Aino Jyrkkiö

KYBERUHKIEN VAIKUTUKSET TERVEYDEHUOLTOON KANSALLISEN TURVALLISUUDEN NÄKÖKULMASTA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Jyrkkiö, Aino
Kyberuhkien vaikutukset terveydenhuoltoon kansallisen turvallisuuden näkökulmasta
Jyväskylä: Jyväskylän yliopisto, 2024, 30 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Clements, Kati

Teknologian kehitys on tuonut lukuisia yhteiskunnallisia hyötyjä terveydenhuollolle. Samalla se on kuitenkin altistanut sektorin erilaisille kyberuhkille, mikä on herättänyt huolta kansallisen turvallisuuden toteutumisen suhteen. Tämä tutkimus tarkastelee kyberuhkien vaikutuksia terveydenhuoltoon korostaen kansallisen turvallisuuden näkökulmaa. Tutkimuksessa otetaan huomioon kyberhyökkäysten vaikutukset potilasturvallisuuteen, terveydenhuollon järjestelmiin ja niiden luotettavuuteen sekä laajemmin yhteiskunnan toimintakykyyn terveydenhuollon kriisitilanteissa. On tärkeää ymmärtää kyberuhkien monimutkaiset haasteet, jotta voidaan luoda vahvoja strategioita, jotka suojelevat sekä yksittäisen potilaan terveyttä että kansallista turvallisuutta. Tämä tutkimus toteutettiin kirjallisuuskatsauksena. Kirjallisuus kerättiin vertaisarvioiduista tutkimusartikkeleista, aikakauslehdistä ja muusta kirjallisuudesta. Tutkielma auttaa ymmärtämään, miten kyberuhat vaikuttavat terveydenhuoltoon ja kuinka kansallinen turvallisuus on kytköksissä aiheeseen. Kyberuhat voivat vaikuttaa terveydenhuoltoon monilla eri tavoilla, kuten kiristyshaittaohjelmilla, palvelunestohyökkäyksillä sekä lääketieteellisiin laitteisiin ja sairaalan infrastruktuuriin kohdistuvilla hyökkäyksillä. Terveydenhuoltoon kohdistuvat hyökkäykset voivat vaarantaa potilaiden yksityisyyden lisäksi myös terveydenhuoltolaitoksen toiminnan ja siten potilaiden terveyden ja hyvinvoinnin. Tutkielmassa ehdotetaan myös toimenpiteitä paremman kyberturvallisuuden saavuttamiseen terveydenhuollossa. Terveysteknologioiden ja potilastietojen turvallisuuden varmistamiseen tulisi sijoittaa enemmän resursseja.

Asiasanat: kyberturvallisuus, kyberuhka, kansallinen turvallisuus, terveydenhuolto.

ABSTRACT

Jyrkkiö, Aino
The impacts of cyber threats on healthcare from a national security perspective
Jyväskylä: University of Jyväskylä, 2024, 30 pp.
Information systems, bachelor's thesis
Supervisor: Clements, Kati

The rapid digitization of healthcare systems has ushered in transformative benefits but has concurrently exposed the sector to escalating cyber threats, prompting concerns for national security. This study examines the consequential impacts of cyber threats on healthcare, emphasizing the critical intersection of digital vulnerabilities within the sector and their wider ramifications for national security. As healthcare becomes increasingly reliant on interconnected technologies, the purpose of this research is to examine the multifaceted impacts of cyber threats on the sector from a national security perspective. This study considers the impacts of cyber threats on patient safety, healthcare systems, and their reliability, as well as more broadly on societal functioning during healthcare crises. It's essential to understand the challenges of cyber threats in healthcare to create strong strategies that protect both individual patient health and the overall national security. This study was conducted as a literature review. The literature was gathered from peer-reviewed research articles, journals, and other literary sources. This study helps to understand how cyber threats affect healthcare and how national security is related to the topic. Cyber threats can affect healthcare in many ways, such as ransomware attacks, denial of service attacks, and attacks targeting medical devices and hospital infrastructure. Cyber assaults targeting healthcare not only endanger the privacy of patients but also imperil the operational integrity of healthcare establishments, thereby compromising the health and welfare of patients. The study also proposes measures to achieve better cybersecurity in healthcare. More resources should be allocated to ensuring the security of healthcare technologies and patient information.

Keywords: cyber security, cyber threat, national security, healthcare

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Kansallinen turvallisuus on muuttunut ajan saatossa monimutkaisemmaksi ja haavoittuvammaksi. Yksi merkittävimmistä haasteista on kyberuhat, jotka voivat vaikuttaa laaja-alaisesti eri yhteiskunnan osa-alueisiin, kuten terveydenhuoltoon. Teknologian kehitys on tuonut lukuisia yhteiskunnallisia hyötyjä terveydenhuoltoalalle (Lehto & Neittaanmäki, 2022, s. 183.) Vaikka teknologian merkitys onkin huomattava, sen integroiminen terveydenhuoltoon on nostanut huomattavasti riskejä. Erityisesti potilastietojen väärinkäytön ja yksityisyyden vaarantumisen riskit ovat korostuneet (Bhuyan ym., 2020). Terveydenhuolto onkin kriittinen yhteiskunnan toiminnan jatkuvuuden kannalta ja sen häiriöt voivat johtaa vakaviin seurauksiin, kuten terveydenhuollon infrastruktuurin romahtamiseen. Eri kyberuhkien tunnistaminen ja niiden vaikutusten ymmärtäminen ovat siis elintärkeitä asioita kansallisen turvallisuuden näkökulmasta.

Tämän kandidaatintutkielman tarkoituksena on tarkastella kyberuhkien vaikutuksia terveydenhuoltoon kansallisen turvallisuuden näkökulmasta. Tarkastelussa on mukana kyberhyökkäysten mahdolliset vaikutukset potilasturvallisuuteen, terveydenhuollon järjestelmiin ja niiden luotettavuuteen sekä laajemmin yhteiskunnan toimintakykyyn terveydenhuollon kriisitilanteissa. Tutkielmassa tarkastellaan erilaisia kyberuhkien tyyppejä ja niiden mahdollisia seurauksia terveydenhuoltoon. Tutkielman tarkoituksena on vastata seuraavaan tutkimuskysymykseen:

- Miten erilaiset kyberuhat vaikuttavat terveydenhuoltoon kansallisen turvallisuuden näkökulmasta?

Tutkielman aiheen valinta perustuu siihen, että terveydenhuolto on yksi yhteiskunnan kriittisistä infrastruktuureista ja sen turvaaminen on keskeinen osa kansallista turvallisuutta. Aiheen tutkiminen on tärkeää, koska sen avulla voidaan tunnistaa ja ymmärtää paremmin mahdolliset terveydenhuoltoon kohdistuvat haavoittuvuudet. Tutkimuksen avulla voidaan parantaa kansallista turvallisuutta ja kehittää strategioita kyberhyökkäysten ennaltaehkäisemiseksi ja torjumiseksi. Tutkimalla eri haavoittuvuuksia ja riskejä, voidaan tunnistaa paremmin terveydenhuoltoon kohdistuvat riskit ja pyrkiä suojaa-

maan sitä paremmin. Tutkielman aihe liittyy läheisesti tietojärjestelmätieteen tieteenalaan, sillä se vaatii syvällistä ymmärrystä tietojärjestelmistä, tietoturvasta sekä kyberuhkista.

Tutkielma on toteutettu kirjallisuuskatsauksena. Lähteiden etsinnässä on hyödynnetty useita tietokantoja, kuten JYKDOK, Scopus ja Google Scholar. Hakusanoina on käytetty: *cyber security, cyber threat, national security, healthcare, kyberturvallisuus, kyberuhka, kansallinen turvallisuus, terveydenhuolto*. Hakusanojen avulla avautui laaja kirjo tuloksia, jotka sisälsivät runsaasti aiheeseen liittyvää kirjallisuutta useilta eri tieteenaloilta. Aineisto on kerätty tutkimusartikkeleista, aikakauslehdistä ja muusta kirjallisuudesta. Suomenkielisiä artikkeleita kyseisestä aiheesta löytyi vain vähän, joten tutkielmassa hyödynnetty lähdeaineisto koostui pääosin englanninkielisestä kirjallisuudesta. Tutkielmassa on pyritty käyttämään aineistoa, joka on mahdollisimman ajantasaista. Ottaen huomioon alan nopeat muutokset, vanhemmat aineistot saattaisivat nykypäivänä olla epätarkkoja ja vanhentuneita. Lähteiden luotettavuutta on arvioitu useilla tekijöillä, kuten niiden julkaisuvuodella sekä viittausten määrällä. Lisäksi JUFO-palvelua on käytetty luotettavuuden arvioinnissa.

Tutkielman rakenne koostuu johdannosta, kolmesta sisältöluvusta sekä yhteenvedosta. Tutkielman ensimmäisessä sisältöluvussa käsitellään kyberuhkia. Ensimmäinen sisältöluku kattaa kyberuhkien keskeiset määritelmät sekä yleisimmät kyberuhkatyypit ja niiden ominaispiirteet. Toisen sisältöluvun tarkoituksena on hahmottaa terveydenhuoltoon liittyviä näkökulmia, keskittyen erityisesti käsitteen määrittelemiseen, haavoittuvuuksiin sekä tietosuojaan ja potilastietojen hallintaan. Kolmas sisältöluku syventyy kyberuhkien vaikutuksiin terveydenhuollossa kansallisen turvallisuuden näkökulmasta. Sisältöluku lähtee liikkeelle kansallisen turvallisuuden määritelmästä, edeten kyberuhkien vaikutuksista terveydenhuoltoon, niiden yhteiskunnallisiin näkökulmiin sekä toimenpiteisiin kyberhyökkäysten varalta. Viimeisen luvun, eli yhteenvedon, tarkoituksena on koota tutkimuksen tulokset yhtenäiseksi kokonaisuudeksi. Viimeisessä luvussa pyritään esittämään loppupäätelmät sekä ehdottamaan mahdollisia jatkotutkimusaiheita.

2 KYBERUHAT

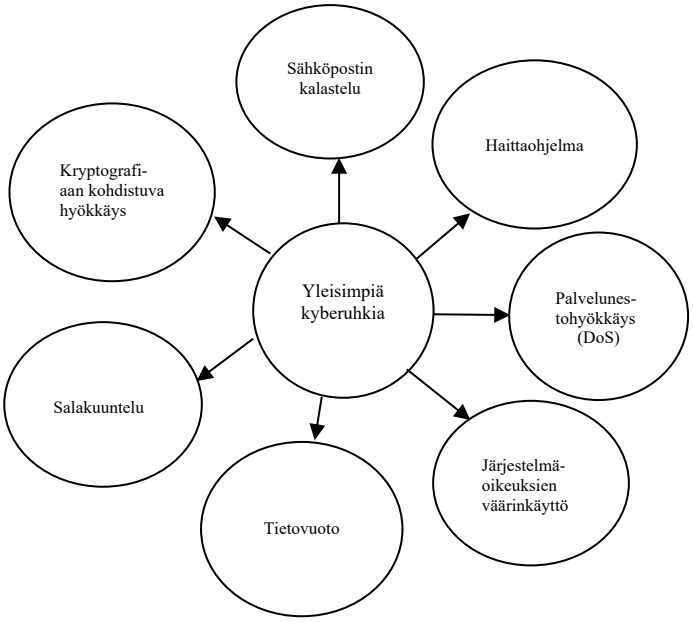
Kyberuhat muodostavat nykypäivän digitalisoituneessa maailmassa merkittäviä haasteita ja niiden vaikutukset ulottuvat laajasti yhteiskunnan eri osa-alueille. Tässä pääluvussa käsitellään kyberuhkia. Käsittely kattaa keskeiset määritelmät sekä yleisimmät kyberuhkatyypit ja niiden ominaispiirteet. Ensimmäisessä alaluvussa määritellään, mitä kyberuhat tarkoittavat nykypäivän kontekstissa. Toisessa alaluvussa käydään läpi yleisimpiä kyberuhkatyyppejä ja niiden ominaispiirteitä erityisesti terveydenhuollon näkökulmasta.

2.1 Kyberuhkien määritelmä

Kyberuhka on määritelty kirjallisuudessa yhtenäisesti. Norri-Sederholm, Laitinen, Lehto, ja Kari (2019, s. 90) kuvaavat teoksessaan ”Terveydenhuolto ja kyberuhkat”, että kyberuhalla tarkoitetaan mahdollisesti toteutuvaa haitallista tapahtumaa tai kehityskulkua, joka kohdistuu kybertoimintaympäristöön. Tapahtuman tai kehityskulun toteutuessa, se vaarantaa siitä riippuvaisen toiminnon (Norri-Sedelholm ym., 2019, s. 90.) Turvallisuuskomitea (ei pvm.) taas määrittelee kyberuhan riskiksi, joka voi toteutuessaan vaarantaa yhteiskunnan elintärkeät toiminnot tai muut kybertoimintaympäristöstä riippuvaiset toiminnot. Lehto ja Neittaanmäki (2022, s. 9) kuvaavat uhan yksinkertaisesti haitalliseksi kybertapahtumaksi, joka voi tapahtua. Norri-Sederholm ja muut kirjoittajat (2019, s. 90) korostavat, että kyberuhat kohdistuvat suoraan tai välillisesti yhteiskunnan kriittisiin toimintoihin ja kansalaisiin joko maan rajojen sisältä tai ulkopuolelta. Kyberuhkina voidaan pitää muun muassa kybervandalismia, kyberrikollisuutta, kybervakoilua, kyberterrorismia sekä kybersodankäyntiä (Norri-Sederholm ym., 2019, s. 90.)

2.2 Erilaiset kyberuhat ja niiden ominaisuudet

Kybermaailma on jatkuvassa muutoksessa, ja sen mukana kehittyvät myös kyberuhat. Tämän päivän digitaalisessa maailmassa kohdataan monenlaisia uhkia, jotka vaihtelevat yksinkertaisista huijauksista monimutkaisiin tietomurtoihin. Tässä alaluvussa käydään läpi yleisimpiä kyberuhkatyyppejä (kuvio 1) ja niiden ominaisuuksia erityisesti terveydenhuollon näkökulmasta. Kuvio 1 on johdettu kirjallisuudessa esitetyistä yleisimmistä kyberuhkatyypeistä, joita tässä alaluvussa käsitellään.



KUVIO 1 Yleisimpiä kyberuhkia terveydenhuollon näkökulmasta

Yksi yleisimmistä kyberuhkatyypeistä on sähköpostin kalastelu (eng. phishing) ja se on vakava uhka kyberturvallisuudelle. Tietojenkalastelua käytetään suurimmassa osassa kyberuhissa (Jones, Greenhill, Shaw, Flores & Schmidt, 2022., s. 58.) Sähköpostin kalastelulla viitataan yritykseen huijata joku antamaan tietoja sähköpostin välityksellä (Chua, 2021, s. 230.) Organisaatioiden sisälle suuntautuva kalastelusähköposti sisältää usein aktiivisen linkin tai tiedoston. Sähköposti näyttää yleensä tulevan laillisesta lähteestä, kuten kollegalta tai esihenkilöltä. Linkkiä tai tiedostoa klikkaamalla käyttäjä ohjataan esimerkiksi verkkosivustolle, joka saattaa pyytää arkaluontoisia tietoja tai tartuttaa tietokoneeseen haittaohjelman. Linkin tai tiedoston avaaminen saattaa johtaa haittaohjelman latautumiseen tai tietokoneella sekä verkkoyhteydellä olevien tietojen paljastumiseen (Chua, 2021.).

Haittaohjelmat uhkaavat niin yksilöiden kuin organisaatioiden kyberturvallisuutta. Haittaohjelmalla tarkoitetaan ohjelmaa, joka on suunniteltu vahingoittamaan tai kompromisoimaan tietojärjestelmää tai laitetta (Bhuyan ym., 2020, s.3.) Haittaohjelmat sisältävät erilaisia toimintoja, kuten vakoilemista, tie-

tojen vahingoittamista, käyttäjätietojen poistamista sekä muuttamista. Haittaohjelmat leviävät joko fyysisesti ulkoisen aseman kautta tai internetin latausten myötä. Yleisiä haittaohjelmia ovat muun muassa kiristyshaittaohjelmat, vakoiluohjelmat, virukset, madot, botit, troijalaiset sekä mainosohjelmat (Bhuyan ym., 2020, s.3.).

Kiristyshaittaohjelma eroaa muista haittaohjelmista siinä, että se pyrkii estämään käyttäjän pääsyn omiin tietoihinsa yleensä kryptaamalla ne avaimella, joka on tiedossa vain haittaohjelman levittäjänä toimivalle hakkerille (Chua, 2021.) Kun käyttäjän tiedot on salattu, kirityshaittaohjelma ohjaa käyttäjän maksamaan lunnaita hyökkääjälle saadakseen salauksen purkuavaimen. Hyökkääjät saattavat myös käyttää kiristyshaittaohjelmia, jotka tuhoavat tai vuotavat tietoa, eikä lunnaiden maksaminen takaa, että varastetut tai lukitut tiedot palautetaan. Kiristyshaittaohjelmat voivat sisältää tekniikoita, jotka ovat samankaltaisia tai jopa identtisiä muiden kyberuhkien kanssa. Esimerkiksi onnistuneet sähköpostin kalasteluhyökkäykset voivat johtaa kiristysohjelman asentamiseen tietokoneelle (Chua, 2021.).

Palvelunestohyökkäyksen (DoS) tarkoituksena on kohdistaa verkkopalveluun niin paljon liikennettä, että palvelu häiriintyy ja käyttäjät estyvät pääsemästä verkon resursseihin (Bhuyan ym., 2020, s. 2.) Tämäntyyppiset hyökkäykset kykenevät merkittävästi hidastamaan tai sulkemaan kokonaan esimerkiksi terveydenhuollon organisaation verkon. Palvelunestohyökkäykset voivat aiheuttaa suuria taloudellisia tappioita organisaatioille (Bhuyan ym., 2020, s. 2.).

Järjestelmäoikeuksien väärinkäyttö luo suuren uhkan kyberturvallisuudelle. Bhuyan ym. (2020, s. 2) kuvaavat, että oikeuksien laajentamishyökkäyksiä (eng. privilege escalation) ohjaa useimmiten tavoite saavuttaa korkeampi pääsy tietoverkkoon tai ohjelmaan, ja niitä suoritetaan hyväksikäyttämällä ohjelman tai verkon haavoittuvuuksia. Hakkerit saattavat käyttää lisättyjä järjestelmäoikeuksia tehdäkseen monenlaisia toimia järjestelmissä. Esimerkiksi terveydenhuollon organisaatioissa, hakkeri voi muuttaa potilaan terveystietoja vaarantaen siten potilaan turvallisuuden (Bhuyan ym., 2020, s. 2.).

Salakuuntelu on myös yksi kyberuhkatyyppi. Se voidaan luokitella tiedusteluhyökkäykseksi (Bhuyan ym., 2020, s. 2.) Hyökkäys tapahtuu, kun tunkeutuja kaappaa viestinnän kahden osapuolen välillä ja kuuntelee salaa tiedonvaihdon sisällön. Hyökkääjä voi myös vakoilla sisältöjä toimimalla salaa välittäjänä tiedonvaihdossa. Tietojen eheys voikin helposti vaarantua, sillä hyökkääjä voi muuttaa tietoja ennen niiden välittämistä toiselle osapuolelle. Hyökkääjä voi hyödyntää salakuuntelussa myös Man-In-The-Browser-haittaohjelmaa (MITB). Kyseinen haittaohjelma on suunniteltu vakoiluun, salakuunteluun, tietojen kaappaamiseen sekä istunnon muokkaamiseen (Bhuyan ym., 2020, s. 2.).

Kryptografiaan kohdistuvat hyökkäykset ovat uhka kyberturvallisuudelle. Tällaisten hyökkäysten tarkoituksena on paljastaa salassa olevaa tietoa (Bhuyan ym., 2020, s. 2.) Kryptografia on prosessi, jossa tieto muutetaan sellaiseen muotoon, joka on ymmärrettävää vain niille, joilla on oikea salausavain. Salauksen avulla varmistetaan, että mahdolliset hyökkääjät eivät voi ymmärtää salattua tietoa ilman oikeanlaista avainta (Bhuyan ym., 2020, s. 2.). Kryptografia onkin keskeinen osa tietoturvaa ja yksityisyyttä tietojenkäsittelyssä ja sähköisessä viestinnässä.

Tietovuodot ovat tunnettuja uhkia kyberturvallisuudelle ja ne voivatkin olla hyvin monitahoisia. Tietovuodot voivat olla esimerkiksi organisaation sisäisiä uhkia (Bhuyan ym., 2020, s. 2.) Sisäisiä uhkia esiintyy organisaatioissa, missä työntekijät, urakoitsijat tai muut käyttäjät käyttävät organisaation teknologiainfrastruktuuria, verkkoa tai tietokantoja. Sisäiset tietovuodot voivat olla joko tahattomia tai tahallisia. Tahaton tietovuoto johtuu aina rehellisestä virheestä, kuten huijatuksi tulemisesta tai huolimattomuudesta (Bhuyan ym., 2020, s. 2.). Tahaton tietovuoto voi tapahtua esimerkiksi onnistuneen sähköpostikalasteluhyökkäyksen takia. Tahallinen tietovuoto tapahtuu henkilökohtaisen hyödyn saamiseksi tai tahallisen vahingon aiheuttamiseksi organisaation työntekijän, urakoitsijan tai muun käyttäjän johdosta (Bhuyan ym., 2020, s. 2.). On kuitenkin tärkeää ymmärtää, että tietovuodot voivat tapahtua myös ulkopuolisen tahon toimesta esimerkiksi kyberhyökkäyksen yhteydessä.

Useat verkkosivut käyttävät ohjelmointikieltä nimeltä Structured Query Language, eli SQL, hallinoidakseen tietokantojaan (Bhuyan ym., 2020, s. 2–3.) Kyseiseen ohjelmointikieleen liittyykin uhkia. SQL:n haavoittuvuudet voivat mahdollistaa hyökkääjille haitallisten SQL-lauseiden suorittamisen, jotka saavat datakeskukset paljastamaan tietoja (Bhuyan ym., 2020, s. 2–3.) Näin hyökkääjät pääsevät muuttamaan tietokannan tietoja, vaikuttaen tietojen eheyteen, luotettavuuteen ja saatavuuteen.

Kyberuhat muodostavat jatkuvan haasteen nykypäivän tietoturvaympäristössä. On tärkeä ymmärtää, että kyberuhat voivat kohdistua niin yksittäisiin käyttäjiin kuin suuriin organisaatioihin. Uhkien monimuotoisuus korostaakin tarvetta tietoturvakäytäntöjen jatkuvalle päivittämiselle ja parantamiselle.

3 TERVEYDENHUOLTO

Terveys on yksi yhteiskunnan keskeisistä peruspilareista ja terveydenhuoltojärjestelmä on elintärkeä osa tätä kokonaisuutta. Tässä pääluvussa käsitellään terveydenhuoltoon liittyviä näkökulmia, keskittyen erityisesti käsitteen määrittelemiseen, haavoittuvuuksiin sekä tietosuojaan ja potilastietojen hallintaan. Pääluvun ensimmäisessä osassa tarkastellaan terveydenhuoltoa. Alaluvussa määritellään, mitä terveydenhuolto pitää sisällään ja millaisia periaatteita sen toimintaan liittyy.

Toisessa alaluvussa tarkastellaan terveydenhuollon haavoittuvuuksia ja käsitellään tekijöitä, jotka voivat altistaa terveydenhuollon haasteille ja ongelmille kyberturvallisuuden näkökulmasta. Alaluvussa käsitellään syitä, jotka tekevät terveydenhuollon houkuttelevaksi kohteeksi kyberuhkille. Kolmannessa alaluvussa keskitytään terveydenhuoltoon liittyvään tietosuojaan ja potilastietojen hallintaan sekä käydään läpi, miten potilastietoja kerätään, säilytetään ja jaetaan terveydenhuollossa Suomessa.

3.1 Terveydenhuollon määritelmä

On tärkeää käsitellä, miten terveydenhuolto määritellään. Lehto ja Neittaanmäki (2022, s. 185) määrittelevät terveydenhuollon laajaksi ja monipuoliseksi sektoriksi, joka tarjoaa valtavan valikoiman hyödykkeitä ja palveluita, jotka ovat välttämättömiä kansan terveydelle, turvallisuudelle ja hyvinvoinnille. Sosiaali- ja terveysministeriö (ei pvm.) taas määrittelee terveydenhuollon tavoitteeksi edistää ja ylläpitää väestön terveyttä, hyvinvointia, työ- ja toimintakykyä ja sosiaalista turvallisuutta sekä kaventaa terveyseroja. Keskeisenä perustana on tehokas järjestelmä, joka tarjoaa kaikille kansalaisille saatavilla olevat terveyspalvelut, jotka kattavat ennaltaehkäisyn, hoidon ja kuntoutuksen (Sosiaali- ja terveysministeriö, ei pvm.) Terveydenhuolto määritellään kirjallisuudessa yhtenäisesti.

Lehdon ja Neittaanmäen (2022, s. 185) mukaan terveydenhuoltoalan kriittiset toiminnot sisältävät muun muassa:

- perusterveydenhuollon, erikoissairaanhoidon ja avohoidon, mukaan lukien lääkärit, sairaanhoitajat ja työterveyshoitajat
- terveyskeskukset ja ensiavun palvelut
- terveysalan suunnitteluorganisaatiot, liikekumppanit ja vakuutusyhtiöt
- kuolleiden hoitoon erikoistuneet yksiköt
- lääkkeiden ja lääkinnällisten laitteiden valmistuksesta vastaavat yritykset
- biopankit ja genomikeskukset
- kansallisen, paikalliset ja alueelliset terveysviranomaiset, jotka tarjoavat väestöön perustuvaa hoitoa ja valvontaa.

Edellä mainittujen toimintojen jatkuvuus ja toimivuus ovat elintärkeitä koko yhteiskunnan hyvinvoinnille. Lehdon ja Neittaanmäen (2022, s. 185) mukaan on kuitenkin tärkeää huomioida, että terveydenhuoltoalan kriittiset toiminnot eivät rajoitu pelkästään edellä mainittuihin osa-alueisiin. Esimerkiksi pandemian tai muiden poikkeusolojen aikana tarvitaan erilaisia lisätoimia ja resursseja, jotka voivat poiketa normaaleista tilanteista.

3.2 Terveydenhuollon haavoittuvuudet

Terveydenhuoltoa tarkastellessa on keskeistä syventyä sen potentiaalisiin haavoittuvuuksiin, jotka voivat olennaisesti vaikuttaa sen toimintakykyyn ja kykyyn vastata terveydenhuollon tarpeisiin. On myös keskeistä ymmärtää, mikä tekee terveydenhuollosta houkuttelevan kohteen kyberuhille. Terveydenhuoltosektoriin kohdistuvat kyberhyökkäykset ovatkin erityisen huolestuttavia, koska ne voivat uhata järjestelmien ja tietojen turvallisuuden lisäksi myös potilaiden terveyttä ja turvallisuutta (Lehto ja Neittaanmäki, 2022, s. 26.) Lehdon ja Neittaanmäen mukaan (2022, s. 26) sairaalat ovat erityisen herkkiä kyberhyökkäyksille, sillä toiminnan häiriintymisellä tai potilaiden henkilötietojen paljastumisella voi olla hyvin kauaskantoisia seurauksia.

Terveydenhuolto onkin hyvin houkutteleva kohde kyberrikollisuudelle useasta eri syystä. Langer (2017, s. 118) määrittelee kyberrikollisuuden laajaksi termiksi, joka kattaa kaikki tietokoneilla tehdyt rikokset. Coventry ja Branley (2018, s. 48) kuvaavat terveydenhuollon houkuttelevaksi kohteeksi kyberrikollisuudelle, koska se toimii rikkaana lähteenä arvokkaalle ja arkaluontoiselle tiedolle, sekä sen puolustuskeinot ovat heikkoja. Motivaatio kyberhyökkäysten tekemiselle sisältää Coventryn ja Branleyn (2018, s. 49) mukaan mahdollisuuden taloudelliseen ja poliittiseen voittoon. Vahvin näistä motivaatioista on taloudellinen voitto, sillä terveystiedot ovat huomattavasti arvokkaampia kuin mitkään muut tiedot (Coventry & Branley, 2018, s. 49.) Myös Norri-Sederholmin ym. (2019, s. 86) mukaan terveydenhuoltoon kohdistuvien hyökkäysten keskeisin motivaatio on potilastietojen arvo pimeillä markkinoilla. Pe-

rakslis (2014, s. 395) taas kuvaa, että osa kyberrikollisista motivoituu juuri taloudellisesta voitosta, kun taas toiset pyrkivät hankkimaan immateriaalista omaisuutta tai kuluttajatietoja, vahingoittamaan terveydenhuoltolaitoksen mainetta tai tekemään poliittisen kannanoton. Taloudellinen voitto on kuitenkin selkeästi motivaatioista suurin.

Coventryn ja Branleyn (2018, s. 48.) mukaan terveydenhuollon kyberturvallisuus ei ole riittävää, ja tämä on johtanut terveystietojen luottamuksellisuuden puutteisiin sekä tietojen eheytymisen vaarantumiseen. Terveydenhuollon haavoittuvuudet kohdistuvat erityisesti terveydenhuollon laitteisiin, ohjelmistoihin, mobiililaitteisiin, etähallittaviin laitteisiin, sekä käyttäjien toimiin, erityisesti liittyen salasanojen ja eri järjestelmien käyttöön (Norri-Sederholm ym., 2019, s. 90.) Lehto ja Neittaanmäki (2022, s. 27) nostavat esiin useita syitä, jotka tekevät terveydenhuollosta haavoittuvaisen kyberuhkille. Heidän mukaansa hyökkääjillä on helppo pääsy lääkinnällisille laitteille, sillä ne yhdistetään yhä useammin verkkoon käyttämällä oletussalasanoja, puuttuvia korjaustiedostoja ja muita heikkouksia (Lehto & Neittaanmäki, 2022, s. 27.) Lääkinnällisellä laitteella tarkoitetaan välinettä, laitetta, konetta, keksintöä, implanttia tai muuta vastaavaa, joka on tarkoitettu käytettäväksi terveydenhuollon diagnooseissa tai sairauden parantamisessa, lieventämisessä, hoidossa tai ennaltaehkäisyssä (Williams & Woodward 2015, s. 306.) Lehdon ja Neittaanmäen mukaan (2022, s. 27) merkittävimpiä haavoittuvuuksia ovat sovellusten, laitteiden ja järjestelmien haavoittuvuudet, korjaamattomat ohjelmistot ja määritysheikkoudet. Järjestelmien monimuotoisuus ja niiden käyttäjien vuorovaikutuksen monimutkaisuus altistavat terveysjärjestelmät ja lääkinnälliset laitteet laajalle määrälle kyberuhkia (Bernard, Bowsher & Sullivan, 2020, s. 135.)

Lehdon ja Neittaanmäen mukaan terveydenhuoltosektorin henkilökunnan on päästävä käsiksi potilastietoihin myös työpaikan ulkopuolella käyttäen etäyhteyksiä, mikä luo lisää mahdollisuuksia hyökkäyksille. Työntekijät ovat myös vastahakoisia häiritsemään käteviä työkäytäntöjään uuden teknologian käyttöönotolla, joka johtaa vanhentuneiden teknologioiden käyttämiseen. Yhdeksi haavoittuvuudeksi on nostettu myös työntekijöiden heikko koulutus kyberuhkista (Lehto & Neittaanmäki, 2022, s. 27.). Myös Norri-Sederholmin ja muiden kirjoittajien (2019, s. 89) mukaan työntekijöiden välinpitämättömyys tietoturvasta ja lisääntynyt sosiaalinen manipulointi (eng. social engineering) ovat merkittävimpiä tekijöitä, jotka altistavat terveydenhuollon kyberuhille. Yhtenä haavoittuvuutena voidaan pitää myös laitteiden suurta määrää terveydenhuoltoyksiköissä. Koska laitteita on paljon, on hyvin vaikeaa pysyä turvallisuuden kärjessä (Lehto & Neittaanmäki, 2022, s. 27.) Lehdon ja Neittaamäen (2022, s. 27) mukaan kyberturvallisuus on usein huonosti hallittua varsinkin pienemmissä terveydenhuoltoyksiköissä. Terveydenhuoltosektorilla onkin siis useita haavoittuvuuksia ja kyberturvallisuudessa löytyy kehitettävää.

3.3 Tietosuoja ja potilastietojen hallinta

Potilastietojen asianmukainen käsittely ja suojaaminen ovat elintärkeitä osatekijöitä terveydenhuoltojärjestelmän toiminnassa. Lehdon ja Neittaanmäen (2022, s. 184–185) mukaan terveydenhuollon sektorilla on erityisen tiukat vaatimukset tietojenkäsittelylle. Potilastietojen eheyttä ja saavutettavuutta korostetaan voimakkaasti, sillä ne ovat keskeisiä tekijöitä potilaiden turvallisen hoidon varmistamisessa. Toisaalta tietojen luottamuksellisuutta on suojeltava paitsi yksityisyyden suojan varmistamiseksi myös henkilötietojen väärinkäyttämisen estämiseksi (Lehto & Neittaanmäki, 2022, s. 184–185.).

Tietoturvan toteutuminen ja tietosuojaloukkaukset ovat ymmärrettävästi monen terveydenhuollon asiakkaan huolenaiheena. Tieto, joka katoaa, varastetaan, siirtyy epäkelpoon paikkaan, joutuu hakkeroinnin kohteeksi tai päätyy epävirallisille vastaanottajille, määritellään tietoturvaloukkaukseksi ja tämä tietojen eheyden häiriö katsotaan kyberhyökkäykseksi (Bhuyan ym., 2020, s. 97). Coventry ja Branley (2018, s. 48) sen sijaan määrittelevät, että tietoturvarikkomuksiin kuuluu terveystietojen varastaminen ja sairaaloiden kiristyshyökkäykset sekä lääketieteellisiin laitteisiin kohdistuvat hyökkäykset. Tietoturvaloukkaukset voivatkin vähentää potilaiden luottamusta, lamauttaa terveydenhuoltojärjestelmiä sekä uhata ihmishenkiä. (Coventry & Branley, 2018)

Valviran (ei pvm) mukaan sellaiset tiedot, jotka koskevat yksilöitä ja mahdollistavat tunnistamisen, luokitellaan henkilötiedoiksi. Potilastiedot ja asiakastiedot rinnastetaan tähän käsitteeseen, ja Suomessa niiden käsittelyssä noudatetaan Euroopan unionin yleistä tietosuoja-asetusta, joka täydentyy kansallisella lainsäädännöllä. Lehdon ja Neittaanmäen (2022, s. 189) mukaan potilaan terveysrekisterissä olevia tietoja pidetään suojattuina terveystietoina, jos on perusteltu syy uskoa, että tiedot mahdollistavat yksilön tunnistamisen. Esimerkkejä tunnistettavista tiedoista terveydenhuollossa ovat muun muassa (Lehto & Neittaanmäki, 2022, s. 189):

- nimi, osoite, puhelinnumero ja sähköpostiosoite
- henkilötunnus
- vakuutuksen tiedot
- kaikki taloudelliset tai muut tiedot liittyen esimerkiksi pankkitileihin, ajoneuvoihin tai lisensseihin.
- lääketieteelliset tai muuten merkittävät laite- tai sarjanumerot
- IP-osoite
- kaikki biometriset tiedot, kuten sormenjälki
- täydet kasvokuvat tai kuvat yksilöllisistä tunnistettavista ominaisuuksista
- röntgenkuvat ja muut diagnostiset kuvat.

Valviran (ei pvm) mukaan Euroopan unionin yleisen tietosuoja-asetuksen ohella potilastietojen hallinnassa noudatetaan erilaisia säädöksiä, ku-

ten tietosuojalakia, potilaan asemasta ja oikeuksista annettua lakia, sosiaalihuollon asiakkaan asemasta ja oikeuksista annettua lakia sekä sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annettua lakia. Tietosuojalainsäädännön mukaiset periaatteet tulee aina ottaa huomioon henkilötietojen käsittelyssä. Henkilötietojen käsittelyllä viitataan muun muassa henkilötietojen keräämiseen, säilyttämiseen, käyttöön ja luovuttamiseen (Valvira, ei pvm.).

Potilastietojen luottamuksellisuus on turvattu potilaan asemasta ja oikeuksista annetun lain perusteella (Tietosuojavaltuutetun toimisto, ei pvm.) Potilastiedot ovat salassa pidettäviä. Suomessa sähköiset potilastiedot arkistoidaan valtakunnalliseen tietojärjestelmäpalveluun nimeltä Potilastiedon arkisto (Kanta.fi, ei pvm.). Arkistoitujen potilastietojen osalta tietoturvallinen säilytys on taattu. Tiedot ovat helposti ja ajantasaisesti saatavilla terveydenhuollon ammattilaisille hoitoa tukevassa kontekstissa. Tietojen luovuttaminen muille terveydenhuollon palvelunantajille tapahtuu vain ja ainoastaan asiakkaan luvalla. Asiakkaalla on mahdollisuus tarkastella omia tietojaan OmaKanta-palvelun kautta, mikä tukee hänen osallistumistansa hoitoon. Potilastiedon arkistoon lisätyt tiedot säilytetään tietoturvallisesti säädetyn ajanjakson ajan, ja kaikki tiedonsiirto suoritetaan salattuna terveydenhuollon ja potilastiedon arkiston välillä (Kanta.fi, ei pvm.).

Potilastietojen tarkastelu terveydenhuollon ammattilaisen toimesta tapahtuu ainoastaan silloin, kun se on välttämätöntä asiakkaan hoidon kannalta (Kanta.fi, ei pvm.) Terveydenhuolto määrittää ja antaa oikeudet potilastietojen käsittelylle tietojärjestelmissä, ja tietoja käsittelevien ammattilaisten on aina tunnistauduttava terveydenhuollon ammattikorteilla. Potilastiedon arkisto kerää lokitietoja, jotka mahdollistavat potilastietojen käsittelyn valvonnan. Potilastietojen tarkastelusta tallentuu aina jälki lokitietoihin. Lokitiedot mahdollistavat potilastietojen käytön lainmukaisuuden valvonnan (Kanta.fi, ei pvm.).

4 KYBERUHAT TERVEYDENHUOLLOSSA KANSALLISEN TURVALLISUUDEN NÄKÖKULMASTA

Kyberuhat terveydenhuollossa edustavat merkittävää uhkaa kansallisen turvallisuuden näkökulmasta. Terveydenhuoltosektori tarvitseekin erikoistuneita strategioita uhkien havaitsemiseksi, välttämiseksi ja arvioimiseksi (Ness & Khinvasara, 2024, s. 111.) Tämä pääluku syventyy tähän kontekstiin alkaen kansallisen turvallisuuden määritelmästä ja edeten kyberuhkien vaikutuksista terveydenhuoltoon, niiden yhteiskunnallisiin näkökulmiin sekä toimenpiteisiin kyberhyökkäysten varalta.

Luvun ensimmäisessä alaluvussa määritellään kansallisen turvallisuuden käsitettä. Toisessa alaluvussa pureudutaan syvemmälle kyberuhkien vaikutuksista terveydenhuoltoon. Alaluvussa käsitellään mahdollisia seurauksia, kuten potilastietojen väärinkäyttöä ja hoitojärjestelmien häiriöitä sekä arvioidaan, miten nämä vaikutukset voivat levitä laajemmalle yhteiskuntaan ja vaarantaa kansallisen turvallisuuden. Kolmannessa alaluvussa keskitytään konkreettisiin toimenpiteisiin ja varautumiseen kyberuhkien varalta terveydenhuollossa.

4.1 Kansallisen turvallisuuden määritelmä

Kansallisen turvallisuuden määritelmä muotoutuu eri tekijöiden, kuten terveydenhuollon, talouden, infrastruktuurin ja huoltovarmuuden kautta. Onkin tärkeää ymmärtää määritelmän monitahoisuus ja laajuus. Kansallisessa turvallisuudessa on kyse yhteiskunnan kokonaisvaltaisesta turvallisuudesta ja Suomen suvereniteetista (Sisäministeriö, ei pvm.) Suomen sisäministeriön mukaan kansallista turvallisuutta kuvataan usein siihen kohdistuvien uhkien kautta. Kyseessä on uhat, jotka vaikuttavat laajasti Suomen yhteiskuntaan, kuten esimerkiksi terrorismi, vakoilu ja vieraan valtion vahingollinen toiminta. Lisäksi hybridivaikuttaminen, kyberuhat ja kriittisen infrastruktuurin turvaaminen ovat olennaisia osatekijöitä kansallisen turvallisuuden näkökulmasta (Sisäministeriö, ei pvm.). Valtion suvereniteetti liittyy olennaisesti sen kykyyn turvata kansallinen turvallisuus (Alguliyev, Imamverdiyev, Mahmudov, & Aliguliyev., 2021, s.

2.) Tämän vuoksi kansallisen turvallisuuden varmistaminen on yksi valtioiden keskeisimmistä tehtävistä. Ne valtiot, jotka eivät kykene takaamaan kansallista turvallisuuttaan, menettävät suvereniteettinsa, ja niiden sisä- ja ulkopolitiikkaa ohjaavat voimakkaammat ulkoiset toimijat (Alquliyev ym., 2021, s. 2.) Onkin keskeistä ymmärtää, että jokaisen valtion kansallinen turvallisuus on myös tärkeä osa kansainvälistä turvallisuutta.

4.2 Kyberuhkien vaikutukset terveydenhuoltoon kansallisen turvallisuuden näkökulmasta

Terveydenhuoltoon kohdistuvat hyökkäykset eivät vaaranna vain potilaiden yksityisyyttä, vaan ne voivat myös vaikuttaa terveydenhuollon laitosten toimintaan ja asettaa potilaiden terveyden ja hyvinvoinnin vaaraan. Kun terveydenhuollon laitosten toiminta vaarantuu, saattaa se kansallisen turvallisuuden epätasapainoon. Esimerkiksi Yhdistyneen kuningaskunnan terveyspalvelun sairaalat joutuivat tunnetun WannaCry-kiristyshyökkäyksen kohteeksi toukokuussa 2017, mikä pakotti sairaalat viivästyttämään hoitosuunnitelmia ja jopa uudelleenohjaamaan saapuvia ambulansseja toisiin terveydenhuoltoyksiköihin tiedonhallintajärjestelmien savuttamattomuuden takia (Argaw ym., 2020, s. 1.) Nämä toiminnalliset häiriöt ja tietomurroista sekä kiristyshaittaohjelmista aiheutuvat taloudelliset seuraukset voivat vaikuttaa pitkällä aikavälillä sairaaloiden ja terveydenhuollon laitosten maineeseen ja tuloihin, unohtamatta kansallisen turvallisuuden vaarantumista (Argaw ym., 2020.) WannaCry-kiristyshaittaohjelma salasi tietoja ja tiedostoja 230 000 tietokoneessa yli 150 maassa (Ghafur, Grass, Jennings, & Darzi, 2019.)

Valtioiden tekemiksi luokitellut kyberhyökkäykset kriittistä kansallista infrastruktuuria vastaan ovat yleistymässä (Bernard ym., 2020, s.135.) Bernardin ja muiden kirjoittajien (2020, s. 135) mukaan erityisesti hyökkäykset, joiden tarkoituksena on aiheuttaa fyysistä ja operatiivista häiriötä toiselle valtiolle, ovat kasvussa. Tällaiset hyökkäykset kohdistuvat yleisesti energiasektoriin. Esimerkiksi joulukuussa 2015 Venäjään liitetyllä kehittyneellä jatkuvalla uhalla (engl. Advanced Persistent Threat, APT) varustettu ryhmä käytti ”BlackEnergy”-troijalaista Ukrainan yritysten käyttämiin teollisuuden ohjausjärjestelmiin sekä valvontaan ja tiedonkeruuseen käytettyihin järjestelmiin aiheuttaen häiriöitä Ukrainan sähköverkkoon. Vaikka sairaaloiden ja terveydenhuollon laitosten infrastruktuuria ei ole niinkään asetettu valtioiden tekemien kyberhyökkäysten kohteeksi, on helppo käsittää, miten samanlaiset häiriöt sairaaloiden verkoissa voisivat aiheuttaa vakavia yhteiskunnallisia seurauksia (Bernard ym., 2020, s. 135.).

Kyberuhat vaikuttavat terveydenhuoltoon useilla eri tavoilla (taulukko 1.) Terveydenhuollon tietojärjestelmien toimivuuden turvaaminen on osa yhteiskunnan turvallisuusstrategiaa, joka kattaa talouden, infrastruktuurin, ja huoltovarmuuden varmistamisen (Norri-Sederholm ym., 2019, s. 87). Norri-Sederholmin ja muiden kirjoittajien (2019, s. 87) mukaan yhteiskunnan varau-

tumisen tavoitteena on taata elintärkeät toiminnot sekä normaaliolojen häiriötilanteissa että poikkeusoloissa.

Koska moderni teknologia on tullut välttämättömäksi terveydenhuollossa, kyberuhat ja terveydenhuollon haavoittuvuudet jatkavat kasvuaan, vaarantaen samalla ihmisten ja terveystietojen turvallisuuden (Ghafur ym., 2019.) Tietoturvaongelmat ovatkin olleet merkittävässä kasvussa terveydenhuollossa ja potilastietoja varastetaan yhä enemmän. Norri-Sederholmin ja muiden kirjoittajien (2019, s. 86) mukaan vuonna 2015 varastettiin jopa yli satamiljoonaa potilastietoa, jotka sisälsivät arvokasta ja arkaluontoista tietoa, kuten luottokorttinumeroita, työnantajatietoja sekä sairaushistoriatietoja. Varastettuja lääketieteellisiä terveystietoja voidaan käyttää esimerkiksi terveyspalvelujen ja reseptilääkkeiden hankkimiseen. Varastettujen terveystietojen avulla kyberrikolliset voivat muun muassa myydä reseptilääkkeitä eteenpäin (Coventry & Branley, 2018, s. 49.). Toisinaan terveystiedoissa voi olla riittävästi tietoa jopa pankkitilien avaamiseen tai lainojen saamiseen (Coventry & Branley, 2018, s. 49.)

Perakslisin (2014, s. 195) mukaan terveydenhuoltoon kohdistuva kyberrikollisuus on ilmennyt neljänä tiettynä uhkamuotona, jotka ovat tietovuodot, taloudellinen varkaus, lääketieteellisiin laitteisiin ja terveydenhuollon infrastruktuuriin kohdistuvat hyökkäykset. Kyseiset uhkamuodot eivät vain vaaranna potilastietojen turvallisuutta ja terveydenhuollon infrastruktuurin eheyttä, vaan ne voivat mahdollisesti johtaa vakaviin yhteiskunnallisiin seurauksiin. Esimerkiksi lääketieteellisiin laitteisiin kohdistuvat hyökkäykset voivat vaarantaa suoraan potilaiden hoidon ja terveydenhuollon toiminnan jatkuvuuden (Perakslis, 2014, s. 195.). Vaikka terveydenhuoltosektori onkin merkittävä kohde kyberrikollisuudelle kriittisten kansallisten infrastruktuurien joukossa sen näkyvyyden ja laajojen vaikutusten vuoksi, terveydenhuollon kyberverkot eivät ole alttiina samanlaisille tiukoille kyberturvallisuusstandardeille kuin muut sektorit, kuten esimerkiksi energiasektori (Bernard ym., 2020, s.134.)

Terveydenhuoltoa vastaan voidaan käyttää useita erilaisia tekniikoita. Williamsin ja Woodwardin (2015, s. 310) mukaan terveydenhuoltoon kohdistuvan hyökkäyksen metodina voi olla muun muassa suora hyökkäys, sosiaalinen manipulointi, haittaohjelma tai näiden kaikkien yhdistelmä. Suora hyökkäys voi tapahtua suoraan laitteeseen yhteydessä olevan, joko langattoman tai fyysisen yhteyden kautta. Hyökkääjän on myös mahdollista muodostaa yhteys laitteeseen verkossa, joko paikallisesti tai internetin kautta. Sosiaalinen manipulointi kuvaa hyökkäyksen vaihetta, jossa hyökkääjä hankkii tietoa ihmisiltä, jotka tuntevat järjestelmän ja sen turvallisuustoimenpiteet. Haittaohjelmat koostuvat muun muassa viruksista, madoista, troijalaisista ja kiristyshaittaohjelmista. Haittaohjelmat hyödyntävät järjestelmien ja laitteiden tunnistettuja haavoittuvuuksia (Williams & Woodward, 2015, s. 310.).

Gordonin, Fairhallin ja Landmanin (2017, s. 1) mukaan erityisesti palvelunestohyökkäykset ovat kohdistuneet terveydenhuollon laitoksiin. Palvelunestohyökkäykset pyrkivät häiritsemään ja estämään järjestelmien toiminnan ylikuormittamalla niitä suurella määrällä verkkoliikennettä. Tällaiset hyökkäykset voivat tehdä kliinisistä järjestelemistä käyttökelvottomia, mikä voi vaikuttaa haitallisesti sairaalan perustoimintoihin, kuten kirurgisten toimenpitei-

den viivästymiseen sekä laboratoriotulosten raportointiin (Gordon ym.,2017, s. 1.) Palvelunestohyökkäyksissä potilastiedot eivät yleensä ole vaarassa, mutta potilasturvallisuus voi kuitenkin kärsiä. Potilasturvallisuus voi kärsiä esimerkiksi, kun terveydenhuollon asiakas ei pääse käsiksi terveystietoihinsa tai kun sairaalan henkilökunta ei pysty toteuttamaan suunniteltuja hoitotoimenpiteitä, koska heidän pääsynsä terveystietoihin on estynyt (Lehto & Neittaanmäki, 2022, s. 200.)

Gordon ja muut kirjoittajat (2017, s. 1) nostavat esille myös haittaohjelmien ja erityisesti kiristyshyökkäysten yleistymisen terveydenhuoltosektorilla viime aikoina. Sairaalat ovat houkutteleva kohde kiristyshyökkäyksille useasta eri syystä. Yhtenä syynä voidaan pitää muun muassa sitä, että sairaaloissa käytetään niin paljon eri laitteita ja järjestelmiä, että niiden pitäminen ajan tasalla esimerkiksi eri suojauspäivitysten suhteen on hyvin haastavaa, jottei hoidonsaanti lakkaa (Lehto & Neittaanmäki, 2022, s. 189.) Näissä hyökkäyksissä tietojärjestelmä, esimerkiksi potilastietoja sisältävä tietokanta, salataan siten, että vain hyökkääjällä on avain tietojen avaamiseen. Vaikka sairaala maksaisikin hyökkääjälle lunnaat tietojen avaamisesta, maksu ei takaa aina pääsyä salattuihin tietoihin. Vaikka palvelunesto- ja kiristyshyökkäykset häiritsevät järjestelmiä ja voivat merkitsevästi haitata tehokkaan hoidon tarjoamista, ne eivät välttämättä paljasta potilastietoja. Huolestuttavimpia ovat hyökkäykset, jotka johtavat suojattujen terveystietojen ja muiden henkilötietojen paljastumiseen (Gordon ym., 2017, s. 2.).

Usein organisaatiot keskittyvät suojaamaan turvallisuuttaan ja eheyttään ulkoisilta uhkilta, mutta unohtavat omassa organisaatiossa mahdollisesti piilevän sisäisen uhan (Lehto & Neittaanmäki, 2022, s. 201.) Esimerkiksi terveydenhuollon työntekijät voivat muodostaa sisäisen uhan, sillä heillä on laillinen pääsy eri järjestelmiin. Heillä voi olla parempi tietämys verkon rakenteesta ja haavoittuvuuksista kuin ulkopuolisilla uhilla. Sisäinen uhka voi aiheuttaa vahinkoa joko tahattomasti tai tahallisesti. Sisäinen uhka voi tarkoittaa esimerkiksi työntekijää, joka painaa vahingossa haitallista linkkiä sähköpostiin tulleen tietojenkalastelun myötä tai myy tietoisesti terveystietoja tavoitellessaan taloudellista voittoa. Sisäisen uhkan myötä potilaiden yksityisyys voikin vaarantua ja kansalaisten luottamus terveydenhuoltoa kohtaan heikentyä esimerkiksi tahallisen tietovuodon sattuessa (Lehto & Neittaanmäki, 2022, s. 201.).

Potilastiedot voivat olla myös vaarassa, kun niitä säilytetään kannettavilla tietokoneilla, jotka viedään sairaalan ulkopuolelle. Kannettavia tietokoneita on varastettu lääkärin vastaanotoilta, autoista ja terveydenhuollon ammattilaisten kodeista (Lehto & Neittaanmäki, 2022, s. 201.) Lehdon ja Neittaanmäen (2022, s. 201) mukaan tällaisten varkauksien ongelmakohta on se, että vaikka tietokoneet ovatkin usein salattuja salasanojen avulla, niiden kovalevyt ja niiden sisältämät tiedot ovat harvoin salattuja. Tietokoneen varastanut henkilö voi siis päästä käsiksi tietoihin, jos hän onnistuu ohittamaan salasanan kyselyn (Lehto & Neittaanmäki, 2022, s. 201–202.)

TAULUKKO 1 Kyberuhkien vaikutukset terveydenhuoltoon kansallisen turvallisuuden näkökulmasta

Kyberuhkatyyppi	**Vaikutukset**	**Lähteet**
Kiristyshaittaohjelma	Toiminnalliset häiriöt sekä taloudelliset seuraukset vaikuttavat negatiivisesti terveydenhuollon laitosten maineeseen ja tuloihin, vaarantaen samalla kansallisen turvallisuuden esimerkiksi hoidonsaannin viivästyessä.	(Argaw ym., 2020) (Gordon ym., 2017) (Chua, 2021)
Tietovuoto	Potilaiden yksityisyys vaarantuu ja terveystietoja voidaan käyttää väärin. Luottamus terveydenhuollon järjestelmiin heikentyy, mikä voi vaikuttaa kansalaisten halukkuuteen hakeutua hoitoon ja noudattaa terveydenhuollon ohjeita.	(Norri-Sederholm ym., 2019) (Perakslis, 2014)
Lääketieteelliseen laitteeseen kohdistuva hyökkäys	Potilaiden hoidonsaanti ja terveydenhuollon toiminnan jatkuvuus vaarantuu.	(Perakslis, 2014) (Lehto & Neittaanmäki, 2022)
Palvelunestohyökkäys	Terveydenhuollon järjestelmien toiminta lakkaa, mikä vaikuttaa negatiivisesti terveydenhuollon perustoimintoihin, kuten hoitotoimenpiteiden viivästymiseen. Potilasturvallisuus vaarantuu, sillä niin asiakkaiden kuin henkilökunnan pääsy terveystietoihin estyy.	(Gordon ym., 2017) (Lehto & Neittaanmäki, 2022) (Bhuyan, ym., 2020)
Tietojenkalastelu sähköpostin välityksellä	Sähköpostissa olevan linkin tai tiedoston avaaminen voi johtaa haittaohjelmien lataamiseen. Linkin tai tiedoston avaaminen voi myös antaa pääsyn hyökkääjälle tietokoneeseen tai muihin verkossa olevien tietokoneiden tietoihin, vaarantaen niin terveydenhuollon laitosten toiminnan kuin potilaiden yksityisyyden.	(Chua, 2021) (Lehto & Neittaanmäki, 2022)
Sisäinen uhka	Esimerkiksi työntekijän tarkastellessa potilastietoja ilman perustetta, potilasturvallisuus vaarantuu ja kansalaisten luottamus terveydenhuoltoa kohtaan heikkenee.	(Lehto & Neittaanmäki, 2022) (Bhuyan, ym., 2020)

Vaikka terveysteknologiat ovatkin avainasemassa väestön terveydessä, ne ovat alttiita kyberuhille johtuen eri yhteyksien välisistä, helposti saatavilla olevista päätepisteistä, vanhentuneista järjestelmistä ja tietoturvaa koskevan painotuksen puuttumisesta organisaation kulttuurissa (Coventry & Branley, 2018, s. 51.) Tietoturva on olennainen osa potilaiden turvallisuuden, yksityisyyden ja luottamuksen ylläpitämistä. Enemmän rahaa ja vaivaa tulisikin sijoittaa terveysteknologioiden ja potilastietojen turvallisuuden varmistamiseen (Coventry & Branley, 2018, s. 51.). Kyberuhat voivat vaikuttaa terveydenhuoltoon kansallisen turvallisuuden näkökulmasta monin eri tavoin ja siksi onkin tärkeää, että terveydenhuollon organisaatiot ja viranomaiset panostavat tietoturvaan ja kyberhyökkäysten ennaltaehkäisyyn.

4.3 Toimenpiteet ja varautuminen

Terveydenhuollon turvaaminen on tärkeä osa kansallista turvallisuutta. Feldbaumin, Patelin, Sondorpin ja Leen (2006) mukaan kansallisen terveydenhuollon strategiset tavoitteet turvallisuuden varmistamiseksi voivat sisältää muun muassa elinaikaodotteen pidentämisen, vammojen ja kuolleisuuden vähentämisen, ensiavun ja lääketieteellisen hoidon tarjonnan parantamisen, lääketieteellisen hoidon standardien parantamisen, lääkkeiden laadun, tehokkuuden ja turvallisuuden valvonnan parantamisen sekä potilaiden oikeuksien suojelemisen. Terveydenhuollon kansallisen turvallisuuden vahvistamiseksi on tarpeen parantaa terveyspalveluiden laatua ja saatavuutta hyödyntämällä tieto- ja viestintätekniikkaa (Blaya, Fraser, & Holt, 2010.)

Terveydenhuoltoon kohdistuvien riskien pienentämistä on tutkittu laajasti kirjallisuudessa. Muun muassa Al-Qarni (2023, s. 138) on käsitellyt sairaaloiden kyberhyökkäysten vaikutusten vähentämiseen käytettäviä riskiluokituksia ja uusimpia teknologioita. Hänen mukaansa riskien pienentämiseen ja välttämiseen on kaksi vaihtoehtoa: ennaltaehkäisevät toimenpiteet ja riskinhallintatoimenpiteet. Ennaltaehkäisevät toimenpiteet pyrkivät vähentämään kyberhyökkäyksen mahdollisuutta tai vaikutuksia, ja ne keskittyvät organisaation heikkouksien ja turvallisuusriskien paikantamiseen ja korjaamiseen. Riskienhallintatoimenpiteisiin voi taas sisältyä esimerkiksi palomuurien käyttöönotto, henkilöstön kouluttaminen ja ohjelmistojen ja laitteiden säännöllinen päivittäminen (Al-Qarni, 2023, s. 138.).

Gordonin ja muiden kirjoittajien (2017, s.2) mukaan terveydenhuoltoon kohdistuvien moninaisten uhkien torjunta on monimutkaista, eikä olemassa ole yhtä ratkaisua riskien poistamiseen. Riskejä voidaan kuitenkin pyrkiä pienentämään. Gordon ja muut kirjoittajat (2017) nostavatkin esiin useita tapoja pienentää terveydenhuoltoon kohdistuvia riskiä. Ensinnäkin on tärkeää noudattaa nykyaikaisia ja parhaiksi todettuja käytäntöjä tietoturvan suhteen. Näihin sisältyvät muun muassa tietojen salaaminen, viruksentorjuntaohjelmisto, ohjelmistopäivitykset ja kaksivaiheinen tunnistautuminen. Myös säännölliset varmuuskopiot ja vahvat varajärjestelmät voivat vähentää hyökkäysten aiheuttamia haittoja. Pääsy suojattuihin terveystietoihin tulisi rajoittaa vain niille hen-

kilöille, jotka todella tarvitsevat kyseisiä tietoja. Riskianalyysit tulisi suorittaa säännöllisesti ja tarvittavat lieventävät toimenpiteet tulisi ottaa käyttöön (Gordon ym., 2017.).

Seuraavaksi Gordon ja muut kirjoittajat (2017, s. 2–3) nostavat esiin teknologian järkevän ja käytännöllisen käytön tärkeyden. Järjestelmiä tulisi suunnitella ottaen huomioon käyttäjien työnkulku. Yhtenä esimerkkinä voitaisiin pitää salasanojen turvallisuutta. Vaikka salasanojen vahvuus onkin tärkeää, ei ole vahvistettu, että yleinen käytäntö, joka vaatii salasanojen vaihtamista säännöllisin väliajoin tekisi salasanoista tai käyttäjätunnuksista vähemmän haavoittuvaisia. Esimerkiksi usein toistuvien salasanojen vaihtojen vaatiminen saattaa johtaa siihen, että työntekijät kirjoittavat salasanat paperille muistiin (Gordon ym., 2017, s. 2–3.). Myös Argaw ja muut kirjoittajat (2020, s. 4) ovat pohtineet toimenpiteitä terveydenhuoltoon kohdistuvien riskien pienentämiseen. Heidän mukaansa terveydenhuollon laitoksen vahva tietoturvamalli vaatii laadukasta tietotekniikkaa. Laadukkaalla tietotekniikalla tarkoitetaan erityisesti vakaata sovellusperustaa ja IT-infrastruktuuria. Argawin ja muiden kirjoittajien (2020, s.4) mukaan tämän saavuttaminen on kuitenkin erityisen vaikeaa terveydenhuollon yksiköissä, johtuen henkilöstöresurssien puutteista, budjettirajoituksista ja monimutkaisesta sovellusalueesta.

Viimeisenä ja kaikkein tärkeimpänä Gordonin ja muiden kirjoittajien mukaan (2017, s. 3) koulutus on olennainen tekijä riskien pienentämisessä. Tahaton huolimattomuus pysyy edelleen suurimpana riskinä, sillä terveydenhuoltoon kohdistuvat kyberhyökkäykset leviävät usein tahattoman työntekijäkäyttäytymisen kautta, kuten sähköpostiliitteen avaamisen, sähköpostiviestiin upotetun linkin tai muun onnistuneen kalasteluhyökkäyksen kautta. Suurin osa tietovuodoista huomataankin vasta jälkikäteen, koska henkilökunta saattaa olla tietämätön siitä, että on joutunut kalasteluhyökkäyksen uhriksi (Gordon ym., 2017, s. 3.). Säännöllinen henkilökunnan opetus ja koulutus tietoturvasta onkin elintärkeää, sillä ihmiset ovat heikoin lenkki terveydenhuollon turvallisuusinfrastruktuurissa.

Myös Argawin ja muiden kirjoittajien (2020, s. 5) mukaan ihmisen toiminta on suurin riski turvallisuudelle, joten terveydenhuollon laitosten tietoturvatoimissa tulisi huomioida tarve lisätä tietoisuutta kaikkien käyttäjien keskuudessa. Jotta terveydenhuollon laitokset voisivat tarjota asiaankuuluvaa ja tehokasta koulutusta työntekijöilleen, on tärkeää, että tietovajeita arvioidaan ja tunnistetaan säännöllisesti. Terveydenhuollon järjestelmien käyttäjien olisi tärkeää ymmärtää mahdolliset riskit esimerkiksi huolimattomuuden takia. Uhat tulisi ymmärtää konkreettisesti (Argaw ym., 2020, s. 5.).

Valitettavasti mikään järjestelmä ei voi taata täydellistä turvallisuutta. Niin kauan kuin informaatiolla on arvoa, terveydenhuoltoon kohdistuvia hyökkäyksiä tulee tapahtumaan (Gordon ym., 2017, s.3.) Siitä huolimatta, jos tietoturvan kansanterveydelliset vaikutukset otetaan huomioon, voidaan parantaa vuoropuhelua ja toteuttaa tarvittavia suojauksia. Coventry ja Branley (2018, s. 52) toteavat, että tietoturvallisuuden tulisi olla tärkeä osa potilashoidon kulttuuria. Kätevät, mutta turvattomat menetelmät tulisi korvata turvallisemmilla ja perusteellisemmilla lähestymistavoilla (Coventry & Branley, 2018.) Turvalli-

suuden ei siis tulisi olla vain näennäistä, esimerkiksi sääntöjen noudattamisen vuoksi, vaan se tulisi integroida sisälle kulttuuriin.

5 YHTEENVETO

Tämän kandidaatintutkielman päätavoitteena oli tutkia kyberuhkien vaikutuksia terveydenhuoltoon kansallisen turvallisuuden näkökulmasta. Tutkielma toteutettiin kirjallisuuskatsauksena, jossa lähteiden hakuun käytettiin useita eri tietokantoja, kuten JYKDOK, Google Scholar ja Scopus. Tutkielmassa arvioitiin kyberuhkien mahdollisia vaikutuksia potilasturvallisuuteen, terveydenhuollon järjestelmiin ja niiden luotettavuuteen sekä laajemmin yhteiskunnan toimintakykyyn terveydenhuollon kriisitilanteissa. Tutkielman aiheen valinta perustui terveydenhuollon rooliin yhteiskunnan kriittisenä infrastruktuurina ja sen merkitykseen kansallisen turvallisuuden näkökulmasta. Tutkielman tarkoituksena oli syventää ymmärrystä mahdollisista terveydenhuoltoon kohdistuvista haavoittuvuuksista sekä kehittää strategioita kyberuhkien ennaltaehkäisemiseksi ja torjumiseksi. Tavoitteena oli vastata seuraavaan tutkimuskysymykseen:

- Miten erilaiset kyberuhat vaikuttavat terveydenhuoltoon kansallisen turvallisuuden näkökulmasta?

Ennen tutkimuskysymykseen vastaamista tutkielmassa pyrittiin luomaan laaja ymmärrys kyberuhkista, terveydenhuollosta ja kansallisesta turvallisuudesta. Ensimmäisenä määriteltiin, mitä kyberuhat tarkoittavat nykypäivän kontekstissa ja käytiin läpi yleisimpiä kyberuhkatyyppejä ja niiden ominaispiirteitä. Kyberuhat ovat jatkuvasti läsnä nykyajan tietoturvaympäristössä, mikä edellyttää jatkuvaa varautumista niihin. Tietoturvakäytäntöjen päivittämisen tarve korostuu uhkien monimuotoisuuden vuoksi.

Seuraavaksi käsiteltiin terveydenhuoltoon liittyviä näkökulmia keskittyen käsitteen määrittelemiseen, haavoittuvuuksiin sekä tietosuojaan ja potilastietojen hallintaan. Terveydenhuollon järjestelmät sisältävät valtavia määriä arvokasta ja arkaluontoista tietoa. Monien terveydenhuoltoon kohdistuvien hyökkäysten motiivina on taloudellinen hyöty, koska terveystiedot ovat arvokkaampia kuin muut henkilötiedot. Hyökkäysten motiivina voi olla myös poliittinen voitto. Kun terveydenhuoltoon kohdistuu kyberuhka, ihmishenget vaarantuvat. Hyökkäykset voivat johtaa kriittisten laitteiden toiminnan menettämiseen sairaaloissa ja hoidonsaannin estymiseen. Terveydenhuollolla onkin

useita haavoittuvuuksia. Haavoittuvuudet kohdistuvat erityisesti laitteisiin, ohjelmistoihin, mobiililaitteisiin, etähallittaviin laitteisiin ja käyttäjien toimintaan. Terveydenhuollon henkilöstön riittämätön koulutus ja välinpitämättömyys tietoturvasta altistaa alan kyberuhkille.

Tutkimuskysymykseen vastattiin neljännessä pääluvussa. Tarkoituksena oli syventyä kandidaatintutkielman aiheeseen aloittaen kansallisen turvallisuuden määritelmästä ja edeten kyberuhkien vaikutuksista terveydenhuoltoon ja niiden yhteiskunnallisiin näkökulmiin sekä toimenpiteisiin kyberuhkien varalta. Kyberuhat vaikuttavat terveydenhuoltoon monin tavoin ja niiden vaikutukset ulottuvat kansallisen turvallisuuden kentälle. Terveydenhuoltoon kohdistuvat hyökkäykset ja uhat voivat vaarantaa potilaiden yksityisyyden, häiritä terveydenhuollon laitosten toimintaa ja asettaa potilaiden terveyden ja hyvinvoinnin vaaraan. Tällaiset hyökkäykset ja uhat voivat johtaa toiminnallisiin häiriöihin ja taloudellisiin menetyksiin vaikuttaen pitkällä aikavälillä terveydenhuollon laitosten maineeseen ja tuloihin. Nämä seuraukset vaarantavat kansallisen turvallisuuden. Kyberuhat voivat vaikuttaa terveydenhuoltoon monilla eri tavoilla, kuten kiristyshaittaohjelmilla, palvelunestohyökkäyksillä sekä lääketieteellisiin laitteisiin ja sairaalan infrastruktuuriin kohdistuvilla hyökkäyksillä.

Terveydenhuollon turvaaminen on olennainen osa kansallista turvallisuutta ja sen strategiset tavoitteet sisältävät muun muassa elinaikaodotteen pidentämisen, vammojen ja kuolleisuuden vähentämisen sekä potilaiden oikeuksien suojelemisen. Tavoitteiden saavuttamiseksi on tarpeen parantaa terveyspalveluiden laatua ja saatavuutta hyödyntämällä tieto- ja viestintätekniikkaa. Terveydenhuoltoon kohdistuvien riskien pienentämiseen on olemassa useita keinoja mukaan lukien ennaltaehkäisevät toimenpiteet ja riskinhallintatoimenpiteet. Näihin sisältyy muun muassa organisaation heikkouksien ja turvallisuusriskien paikantaminen ja korjaaminen, nykyaikaisten tietoturvakäytäntöjen noudattaminen, teknologian järkevä ja käytännöllinen käyttö sekä henkilöstön säännöllinen koulutus tietoturva-asioissa.

Vaikka täydellistä turvallisuutta ei voida taata, asianmukaisilla toimenpiteillä ja koulutuksella voidaan pienentää terveydenhuoltoon kohdistuvia riskejä. Tietoturva on olennainen osa potilaiden turvallisuuden, yksityisyyden ja luottamuksen ylläpitämistä. Terveydenhuollon useat haavoittuvuudet todistavat, että terveydenhuollon kyberturvallisuus ei ole riittävää. On tarpeen sijoittaa enemmän rahaa ja vaivaa terveysteknologioiden ja potilastietojen turvallisuuden varmistamiseen. Tietoturva on suunniteltava terveydenhuollon strategioihin, tuotteisiin ja palveluihin alusta alkaen ennakoiden, eikä se saa olla jälkikäteen korjaava toimenpide. Tietoturva onkin sisällytettävä osaksi terveydenhuollon kulttuuria kokonaisuudessaan.

On tärkeää huomioida, että tämä tutkielma on vain kevyt katsaus kyberuhkien maailmaan terveydenhuollossa. Vaikka tutkielma tarjoaa yleiskuvan kyberuhkien vaikutuksista terveydenhuoltoon, se jättää huomiotta erilaisia näkökulmia ja syvällisempiä analyyseja. Tutkielmassa ei esimerkiksi syvennytty kaikkiin kyberuhkiin, vaan ainoastaan kirjallisuudessa eniten esiintyneisiin kyberuhkatyyppeihin. On myös tärkeää tunnistaa, että tutkielmassa jäi tutkimatta laaja joukko alan kirjallisuutta. On siis todennäköistä, että joitakin merkit-

täviä tutkimuksia ja näkökulmia on jätetty huomioimatta. Tämä saattaa vaikuttaa tutkielman esittämien näkökulmien ja johtopäätösten kattavuuteen ja tarkkuuteen. Tämä tutkielma tarjoaakin mahdollisuuden laajemmalle keskustelulle ja tutkimukselle tällä alalla.

Kirjallisuuskatsauksessa käytetyn kirjallisuuden ja tutkielman tulosten myötä, terveydenhuollon tietoturvakulttuurin vahvistamista voisi tutkia lisää. Koska ihmiset ovat edelleen heikoin lenkki organisaatioiden tietoturvallisuudessa, olisi aiheen tutkiminen tärkeää. Tietoturvakulttuurin vahvistaminen terveydenhuollon organisaatioissa on tärkeä ja ajankohtainen aihe, joka vaikuttaa merkittävästi terveydenhuollon kyberturvallisuuteen. Jatkotutkimus voisi analysoida organisaation nykytilaa eli kartoittaa millainen tietoturvakulttuuri terveydenhuollon organisaatioissa on tällä hetkellä. Nykytilan analyysi johtaisi tietoturvakulttuurin osaamis- ja kehittämistarpeiden tunnistamiseen. Tämän kaltainen jatkotutkimus voisi tuottaa tärkeää tietoa siitä, miten terveydenhuollon organisaatioissa suhtaudutaan tietoturvaan ja minkälainen osaamistaso henkilökunnalla on. Edellä mainittuihin asioihin panostaminen auttaisi kehittämään parempia strategioita terveydenhuollon kyberturvallisuuden varmistamiseksi.

LÄHTEET

Al-Qarni, E. A. (2023). Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies. *International Journal of Advanced Computer Science and Applications*, *14*(5). https://doi.org/10.14569/IJACSA.2023.0140513

Alguliyev, R. M., Imamverdiyev, Y. N., Mahmudov, R. Sh., & Aliguliyev, R. M. (2021). Information security as a national security component. Information Security Journal: A Global Perspective, 30(1), 1–18. https://doi.org/10.1080/19393555.2020.1795323

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M.-V., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J.-M., O'Leary, C., Eshaya-Chauvin, B., & Flahault, A. (2020). Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. BMC Medical Informatics and Decision Making, 20(1), 146. https://doi.org/10.1186/s12911-020-01161-7

Bernard, R., Bowsher, G., & Sullivan, R. (2020). Cyber security and the unexplored threat to global health: A call for global norms. Global Security: Health, Science and Policy, 5(1), 134–141. https://doi.org/10.1080/23779497.2020.1865182

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Kenya, E., Sandeep, P., Wyant, D., Sajeesh, K., Levy, M., Satish, K., Dipankar, D., & Aram, D. (2020). Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations. *Journal of Medical Systems*, *44*(5). https://doi.org/10.1007/s10916-019-1507-y

Blaya, J. A., Fraser, H. S. F., & Holt, B. (2010). E-Health Technologies Show Promise In Developing Countries. *Health Affairs*, 29(2), 244–251. https://doi.org/10.1377/hlthaff.2009.0894

Chua, J. A. (2021). Cybersecurity in the Healthcare Industry. *The Journal of Medical Practice Management*, *36*(4), 229–231.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*, *113*, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

Feldbaum, H., Patel, P., Sondorp, E., & Lee, K. (2006). Global health and national security: The need for critical engagement. *Medicine, Conflict and Survival*, 22(3), 192–198. https://doi.org/10.1080/13623690600772501

Ghafur, S., Grass, E., Jennings, N. R., & Darzi, A. (2019). The challenges of cybersecurity in health care: The UK National Health Service as a case study. The Lancet Digital Health, 1(1), e10–e12. https://doi.org/10.1016/S2589-7500(19)30005-6

Gordon, W. J., Fairhall, A., & Landman, A. (2017). Threats to Information Security—Public Health Implications. New England Journal of Medicine, 377(8), 707–709. https://doi.org/10.1056/NEJMp1707212

Jones, D., Greenhill, R., Shaw, C., Flores, D., & Schmidt, R. N. (2022). Cybersecurity Threats in the Healthcare Industry. *Journal of Business and Educational Leadership*, *12*(1), 57–67.

Kanta.fi. *Potilastiedon arkisto – Sote-ammattilaiset.* (ei pvm.). Kanta.fi. Noudettu 24. tammikuuta 2024, osoitteesta https://www.kanta.fi/ammattilaiset/potilastiedon-arkisto

Langer, S. G. (2017). Cyber-security issues in healthcare information technology. Journal of digital imaging, 30, 117-125. https://doi.org/10.1007/s10278-016-9913-x

Lehto,M., & Neittaanmäki, P. (2022). *Cyber Security: Critical Infrastructure Protection*. Springer.

Ness, S., & Khinvasara, T. (2024). Emerging Threats in Cyberspace: Implications for National Security Policy and Healthcare Sector. *Journal of Engineering Research and Reports*, 26(2), 107-117. https://doi.org/10.9734/jerr/2024/v26i21075

Norri-Sederholm, T., Laitinen, T., Lehto, M., & Kari, M. J. (2019). Terveydenhuolto ja kyberuhkat. Finnish Journal of eHealth and eWelfare, 11(1), 86-99. https://doi.org/10.23996/fjhw.74183

Perakslis, E. D. (2014). *Cybersecurity in Health Care.* New England Journal of Medicine, 371(5), 395–397. https://doi.org/10.1056/NEJMp1407326

Sisäministeriö. *Mitä on kansallinen turvallisuus?* (ei pvm.). Noudettu 2. marraskuuta 2023, osoitteesta https://intermin.fi/kansallinen-turvallisuus/mita-on-kansallinen-turvallisuus

Sosiaali- ja terveysministeriö *Terveydenhuoltoalan kyberuhkia* (ei pvm.). Noudettu 6. marraskuuta 2023, osoitteesta https://stm.fi/terveyspalvelut

Sosiaali- ja terveysministeriö. *Terveyspalvelut.* (ei pvm.) Noudettu 6. marraskuuta 2023, osoitteesta *https://stm.fi/terveyspalvelut*

Tietosuojavaltuutetun toimisto. *Sosiaalihuollon asiakastietojen käsittely.* (ei pvm.) Noudettu 24. tammikuuta 2024 osoitteesta https://tietosuoja.fi/usein-kysyttya-sosiaalihuolto

Turvallisuuskomitea. *Kokonaisturvallisuuden sanasto* (ei pvm.). Noudettu 11. joulukuuta 2023, osoitteesta https://turvallisuuskomitea.fi/viestinta/kokonaisturvallisuuden-sanasto/

Valvira. *Potilas- ja asiakastietojen ja henkilötietojen käsittely*. (ei pvm.). Noudettu 24. tammikuuta 2024, osoitteesta https://valvira.fi/sosiaali-ja-terveydenhuolto/potilas-ja-asiakastietojen-ja-henkilotietojen-kasittely

Williams, P. A., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. Medical Devices : Evidence and Research, 8(default), 305–316. https://doi.org/10.2147/MDER.S50048