kehittämistä kyberturvaan ja lääkintälaitehankintoihin liittyen. Siinä yhtenä ideana on saada kansallisesti nostettua laitetoimittajien tämmöistä kykyä vastata näihin tietoturva- ja tietosuojavaatimuksiin.”* – Hoitotekniikka A

Terveydenhuolto-organisaatiot ovat yrittäneet saada laitevalmistajia ymmärtämään puutteet tietoturvallisuudessa ja tekemään tuotekehitystä tietoturvavaatimuksien täyttämiseksi, mutta tässä on koettu paljon haasteita valmistajien vahvan neuvotteluaseman takia. Ongelman ratkaisemiseksi suomalaiset terveydenhuolto-organisaatiot ja muut niiden sidosryhmät ovatkin pyrkineet ryhmittäytymään yhteen ja esittämään tietoturvavaatimuksia laitevalmistajille yhdessä. Myös kilpailun lisääntyminen alalla voisi helpottaa terveydenhuolto-organisaatioiden tilannetta, kun niillä olisi varaa valita useampien vaihtoehtojen joukosta. (Hoitotekniikka A)

# 7. TAPAUSTUTKIMUS SUHTEESSA AIEMPAAN KIRJALLISUUTEEN

Tässä luvussa tutkimuksen kirjallisuusosassa ja tapaustutkimuksessa tehtyjä löydöksiä käsitellään yhdessä. Aluksi tarkastellaan edellisessä luvussa esiteltyjä kohdeorganisaation ongelmakohtia suhteessa kirjallisuuteen ja esitetään niille haastatteluihin ja kirjallisuuteen perustuvat ratkaisuehdotukset. Seuraavassa alaluvussa selvitetään, missä määrin tapaustutkimuksen ja kirjallisuuden löydökset vastaavat toisiaan, missä ne täydentävät toisiaan ja miten ne eroavat toisistaan. Lopuksi muodostetaan vielä tapaustutkimuksen ja kirjallisuuden synteesinä kokonaiskuva terveydenhuolto-organisaation kybervarautumisen nykytilasta ja vastataan samalla tutkimuksen päätutkimuskysymykseen. Nykytilan kuvauksessa arvioidaan, mitkä kybervarautumisen osa-alueet tunnetaan jo hyvin, mitä asioita siinä voi ja kannattaa juuri nyt kehittää ja mitkä asiat ovat vielä kohdeorganisaatiolle, ja kybervarautumisen tutkimukselle suhteellisen tuntemattomia ja tarvitsevat lisää tutkimusta.

## 7.1 Ongelmakohdat ja niiden ratkaiseminen kirjallisuuden pohjalta

Tapaustutkimuksessa onnistuttiin havaitsemaan ongelmakohtia kohdeorganisaation kybervarautumistoiminnasta. Tässä alaluvussa esitellään ongelmakohtien esiintymistä tutkitussa kirjallisuudessa sekä arvioidaan, mitä kohdeorganisaation olisi tarpeen tehdä tunnistetuille ongelmakohdille tulevaisuudessa. Jokaiseen luvussa 6 tunnistettuun alakohtaan tarjotaan muutamia jatkokehitysehdotuksia, jotka perustuvat tapaustutkimuksessa tehtyjen havaintojen lisäksi kirjallisuusosiossa tutkittuun lähdemateriaaliin. Suosituksissa viitataan akateemisen kirjallisuuden lisäksi myös Sosiaali- ja terveysministeriön (2019) kyberturvallisuusohjeeseen terveydenhuolto-organisaatioille, siltä osin, kun ohjeissa mainituissa asioissa havaittiin puutteita kohdeorganisaation toiminnassa. Ongelmakohtia ja jatkosuosituksia esitellään taulukossa 9.

Taulukko 9. *Kohdeorganisaatiolle esitettävät jatkosuositukset*

| **Ongelmakohta** | **Jatkosuositukset** |
|---|---|
| 6.1 Asenneilmapiiri ja tietämyskuilu | - Kyberturvallisuustietoisuuden vahvistaminen koulutuksen ja tietoiskujen avulla, kyberturvallisuuskulttuurin luominen (Owens 2020; Norri-Sederholm et al. 2019; Coronado & Wong 2014; Haastattelut)<br><br>- Jokaisen henkilön ja työroolin tietoturvavastuiden selkiyttäminen ja niihin vastuuttaminen johdosta lähtien (NIST 2018; Norri-Sederholm 2019; Willing et al. 2021; Coronado & Wong 2014; Haastattelut) |
| 6.2 Haasteet tilannekuvan viestinnässä | - Visuaalista viestintää tukevan kommunikointityökalun tai -prosessin käyttöönotto johdon ja tietohallinnon väliseen tilannekuvan viestintään (Mykkänen et al. 2019, Tikanmäki & Ruoslahti 2021; Haastattelut)<br><br>- Tietohallinnon ja hoitotoiminnan yhteistyön lisääminen kriittisten toimintojen ymmärtämiseksi (Norri-Sederholm et al. 2019) NIST 2018, Sosiaali- ja terveysministeriö 2019, Haastattelut)<br><br>- Viestintävastuiden selkiyttäminen kriisitilanteen ajalle, kaikkien tahojen tiedonsaanti ja asiantuntijoiden työrauha varmistettava samanaikaisesti (Hellenberg et al. 2011; Haastattelut) |
| 6.3 Toimintaohjeiden puute ja sisäistämisongelmat | - Kyberhyökkäystilanteeseen, myös pitkäkestoiseen, kokonaisuudessaan soveltuvien toimintaohjeiden valmistelu kaikille organisaation toimialueille ja toimijoille (NIST 2018; Sosiaali- ja terveysministeriö 2019; Haastattelut)<br><br>- Hyökkäysvalmiuden arviointi (harjoittelu/simulointi) koko organisaatiossa (osa/kaikki kerrallaan) (Willing et al. 2021; Sosiaali- ja terveysministeriö 2019; Haastattelut) |
| 6.4 Lääkintälaitteiden heikko tietoturva | - Laitteiden ja niiden välisten yhteyksien tietoturvan kehittäminen (Willing et al 2021; Norri-Sederholm et al. 2019; Coronado & Wong 2014)<br><br>- Kehitys yhdessä muiden alojen toimijoiden kanssa, vaatimusten esittäminen laitetoimittajille (Haastattelut) |

Merkittävimmät ongelmakohdat kohdeorganisaation tapauksessa löydettiin teknisten prosessien ulkopuolelta, ihmisten osaamisesta ja toiminnasta. Myös kirjallisuudessa todettiin, että terveydenhuollon kybervarautumisen heikoin lenkki löytyy usein ihmisistä, joiden tietotekninen osaaminen ja ymmärrys kyberturvasta saattaa olla riittävää tasoa alhaisempi, mikä altistaa inhimillisille virheille (Willing et al. 2021; Owens 2020; Norri-Sederholm et al. 2019; Ayala 2016). Koko henkilöstön kybertietoisuuden ja riittävän osaamisen merkitys hyökkäystilanteissa korostui myös useissa lähteissä kirjallisuudessa (Willing et al. 2021; Norri-Sederholm et al. 2019; NIST 2018; Ayala 2016; Coronado & Wong 2014). Kohdeorganisaation haastatteluissa nostettiin esiin erilaisia huolia henkilöstön tietämyksen ja osaamisen riittävyydestä erilaisissa tilanteissa ja hoitohenkilökunnan kybertietoisuuden puute nousi esiin yhtenä kohdeorganisaation merkittävimpänä ongelmakohtana. Henkilöstön kyberosaamisessa koettiin olevan vakaviakin puutteita, jotka näkyivät esimerkiksi skeptisyytenä, välinpitämättömyytenä ja osaamattomuutena. Ratkaisuna näihin ongelmiin esitetään kirjallisuuden ja haastateltavien kommenttien pohjalta kyberturvallisuustietoisuuden vahvistamista koulutuksen ja tietoiskujen avulla, sekä koko organisaation laajuisen kyberturvallisuuskulttuurin luomista. (Owens 2020; Norri-Sederholm et al. 2019; Coronado & Wong 2014; Haastattelut). Lisäksi jokaisen henkilön ja työroolin tietoturvavastuita tulisi selkiyttää ja niihin vastuuttamisen tulisi tapahtua johdosta lähtien (NIST 2018; Norri-Sederholm 2019; Willing et al. 2021; Coronado & Wong 2014; Haastattelut).

Myös tilanneanalyysin ja selkeän tilannekuvan tärkeys nousivat esiin sekä kirjallisuudessa että tapaustutkimuksessa (Tikanmäki & Ruoslahti 2021; Norri-Sederholm et al. 2019; NIST 2018; Hellenberg et al. 2011). Tilannekuvan havainnollistaminen ja viestintä oli yksi merkittävimmistä tutkimuksessa havaituista ongelmakohdista, ja haastateltavat kaipasivatkin kommunikaation ja päätöksenteon tueksi visuaalista tietoa kokonaistilanteesta. Kirjallisuudesta löydettiin lupaavia tuloksia aiemmin onnistuneesta terveydenhuollon tietojärjestelmäinfrastruktuurin visuaalisesta mallintamisesta ja näiden tulosten mukaan terveydenhuolto-organisaation reaaliaikaisen ja visuaalisen tilannekuvan muodostaminen eri tietojärjestelmistä on teknisesti mahdollista. (Mykkänen et al. 2019; Haastattelut) Tilannekuvan mallintamisen lisäksi tapausorganisaatiolle suositellaan tietohallinnon ja hoitotoiminnan yhteistyön lisäämistä kriittisten toimintojen ymmärtämiseksi, sekä viestintävastuiden selkiyttämistä kriisitilanteen ajalle siten, että samanaikaisesti myös kaikkien tahojen tiedonsaanti ja asiantuntijoiden työrauha säilyy. (Norri-Sederholm et al. 2019; NIST 2018; Sosiaali- ja terveysministeriö 2019; Hellenberg et al. 2011; Haastattelut)

Yksi kohdeorganisaation ongelmakohdista oli kyberhyökkäystilanteen toimintaohjeiden puutteellisuus, niiden vajaa soveltuminen kyberhyökkäystilanteisiin ja ohjeiden sisäistämisen puute. Ongelmana oli myös se, että olemassaolevat ohjeet soveltuivat vain lyhytkestoisiin tilanteisiin. Organisaatiota suositellaankin valmistelemaan juuri kyberhyökkäystilanteeseen, myös pitkäkestoiseen, kokonaisuudessaan soveltuvat toimintaohjeet kaikille organisaation toimialueille ja toimijoille (NIST 2018; Sosiaali- ja terveysministeriö 2019; Haastattelut). Kirjallisuudessa korostettiin tarkkaa vastuunjaon huolellista määrittelyä ja toimintasuunnittelua, sekä kriisiosaamisen nykytilan varmistamista erilaisin mittauskeinoin. (Bahuguna et al. 2019; NIST 2018; Norri-Sederholm et al. 2019; Hellenberg et al. 2011). Kaikkia olennaisia asioita, kuten henkilöstön kyberhyökkäysosaamista, ei vielä järjestelmällisesti mitata kohdeorganisaatiossa. Koko henkilöstön harjoittelu tunnistettiin hyväksi keinoksi ohjeiden jalkauttamiseen ja valmiuden mittaamiseen sekä haastatteluissa että kirjallisuudessa, ja hoitohenkilökunnalle simuloidusta kyberhyökkäystilanteesta löytyi esimerkkitutkimuskin. (Willing et al. 2021; Norri-Sederholm et al. 2019; Sosiaali- ja terveysministeriö 2019) Kohdeorganisaatiota suositellaan ulottamaan kyberhyökkäysvalmiuden harjoittelu ja arviointi koko organisaatioon, esimerkiksi osastokohtaisilla harjoituksilla. (Willing et al. 2021; Sosiaali- ja terveysministeriö 2019; Haastattelut) Useampi haastateltava totesi toimintaohjeiden olevan hyödyttömiä niin kauan kunnes ne on koeponnistettu käytännössä. Samaa kertoo Hellenberg et al. (2011) siteeraama sotafilosofi Clausewitzin teesi: ”Mikään suunnitelma ei kestä kuin ensimmäiseen vihollisen kohtaamiseen saakka”. (Hellenberg et al. 2011)

Yhtenä terveydenhuolto-organisaatioihin niiden oman toiminnan ulkopuolelta kohdistuvana uhkana tunnistettiin sekä tapaustutkimuksen että erityisesti kirjallisuustutkimuksen kautta lääkinnällisten laitteiden usein tarvittavaa heikompi tietoturva ja häiriötilanteiden sietokyky. Kirjallisuudesta nousi esiin, että erityisesti laitteiden aiempaa korkeampi integroitavuus ja lisääntyvät verkkoyhteydet luovat kyberturvallisuudelle paljon uusia haasteita ja kehitystarpeita. (Willing et al. 2021; Norri-Sederholm 2019; Ayala 2016; Coronado & Wong 2014) Tapaustutkimuksen mukaan terveydenhuolto-organisaatioiden kokemat haasteet voivat usein johtua laitetoimittajista, joiden ei välttämättä monopoliasemansa ansiosta tarvitse vastata asiakkaidensa tietoturvavaatimuksiin. Tätä ongelmakohtaa olikin jo lähdetty ratkaisemaan organisaatiossa muiden terveydenhuolto-organisaatioiden ja viranomaisten kanssa tehtävällä yhteisellä vaikuttamisella. Eri toimijoiden välisen yhteistyön merkitys kybervarautumisessa korostui myös kirjallisuudessa (Norri-Sederholm et al. 2019; Haastattelut).

## 7.2 Tapaustutkimuksen ja kirjallisuuden yhteys

Tapaustutkimus ja kirjallisuus muovasivat kumpikin osaltaan käsityksen terveydenhuolto-organisaatioiden kybervarautumisesta. Tässä alaluvussa arvioidaan, miten nämä käsitykset vastaavat toisiaan. Aluksi käsitellään tapaustutkimuksen tulosten ja kirjallisuuden yhteneviä piirteitä, sitten sitä, miten kumpikin osaltaan täydentää toisiaan ja sitä, millaisia eroja niiden välillä havaittiin. Lopuksi pohditaan vielä, että oliko joitakin sellaisia tutkimusaukkoja, joista kirjallisuus tai tapaustutkimus ei kumpikaan tuottaneet tietoa.

Kirjallisuuden ja tapaustutkimuksen tulosten yhteiset piirteet liittyivät erityisesti varautumisen formaaleihin prosesseihin sekä johdon ja tietohallinnon toimintaan. Varautumisen prosessit näyttivät eri kirjallisuuslähteissä ja tapausorganisaatiossa hyvin samalta. Esimerkiksi luvussa 4.1 käsitellyt NIST:in (2018) varautumisen vaiheet nousivat kaikki selkeästi esiin tutkittavan organisaation haastatteluvastauksissa. Teknisen varautumisen hyvät käytännöt ja prosessit vaikuttaisivatkin olevan yleisesti tunnettua tietoa, mistä myös eri kirjallisuuslähteet olivat keskenään samoilla linjoilla. (NIST 2018; Norri-Sederholm et al. 2019; Ayala 2016; Huang et al. 2018; Coronado & Wang 2014; Hubbard et al. 2017). Myös Norri-Sederholmin et al. (2019) esittelemät kyberturvallisuuden johtamisen suositukset toteutuivat organisaatiossa monilta osin hyvin (Norri-Sederholm et al. 2019). Yhteistä kirjallisuudelle ja tapaustutkimukselle oli sekin, että molemmissa tunnistettiin aiempien kriisien merkitys uusiin poikkeustilanteisiin valmistautumisessa. Molemmissa kuitenkin nousi esiin myös se, ettei reaktiiviseen kantapään kautta oppimiseen välttämättä ole varaa yhteiskunnan toimivuuden kannalta näin vakavissa tilanteissa. (Gkeredakis et al. 2021; Hellenberg et al. 2011). Sekä kirjallisuuden, että tapaustutkimuksen perusteella vaikuttaisi siltä, että kyberhyökkäysvarautumisen merkittävimmät haasteet kohdeorganisaation kaltaisessa suuressa organisaatiossa aiheutuvat siitä, miten paljon osaamista varautuminen vaatii lähes kaikilta organisaation toimijoilta, terveydenhuollon kohdalla erityisesti hoitohenkilöstöltä.

Kirjallisuusosuudessa tunnistetut erilaiset kyberhyökkäysskenaariot nousivat monipuolisesti esiin myös haastateltavien vastauksissa (Willing et al. 2021; Norri-Sederholm et al. 2019; Ayala 2016; Kwon & Hwang 2016; Coronado & Wong 2014). Useammissa haastatteluissa nousi kuitenkin esiin myös yhdistelmätilanteen, kuten yhtäaikaisen kyberhyökkäyksen ja suuronnettomuuden uhka, josta ei juurikaan löytynyt terveydenhuoltoon liittyvää materiaalia kirjallisuudesta. Hybridiuhkia käsittelevä kirjallisuus koski lähinnä sotatilanteita ja puolustusvoimien toimintaa. Haastatteluissa pohdittiin myös skenaariota, jossa hyökkääjä pääsisi etäohjaamaan lääkintälaitteita. Tällainen tilanne olisi haastateltavien mukaan erittäin tuhoisa. Näiden ”kyberhyökkäyserikoistilanteiden”, joihin nykyiset normaalit varautumistoimet eivät riitä, uhan tunnistaminen terveydenhuollossa

voidaan nähdä myös olemassa olevaa kirjallisuutta täydentävänä havaintoina. Sekä kirjallisuudessa että tapaustutkimuksessa tunnistettiin skenaariona myös tilanne, jossa hyökkääjä muokkaa tietoja salaa (Willing et al. 2021; Huang et al. 2018; Kwon & Hwang 2016; Coronado & Wong 2014). Tähänkin skenaarioon varautuminen oli kohdeorganisaatiossa hyvin alkutekijöissään ja skenaarion kohdalla haastatteluissa todettiin vain, että tämä tilanne olisi todella paha, eikä ihan tiedetä, miten se huomattaisiin tai miten siihen varauduttaisiin. Kirjallisuus täydentää tapaustutkimusta tältä osin, sillä kirjallisuudesta löydettiin esimerkkejä siitä, miten tällaiseen tilanteeseen voidaan simuloidun harjoitustilanteen avulla varautua.

Kirjallisuus täydensi tapaustutkimusta hyvin myös liittyen kohdeorganisaation ongelmakohtaan tilannekuvan ymmärtämisessä ja viestinnässä. Tilannekuvaan ja sen selkeyteen liittyvät tarpeet ja haasteet vaikuttivat olevan kohdeorganisaation lisäksi yleisiä muussakin julkisen sektorin johtamisessa (Tikanmäki & Ruoslahti 2021; Mykkänen et al. 2019; Hellenberg et al. 2011). Kirjallisuudesta löydetty tieto muissa terveydenhuolto-organisaatioissa onnistuneista tilannekuvan mallinnuksista täydentää tapaustutkimusta ja rohkaisee ajattelemaan, että samankaltaisen tilannemallintamisen hyödyntäminen voisi olla mahdollista myös kohdeorganisaation kyberhyökkäystilanteessa. (Mykkänen et al. 2019; Tikanmäki & Ruoslahti 2021) Kirjallisuudesta nousi esiin myös mielenkiintoinen ajatus siitä, pitäisikö koko julkisen sektorin terveydenhuollon kyberturvallisuus tulevaisuudessa keskittää sen sijaan, että kaikki organisaatiot vastaavat siitä itse (Candolin 2020).

Norri-Sederholm et al. (2019) esittivät henkilöstön kybertietoisuuden nykytilan tärkeänä tulevaisuuden tutkimusaiheena varautumisen kehittämisessä (Norri-Sederholm et al. 2019). Tapaustutkimuksen voidaan katsoa vastanneen osaltaan tähän tutkimustarpeeseen ja täydentävän täten olemassa olevaa kirjallisuutta. Tapaustutkimuksessa nostettiin esiin esimerkiksi organisaation arjessa havaittuja ristiriitoja ja konflikteja kyberturvallisuutta edistävien vastuiden ymmärtämisessä ja niihin liittyvien tehtävien suorittamisessa, mikä selittää osaltaan kirjallisuudessakin tunnistettuja haasteita henkilöstön osallistumisessa. Juuri tästä, tosielämän näkökulman mukaan tuomisesta, muodostuukin tämän tutkimuksen merkittävin kontribuutio olemassa olevalle kirjallisuudelle. Arkipäivän toiminnan realiteettien tunnistaminen auttaa ymmärtämään, mitkä asiat varautumisessa ovat organisaatiolle haastavia ja miten varautuminen oikeasti jalkautetaan suunnitelmapapereilta toimintaan. Tämä näkyi myös siinä, että välillä kirjallisuus ja tapaustutkimus toivat esiin samanlaisia asioita, mutta selittivät niitä eri tavoilla. Näin oli esimerkiksi laitteiden puutteellisen tietoturvallisuuden kohdalla, jota kirjallisuus yleisellä tasolla selitti johtuvaksi laitteiden ja niiden integroitavuuden nopeasta kehityksestä. Tapaustutkimuk-

sessa asiaa käsiteltiin terveydenhuolto-organisaation näkökulmasta, jolloin haastateltavien vastaukset täydensivät kirjallisuutta huomiolla siitä, että laitetoimittajat saattavat tosielämässä olla myös haluttomia tekemään tarvittavia korjauksia tietoturvaan, koska monopoliasemansa takia näiden ei ole edes pakko. Tämä on erinomainen esimerkki siitä, miksi teoreettisen kirjallisuuden ja todellisen organisaation tutkiminen tapaustutkimuksessa on hyödyllistä. Erilaiset näkökulmat erilaisiin haasteisiin syventävät ymmärrystä ilmiöiden juurisyistä.

Kirjallisuudessa esitettiin väite siitä, että kyberturvallisuuden tutkimuksessa tunnetaan hyvin ainoastaan prosessin ne vaiheet, jotka liittyvät arkipäiväiseen uhkien estämiseen ja riskien minimoimiseen ennen häiriötilanteita. Väitteen mukaan reagoinnin ja palautumisen vaiheet, joissa tapahtuvaa kriisitilannetta aktiivisesti hallitaan, muodostavat tutkimusaukon. (Weber et al. 2021) Tämä tutkimus tutki juuri näitä vaiheita, joten tapaustutkimuksen voidaan katsoa osaltaan täydentävän tätä tutkimusaukkoa. Kohdeorganisaation haastatteluissa puolestaan nousi esiin, että ennaltaehkäisevien toimintojen lisäksi myös varsinaiseen reagointivaiheeseen on valmistauduttu organisaatiossa hyvin. Erityisesti tietohallinnon ja johdon toimintaa sekä vastuunjakoa häiriötilanteessa oli suunniteltu hyvin tarkkaan ja siitä oli saatu positiivista palautetta ulkopuolelta, joten sitä voidaan pitää myös kohdeorganisaation vahvuutena. Hyökkäystilanteen jälkeistä palautumisvaihetta puolestaan on suunniteltu kohdeorganisaatiossakin vähemmän.

Tutkimuksen aikana aineistossa havaittiin myös ristiriitaisuuksia, mutta ei niinkään kirjallisuuden ja tapaustutkimuksen välillä. Enemmän ristiriitoja havaittiin yksittäisten haastateltavien vastauksissa suhteessa toisiinsa. Nämä ristiriidat selittyivät usein erilaisista näkökulmista keskenään hyvin erilaisia työtehtäviä tekevien ihmisten välillä. Tapaustutkimuksen vastaajille oli kuitenkin yhteistä se, että he vastasivat varautumiseen liittyviin kysymyksiin aina ihmisten toiminnan näkökulmasta ja suhteessa siihen, mikä on arjen toiminnan ja resurssien puitteissa mahdollista. Kybervarautumiseen liittyvässä kirjallisuudessa ja ohjeistuksissa ihmisen toiminta mainittiin myös usein keskeisenä elementtinä, mutta käsittely keskittyi silti enemmän tehtävälistoihin ja teknisiin prosesseihin. Tämän tutkimuksen aineiston osalta voidaan siis todeta, että kirjallisuuden ja tapaustutkimuksen suurin ero oli, että kirjallisuuden tarjoama tieto oli tehtäväkeskeisempää ja tapaustutkimuksen puolestaan ihmiskeskeisempää. Tehtäväkeskeisestä näkökulmasta katsottuna varautuminen on riittävää, kun varautuminen on tarkkaan suunniteltua, tehtävät ja vastuut on määritelty ja tarvittavat työkalut ja prosessit ovat olemassa. Ihmiskeskeiselle näkökulmalle tärkeämpää on se, osaisivatko ihmiset aidosti toimia tilanteen sattuessa. Tutkimuksessa tehtiinkin paljon mielenkiintoisia havaintoja tarkastelemalla asioita juuri tästä näkökulmasta. Kohdeorganisaatiossa haasteita koettiin esimerkiksi siinä,

miten organisaation ohjeistuksissa määritellyt tehtävät muutetaan osaksi ihmisten käytännön osaamista ja toimintaa. Tapaustutkimuksen perusteella todettiin, etteivät tehtävälistat yksinään riitä varautumisen onnistumisen takeeksi, vaan formaalien prosessien sisäistämiseen olisi todennäköisesti tarpeen kiinnittää enemmän huomiota. Tämän huomion voidaan katsoa täydentävän kirjallisuutta.

Vaikka tapaustutkimus ja kirjallisuus loivat varsin kattavan käsityksen terveydenhuolto-organisaation kyberhyökkäysvarautumisesta, tunnistettiin tutkimuksen aikana myös sellaisia tutkimusaukkoja, joista tietoa ei ole vielä tarpeeksi. Käytännössä tällaisia asioita olivat esimerkiksi aiemmin mainitut erikoisemmat kyberhyökkäystilanteet, jotka haastatteluissa tunnistettiin kyllä terveydenhuolto-organisaatioihin kohdistuviksi uhkiksi, mutta niihin ei ollut juurikaan varauduttu. Sekä tapaustutkimus että kybervarautumiseen liittyvä kirjallisuus keskittyi erityisesti muutamaan nykypäivän yleisimpään kyberhyökkäysskenaarioon, joissa joko varastetaan tietoa tai sitten joidenkin järjestelmien tai laitteiden käyttö estetään. Harvinaisempia skenaarioita ovat esimerkiksi hybridikriisitilanteet, erittäin pitkäkestoiset kyberhyökkäystilanteet, hyökkääjän suorittama lääkinnällisten laitteiden etäohjaus ja salassa tapahtuva järjestelmien sisältämän tiedon muokkaaminen. Harvinaisempiin skenaarioihin varautumisesta löytyi huomattavasti vähemmän tietoa kirjallisuudesta, ja erityisesti hybridikriisiskenaarioihin liittyen ei löytynyt mitään. Haastateltavien mukaan moni näistä harvinaisemmista skenaarioista olisi vielä ”tavallista” kyberhyökkäystä paljon vakavampia ja vaarallisempia. Näistä tarvittaisiin siis lisää tietoa, sillä tällä hetkellä näitä voidaan pitää kyberhyökkäysvarautumisen sokeina pisteinä. Hellenberg et al. (2011) pitivät vakavana ongelmana sitä, että yhteiskunnassa herätään tekemään korjaus- ja kehittämistoimia usein vasta tapahtuneiden kriisien jälkeen. Reaktiivinen kehittäminen on huono lähtökohta, sillä yhteiskuntaa ravistelevat kriisit yllättävät aina, eivätkä ne yleensä seuraa aiemmin tapahtuneiden tilanteiden kulkua. (Hellenberg et al. 2011) Juuri tästä syystä myös harvinaisemmilta vaikuttaviin skenaarioihin tulisi varautua ennen, kuin joudutaan oppimaan kantapään kautta.

## 7.3 Pohdintaa

Seuraavaksi pohditaan sitä, mitä päätelmiä tutkittavasta ilmiöstä voidaan tehdä tutkimuksessa tehtyjä edellä esiteltyjä löydöksiä yhdistelemällä. Päätelmien perusteella voidaan arvioida sitä, mihin suuntaan varautumisen ja sen tutkimuksen tulisi tulevaisuudessa kehittyä, jotta terveydenhuolto organisaatioiden valmius toimia erilaisissa kyberhyökkäystilanteissa olisi tulevaisuudessa parempi.

Edellisessä alaluvussa todettiin, että kyberhyökkäysvarautumiseen liittyvä kirjallisuus on tämän tutkimuksen näkökulmiin verrattuna varsin tehtäväkeskeistä ja tämä tutkimus toi

mukanaan ihmiskeskeisemmän näkökulman. Tutkimuksen aikana tunnistetut ongelmat liittyivät erityisesti ihmisten toimintaan ja siihen, että nykyinen varautuminen ei riitä, sillä hoitohenkilökunta ei ymmärrä riittävästi kyberturvallisuudesta. Tapaustutkimuksen perusteella voidaan arvioida, että kybervarautumista käsitellään sekä kohdeorganisaatiossa että kirjallisuudessa liiaksi varautumiseen liittyvien tehtävien näkökulmasta, jolloin ajatellaan, että kun tehtävät ja vastuut on määritelty paperille, on varauduttu. Ihmisten ja hoitotyön näkökulman mukaan tuominen nosti kuitenkin esiin uusia vaiheita, joissa varautuminen voi mennä pieleen. Ihmiskeskeisen näkökulman avulla saatiin myös hahmotettua uusia juurisyitä haasteille, jotka oli jo tunnistettu aiemmin. Kaikkien organisaatioissa ja niiden sidosryhmissä työskentelevien ihmisten toimintavalmius on ratkaiseva osa varautumista, mutta nykyinen kybervarautuminen käsittelee liikaa tehtävälistojen muodostamista ja keskittyy liian vähän siihen, mikä on jokaisen ihmisen osaamisen ja ymmärryksen rooli osana hyökkäyksiin varautumista.

Tutkimuksessa tehdyistä löydöksistä voidaan myös päätellä, että terveydenhuolto-organisaation ydintoimintaa, eli ihmisten tekemää hoitotyötä ja sen toimintaympäristön realiteetteja ja haasteita, ei vielä riittävästi ymmärretä terveydenhuolto-organisaatioiden kyberhyökkäystilanteisiin varautumisessa. Vielä ei ole riittävästi tutkittua tietoa tai ymmärrystä siitä, mitä erityistä juuri terveydenhuollon toimintaympäristö tuo kyberhyökkäysvarautumiseen Esimerkiksi terveydenhuollolle spesifien uhkaskenaarioiden hahmottaminen on nykytilanteessa vielä puutteellista. Kirjallisuudessa tämä näkyi siten, että kyberhyökkäyksen aikana toimimiseen liittyvä aineisto käsitteli pääosin yleisimpiä uhkaskenaarioita, eikä pysähtynyt miettimään sitä, millaisia uhkaskenaarioita juuri terveydenhuoltoala voi tuoda mukanaan. Myös kohdeorganisaatiossa suunnitelmallinen varautuminen oli keskittynyt erityisesti yleisten kyberhyökkäysskenaarioiden toteutumiseen, mutta organisaation henkilöstö pystyi nimeämään erityisesti terveydenhuollon toimintaympäristöstä nousevia uhkatilanteita, kuten yhtäaikaista hyökkäys- ja onnettomuustilannetta tai lääkintälaitteiden etäohjausta. Näitä ei ollut kuitenkaan juurikaan varautumisessa ajateltu. Huolenaiheita ilmeni myös liittyen siihen, ymmärretäänkö varautumis- ja reagointitoimenpiteiden valinnassa tilanteita riittävän hyvin hoitotoiminnan kannalta.

Niin kohdeorganisaatiossa kuin yleisestikin koetut ongelmat lienevät seurausta vuoropuhelun ja yhteistyön puutteesta sekä siitä, että samankaan organisaation sisällä työskentelevät eri alojen asiantuntijat eivät ymmärrä toisiaan riittävästi. Kohdeorganisaation kyberhyökkäyksiin varautuminen noudatteli ansiokkaasti yleisiä ja tunnettuja toimialariippumattomia hyvän varautumisen käytäntöjä, joka kertonee siitä, että varautumisesta vastaavat henkilöt tuntevat kyberturvallisuuden kentän yleisesti hyvin. Kuitenkin tutki-

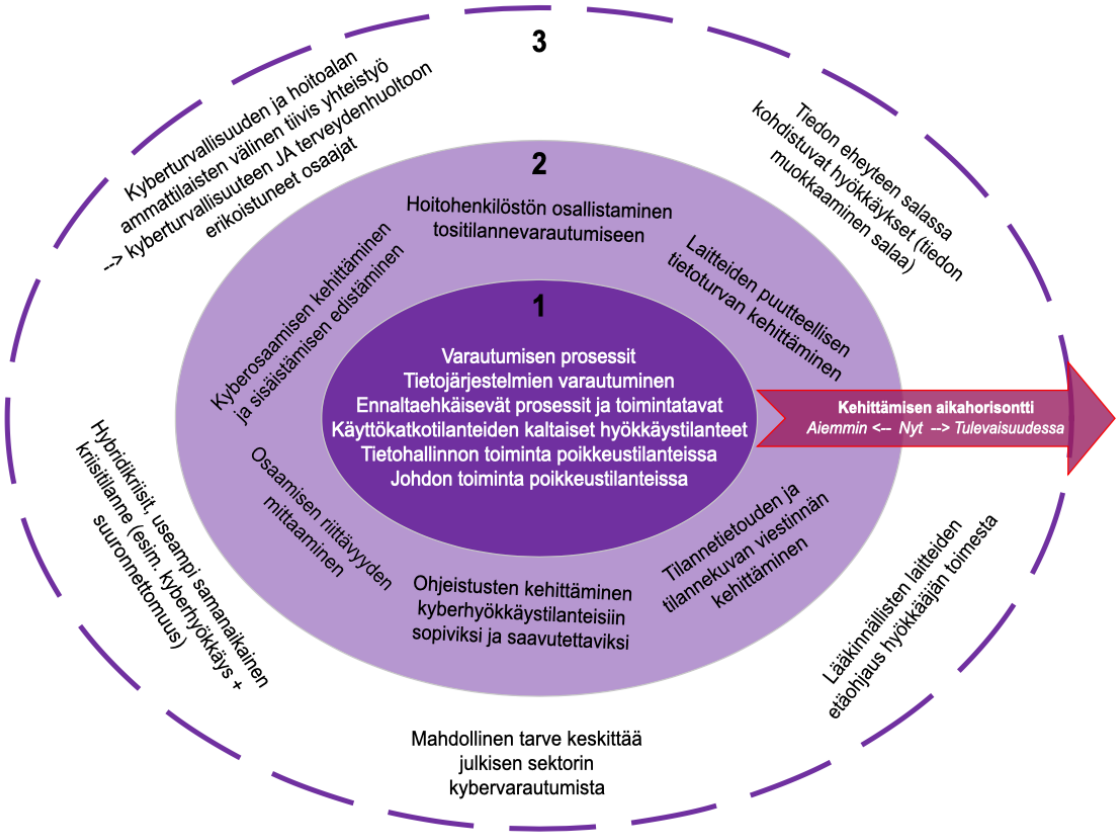
muksessa nousi esiin myös se, että näillä henkilöillä ei ole kovinkaan kattavaa näkyvyyttä organisaation ydintoimintaan, eli varsinaiseen hoitotyöhön. Organisaation hoitohenkilöstö taas tietää todella paljon siitä, miten hoitoa voidaan toteuttaa poikkeustilanteissa ja miten häiriötilanteisiin yleisellä tasolla kannattaa varautua. Kyberhyökkäystilanteisiin liittyen heillä ei kuitenkaan ollut riittävästi osaamista tai ymmärrystä. Kybervarautumista suunnittelevilta henkilöiltä puuttuu siis ymmärrys hoitotoiminnan vaatimuksista ja hoitotoiminnalta puuttuu ymmärrys kybervarautumisen heille asettamista vaatimuksista.

Tämän tutkimuksen perusteella voidaan arvioida, että eri toimijoiden välinen ymmärrys ja yhteistyö on erittäin kriittistä varautumisen onnistumiselle. Jatkossa terveydenhuolto-organisaatioille voisi olla myös valtavasti hyötyä sellaisista osaajista, jotka hallitsisivat sekä kyberturvallisuuden että terveydenhuollon kentän. Tällöin ei tarvitsisi jatkuvasti pohtia sitä, miten eri alojen asiantuntijat saataisiin ymmärtämään toisiaan. Esimerkiksi kohdeorganisaatiossa on tutkimuksen perusteella huipputasoista osaamista sekä hoitotyöstä että kyberhyökkäysvarautumisesta, joten vuoropuhelun sekä vastavuoroisen opettamisen ja oppimisen kautta voitaisiin saavuttaa paljon kehitystä. Tämä päätelmä voidaan yleistää koskemaan myös terveydenhuolto-organisaatioiden kyberhyökkäysvaratumista ja sen tutkimusta yleisesti. Varautumista ei voida tutkia irrallisena hoitotyöstä, vaan sen asettamat vaatimukset on pidettävä läsnä koko ajan.

## 7.4 Synteesi – terveydenhuolto-organisaation kyberhyökkäysvarautuminen nyt ja tulevaisuudessa

Lopuksi kuvataan vielä sitä, millaisen kuvan koko tutkimus yhdessä muodostaa terveydenhuolto-organisaation kyberhyökkäysvarautumisen ja sen tutkimuksen nykytilasta ja tulevaisuuden haasteista. Aiemmin tässä luvussa esiteltyjen löydösten perusteella muodostettu kirjallisuuden ja tapaustutkimuksen synteesi esitetään kaavion muodossa kuvassa 8. Kaavion sisimmällä kehällä nähdään sellaiset varautumisen osa-alueet, jotka vaikuttaisivat olevan jo yleisemmin tunnettua tietoa ja hyvin jalkautettua toimintaa niin tapaustutkimuksessa kuin yleisestikin. Toisella kehällä nähdään sellaiset kyberhyökkäysvarautumisen osa-alueet, jotka on tunnistettu haastaviksi kirjallisuuden ja/tai tapaustutkimuksen kautta ja joiden ratkaisemiseksi on jo tunnistettu keinoja. Tällaisia olivat erityisesti tutkimuksessa tunnistetut ihmisten osaamiseen liittyvät haasteet. Uloimmalla kehällä nähdään tutkimuksessa tunnistetut niin sanotut kybervarautumisen ”sokeat pisteet”. Sokeat pisteet ovat kybervarautumiseen liittyviä osa-alueita tai uhkia, jotka tunnistettiin tässä tutkimuksessa joko kirjallisuudessa tai tapaustutkimuksessa, mutta joihin liittyviä toimia ei ollut vielä käytössä eikä suunnitteilla tapausorganisaatiossa ja jotka eivät

nousseet esiin kirjallisuudestakaan. Sokeiden pisteiden joukossa on harvinaisempia, erityisesti terveydenhuoltoalalle spesifejä, kyberhyökkäysskenaarioita, sekä kirjallisuudessa ja tutkimuksen pohdinnassa tunnistettuja mahdollisia tulevaisuuden kehitystarpeita terveydenhuolto-organisaatioiden kybervarautumistyölle.




***Kuva 8.*** *Kybervarautuminen ja sen kehittäminen terveydenhuolto-organisaatioissa – nyt ja tulevaisuudessa*

Synteesin perusteella voidaan arvioida, että sisimmän kehän asiat tunnetaan terveydenhuolto-organisaatioiden kyberhyökkäyksiin varautumisessa jo suhteellisen hyvin ja kohdeorganisaatiossa niihin liittyviä tehtäviä suorittavien henkilöiden osaaminen oli riittävällä tasolla. Mahdolliset tulevat kehitystoimet, -resurssit ja jatkotutkimus tulisikin kohdentaa kaavion kahdelle uloimmalle kehälle. Toisen kehän haasteet ja niiden taustalla vaikuttavat juurisyyt tunnistettiin tässä tutkimuksessa, niille osattiin nimetä ratkaisuja ja osaa oli jo alettu ratkaisemaan kohdeorganisaatiossakin. Tulevaisuuden kannalta haastavimman tilanteen aiheuttavat uloimman kehän sokeat pisteet, jotka onnistuttiin tunnistamaan tässä tutkimuksessa, mutta tutkimuksen perusteella ei vielä tiedetä, mitä niiden osalta pitäisi tehdä. Sokeita pisteitä tulisi tutkia tulevaisuudessa lisää, sillä esimerkiksi niihin kuuluvat harvinaisemmat erityisesti terveydenhuoltoalalla toimintaan liittyvät hyökkäysskenaariot voivat muodostaa organisaatioille merkittäviä riskejä, jos niiden toteutumiseen ei olla varauduttu.

Synteesi kuvaa siis osuvasti myös varautumisen aikaperspektiiviä: 1. tason asiat kuvaavat jo aiemmin tehtyä kehitystä ja 2. taso kuvaa nykyhetkessä tehtävää kehitystyötä. 3. taso puolestaan kuvaa mahdollisia tulevaisuuden haasteita, jotka saattavat nousta merkittäviksi terveydenhuolto-organisaatioiden kyberhyökkäysvarautumisessa tulevaisuudessa. Aiemmin tässä luvussa todettiin, että tapaustutkimuksessa käytettiin hyvin ihmiskeskeistä lähestymistapaa tutkittavaan ilmiöön, kun taas aiemmin julkaistussa kirjallisuudessa näkökulma on usein tehtäväkeskeisempi. Synteesissä tämä näkyy siinä, että eniten tutkitut ja kehitetyt tehtäväkeskeiset asiat löytyvät sisimmältä, jo hyvin osattujen varautumisen osa-alueiden kehältä. Ulompien tasojen osa-alueet puolestaan liittyvät enemmän eri tahoilla toimivien erilaisten ihmisten osaamiseen, toimintaan, osallistumiseen ja yhteistyöhön. Myös uloimman kehän hyökkäysskenaariot ovat sellaisia, että niiden toteutuminen vaikuttaisi erityisen paljon hoitotyötä tekevien ihmisten työhön.

# 8. JOHTOPÄÄTÖKSET JA YHTEENVETO

Tässä luvussa vedetään yhteen tehty tutkimus ja arvioidaan sen onnistumista. Aluksi vastataan tutkimuksen alussa asetettuihin tutkimuskysymyksiin kirjallisuuden ja empiirisen tapaustutkimuksen, sekä niiden synteesin perusteella. Sitten arvioidaan sitä, miten tutkimuksen suorittaminen on kokonaisuudessaan onnistunut ja miten laadukkaina ja luotettavina sen tuloksia voidaan pitää. Tämän jälkeen arvioidaan, millainen merkitys saavutetuilla tuloksilla on ja miten niitä voidaan hyödyntää tulevaisuudessa. Lopuksi nostetaan vielä esiin tutkimuksen aikana tunnistetut mahdolliset jatkotutkimuskohteet.

## 8.1 Johtopäätökset

Tutkimuksen aikana saatiin hyvä käsitys siitä, millaisia asioita terveydenhuolto-organisaatiot voivat tehdä ollakseen mahdollisimman hyvin varautuneita kyberhyökkäyksen tapahtumiseen. Empiirisen tapaustutkimuksen tuloksina saatiin kattava kuvaus tapausorganisaation varautumisen nykytilasta, sekä varautumisen ongelmakohdista, jotka vaativat vielä kehittämistyötä. Lisäksi tutkimuksessa tunnistettiin asioita, joista tarvitaan vielä lisää tietoa tulevaisuuden kehitystä varten. Tapaustutkimuksen ja kirjallisuuden vuoropuhelun kautta voidaan muodostaa vastaukset tutkimuksen alatutkimuskysymyksiin.

A1: Millaisia ovat terveydenhuolto-organisaatioihin kohdistuvat kyberhyökkäysuhat? (luvut 3 ja 5)

A2: Mitä terveydenhuolto-organisaatiossa tapahtuu toteutuvan hyökkäyksen aikana ja sen jälkeen?
(luvut 4 ja 5)

A3: Miten terveydenhuolto-organisaatiot edistävät hyökkäyksestä selviämistä? (luvut 4 ja 5)

A4: Mitkä ovat mahdollisia kehittymiskohteita?
(luvut 6 ja 7)

Kysymykseen A1 vastattiin luvuissa 3 ja 5. Sekä kirjallisuudesta, että haastattelujen pohjalta saatiin tunnistettua useita erilaisia kyberhyökkäysskenaarioita, joita terveydenhuolto-organisaatioihin voi kohdistua. Tapaustutkimuksessa keskeisimpään rooliin nousivat tietojärjestelmiä lamaannuttavat tai hajottavat hyökkäykset. Myös muunlaisia hyökkäyksiä kuitenkin tunnistettiin sekä haastatteluissa että kirjallisuudesta. Näitä olivat muun muassa tietovuodot ja -varkaudet, lääkintälaitteisiin kohdistuvat hyökkäykset ja

tietojärjestelmissä olevien tietojen muokkaaminen salaa. Lisäksi vakavan uhan voisi aiheuttaa myös useamman kriisitilanteen, kuten suuronnettomuuden ja kyberhyökkäyksen, samanaikainen tapahtuminen. Luvussa 7 todettiin, että harvinaisemmat, erityisesti terveydenhuolto-organisaatioille spesifit hyökkäysskenaariot vaativat vielä lisää tutkimusta, jotta niiden toteutumiseen voidaan asianmukaisesti varautua.

Kysymykseen A2 vastattiin luvuissa 4 ja 5 kirjallisuuden ja haastattelujen perusteella. Löydösten mukaan tietohallinnon tehtävänä on reagoida hyökkäykseen ja koordinoida tilannetta teknisestä näkökulmasta. Johto puolestaan koordinoi koko organisaation toimintaa sekä sisäistä ja ulkoista viestintää. Hoitotoiminnassa työskentelevät henkilöt vastaavat potilaiden hoidon turvaamisesta. Kyberhyökkäys voi häiritä hoitotyön normaaleja työskentelytapoja, jolloin otetaan käyttöön korvaavat toimintatavat. Toimintaa auttaa, jos tilanteeseen on olemassa ja saatavilla selkeät tilanteeseen soveltuvat toimintaohjeet. Keskeisimmiksi asioiksi organisaation hyökkäyksen aikaisessa toiminnassa nousivat selkeä toimintasuunnitelma, reaaliaikainen tilannekuva, tehokas toiminnan koordinointi kaikilla toiminnan osa-alueilla, toimiva viestintä ja se, että kaikki tietävät oman vastuunsa ennalta. Haastatteluissa koettiin tärkeäksi, että kriisijohtamiseen soveltuvat toimintatavat ovat eri toimintoja johtavilla henkilöillä hallussa jo valmiiksi, henkilöstön osaaminen on sisäistettyä ja mielellään myös etukäteen harjoiteltua. Tekniset suojautumismenetelmät vaikuttavat hyökkäykseen reagoinnin ja tilanteesta palautumisen onnistumiseen ja tehokkuuteen. Myös tilanteen aikana tehtävä aktiivinen yhteistyö organisaation ulkopuolisten sidosryhmien, kuten viranomaisten ja median kanssa korostui tutkimuksessa.

Kyky toimia hyökkäystilanteessa realisoituu vasta hyökkäyksen tapahtuessa, mutta sekä tapaustutkimus että kirjallisuus antoivat viitteitä siitä, että ennakkoon varautumalla voidaan edistää terveydenhuolto-organisaation kykyä toimia tapahtuvan kyberhyökkäyksen aikana. Varautumiskeinoja kysymykseen A3 vastaamiseksi esiteltiin luvuissa 4 ja 5. Sekä kirjallisuus että tapaustutkimus osoittivat, että varautuminen koskee koko organisaatiota ja sen koko henkilöstöä, ja varautumistoimenpiteitä tehdään kaikkialla organisaatiossa. Varautumiseen liittyy toisaalta hyökkäystilanteen toimintasuunnittelua, mutta myös reagointi- ja palautumiskykyä parantavien teknisten suojausmekanismien rakentamista, johtamisjärjestelmän ja viestinnän kehittämistä sekä henkilöstön osaamisen ja toimintavalmiuden kehittämistä. Olennainen osa varautumista on myös valmiuden mittaaminen ja arviointi erilaisin keinoin, jotta voidaan tunnistaa kehityskohteita ja osaamistarpeita. Erityisesti tapaustutkimus nosti hyökkäystilanteiden käytännön harjoittelun tärkeäksi keinoksi arvioida organisaation kykyä toimia häiriötilanteessa.

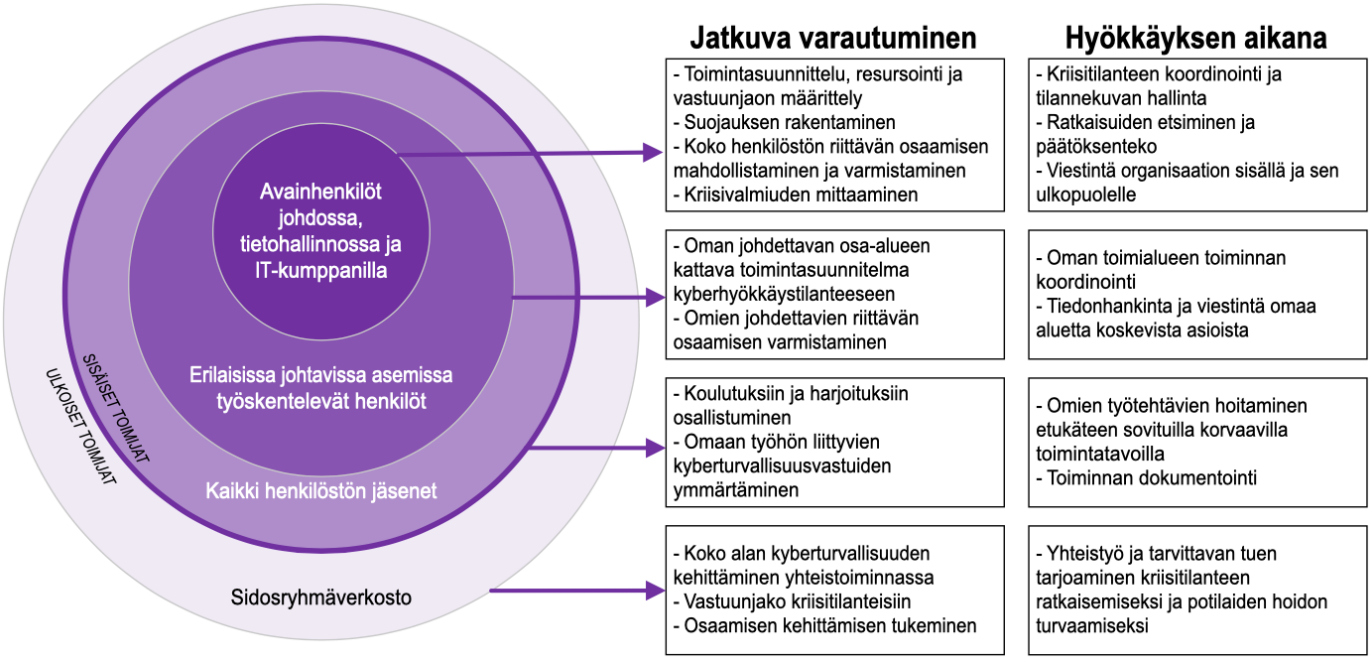
Kehityskohteita kysymykseen A4 vastaamiseksi tunnistettiin tapaustutkimuksen osalta luvussa 6. Luvussa 7 niitä verrattiin kirjallisuuteen ja arvioitiin toimia niiden ratkaisemiseksi. Tämän tutkimuksen perusteella haasteita terveydenhuolto-organisaation kyberhyökkäykseen varautumiselle aiheutuu tällä hetkellä etenkin siitä, miten suurelta osalta henkilöstöä varautuminen vaatii toimia ja sisäistettyä osaamista kaikilla organisaation tasoilla. Etenkin hoitohenkilöstön kyberosaaminen on sekä kirjallisuuden että tapaustutkimuksen perusteella usein puutteellista. Lisäksi kohdeorganisaatiossa haasteita koettiin tietohallinnon hyökkäystilanteen aikaisessa kommunikaatiossa hoitotoiminnan suuntaan, sekä tilannekuvan ymmärtämisessä ja viestinnässä koko organisaation kesken. Organisaation kehityskohteeksi tunnistettiin myös toimintaohjeiden puutteellinen saatavuus ja soveltuvuus erilaisiin, etenkin pitkäkestoisempiin kyberhyökkäystilanteisiin. Sekä tapaustutkimuksessa että kirjallisuudessa kyberhyökkäysvarautumisen ongelmaksi nousi myös lääkintälaitteiden heikko tietoturva. Luvussa 7 tunnistettiin yleisemmällä tasolla tulevaisuuden kehityskohteita terveydenhuolto-organisaatioiden kyberhyökkäyksiin varautumiseen ja aiheen tutkimukseen. Tällaisia olivat esimerkiksi harvinaisempien kyberhyökkäysskenaarioiden toteutumiseen varautuminen sekä tulevaisuudessa mahdollisesti lisääntyvä tarve keskittää julkisten toimijoiden kyberturvallisuustoimintoja yhteen. Myös hoitotyön ja kyberhyökkäysvarautumisen yhteensovittaminen on vielä kesken. Molempien alojen asiantuntijoiden välisen yhteistyön ja vuoropuhelun lisääminen on tarpeen, jotta hoitotyön asettamat vaatimukset tulevat paremmin huomioiduiksi varautumisessa. Myös molemmat alat tunteville spesialisteille voi olla tulevaisuudessa tarvetta.

Alatutkimuskysymyksiin muodostettujen vastausten perusteella voidaan vastata tutkimuksen päätutkimuskysymykseen, joka kuului seuraavasti:

**P: Miten terveydenhuolto-organisaatio varautuu kyberhyökkäystilanteesta selviämiseen ja miten varautumista voitaisiin kehittää?**

Koska päätutkimuskysymys on kaksiosainen, myös vastaus päätutkimuskysymykseen jakautuu kahteen osaan. Kysymyksen ensimmäiseen osaan siitä, mistä terveydenhuolto-organisaation kybervarautuminen muodostuu, vastataan kuvassa 9, luvuissa 4, 5 ja 6 tehtyjen havaintojen perusteella. Kuvassa varautuminen esitetään organisaation eri toimijoiden ja heidän vastuidensa näkökulmasta. Yksi tutkimuksen tärkeimmistä löydöksistä oli ymmärrys siitä, miten kyberhyökkäysvarautuminen vaatii osaamista ja osallistumista organisaation kaikilta ihmisiltä kaikilla sen tasoilla, ja jopa sen sidosryhmiltä. Kuvan ympyrät kuvaavat eritasoisia toimijoita ja tekstikenttiin toimijoiden viereen on kuvattu kunkin toimijatason vastuita jatkuvassa varautumisessa sekä kriisitilanteen aikana. Keskimmäisenä ympyräkaaviossa ovat tilanteen hoidosta päävastuussa olevat kriisitilanteen

kannalta keskeisimmät avainhenkilöt tietohallinnossa ja johdossa, tämän jälkeen tulevat toiminnan osakokonaisuuksien, kuten tiettyjen hoito-osastojen, johtamisesta vastaavat henkilöt. Organisaation sisällä uloimmalta kehältä löytyy jokainen henkilöstön jäsen, joilla jokaisella on myös kybervarautumiseen liittyviä vastuita. Organisaatiota rajaavan paksumman viivan ulkopuolella nähdään vielä erilaiset sidosryhmät, joilla on omat roolinsa niin varautumisessa kuin kriisitilanteen aikanakin.




***Kuva 9.*** *Terveydenhuolto-organisaatio kyberhyökkäystilanteessa: varautuminen ja toiminta eri toimijoiden vastuiden näkökulmasta*

Terveydenhuolto-organisaation kyberhyökkäysvarautumisen kehityskohtia käsiteltiin luvuissa 6 ja 7. Päätutkimuskysymyksen jälkimmäiseen osaan varautumisen kehittämisestä vastattiin jo luvussa 7, sekä pohdinnassa että kuvassa 8. Synteesikaaviossa esitettiin kuvaus terveydenhuolto-organisaatioiden kyberhyökkäysvarautumisen kehityksestä suhteessa aikaperspektiiviin. Luvussa selitettiin, minkälaiset asiat kyberhyökkäysvarautumisessa on jo aiemmin jalkautettu hyvin osaksi toimintaa, mitä asioita taas kehitetään juuri nyt ja mitä uusia asioita mahdollisesti pitää kehittää tulevaisuudessa. Nykyinen tietämys ja osaaminen kirjallisuuden ja tapaustutkimuksen mukaan on hyvin tehtäväkeskeistä ja keskittyy varautumisen formaaleihin prosesseihin. Tämän tutkimuksen perusteella varautumiseen tarvitaan lisää ihmiskeskeistä ymmärrystä erityisesti siitä, miten jokainen ihminen saadaan osaksi varautumista. Lisää tietoa ja osaamista tarvitaan myös siitä, miten hoitotyö, kyberhyökkäysvarautuminen ja näiden toisilleen asettamat vaatimukset voidaan parhaiten sovittaa yhteen.

Tutkimuksen perusteella voidaan todeta, että terveydenhuolto-organisaatio voi varautua kyberhyökkäyksestä selviämiseen muun muassa kuvassa 9 esitetyillä toimintatavoilla. Varautumiseen voidaan varmasti tunnistaa muitakin keinoja ja esimerkiksi tekniseen varautumiseen perehdyttiin tässä tutkimuksessa vain pintapuolisesti. Koska varautumisen eri osa-alueilla tehdyt valinnat vaikuttavat toisiinsa, on tärkeää ymmärtää, että varautuminen on kokonaisuus, jonka kaikkia osia tulee kehittää laaja-alaisesti yhteistyössä eri alojen asiantuntijoiden välillä. Varautumiseen on jo kirjallisuudessa ja tapaustutkimuksessa tunnistettu hyviä käytäntöjä, mutta kyberrikollisuuden ja -hyökkäysten kehittyessä myös uusia uhkia syntyy jatkuvasti. Tästä syystä kyberhyökkäyksiin varautuminen vaatii organisaatioilta jatkuvaa kehittymistä ja tulevaisuuden uhkien tunnistamista, esimerkiksi kuvassa 8 kuvattujen sokeiden pisteiden osalta. Jos varautumisessa luotetaan kaiken olevan valmista ja jäädään paikalleen, jäädään todennäköisesti askeleen verran jälkeen hyökkäysten kehityksestä ja joudutaan oppimaan asiat kantapään kautta.

## 8.2 Tutkimuksen arviointi

Alaluvussa 2.3.1 asetettiin tapaustutkimukselle laatukriteerit, joiden täyttymiseen tutkimuksessa haluttiin pyrkiä. Samoja laatukriteerejä hyödynnetään nyt tutkimuksen jälkeen tutkimuksen ja sen tulosten laadun arvioinnissa. Taulukossa 10 esitetään uudelleen alaluvun 2.3.1 laatukriteeritaulukko.

Taulukko 10. *Tutkimuksen laatukriteerit ja niiden kannalta olennaiset tutkimusvaiheet (Perustuen Yin 2014, s. 45)*

| **Laatukriteeri** | **Tutkimuksen vaihe** |
|---|---|
| Rakenteellinen validiteetti | Tutkimusmenetelmien valinta, tiedonkeruu, otannan valinta |
| Ulkoinen validiteetti | Teorian käyttö, kirjallisuuden ja empirian tutkimustulosten vertailu ja synteesi |
| Sisäinen validiteetti | Ongelmakohtien taustasyiden analyysi, hypoteesien rakennus |
| Reliabiliteetti | Tutkimusmenetelmien valinta, tiedonkeruun toteutus ja dokumentointi |

**Tutkimuksen rakenteellinen validiteetti**

Tutkimuksen rakenteellisella validiteetilla pyrittiin siihen, että valittavat tutkimusmenetelmät ja tutkimuskohteet soveltuisivat mahdollisimman hyvin tutkimuskohteena olevan ilmiön tutkimiseen (Yin 2014, s. 46). Tässä tutkimuksessa tutkimusmenetelmiksi valittiin mahdollisimman monipuolisen haastateltavajoukon haastattelut, joilla haluttiin saavuttaa kattavin ja syvällisin mahdollinen käsitys siitä, mitä eri puolella organisaatiota tapahtuu. Haastateltavien henkilöiden valinta onnistui tutkimuksessa erityisen hyvin. Haastateltavien joukossa oli todella paljon erilaista osaamista ja keskenään erilaisia näkökulmia organisaation toimintaan. Jokainen haastateltava toi kuvaan jotakin sellaista uutta tietoa, mitä muilla ei ollut.

Rakenteelliselle validiteetille eniten haasteita aiheutti tutkimuksen rajallinen resurssikehys, sillä koko organisaation toimintaa olisi voinut kuvata vielä kattavammin suuremman otannan tutkimisella. Toteutuneella haastateltavamäärällä jäi tutkimukseen väistämättä aukkoja sellaisiin organisaation osiin, joita ei tutkittu. Haastateltavat pyrittiin toki löytämään erityisesti sellaisista organisaation osista, joissa kyberhyökkäyksen vaikutukset voisivat olla erityisen kriittisiä ja joissa varautumisen tarve on siksi merkittävä. On kuitenkin mahdollista, että organisaation tutkimattomista osista olisi löydetty uusia kehityskohteita tai uusia käytössä olevia varautumiskeinoja. Haastatteluotannan kattavaa hankintaa hankaloitti osaltaan myös tutkimuksen ajoitus, kun haastattelujen aloituksen viivästymisen seurauksena monet haastattelut osuivat kesäaikaan, jolloin aikataulujen sopiminen oli haastavaa.

**Tutkimuksen ulkoinen validiteetti**

Ulkoinen validiteetti tutkii sitä, miten hyvin tutkimuksesta saatavia tuloksia voidaan yleistää koskemaan muita kuin tutkittavina olevia tilanteita tai organisaatioita (Yin 2014, s. 234). Kuten aiemmin todettiin, tämän tutkimuksen empiirisessä osassa tutkittiin vain yhtä organisaatiota, joten tapaustutkimuksesta saatuja tuloksia ei voida suoraa yleistää kuvaamaan kaikkia terveydenhuolto-organisaatiota. Koska organisaation kaikkia osastoja ei tutkittu, on myös kyseenalaista, voidaanko tutkimustuloksia yleistää täysin koskemaan edes tutkittua organisaatiota. Yleistettävämpiä tuloksia olisi voitu saavuttaa tutkimalla useampia osastoja tai jopa useampia organisaatioita, mutta se ei tutkimuksen resurssien ja aikakehyksen puitteissa ollut mahdollista. Vastaavanlaisen tutkimuksen toteuttaminen jälkikäteen organisaation muissa osissa tai toisissa organisaatioissa on kuitenkin mahdollista tutkimusmenetelmien huolellisen raportoinnin ansiosta.

Tutkimustulosten yleistettävyyttä haettiin tässä tutkimuksessa vertailemalla empiirisessä osuudessa tehtyjen havaintoja kirjallisuudesta löydettävään teoriatietoon ja hakemalla

näistä yhtäläisyyksiä ja eroavaisuuksia tutkimuksen synteesiosiossa. Näitä yhtäläisyyksiä onnistuttiin löytämään kattavasti ja vaikuttaisikin siltä, että tapaustutkimuksen organisaation toiminta ja haasteet vastasivat alalla yleisesti vallitsevia käsityksiä.

**Tutkimuksen sisäinen validiteetti**

Tutkimuksen sisäinen validiteetti arvioi sitä, miten hyvin ja uskottavasti tutkimuksen perusteella pystytään hahmottamaan syy-seuraus-suhteita, selittämään tutkittavaa ilmiötä ja sitä, miksi jotkin asiat tapahtuvat. (Yin 2014, s. 47) Tässä tutkimuksessa pääpaino oli tutkittavan organisaation toiminnan kuvailemisella, mutta esimerkiksi organisaation kokemiin haasteisiin pyrittiin myös etsimään syitä niin tapaustutkimuksesta kuin kirjallisuudestakin. Sisäiseen validiteettiin pyrittiin tässä tutkimuksessa vertailemalla haastateltavien vastauksia ja kirjallisuutta, sekä rakentamaan niitä yhdistelemällä mahdollisia selityksiä ilmiöille. Tämä onnistui tutkimuksessa hyvin, sillä tapaustutkimus ja kirjallisuus täydensivät hyvin toisiaan ja ne tarjosivat tunnistetuille ilmiöille toisiaan tukevia selityksiä.

Sisäisen validiteetin kannalta huomionarvoista tässä tutkimuksessa on myös se, että kaikki haastateltavien esittämät kommentit olivat yhtä tärkeitä tutkimustulosten tulkinnassa. Kaikilla oli omat spesifit osaamisalueensa, ja siten myös paras tietämys niihin liittyvistä asioista. Näin ollen tässä tutkimuksessa ei ollut merkitystä sillä, kuinka monta kertaa jokin asia mainittiin haastateltavien vastauksissa. Jotkin asiat toki toistuivat, mutta jos vain yksi henkilö mainitsi jonkin yksityiskohdan, se johtui todennäköisesti yleensä siitä, etteivät muut tienneet siitä.

Sisäisen validiteetin haasteet liittyivät tässä tapaustutkimuksessa erityisesti siihen, että osalla haastateltavista ei välttämättä ollut kovin kokonaisvaltaista käsitystä koko organisaation varautumisen tilanteesta. Osa haastateltavien vastauksista perustui siis enemmänkin spekulaatioon ja arvailuun kuin tietoon, ja jotkut vastaukset sisälsivät myös ristiriitaisuuksia toisten haastattelujen kanssa. Eri organisaation osissa vallitsevien ristiriitaisten käsitysten havaitseminen on toki hyödyllinen havainto, mutta toisinaan se saattaa antaa myös aihetta vastausten uskottavuuden kyseenalaistamiselle. Alustavia tutkimustuloksia päästiin myös katsastamaan tutkimuksen aikana organisaation avainhenkilöiden kanssa validiteetin varmistamiseksi.

**Tutkimuksen reliabiliteetti**

Tapaustutkimuksen reliabiliteetilla tarkoitettiin tutkimuksessa käytettävien tutkimusmenetelmien johdonmukaisuutta ja toistettavuutta (Yin 2014, s. 240). Tässä tutkimuksessa reliabiliteetin varmistamiseen pyrittiin objektiivisen tutkimusotteen ja hyvän tieteellisen käytännön noudattamisella haastattelutilanteissa, ja sillä, että tutkimuksen suorittaminen

ja tiedonkeruussa käytetyt menetelmät dokumentoitiin lukuun 2 mahdollisimman kattavasti ja läpinäkyvästi.

Tämän tutkimuksen reliabiliteetille haasteita aiheutti erityisesti osan haastateltavista henkilöistä vajavainen tietämys kyberhyökkäyksistä yleisesti. Tämä johti tarpeeseen antaa haastateltaville pohjatietoa kyberhyökkäystilanteista. Tämä saattoi osaltaan johdatella haastateltavien vastauksia ja vaikuttaa siten tutkimuksen objektiivisuuteen. Toisaalta selvennys siitä, mistä kyberhyökkäystilanteessa on kyse, oli tarpeen, jotta haastateltavat pystyivät vastaamaan kysymyksiin. Tulokset olisivat kuitenkin saattaneet olla erilaisia, mikäli haastateltaville olisi annettu erilaista tietoa mahdollisista kyberhyökkäystilanteista tai mikäli tietoa ei olisi annettu ollenkaan. Tämän haasteen vaikutuksia tutkimuksen reliabiliteettiin pyrittiin minimoimaan tekemällä haastateltaville annetut tiedot mahdollisimman näkyviksi tässä tutkimusraportissa.

On vaikeaa arvioida, olisiko objektiivisuuden säilyttämisessä koettu haaste ollut vältettävissä jollakin keinolla. Ohjaavan vaikutuksen läpinäkyvyyttä olisi voinut kehittää siten, että olisi valmisteltu ennakkotietopaketti, joka olisi jaettu samanlaisena kaikille haastateltaville ja sitten liitetty osaksi tutkimusraporttia. Nyt jokaista haastateltavaa tuettiin tilanteissa vain sen verran, kun nämä tarvitsivat. Ennakkotietopaketti olisi antanut haastateltaville yhtenäisemmät lähtökohdat haastattelutilanteisiin, mutta toisaalta tällöin eroavaisuudet henkilökunnan tietämyksessä olisi voinut olla haastavampaa havaita. Sama vaikutus olisi voinut olla myös sillä, että kysymykset olisi jaettu haastateltaville ennakkoon, jolloin he olisivat voineet etsiä tietoa itse etukäteen. Tietämyspuutteiden havaitsemisessa nyt käytetty menettely toimi, sillä ensin saatiin selville haastateltavien sen hetkinen tietämys ja sitten sitä täydennettiin sen verran, että he saattoivat vastata omaa toimintaansa häiriötilanteessa koskeviin kysymyksiin. Tällaisen menettelyn voidaan myös katsoa jossakin määrin vastaavan kyberhyökkäyksen tositilannetta, jossa henkilöstön jäsen ei aluksi tiedä, mistä on kyse, mutta hänelle pyritään antamaan sen verran tietoa, että hän pystyy toimimaan ja tekemään päätöksiä omiin tehtäviinsä liittyen.

**Muita huomioita tutkimuksen tekemisestä**

Tutkimusta tehtäessä huomattiin, että rajauksen asettaminen kyberhyökkäystilanteen varautumiskäytäntöjen ja ennaltaehkäisevien tietoturvakäytäntöjen väliin on haastavaa. Osa ennaltaehkäisevistä tietoturvakäytännöistä nimittäin toisaalta ehkäisee hyökkäyksien mahdollisuutta, mutta samanaikaisesti myös parantaa organisaatioiden edellytyksiä selvitä kyberhyökkäystilanteesta tehokkaasti ja nopeasti. Tutkimuksen alussa ajatuksena oli tutustua erityisesti sellaisiin käytäntöihin, jotka liittyvät hyökkäykseen reagoimiseen ja siitä palautumiseen. Tutkimuksen edetessä oivallettiin kuitenkin hyvin nopeasti,

että myös esimerkiksi teknisten suojauskäytäntöjen valinnalla, tietoturvan resursoinnilla ja henkilöstön tietoturvatietoisuudella on ratkaisevia vaikutuksia siihen, kuinka hyvin tilanteesta voidaan selvitä.

## 8.3 Tutkimustulosten merkitys ja hyödyntäminen

Tämä tutkimus tuotti lisää tietoa siitä, mitä terveydenhuolto-organisaatioissa pitäisi tapahtua kyberhyökkäyksien toteutuessa, sekä erityisesti siitä, mitä siellä oikeasti saattaisi tapahtua. Lisäksi tutkimuksen aikana tunnistettiin monia toimia, joilla organisaatiot voivat etukäteen parantaa toimintakykyään yllättävissäkin kriisitilanteissa. Erilaisia tehtäväkeskeisiä kyberturvallisuusoppaita terveydenhuolto-organisaatioiden toimintaan ja varautumiseen on tuotettu Suomessa jo useita eri tahojen toimesta. Tämän tutkimuksen uutuusarvo suhteessa olemassa olevaan tutkimukseen muodostuu ihmiskeskeisestä näkökulmasta, henkilöstön toimintaan keskittyvästä tapausorganisaation nykytilan kuvauksesta, ja Norri-Sederholm et al. (2019) peräänkuuluttamasta hoitohenkilökunnan näkökulman mukaan tuomisesta. Myös tapausorganisaation kohdalla tietoa varautumisen tilasta oli aiemmin saatu vain tietohallinnon ja johdon näkökulmasta, joten tutkimuksella onnistuttiin tuottamaan myös organisaatiolle täysin uutta tietoa siitä, miten varautuneita sen muissa osissa ollaan.

Uutuusarvoa kybervarautumisen tutkimukselle tuottaa myös luvussa 7 tehty kirjallisuuden ja tapaustutkimuksen synteesi, jossa terveydenhuolto-organisaation kyberhyökkäysvarautumista tarkasteltiin suhteessa jo tehtyyn kehitykseen, nykyhetkessä tapahtuvaan kehitykseen ja tulevaisuuden kehitystarpeisiin. Erityisesti tulevaisuuden kehityskohteiksi tunnistetut kybervarautumisen ”sokeat pisteet” luovat tietoa siitä, millaisia asioita terveydenhuolto-organisaatioiden on otettava tulevaisuudessa huomioon kyberrikollisuuden kehittyessä jatkuvasti. Myös haastatteluissa tunnistetut nykyhetken ongelmakohdat, niiden vertailu kirjallisuuden kanssa sekä löydösten yhdistämisen perusteella muodostetut ratkaisuehdotukset tuovat etenkin kohdeorganisaatiolle käyttökelpoista tietoa tulevaisuuden toimintaan. Monia kybervarautumisen ongelmakohtiin esitettyjä ratkaisuita on kirjallisuuden mukaan jo onnistuneesti toteutettu hieman erilaisissa konteksteissa muualla, mikä luo uskoa siihen, että tapausorganisaationkin ongelmakohdat ovat ratkaistavissa. Tutkimuksessa tunnistettiin myös tarve kehittää monialaista, sekä hoitotyön että kyberturvallisuuden kattavaa, osaamista ja ymmärrystä, jotta terveydenhuollon ja kyberhyökkäysvarautumisen vaatimukset ja tarpeet saataisiin sovitettua paremmin yhteen. Kohdeorganisaatiossa tällaista ymmärrystä voidaan tulevaisuudessa lisätä esimerkiksi sen nykyisten osaajien välisen yhteistyön tiivistämisellä.

Tutkimustuloksia päästään toivottavasti hyödyntämään käytännössä niin tutkitussa organisaatiossa kuin terveydenhuollon toimialalla laajemminkin. Toiminnan kehittäminen ratkaisuehdotusten mukaisesti, tunnistetut tulevaisuuden kehitystarpeet huomioiden, voi nostaa organisaatioiden toimintakykyä ja valmiutta toimia tapahtuvassa kyberhyökkäystilanteessa. Tutkimuksen tuloksia voidaan hyödyntää myös osana REPCHEALS-tutkimusprojektin lopputuloksia, joissa arvioidaan terveydenhuoltojärjestelmän kriisivalmiutta laajemmassa mittakaavassa. Tällöin tämän tutkimuksen löydöksiä voidaan verrata muiden tutkimusalueiden tuloksiin ja sitä kautta voidaan selvittää, onko terveydenhuolto-organisaatioiden kriisitoiminnassa ja -varautumisessa joitakin sellaisia erityispiirteitä tai haasteita, jotka toistuvat kriisien tyypeistä riippumatta. Erilaisten kriisitilanteiden toimintaa vertailemalla voidaan myös siirtää oppeja ja hyviä käytäntöjä kriisitilanteesta toiseen varautumisen eri osa-alueille. Jo tämän tutkimuksen haastatteluissa kävi ilmi, että Covid-19 –kriisi oli opettanut henkilöstölle paljon käytännön toiminnasta kriisitilanteissa, joten tällaisia synergiamahdollisuuksia kannattaa etsiä lisää tämän tutkimuskokonaisuuden kautta. Parhaimmillaan REPCHEALS-projektin tulosten avulla voidaan kehittää koko Suomen terveydenhuoltojärjestelmän kriisivalmiutta aiempaa paremmaksi.

## 8.4 Jatkotutkimustarpeet tulevaisuuteen

Tämän tutkimus ja etenkin sen empiirisen tapaustutkimuksen toimintakuvaus keskittyi erityisesti tunnetuimpien kyberhyökkäysskenaarioiden käsittelyyn. Tämä oli luonnollista, sillä haastateltavien oli helpompaa ajatella toimintaansa jo jossakin tapahtuneissa skenaarioissa, kuin keksiä itse uusia. Mielenkiintoisena jatkotutkimuskohteena voidaan tämän tutkimuksen perusteella kuitenkin nostaa esiin varautuminen ja toiminta vielä harvinaisemmissa, erityisesti terveydenhuollon toimintaympäristölle spesifeissä kyberhyökkäysskenaarioissa, joita käsiteltiin luvussa 7. Tällaisia voivat olla esimerkiksi hybridikriisitilanteet, tietojen muokkaaminen salaa tai potilaissa kiinni olevien laitteiden etäohjaus, joita tässä tutkimuksessa sivuttiin muutamaan otteeseen. Tällaisia skenaarioita ei vielä kirjallisuudesta tai haastateltavien kokemuspiiristä juuri löytynyt, mutta haastateltavien vastauksista nousi esiin, että sellaisten sattuessa kyberhyökkäysvalmius voisi olla heikompi ja toisaalta seuraukset vakavampia, kuin tunnetummissa hyökkäysskenaarioissa, eikä harvinaisempiin skenaarioihin välttämättä ole ohjeistuksiakaan. Erityisesti hybridikriisitilanteista oli hyvin haastavaa löytää tietoa kirjallisuudesta. Kuten jo luvussa 7 todettiin, näiden skenaarioiden tutkiminen ja niihin varautuminen voi olla tarpeen tulevaisuudessa kyberrikollisuuden kehittyessä jatkuvasti.

Toinen mielenkiintoinen, tähän tutkimukseen liittyvä tutkimusaihe voisi olla Candolinin (2020) mainitsema mahdollinen tarve keskittää yhteiskunnan kriittisten toimintojen kyberturvallisuutta ja -puolustautumista, sekä sen johtamista entisestään. Monissa muissa yhteiskunnan toimintakykyä koskevissa puolustautumistilanteissa vastuu koko infrastruktuurin suojelemisesta on keskitetysti puolustusvoimilla. Kuten tutkimuksen aikana todettiin, tulevaisuuden jatkuvasti kehittyvä rikollisuus ja entisestään digitalisoituva toimintaympäristö vaativat organisaatioilta paljon osaamisen ja suojausinfrastruktuurin jatkuvaa kehittämistä ja terveydenhuolto-organisaatioiden ja niiden työntekijöiden vastuulla on merkittävä osa yhteiskunnan huoltovarmuudesta ja toimintakyvystä. Kybervarautuminen on vaativaa ja useissa kirjallisuuslähteissä todettiinkin valmiuden olevan terveydenhuolto-organisaatioissa usein liian alhainen. Sekä kirjallisuus että tapaustutkimus korostivat sidosryhmäyhteistyön merkitystä, joten olisikin mielenkiintoista tutkia, olisiko julkisen sektorin terveydenhuollon kyberturvallisuustoimintaa mahdollista tai tarpeellista keskittää entisestään, ja saataisiinko suojausta siten kehitettyä vahvemmaksi.

Koska tämän tutkimuksen empiirinen osio käsitteli vain yhtä organisaatiota, voisi olla mielenkiintoista tutkia samoja asioita myös muissa terveydenhuollon organisaatioista. Toisista organisaatioista kerättyä tietoa voitaisiin tällöin verrata tämän tutkimuksen tuloksiin, jolloin tuloksista voitaisiin saada yleistettävämpiä. Tällöin olisi myös mahdollista muodostaa yleisempiä johtopäätöksiä suomalaisen terveydenhuoltojärjestelmän kybervarautumisen nykytilasta. Toiset tutkittavat organisaatiot voisivat olla kooltaan ja tehtävältään joko samankaltaisia tai aivan erilaisia. Samankaltaisten organisaatioiden tutkimisella voitaisiin saavuttaa vertailukelpoisempia tuloksia, mutta toisaalta esimerkiksi pienempien organisaatioiden tutkiminen voisi antaa aiheeseen aivan uusia näkökulmia. Pienemmillä organisaatioilla on usein käytössään vähemmän resursseja, joten voisi olla mielenkiintoista selvittää, miten se vaikuttaa kybervarautumisen toteuttamiseen.

Kokonaisuudessaan terveydenhuolto-organisaation kybervarautumisen tutkimusaihe oli erittäin mielenkiintoinen ja siinä on vielä paljon sijaa lisätutkimukselle. Erityisen tärkeää olisi tutkia vielä paljon lisää sitä, millaisia erityispiirteitä juuri terveydenhuoltoalalla toiminen tuo kyberhyökkäyksiin varautumiseen. Tarvetta olisi etenkin tutkimukselle siitä, miten terveydenhuollon ja kyberturvallisuuden toimialojen välistä yhteistyötä ja ymmärrystä voidaan lisätä kyberhyökkäysvarautumisen kehittämiseksi. Lisäksi organisaatioiden hoitohenkilökunnan varautumisen tasoa ja keinoja voisi olla syytä tutkia enemmänkin. Kyberhyökkäykset voivat tuoda mukanaan suuria ja vaarallisiakin seurauksia, joten hyökkäystilanteissa toimimista ei kannata jättää opeteltavaksi kantapään kautta. Tulevaisuudessa olisikin syytä selvittää, miten eri alojen ammattilaiset voidaan aidosti valmentaa toimintaan jatkuvasti kehittyvien kyberuhkien edessä.

# LÄHTEET


Ahn, M. K., Kim, Y. H. & Lee, J-R. (2020). *Hierarchical Multi-Stage Cyber Attack Scenario Modeling Based on G&E Model for Cyber Risk Simulation Analysis.* Applied sciences 10.4 (2020): 1426–.

Ayala, L. (2016). *Cyber-Physical Attack Recovery Procedures A Step-by-Step Preparation and Response Guide*. 1st ed. 2016. Berkeley, CA: Apress, 2016.

Bahuguna, A., Bisht, R. K. & Pande J. (2019) *Assessing cybersecurity maturity of organizations: An empirical investigation in the Indian context*. Information Security Journal: A Global Perspective, 28:6, pp. 164-177

Bhamra, R., Dani, S., & Burnard, K. (2011). *Resilience: The Concept, a Literature Review and Future Directions*. International journal of production research 49.18): pp. 5375–5393.

Burnard, K. J. & Bhamra, R. (2019). *Challenges for Organisational Resilience. Continuity & Resilience Review.* 1.1. pp. 17–25.

Candolin, C. (2020) *CyberCatch FI – Vieraana Catarina Candolin.* 11.8.2020. Saatavilla: https://www.cyberwatchfinland.fi/fi/cybercatchfi-vieraana-catharina-candolin/ (viitattu 1.9.2021)

Candolin, C. (2008). *A Security Framework for Service Oriented Architectures.* MILCOM 2007 - IEEE Military Communications Conference, 2007, pp. 1-6

Casson-Moreno, V., Reniers, G., Salzano, E. & Cozzani, V. (2018). *Analysis of physical and cyber security-related events in the chemical and process industry.* Process Safety and Environmental Protection. Volume 116. 2018. pp. 621-631

Coronado, A. J., & Wong, T. L. (2014). *Healthcare Cybersecurity Risk Management: Keys to an Effective Plan.* Biomedical instrumentation & technology 48. SPRING (2014). 26–30.

Digi- ja väestötietovirasto. (2021). *Testaa organisaatiosi digiturva TAISTO-harjoituksessa!* Saatavilla: https://dvv.fi/taisto (viitattu 15.1.2022)

Donchin, Y., & Daniel Gopher. (2014). *Around the Patient Bed: Human Factors and Safety in Health Care.* 1st edition. Boca Raton: Taylor & Francis, 2014.

Feng X. Q., Acord L., Cheng, Y. J., Zeng, J. H. & Song, J. P. (2011). *The Relationship between management safety commitment and patient safety culture.* International Nursing Review 58 (2), pp. 249—254.

Finto. (2021). *Elective Surgical Procedures*. Suomalainen asiasanasto- ja ontologiapalvelu. Muokattu 3.5.2021. Saatavilla: http://finto.fi/mesh/fi/page/D017558?clang=en (viitattu 28.10.2021)

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, Volume 31, Issue 1.

Groves, P. S., Meisenbach, R. J. & Scott-Cawiezell J. (2011). *Keeping patients safe in healthcare organizations: structuration theory of safety culture.* Journal of Advanced Nursing 67 (8), pp. 1846-1855.

Hacker, J. S. (2004). *Review Article: Dismantling the Health Care State? Political Institutions, Public Policies and the Comparative Politics of Health Reform*. British journal of political science 34.4 (2004): pp. 693–724.

Hakkarainen, K. (2020). *Vastaamo: Tietomurtoja saattoi olla kaksi – Toimi näin, jos epäilet tietojasi varastetun tai olet saanut kiristysviestin.* Helsingin Sanomat. 25.10.2020. Saatavilla: https://www.hs.fi/kotimaa/art-2000006698960.html (viitattu 1.9.2021)

Heikkilä, M. (2020). *Nainen kuoli ambulanssiin, kun kyberhyökkäys jumitti saksalaisen sairaalan tietojärjestelmän – syyttäjä avasi harvinaisen henkirikostutkimuksen*. YLE. 19.9.2020. https://yle.fi/uutiset/3-11553530 (viitattu 1.9.2021)

Hellenberg, T., Talvitie, H., Visuri, P. & Volanen, R. (2011). *Myrskyn silmässä: Suomi ja uudet kriisit.* WSOYpro.

Huang, K., Siegel, M. & Madnick, S. (2018). *Systematically Understanding the Cyber Attack Business: A Survey*. ACM computing surveys, 2018-09-06, Vol.51 (4), pp. 1-36

Hubbard, T. Weber, T. G. & Steinhoff, J. C. (2017) *Protecting Data Assets in a Perilous Cyber World*. The journal of government financial management 66.3: pp. 26–31.

Kiviluoma, A., Roos, M., Herttuala, N., Leikkola, P. & Suominen, T. (2020). *Hoitohenkilökunnan arvio leikkausosastosta ammatillisena toimintaympäristönä.* Yhteiskuntatieteiden tiedekunta - Faculty of Social Sciences. Tampere University N.p.

Kshetrimayum, N., Bennadi, D. & Siluvai, S. (2019). *Stress Among Staff Nurses: A Hospital-Based Study.* Journal of Nature and Science of Medicine 2.2 (2019): pp. 95–100.

Kwon, C. & Hwang, I. (2016). *Cyber attack mitigation for cyber–physical systems: hybrid system approach to controller design.* IET Control Theory & Applications. Volume 10. Issue 7 April 2016. pp. 731–741.

Kyberturvallisuuskeskus. (2021a). *Kyberturvallisuuskeskus kriittisten toimijoiden tukena vakavissa kyberhyökkäyksissä.* 11.1.2021. Saatavilla: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kyberturvallisuuskeskus-kriittisten-toimijoiden-tukena-vakavissa-kyberhyokkayksissa (viitattu 1.9.2021)

Kyberturvallisuuskeskus. (2021b). *Kybermittari.* Saatavilla: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittari_esittely_v1.pdf (viitattu 15.1.2022)

Krexner, R. & Duftschmid, G. (2014). *Plug-and-play Integration of dual-model based Knowledge Artefacts into an Open Source EHR System.* Section for Medical Information Management and Imaging Center for Medical Statistics. Informatics and Intelligent Systems Medical. University of Vienna, Itävalta.

Kvist, T., Voutilainen, A., Mäntynen, R., & Vehviläinen-Julkunen, K. (2014). *The relationship between patients' perceptions of care quality and three factors: Nursing staff job satisfaction, organizational characteristics and patient age*. BMC Health Services Research, 14:466.

Kyytsönen, M., Hyppönen, H., Koponen, S., Kinnunen, U-M., Saranto, K., Kivekäs, E., Kaipio, J., Lääveri, T., Heponiemi, T. & Vehko, T. (2020). *Tietojärjestelmät Sairaanhoitajien Työn Tukena Eri Toimintaympäristöissä: Kokemuksia Tuotemerkeittäin*. 12.3.2020. Finnish Journal of eHealth and eWelfare.

Leineweber, C. et al (2016). *Nurses' Practice Environment and Satisfaction with Schedule Flexibility Is Related to Intention to Leave Due to Dissatisfaction: A Multi-Country, Multilevel Study.* International journal of nursing studies 58 (2016): pp. 47–58.

Libicki, M. C. (2012). *Crisis and Escalation in Cyberspace*. Santa Monica, CA: RAND, Project Air Force, 2012.

Lovis, C. (2014*). EHealth - For Continuity of Care: Proceedings of MIE2014*. Amsterdam: IOS Press. Studies in Health Technology and Informatics.

Maryati, M. J. (2015). *A case study evaluation of a Critical Care Information System adoption using the socio-technical and fit approach*. International Journal of Medical Informatics. Volume 84. Issue 7.

Misser, N. S., Jaspers, J., Van Zaane, B., Gooszen, H. & Versendaal, J. (2020). *A Protocol for the Implementation of New Technology in a Highly Complex Hospital Environment: The Operating Room.* International journal of networking and virtual organisations. 22.2.2020. (2020): pp. 199–217.

Mykkänen, M., Miettinen, M., Siponen, T., & Saranto, K. (2021). *Sairaalan reaaliaikainen tilannekuva päivittäisessä johtamisessa*. Finnish Journal of EHealth and EWelfare, 13(4), pp. 425–441.

National Institute of Standards and Technology: NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. 16.4.2018. Version 1.1.

Norri-Sederholm, T., Laitinen, T., Lehto, M & Kari, M. J. (2019). *Terveydenhuolto Ja Kyberuhkat*. Finnish Journal of eHealth and eWelfare 11.1-2 (2019): pp. 86–99.

Opedal, S. & Rommetvedt, H. (2010). *From Politics to Management – or More Politics?* Public Management Review, 12:2, pp. 191-212.

Owens, B. (2020). *How Hospitals Can Protect Themselves from Cyber Attack.* Canadian Medical Association journal (CMAJ) 192.4 E101–E102.

Pulliainen, M. (2020). *Varoitus: kyberhyökkäyksistä sairaaloihin tulossa globaali trendi, kasvu Euroopassa ”hälyttävää”*. Tekniikka ja talous. 12.11.2020. Saatavilla: https://www.tekniikkatalous.fi/uutiset/tt/f3d302d3-8fff-43ee-80f8-cda61a1eaf34 (viitattu 1.9.2021)

Sanastokeskus TSK ry. (2018). *Kyberturvallisuuden sanasto*. TSK 52. Viestintävirasto. Huoltovarmuuskeskus. Turvallisuuskomitea. Helsinki 2018. Saatavilla: https://www.tsk.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf (viitattu 26.3.2021)

Saranto, K., Koponen, S., Kivekäs, E., & Vehko, T. (2021). *Assessments of nurses' experiences of patient and client information system usage in joint health care and social welfare services and overall in health care.* Finnish Journal of EHealth and EWelfare, 13(4), pp. 332–346.

Saunders, M., Lewis, P. & Thornhill, A. (2009). *Research Methods for Business Students*. 5. ed. Harlow: Prentice Hall, Print.

Scandurra, I., Hägglund, M., Persson, A. & Åhlfelt, R-M. (2013). *Disturbing or facilitating? – On the Usability of Swedish eHealth Systems*. Uppsala University. Department of Information Technology. Karolinska Institutet. Health Informatics Centre. University of Skövde. School of Informatics.

Schramm, W. (1971). *Notes on the case studies of instructional media projects*. Working paper for the Academy for Educational development. Washington, DC.

Sharma, M., Branscum, P. W., & Atri, A. (2014) *Introduction to Community and Public Health*. Hoboken: Wiley, 2014.

Somers, S. (2009). *Measuring Resilience Potential: An Adaptive Strategy for Organizational Crisis Planning.* Journal of contingencies and crisis management 17.1 pp. 12–23.

Sosiaali- ja terveysministeriö. (2019). *Kyberturvallisuus. Ohje sosiaali- ja terveydenhuollon toimijoille.* Saatavilla: http://urn.fi/URN:ISBN:978-952-00-4085-7 (viitattu 1.9.2021)

STT. (2021). *Kiristysohjelma sulki Irlannin terveydenhuollon tietojärjestelmän – ministeri: Todennäköisesti vakavin kyberhyökkäys Irlannissa*. YLE. 14.5.2021. Saatavilla: https://yle.fi/uutiset/3-11932194 (viitattu 1.9.2021)

Taleb, N. N. (2007). *Musta joutsen: erittäin epätodennäköisen vaikutus*. Helsinki: Terra Cognita. Suom: Pietiläinen, K.

Terveyden ja hyvinvoinnin laitos. (2020). *Muutosjoustavuus, kriisivalmius ja huoltovarmuus suomalaisessa terveydenhuolto-järjestelmässä (RECPHEALS).* Päivitetty: 22.9.2021. Saatavilla: https://thl.fi/fi/tutkimus-ja-kehittaminen/tutkimukset-ja-hankkeet/muutosjoustavuus-kriisivalmius-ja-huoltovarmuus-suomalaisessa-terveydenhuoltojarjestelmassa-recpheals- (viitattu 5.11.2021)

Terveydenhuoltolaki 1326/2010, Annettu 01.05.2011. Saatavilla: https://www.finlex.fi/fi/laki/smur/2010/20101326 (viitattu 1.9.2021)

Tikanmäki, I & Ruoslahti, H. (2021). *Interdependence of Internal and External Security.* European Conference on Cyber Warfare and Security. Reading: Academic Conferences International Limited. 2021. 425–XV.

Tipton, H. & Krause, M. (2004). *Information Security Management Handbook*. Fifth Edition. Auerbach.

Turunen, E., Mäntynen, R., Kvist, T., Miettinen, M., Vehviläinen-Julkunen, K., Turunen, H. & Partanen, P. (2015). *Sairaalan potilasturvallisuuskulttuuri sairaanhoitajien arvioimana: Pitkittäistutkimus yhden yliopistosairaalan erityisvastuualueella.* Hoitotiede, 27(2). pp. 148–162.

Turvallisuuskomitea. (2021). *Ennakointi ja varautuminen*. Saatavilla: https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/ennakointi-ja-varautuminen/ (viitattu 1.9.2021)

Valmiuslaki 1552/2011, Annettu 01.03.2012. Saatavilla: https://www.finlex.fi/fi/laki/ajantasa/2011/20111552#O1L3P12 (viitattu 1.9.2021)

Virkanen, H. & Mykkänen, J. (2014). *Analysis of Central Enterprise Architecture Elements in Models of Six eHealth Projects.* Studies in health technology and informatics 205 (2014): pp. 141–145.

Watters, P. A., McCombie, S., Layton, R. & Pieprzyk, J. (2012). *Characterising and Predicting Cyber Attacks Using the Cyber Attacker Model Profile.* Journal of money laundering control 15.4 (2012): pp. 430–441.

Weber, M., Hacker, J. & Brocke, J. (2021). *Resilience in Information Systems Research - A Literature Review from a Socio-Technical and Temporal Perspective.* Conference: 42nd International Conference on Information Systems (ICIS 2021).

Willing, M., Dresen, C., Gerlitz, E., Haering, M., Smith, M., Binnewies, C., Guess, T., Haverkamp, U. & Schinzel, S. (2021). *Behavioral Responses to a Cyber Attack in a Hospital Environment.* Scientific reports 11.1 (2021): pp. 19352–19352.

Witkoski, A & Dickson, V. V. (2010). *Hospital Staff Nurses' Work Hours, Meal Periods, and Rest Breaks: A Review from an Occupational Health Nurse Perspective*. Workplace health & safety 58.11 (2010): pp. 489–497.

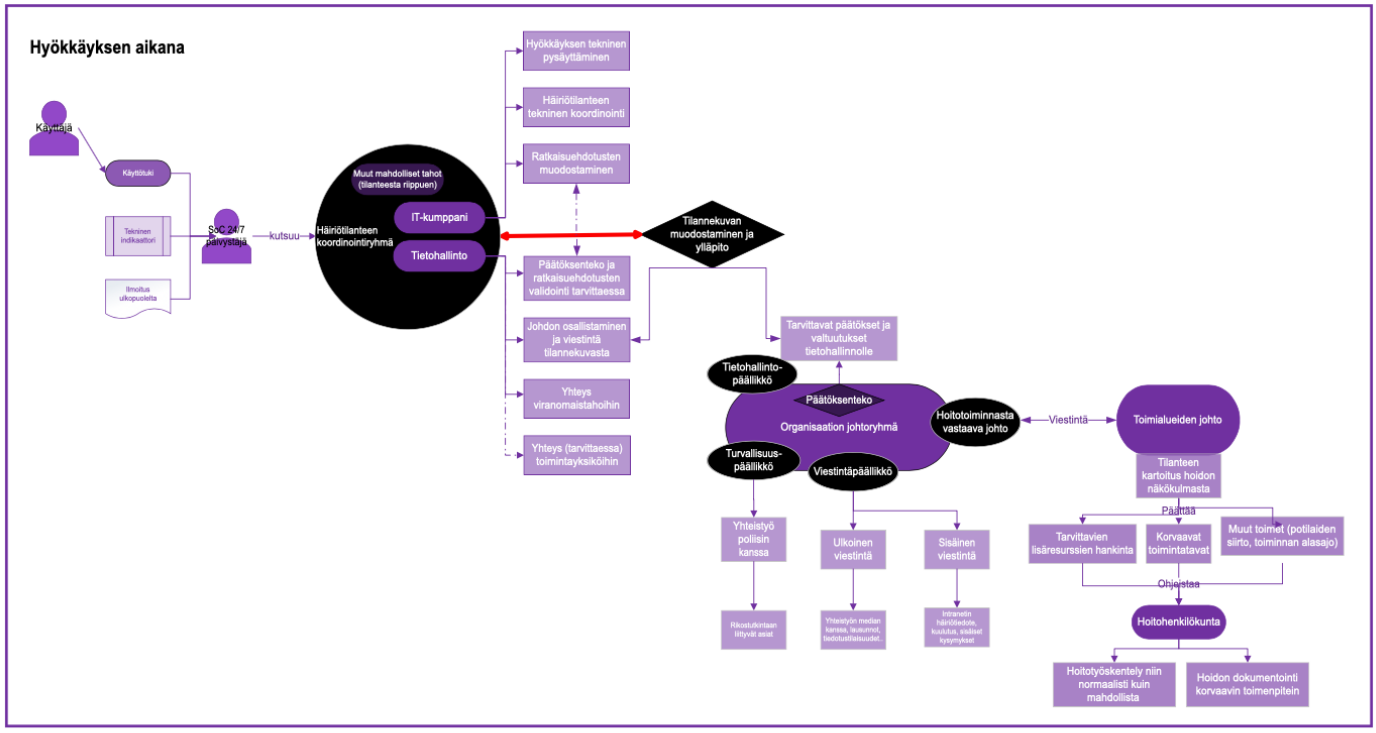
Yin, R. K. (2014). *Case Study Research: Design and Methods*. 5th edition. Los Angeles: SAGE.

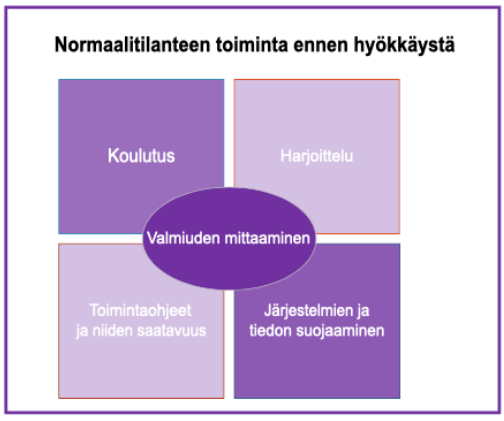
Zhang, L-F., You, L-M., Liu, K., Zheng, J., Fang, J-B., Lu, M-M., Lv, A-L., Ma, W-G., Wang, J., Wang, S-H., Wu, X., Zhu, X-W. & Bu, X-Q. (2014). *The Association of Chinese Hospital Work Environment with Nurse Burnout, Job Satisfaction, and Intention to Leave*. Nursing outlook. 62.2. pp. 128–137.

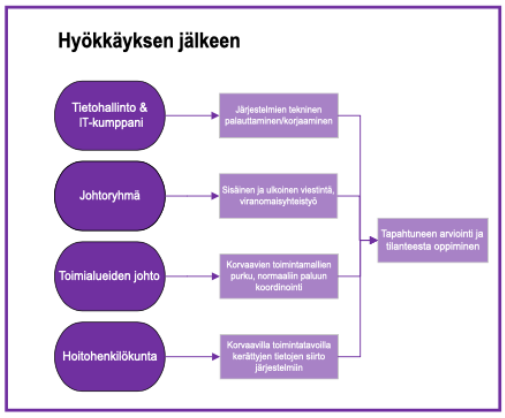
# LIITTEET

LIITE 1: Kokonaiskuva kohdeorganisaation toiminnasta kyberhyökkäystilanteessa
LIITE 2: Haastateltavien informointi

# LIITE 1: KOKONAISKUVA KOHDEORGANISAATION TOIMINNASTA KYBERHYÖKKÄYSTILANTEESSA



# LIITE 2: HAASTATELTAVIEN INFORMOINTI

Dokumentin tarkoitus: Tällä dokumentilla haastateltavaa informoidaan haastattelun tarkoituksesta, haastattelumateriaalin käytöstä ja siihen liittyvistä yksityiskohdista

Tutkimushanke: "They should be tested like banks are" – Resilience, crisis preparedness and security of supply of the Finnish health system (Muutosjoustavuus, kriisivalmius ja huoltovarmuus suomalaisessa terveydenhuoltojärjestelmässä), rahoittaja Suomen akatemia ajalle 2020-2022

Haastattelujen tarkoitus: haastatteluissa kartoitetaan kohdeorganisaation toimintaa kyberhyökkäyksen sattuessa. Tavoitteena on selvittää mitä organisaatio käytännössä tekee mahdollisen hyökkäyksen sattuessa ja siitä toipuessa, miten tätä toimintaa voisi parantaa.

Kerättävä aineisto: laadullista haastatteluaineistoa ja siihen liittyviä kuvia. Aineisto keskittyy organisaation toimintaa, joten yksittäisen henkilön arkaluonteisia tietoja (politiikka, uskonto, jne.) ei kerätä.

Aineiston käsittely: Haastatteluaineiston käsittely anonymisoidaan. Tämä tarkoittaa sitä, että yksittäisen haastateltavan nimi tai muu mahdollinen henkilön yksilöivä tieto poistetaan. Aineistosta analysoidaan tutkimuskysymyksiä (ks. haastattelujen tarkoitus –kohta) selvittäviä teemoja.

Aineistoon pohjautuvat julkaisut kirjoitetaan anonyymeinä, eli niistä ei paljastu organisaatio, sen yksikkö tai haastateltavat henkilöt. Julkaisut tarkistutetaan kohdeorganisaatiolla ennen niiden julkaisemista.

Aineisto tallennetaan Tampereen yliopiston salatuille palvelimille. Niihin pääsevät käsiksi vain tutkimusryhmän jäsenet.

Tutkimushankkeen päättymisen jälkeen kerätyt haastatteluaineistot tuhotaan.

Tutkimusryhmä: Tutkimusapulainen Laura Karintaus, tutkija Maija Ylinen ja professori Samuli Pekkola

### Yhteystiedot

Professori Samuli Pekkola,
Tutkimusapulainen Laura Karintaus
Tietojohtamisen yksikkö, Johtamisen ja talouden tiedekunta, Tampereen yliopisto