Kyberuhkat sosiaali- ja terveydenhuollossa – kuvaileva kirjallisuuskatsaus

Enna Alastalo

KANDIDAATINTUTKIELMA

Hoitotiede

Turun yliopisto

Hoitotieteen laitos

Toukokuu 2024

Kandidaatintutkielma

Oppiaine: Hoitotiede
Tekijä: Enna Alastalo
Otsikko: Kyberuhkat sosiaali- ja terveydenhuollossa – kuvaileva kirjallisuuskatsaus
Ohjaajat: professori Minna Stolt, yliopisto-opettaja Sanna Koskinen ja valmiusasiantuntija Aleksi Kasvi
Sivumäärä: 42 sivua, 4 liitesivua
Päivämäärä: 17.5.2024

Tässä tutkielmassa tarkastellaan kyberuhkia sosiaali- ja terveydenhuollossa. Sosiaali- ja terveydenhuoltoon kohdistuvien kyberhyökkäysten määrä on kasvanut tasaisesti 2010-luvulta lähtien. COVID-19-pandemian aikana sosiaali- ja terveydenhuolto jäivät haavoittuvaisiksi kyberhyökkäyksille ja kyberhyökkäysten määrä viisinkertaistui. Tutkielman tarkoituksena oli kansainväliseen kirjallisuuteen pohjaten kuvata sosiaali- ja terveydenhuollossa kohdattuja kyberhyökkäyksiä, niiden vaikutuksia ja niihin varautumista. Tutkielmassa tuotetun tiedon avulla voidaan kehittää kyberuhkien valmiussuunnitelmia.

Tutkielma toteutettiin kuvailevana kirjallisuuskatsauksena. Tiedonhaku toteutettiin helmikuussa 2024 neljään eri tietokantaan: PubMed, CINAHL, Cochrane ja Scopus. Näistä tietokannoista saatiin viitteitä 793. Mukaanotto- ja poissulkukriteerien perusteella tutkielmaan valittiin 10 tutkimusta. Aineisto analysoitiin induktiivisella sisällönanalyysilla.

Tutkimuskysymysten ohjaamana muodostettiin kolme kategoriaa: kyberhyökkäykset, kyberhyökkäysten vaikutukset ja kyberhyökkäyksiin varautuminen. Sosiaali- ja terveydenhuoltoon oli kohdistettu viisi tunnettua kyberhyökkäystä. Kyberhyökkäysten keskeisiä vaikutuksia olivat potilastietojen menetys, laboratoriojärjestelmän kaatuminen, internet-yhteyden katkeaminen, päivittäisten poliklinikkakäyntien ja kiireettömän leikkaustoiminnan vähentyminen sekä henkilökunnan uupuminen. Kyberhyökkäyksiin ei ollut varauduttu sosiaali- ja terveydenhuollon organisaatioissa, ja valmiussuunnitelmien puuttuminen pahensi kyberhyökkäyksien vaikutuksia. Kyberhyökkäyksiä tarkasteltaessa tunnistetiin hyviä toimintatapoja niihin varautumiseen, joita voidaan hyödyntää valmiussuunnitelman luomisessa.

Sosiaali- ja terveydenhuollon organisaatioissa tulisi luoda kyberhyökkäyksiä varten valmiussuunnitelma, jotta sosiaali- ja terveydenhuollossa palvelut pystyttäisiin tuottamaan poikkeustilanteesta huolimatta. Suurin osa sosiaali- ja terveydenhuoltoon kohdistuvista kyberhyökkäyksistä ovat kiristyshaittaohjelmia, ja kiristyshaittaohjelman yhteydessä voi tapahtua myös tietomurto. Tietomurtojen vaikutuksista tarvitaan lisätutkimusta potilaan sekä organisaation näkökulmasta.

Avainsanat: sosiaali- ja terveydenhuolto, kyberhyökkäys, kyberuhka, varautuminen

Sisällys

1 Johdanto

Sosiaali- ja terveydenhuoltoon kohdistuvat kyberuhkat ovat aiheuttaneet yhä enemmän huolta maailmanlaajuisesti. Kyberuhkilla tarkoitetaan haitallisia tapahtumia, jotka voivat vaarantaa kybertoimintaympäristöstä riippuvaisen toiminnon (Sanastokeskus ym., 2018). Tällaisia kyberuhkia ovat esimerkiksi kyberhyökkäykset, kuten tietomurto, palvelunestohyökkäys tai kiristyshaittaohjelma. Sen lisäksi, että kyberhyökkäyksien määrä sosiaali- ja terveydenhuoltoa kohtaan on kasvanut, niistä on tullut entistä vakavampia. Sairaalat eivät ole valmiita vastaamaan uhkakuviin, vaikka sosiaali- ja terveydenhuoltoon kohdistuvat kyberhyökkäykset ovat lisääntyneet jo 2010- luvulta lähtien. (Ponemon, 2016.)

Sosiaali- ja terveydenhuolto on nykyään kansainvälisesti yksi yleisimmistä kyberhyökkäyksien kohteista. Sen altistaa tietomurroille tiedon muuttumattomuus ja sensitiivisyys, kuten henkilötunnukset ja potilaiden terveyshistoria. (Argaw ym., 2020.) Viime vuosina kyberuhkien kasvuun merkittävästi on vaikuttanut COVID-19-pandemia, jonka aikana sosiaali- ja terveydenhuolto jäi haavoittuvaisemmaksi kyberuhkille. Maailman terveysjärjestö (World Health Organization [WHO], 2020) raportoi, että kyberhyökkäysten määrä on viisinkertaistunut COVID-19-pandemian aikana ja kansainvälinen rikospoliisijärjestö (Interpol, 2020) julkaisi samana vuonna raportin, jossa varoitettiin maailmanlaajuisesti kyberhyökkäyksien lisääntymisestä. Kyberrikollisille avautui tilaisuus pandemian aikana esittäytyä esimerkiksi viranomaisina ja etätyöskentelyn lisääntyminen toi huomattavan haasteen sekä riskin tietoturvalle (Lallie ym., 2021). Pandemia lisäsi teknologian käyttöä terveyspalveluissa ja merkittävä osa potilastiedoista on nykyään internet-palvelimilla alttiina väärinkäytöille. Sairaaloihin kohdistuvia kyberhyökkäyksiä kutsutaan elämää uhkaaviksi rikoksiksi, koska niistä johtuvilla potilashoidon häiriöillä voi olla kauaskantoisia ja vakavia seurauksia potilaiden terveydelle. (Riggi, 2020.)

Sosiaali- ja terveydenhuollon tehtävänä on turvata kaikille terveyden ja toimintakyvyn kannalta keskeiset sosiaali- ja terveydenhuollon palvelut olosuhteista riippumatta. Tämä tarkoittaa sitä, että sosiaali- ja terveydenhuollossa on varauduttava poikkeusoloihin ja häiriötilanteisiin. Suomessa sosiaali- ja terveydenhuollon varautumisesta vastaa sosiaali- ja terveysministeriö. (Sosiaali- ja terveysministeriö [STM], n.d..) Kansallinen riskinarvio vuodelta 2023 tunnistaa, että sosiaali- ja terveydenhuoltoon kohdistettu kyberhyökkäys voi saada aikaan ihmishenkien menetyksiä (Sisäministeriö, 2023).

Kasvaviin kyberuhkiin on tärkeä varautua myös Suomessa oppimalla aikaisemmista kansainvälisistä kyberhyökkäyksistä. Tutkielman tarkoituksena on kansainväliseen kirjallisuuteen pohjaten kuvata sosiaali- ja terveydenhuollossa kohdattuja kyberhyökkäyksiä, niiden vaikutuksia ja varautumista. Tutkielmassa tuotetun tiedon avulla voidaan kehittää kyberuhkiin varautumisen menetelmiä.

2 Keskeiset käsitteet

2.1 Kyberturvallisuus, tietoturvallisuus ja kybertoimintaympäristö

Kyberturvallisuus määritellään Suomessa seuraavasti: ”tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan”. Käsitteellä on eroa tietoturvallisuuden määritelmään, joka on kuvattu: ”järjestely, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus”. (Sanastokeskus ym., 2018.) Kybertoimintaympäristö tarkoittaa useita toisiinsa yhdistyneitä tietoverkkoja, tietoliikennetekniikkaa, tietokoneita sekä eri tehtäviä hoitavia datasäilöjä, reitittimiä ja palvelimia. Koska tietokoneita ja tietoverkkoja käyttää ihminen, kybertoimintaympäristön voidaan ajatella koostuvat kolmesta tasosta; teknologiasta, informaatiosta ja ihmistoimijoista. (Jansson & Sihvonen, 2021.) Kiristynyt kansainvälinen tilanne on johtanut uhkatason nousuun kybertoimintaympäristössä (Sisäministeriö, 2023). Kyberturvallisuuden tavoitteena on siis varmistaa, että kybertoimintaympäristössä olevan informaation käsittely on turvallista ja siitä ei koidu vaaraa tai häiriötä sen toiminnalle (Jansson & Sihvonen, 2021).

2.2 Kyberuhka ja kyberhyökkäys

Kyberuhka määritellään mahdolliseksi haitalliseksi tapahtumaksi tai kehityskuluksi, joka voi ilmetä kybertoimintaympäristössä ja vaarantaa siitä riippuvaisen toiminnon toteutuessaan (Sanastokeskus ym., 2018). Kyberuhka voi vahingoittaa tai häiritä tieto- ja verkkojärjestelmiä, tai niiden käyttäjiä (Sisäministeriö, 2023).

Kyberuhka eroaa siten kyberhyökkäyksestä, että se voi olla myös mahdollisesti haitallinen tapahtuma, kuten yksittäisen terveydenhuollon työntekijän tietämättömyys kyberturvallisesta käyttäytymisestä. Kyberhyökkäys määritellään Suomessa seuraavasti ”tietoverkon kautta tapahtuva teko tai toiminta, jolla pyritään tietoverkon, tietojärjestelmän, laitteen tai datan vahingoittamiseen tai oikeudettomaan käyttöön”. (Sanastokeskus ym., 2018.)

Kyberuhkan määrittelyssä on otettava huomioon myös tietoturvauhka. Tietoturvauhka määritellään mahdollisesti toteutuvaksi tietoturvaan kohdistuvaksi haittatapahtumaksi, joka edetessään vaarantaa tietoturvan. Kyberuhkat voivat juontua paitsi konkreettisista tietoturvauhkista, myös sellaisista yhteiskunnan turvallisuutta vaarantavista teoista, jotka

tapahtuvat digitaalisessa viestintäympäristössä. Nämä uhkat voivat kohdistua suoraan tai epäsuorasti yhteiskunnan elintärkeisiin toimintoihin, kansalliseen kriittiseen infrastruktuuriin, tai kansalaisiin. Ne saattavat lähteä liikkeelle sekä maan sisä- että ulkopuolelta. (Sanastokeskus ym., 2018.)

Kybertoimintaympäristöistä riippuvaisia toimintoja ovat muun muassa ydinvoimaloiden ohjaus, elintarvikkeiden kuljetus ja logistiikka sekä liikenteen ohjaus (Sanastokeskus ym., 2018). Sosiaali- ja terveydenhuolto on riippuvainen kuljetusten jatkuvuudesta, energia- ja vesihuollosta sekä tieto- ja viestintäverkkojen toimivuudesta. Nämä osa-alueet tunnistetaan uhkamalleiksi myös vuoden 2023 Kansallisessa riskinarviossa. (Sisäministeriö, 2023.)

Kyberuhkia on erilaisia ja ne on nimetty uhan tarkoitusperän mukaan. Yleisimmät kyberuhkatyypit ovat palvelunestohyökkäys, kiristyshaittaohjelma, tietojenkalastelu ja tietomurto.

Palvelunestohyökkäys (eng. Denial-of-service attack, DoS attack). Palvelunestohyökkäyksen tarkoitus on saada lamaannutettua tietojärjestelmä tai jokin palvelu. Palvelunestohyökkäyksessä palvelua kuormitetaan niin paljon, että sen toiminta huononee tai pysähtyy. (Sanastokeskus ym., 2018.)

Kiristyshaittaohjelma (eng. Ransomware). Kiristyshaittaohjelman määritellään ”haittaohjelmaksi, joka salaa tai manipuloi laitteella olevia tietoja ja tyypillisesti vaatii käyttäjältä lunnaita salauksen purkamisesta” (Kyberturvallisuuskeskus, 2020; Sanastokeskus ym., 2018). Kiristyshaittaohjelman voi saada sosiaali- terveydenhuollossa työpaikan tietokoneelle esimerkiksi työsähköpostin liitetiedostona. Työntekijän avattua liitetiedoston, kiristyshaittaohjelma latautuu tietokoneelle. Ohjelma voi kalastaa tietoja tai salata tiedostoja niin, ettei tiedostoja pystytä enää avaamaan ilman oikeaa salauksenpurkuavainta. Kyberrikollinen voi luvata toimittaa avaimen lunnaita vastaan tai esimerkiksi uhata levittää tai paljastaa luottamuksellista tietoa. (Sanastokeskus ym., 2018.)

Tietojenkalastelu (eng. Phishing). Tietojenkalastelussa kyberrikollinen yrittää saada haltuunsa käyttäjätunnuksia, salasanoja, maksukorttitietoja tai muita arvokkaita tietoja. Tietojenkalastelu voi kohdistua yksilöihin tai esimerkiksi yrityksiin. (Kyberturvallisuuskeskus, 2020.)

Tietomurto (eng. Data break). Tietojenkalastelun onnistuttua rikolliset voivat tehdä tietomurron. Tietomurto tarkoittaa luvatonta tunkeutumista tietojärjestelmään, palveluun, laitteeseen tai sovellukseen. Jos tietojenkalastelulla on saatu selvitettyä käyttäjän sähköpostiosoite ja sähköpostin salasana, tietomurron tekijä voi ottaa luvattomasti sähköpostitilin haltuunsa. (Kyberturvallisuuskeskus, 2020.)

2.3 Sosiaali- ja terveyspalvelujen varautuminen kyberuhkiin

Sosiaali- ja terveysministeriö on määritellyt sosiaalipalvelut ja terveyspalvelut erillisinä termeinä. Sosiaalipalvelut on määritelty palveluiksi, joiden tavoitteena on sosiaalisen turvallisuuden ja hyvinvoinnin edistäminen sekä yleis- ja erityislainsäädännön mukaiset sosiaalihuollon tehtävät ja palvelut. Sosiaalihuoltolain alle kuuluu useita sosiaalipalveluita, joita ovat esimerkiksi sosiaalityö ja sosiaaliohjaus, päihdetyö ja kotihoito. Terveyspalvelut ovat palveluita, joiden tavoitteena on edistää ja pitää huolta väestön terveydestä, hyvinvoinnista, työ- ja toimintakyvystä ja sosiaalisesta turvallisuudesta sekä kaventaa terveyseroja. (STM, 2024.) Sosiaali- ja terveyspalveluista käytetään yleisimmin termiä sosiaali- ja terveydenhuolto. Sosiaali- ja terveydenhuoltoa ohjaa Suomessa esimerkiksi laki sosiaali- ja terveydenhuollon järjestämisestä (612/2021), laki hyvinvointialueesta (611/2021), sosiaalihuoltolaki (1301/2014) ja terveydenhuoltolaki (1326/2010) (STM, 2023).

Sosiaali- ja terveydenhuollon tehtävänä on turvata kaikille terveyden ja toimintakyvyn kannalta keskeiset sosiaali- ja terveydenhuollon palvelut olosuhteista riippumatta (STM, n.d.). Sosiaali- ja terveydenhuollossa on varauduttava poikkeusoloihin ja häiriötilainteisiin. Varautuminen tarkoittaa toimintaa, jolla varmistetaan keskeisen tehtävän mahdollisimman häiriötön hoitaminen kaikissa turvallisuustilanteissa. Varautumisessa on otettava huomioon oman organisaation sekä erityistehtävien hoitaminen. Varautumisen yksi keskeinen keino on valmiussuunnittelu. Valmiussuunnitelma on etukäteen kehitetty suunnitelma niistä tavoista, joilla poikkeustilanteeseen on varauduttu. Sen tavoitteena on valmius vastata kaikkiin mahdollisiin tiedossa oleviin uhkiin. (STM, 2008.)

3 Tutkielman tarkoitus ja tutkimuskysymykset

Tutkielman tarkoituksena on kansainväliseen kirjallisuuteen pohjaten kuvata sosiaali- ja terveydenhuollossa kohdattuja kyberhyökkäyksiä, niiden vaikutuksia ja varautumista. Tutkielmassa tuotetun tiedon avulla voidaan kehittää kyberuhkiin varautumisen menetelmiä.

Tutkimuskysymykset:

1. Millaisia kyberhyökkäyksiä sosiaali- ja terveydenhuoltoa kohtaan on tehty kansainvälisesti?
2. Mikä vaikutus kyberhyökkäyksellä on ollut sosiaali- ja terveydenhuoltoon?
3. Miten kyberuhkiin oli varauduttu sosiaali- ja terveydenhuollossa ennen kyberhyökkäystä?

4 Menetelmät

Tutkimusmenetelmäksi valittiin kuvaileva kirjallisuuskatsaus, johon valittuja tutkimuksia analysoidaan induktiivisella sisällönanalyysilla. Kuvaileva kirjallisuuskatsaus valittiin menetelmäksi, koska tavoitteena on etsiä vastauksia siihen, mitä tietoa toteutuneet kyberhyökkäykset ovat tuottaneet. Kuvailevan kirjallisuuskatsauksen tarkoituksena onkin löytää vastauksia seuraaviin kysymyksiin; mitä ilmiöstä tiedetään ja mitkä ovat ilmiön keskeiset käsitteet. (Burns & Grove, 2005.)

4.1 Hakustrategia

Systemaattinen tiedonhaku aloitettiin etsimällä sopivia synonyymeja ja sanoja kyberuhkalle ja sosiaali- ja terveydenhuollolle. Hakulausekkeen muodostamisessa oli tärkeää, että haku tuottaisi nimenomaan sosiaali- ja terveydenhuollon palvelimiin kohdistuvia kyberuhkia. Tarkoitus oli saada rajattua pois vain kyberturvallisuutta käsittelevät artikkelit ja sellaiset hakutulokset, joissa kyberuhkaa tarkasteltiin tietoteknisestä näkökulmasta.

Tärkeimmiksi hakusanoiksi muodostuivat ”cyber attack” ja ”health care”, sekä näiden synonyymit. Hakulausekkeeksi muodostui seuraava:

("cyber attack*" OR "cyber assault*"[tw] OR "cyber intrusion*" OR "cyber breach*" OR "cyber offence*" OR "digital attack*" OR "cybersecurity incident*" OR "information security breach*" OR "security breach*" OR "data breach*" OR malware* OR ransomware* OR phishing* OR "cybersecurity breach*") AND ("Delivery of Health Care"[Mesh] AND healthcare* OR "health care*" OR "medical care*" OR "health service*" OR "wellness service*" OR "health system*" OR "medical service*" OR "healthcare service*" OR "health maintenance*" OR "health provision*")

Tätä lauseketta käytettiin kuhunkin tietokantaan sopivaksi muunneltuna neljässä eri tietokannassa, jotka olivat PubMed, CINAHL, Cochrane ja Scopus. Haku rajattiin suomenkielisiin ja englanninkielisiin artikkeleihin ja tutkimuksiin. Scopus-tietokannassa käytettiin rajauksena lisäksi avainsanaa ”health care”, koska muuten haku tuotti huomattavasti terveydenhuoltoon liittymättömiä tuloksia. Hakulausekkeet ja rajaukset on esitetty liitteessä 1. Haku rajattiin vuosille 2007–2024, koska kansainvälinen televiestintäliitto (International

Telecommunication Union [ITU]) julkaisi vuonna 2007 kansainvälisen kyberturvallisuussuosituksen (Global Cybersecurity Agendan, GCA). GCA luotiin kehykseksi kansainväliselle yhteistyölle, jonka tavoitteena lisätä luottamusta ja turvallisuutta informaatioyhteiskunnassa (ITU, 2007). ”The history of cybercrime (1976–2016)” teoksessa mainitaan tämän olleen ensimmäinen kansainvälinen aloite, joka otti huomioon kyberturvallisuuden globaalista näkökulmasta (Schjølberg, 2017). GCA mainitaan muualla kirjallisuudessa kyberturvallisuuden kehityksen tärkeänä asiakirjana yhdessä ITU:n WSIS (World Summit on the Information Society) -velvoitteiden kanssa (Radoniewicz, 2021; Choucri, 2013). Suomen Kyberturvallisuusstrategiassa vuodelta 2013 on myös maininta GCA:sta (Puolustusministeriö, 2013). Ponemon-instituutin (2016) tuottaman raportin mukaan sosiaali- ja terveysalaa kohtaan tehdyt kyberhyökkäykset ovat selkeästi lisääntyneet 2010-luvun aikana, joten GCA:n jälkeinen aikarajaus osuu hyvin myös tähän ajanjaksoon.

4.2 Mukaanotto- ja poissulkukriteerit

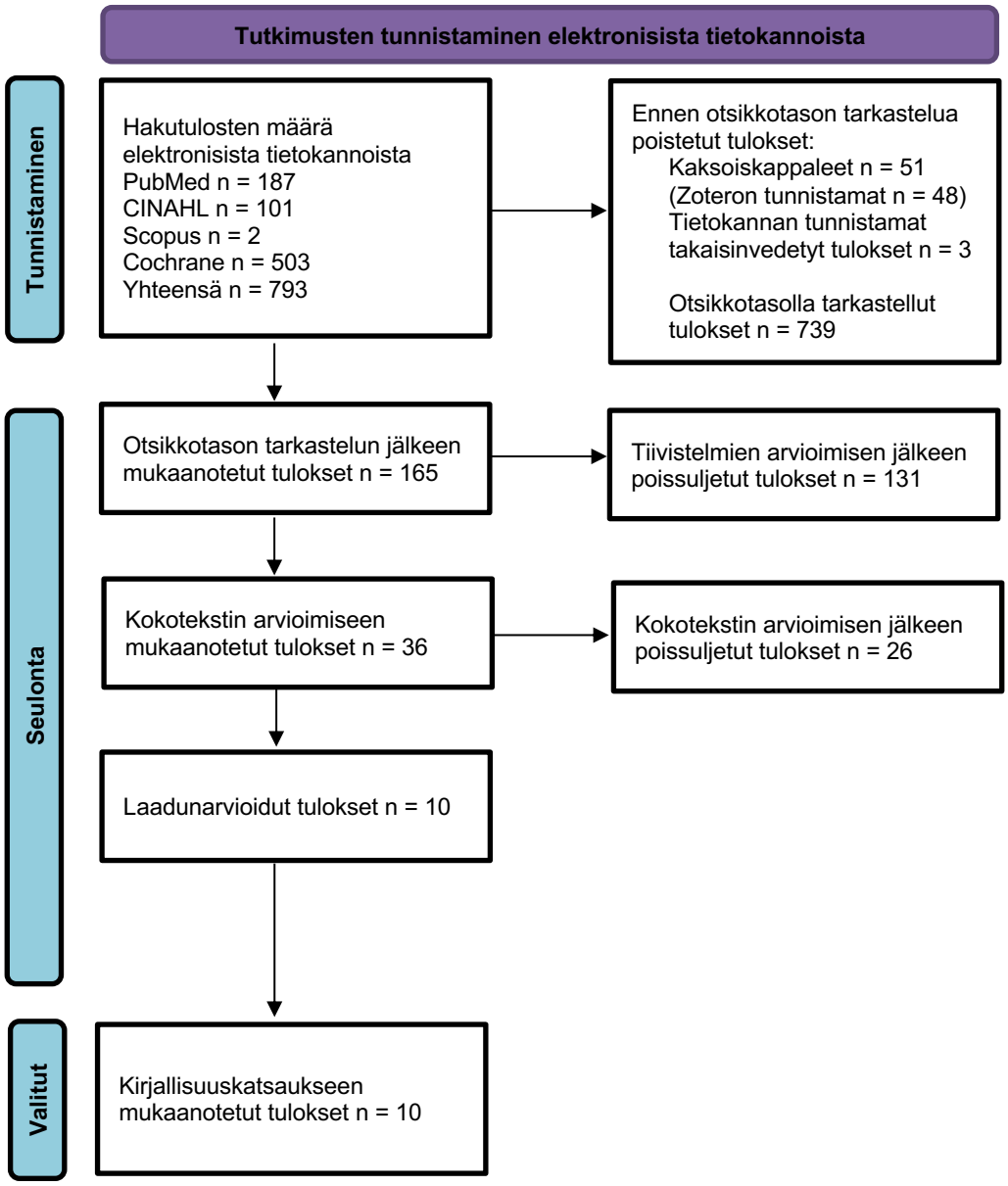
Mukaanotto- ja poissulkukriteerejä muodostui kumpaankin neljä kappaletta. Kriteerit nimettiin A- ja B- tunnuksilla, jotta ne on helpompi myöhemmin tunnistaa. Kriteerit on esitetty taulukossa 1.

Taulukko 1. Mukaanotto- ja poissulkukriteerit

Mukaanottokriteerit	Poissulkukriteerit
A1 = Artikkeli käsittelee kyberuhkaa tai kyberuhkia A2 = Kyberuhat tai -uhka kohdistuu sosiaali- ja terveydenhuoltoon A3 = Artikkeli on empiirinen tutkimus A4 = Artikkeli tuottaa tietoa kyberuhista, niiden vaikutuksista tai niihin varautumisesta	B1 = Artikkeli käsittelee vain kyberturvallisuutta terveydenhuollossa B2 = Artikkelissa käsitellään kyberuhkan havaitsemiseen kehitettyjä algoritmeja tai menetelmiä B3 = Artikkelissa tutkittiin vain kyberuhkien syitä B4 = Artikkeli ei ole saavutettavissa Turun yliopiston tietokannoista

4.3 Kirjallisuuden hakuprosessi

Koko kirjallisuuden haku- ja valintaprosessin aikana seurattiin systemaattisesti mukaanotto- ja poissulkukriteereitä. Otsikkotasolla pidettiin kriteerinä, että otsikossa on mainittava ”cyber attack” tai ”health care” käsitteet tai niiden synonyymit. Myös nimettyjen kyberhyökkäysten nimet laskettiin ”cyber attack” käsitteen alle. Otsikkotasolla pystyttiin poissulkemaan paljon tuloksia, iso osa käsitteli kyberturvallisuutta tai tietoturvaa (B1). Scopus-tietokannan tuloksista monet käsittelivät kyberhyökkäyksen havaitsemiseen kehitettyä algoritmia tai menetelmää (B2). Tiivistelmien tarkastelussa suurimmat syyt artikkelin hylkäämiseen olivat artikkeli ei ollut empiirinen tutkimus (A3=29 kpl), artikkelin saatavuusongelma (B4=28 kpl), artikkeli käsitteli vain tietoturvaa tai kyberturvallisuutta (B1=17 kpl) tai artikkeli esitteli kyberhyökkäyksen estämiseen tai havaitsemiseen tarkoitettua algoritmia tai menetelmää (B2=14 kpl). Loput artikkelit poissuljettiin jäljelle jääneiden mukaanotto- ja poissulkukriteerien mukaisesti (42 kpl). Kokotekstin tarkastelussa poissuljettiin 26 artikkelia ja laadunarvioitiin valittiin mukaan 10 artikkelia. Artikkelien valintaprosessi on esitetty kuviossa 1.



Kuvio 1. Artikkelien valinnan eteneminen (mukaillen Page ym., 2021).

4.4 Tutkimusten laadunarviointi

Kokotekstien lukemisen jälkeen tutkimusten menetelmällinen laatu arvioitiin. Tutkimukset ja laadunarvioinnin tulokset on esitetty taulukossa 2. Tarkempi kuvaus valituista tutkimuksista on esitetty liitteissä 2.

Taulukko 2. Tutkimukset ja niiden laadunarviointi.

Nro.	Tutkimus	Tutkimuksen tekijät	Laadunarvioinnin pisteytys
1.	A resilient workforce: patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland	Moore ym. 2023	7/7 (100 %)[a]
2.	A retrospective impact analysis of the WannaCry cyberattack on the NHS	Ghafur ym. 2019	7/7 (100 %)[b]
3.	Case Study on a Session Hijacking Attack: The 2021 CVS Health Data Breach	Prentosito ym. 2022	4/7 (57 %)[c]
4.	Dealing with digital paralysis: Surviving a cyberattack in a National Cancer center	Keogh ym. 2023	7/7 (100 %)[a]
5.	Digital Healthcare - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilites, Risks, NIST Perspectives, and Recommendations	Kandasamy ym. 2022	6/7 (86 %)[a]
6.	Hacking Acute Care: A Qualitative Study on the Health Care Impacts of Ransomware Attacks Against Hospitals	Van Boven ym. (2023)	7/7 (100 %)[c]
7.	Ramsomeware Attack Associated with Disruptions at Adjacent Emergency Departments in the US	Dameff ym. (2023)	7/7 (100 %)[d]
8.	The crippling effects of a cyberattack at an academic level 1 trauma center: An orthopedic perspective	Tarka ym. (2023)	7/7 (100 %)[d]
9.	The Impact of a National Cyberattack Affecting Clinical Trials: The Cancer Trials Ireland Experience	Harvey ym. (2023)	7/7 (100 %)[c]
10.	A National Survey of Hospital Cyber Attack Emergency operation preparedness	Sullivan ym. (2023)	7/7 (100 %)[e]

[a] Monimenetelmätutkimus
[b] Retrospektiivinen vaikutusanalyysi
[c] Laadullinen tutkimus
[d] Kohorttitutkimus
[e] Kvantitatiivinen kyselytutkimus

Laadunarviointiin käytettiin vuoden 2018 MMAT-työkalua (Mixed Methods Appraisal Tool) (Hong ym., 2018). Kaikkien artikkelien laatu arvioidaan 0–7 pisteen välille, joista kaksi ensimmäistä pistettä ovat kaikille tutkimuksille samat. Sen jälkeen kukin tutkimus arvioidaan tarkemmin asetelmansa perusteella. Tässä tutkielmassa tarkastettiin myös, että kaikki artikkelit olivat vertaisarvioituja.

Suurimmassa osassa tutkimuksia menetelmällinen laatu oli MMAT-työkalulla arvioituna hyvä. Silti tutkimuksissa huomattiin tutkimusmetodiikan raportoinnin eroja. Taulukko 2 mukaan tutkimus numero 3 sai laadunarvioinnissa heikomman tuloksen (4/7). Tutkimuksessa ei esitelty tiedonhaun toteutusta, havaintojen johtaminen aineistosta oli puutteellista ja tulosten tulkintaa olisi voinut enemmän perustella aineistolla. Tutkimus numero 6 sai

laadunarvioinnissa kuusi pistettä (6/7), koska tutkimuksessa ei mainittu monimenetelmätutkimuksen hyödyntämisen perusteluja.

4.5 Aineiston analyysi

Sisällönanalyysi on tutkimusmenetelmä, jonka päämääränä on luoda toistettavissa olevia päätelmiä tiedosta niiden kontekstissa. Sisällönanalyysi tarjoaa keskitettyä tietoa, uusia näkökulmia, tiedon määrittelyä ja sen avulla voi luoda toimintaohjeita. Analyysin tuloksena voi syntyä käsitteitä ja luokkia, minkä avulla on tarkoituksena saavuttaa tiivistetty, mutta laaja kuvaus ilmiöstä. (Elo & Kyngäs, 2008.) Koska kyberuhkista sosiaali- ja terveydenhuollossa on olemassa vain vähän tutkittua tietoa, lähestymistavaksi valittiin induktiivinen sisällönanalyysi.

Artikkelit luettiin useaan kertaan ja analyysin perusteella aineistosta tunnistettiin samankaltaisuuksia. Samankaltaisuuksista tunnistettiin alaluokkia. Alaluokat järjesteltiin yksiköittäin. Pääluokiksi tunnistettiin kyberhyökkäykset, kyberhyökkäyksien vaikutukset ja kyberhyökkäyksiin varautuminen. Näistä muodostettiin tulosten jaottelu. Induktiivisen sisällönanalyysin prosessista on esitetty esimerkki taulukossa 3. Sisällönanalyysissa muodostettiin kolme pääluokkaa, jotka vastaavat myös tutkimuskysymyksiä. Tulokset käsiteltiin kolmen pääluokan alla.

Taulukko 3. Induktiivisen sisällönanalyysin luokat

Pääluokat		
Kyberhyökkäykset	Kyberhyökkäysten vaikutukset	Kyberhyökkäyksiin varautuminen
Alaluokat		
Kohdejärjestelmä	Vaikutuksen kesto	Varautuminen yksilötasolla
Kohdevaltio	Vaikutukset yksilötasolla	Varautuminen organisaatiossa
Kyberhyökkäyksen luokka	Hoidon toteuttamisen vaikutukset	Varautumiseen tehdyt muutokset
Kyberhyökkäyksen tunniste	Taloudelliset vaikutukset	Varautumisehdotukset

5 Tulokset

5.1 Mukaan valittujen tutkimusten kuvaus

Mukaan valittujen artikkelien lukumäärä oli 10 ja kaikki valitut artikkelit olivat empiirisiä tutkimuksia. Tutkimukset sijoittuivat vuosien 2019–2023 välille. Tutkimukset olivat toteutettu Irlannissa (n=2), Yhdysvalloissa (n=4), Englannissa (n=2), Intiassa (n=1) ja Alankomaissa (n=1). Valituista tutkimuksista kolme oli kvalitatiivisia tutkimuksia, kolme monimenetelmätutkimuksia ja neljä kvantitatiivisia tutkimuksia. Kvantitatiiviset tutkimukset olivat kohorttitutkimuksia (n=2), vaikutusanalyyseja (n=1) tai kyselytutkimuksia (n=1). Tutkimuksien tarkempi kuvaus on esitetty liitteessä 2.

Kaikki tutkimukset keskittyivät terveydenhuollon kyberhyökkäyksiin, mutta tarjosivat niistä erilaisia näkökulmia. Conti-kyberhyökkäystä käsitteli kolme tutkimusta: Harveyn ja hänen kollegoidensa (2023) tutkimus käsitteli kyberhyökkäyksen vaikutusta syöpäsairauksien kliiniseen tutkimustoimintaan ja Keoghin ym. (2023) tutkimus arvioi kyberhyökkäyksen vaikutuksia ja seurauksia syöpäkeskukselle. Mooren ja kumppaneiden (2023) tutkimus taas arvioi henkilökunnan reagointia kyberhyökkäyksen alla.

WannaCry-kyberhyökkäys mainittiin kahdessa tutkimuksessa, joista toinen käsitteli suoraan kyseisen kyberhyökkäyksen vaikutuksia Englannissa (Ghafur ym., 2023) ja toinen käsitteli Aasiaan kohdistuneita kyberhyökkäyksiä, kuten WannaCry ja SingHealthin tietomurto (Kandasamy ym., 2022). Kaksi tutkimusta esittelivät yksittäiset kyberhyökkäykset, kuten CVS Health -verkkosivuston tietovuodon (Prentosito ym., 2022) ja yliopistollisen traumasairaalan kiristyshaittaohjelman vaikutukset (Tarka ym., 2023). Vaikka osa tutkimuksista käsitteli samaa kyberhyökkäystä, niissä käsiteltiin eri yksiköitä ja niihin kohdistuneita erilaisia vaikutuksia.

Kolme tutkimusta ei käsitellyt yksittäisiä kyberhyökkäyksiä. Ne tutkivat kiristyshaittaohjelmien vaikutuksia sairaaloihin Euroopassa ja Yhdysvalloissa (Van Boven ym., 2023), kyberhyökkäykseltä säästyneiden lähisairaalojen kohtaamia sekundaarisia vaikutuksia (Dameff ym., 2023) sekä Yhdysvalloissa sijaitsevien sairaaloiden valmiutta kyberhyökkäyksiä vastaan (Sullivan ym., 2023). Näistä kahdessa tutkimuksessa terveydenhuollossa toteutuneet kyberhyökkäykset ja kohdesairaalat olivat anonymisoitu (Dameff ym., 2023; Van Boven ym., 2023) ja yhdessä tutkimuksessa käsiteltiin kyberuhkiin

varautumista varautumisesta vastaaville henkilöille toteutetulla kyselyllä, minkä vuoksi niissä ei ollut tietoa itse kyberhyökkäyksestä. Näissä tutkimuksissa keskityttiin varautumiseen ja kyberhyökkäysten vaikutuksiin.

5.2 Kyberhyökkäykset sosiaali- ja terveydenhuollossa

Kirjallisuudessa mainittiin useita kyberhyökkäyksiä, joista viittä eri kyberhyökkäystä kuvailtiin laajimmin. Suurimmat vaikutukset olivat Conti- ja WannaCry-kyberhyökkäyksillä, joiden vaikutus näkyi Irlannin ja Englannin terveydenhuolloissa (Moore ym., 2023; Keogh ym., 2023; Harvey ym., 2023). Taulukossa neljä on esitelty laajimmin kuvailtujen kyberhyökkäysten ajankohta, kohdevaltio ja -järjestelmä, kyberhyökkäyksen alaluokka ja lähdetutkimus.

Taulukko 4. Kirjallisuuskatsauksessa tunnistetut sosiaali- ja terveydenhuoltoon kohdistuneet kyberhyökkäykset

Kohdevaltio ja vuosi	Hyökkäyksen tunniste	Kohdejärjestelmä	Kyberhyökkäyksen alaluokka	Lähdetutkimus
Irlanti, 2021	Conti- cyber attack	Irlannin terveyspalvelujen toimeenpaneva elin (Health Service Executive, HSE)	Kiristyshaittaohjelma	Moore ym., 2023; Keogh ym., 2023; Harvey ym., 2023
Englanti (& Indonesia), 2017	WannaCry	Englannin kansallinen terveyspalvelu (NHS)	Kiristyshaittaohjelma	Ghafur ym., 2019; Kandasamy ym., 2022
Yhdysvallat, 2021	The 2021 CVS Health Data Breach	CVS Health -verkkosivusto	Tietomurto	Prentosito ym., 2022
Singaporen tasavalta, 2018	The 2018 SingHealth data breach	SingHealth - Singapore Health Service	Tietomurto	Kandasamy ym., 2022
Yhdysvallat, 2020	ACS level 1 traumacenter ransomware	EMR-järjestelmä (electric medical records)	Kiristyshaittaohjelma	Tarka ym., 2023

Kyberhyökkäykset kohdistuivat Irlantiin, Englantiin, Indonesiaan, Yhdysvaltoihin ja Singaporen tasavaltaan. Yhdysvaltoihin tehtyjä kyberhyökkäyksiä oli kaksi ja ne olivat kohdistettu suoraan järjestelmiin, joihin ne vaikuttivat (Tarka ym., 2023; Prentosito ym.,

2022). Samoin Singaporen tasavallan terveydenhuoltoon tehty tietomurto oli vain kyseiseen järjestelmään kohdistettu (Kandasamy ym., 2022).

Englannissa ja Indonesiassa vaikuttanut kyberhyökkäys ei kohdistunut suoraan terveydenhuollon järjestelmään, vaikka niissä koettiin laajoja vaikutuksia. Tämä WannaCry-hyökkäykseksi nimetty kyberhyökkäys vaikutti maailmanlaajuisesti myös muissa terveydenhuollon järjestelmissä, mutta muut haavoittuneet järjestelmät ja maat eivät tulleet esiin tutkimuksissa. (Ghafur ym., 2019; Kandasamy ym., 2022.) Conti-kyberhyökkäys oli huomattavan laaja ja kohdennettu kiristyshaittaohjelma, joka vaikutti koko Irlannin julkisen terveydenhuollon (HSE) tieto- ja viestintätekniikkapalveluihin. Conti oli ensimmäinen kyberhyökkäys, joka oli kohdistettu suoraan kansalliseen ja julkiseen terveysjärjestelmään. (Keogh ym., 2023; Moore ym., 2023.)

Kyberhyökkäykset tapahtuivat vuosien 2017–2021 aikana. Viidestä taulukossa 4 käsitellystä kyberhyökkäyksestä kolme (60 %) olivat kiristyshaittaohjelmia ja kaksi tietomurtoja. Yhdysvalloissa toimivan CVS Healthin kyberturvallisuuspoikkeamaa käsiteltiin tutkimuksessa tietomurtona, vaikka sopivampi termi tapahtumalle olisi tietovuoto. CVS Healthin huolimattoman tietoturvallisen käsittelyn vuoksi potilaiden ajanvaraus, rokoteostos- ja reseptitietoja sisältänyt tietokanta julkaistiin internetissä suojaamattomana. Tietokanta ehti olla kenen tahansa saatavilla kaksi päivää. CVS Healthin tietomurto eroaa muista kyberuhkista, koska tutkimuksissa ei löydetty suoraa todistetta siitä, olivatko kyberrikolliset löytäneet vaarantuneet tiedot ja hyödyntäneet niitä. (Prentosito ym., 2022.)

Kahdessa tutkimuksessa mainittiin laajasti vaikuttaneita kyberhyökkäyksiä, mutta tutkimuksien tiedot kyberhyökkäyksestä ja vaikutusjärjestelmästä olivat salattu. Tämän vuoksi niiden tietoja ei voitu esittää taulukossa neljä. Kyberhyökkäykset, joita ei voitu sisällyttää taulukkoon olivat viisi kiristyshaittaohjelmaa. (Van Boven ym., 2023; Dameff ym., 2023.) Näistä viidestä kyberhyökkäyksestä neljän vaikutuksia ei voitu yhdistää ollenkaan tiettyyn kyberhyökkäykseen (Van Boven ym., 2023). Yhden kyberhyökkäyksen raportoitiin tapahtuneen vuonna 2021 ja sen kohdistuneen terveysjärjestelmään, johon kuului neljä akuuttia sairaalaa ja 19 avohoitoyksikköä (Dameff ym., 2023).

5.3 Kyberhyökkäysten vaikutukset sosiaali- ja terveydenhuollossa

Kyberhyökkäyksillä oli monitahoisia vaikutuksia sosiaali- ja terveydenhuoltoon. Laajemmin käsiteltyjen kyberhyökkäysten vaikutuksia on esitetty taulukossa 5.

Taulukko 5. Kyberhyökkäysten vaikutukset sosiaali- ja terveydenhuoltoon

Kyberhyökkäyksen tunniste	Vaikutukset	Vaikutuksen kesto	Lähde
Conti- cyber attack	Potilastiedot, talousjärjestelmät, palkanmaksu ja hankintajärjestelmät, sähköposti ja verkottuneet puhelinlinjat menetettiin. Kliiniset hoito- ja laboratoriojärjestelmät menetettiin tai niissä koettiin häiriöitä. Hoito- ja lääketieteellisiin tutkimuksiin tuli häiriöitä. Sairaalan internet-yhteys suljettiin. Yksityisiä tietoja vuosi 94 800 potilaasta ja 18 200 henkilökunnan jäsenestä.	Yli 4 kuukautta	Moore ym., 2023; Keogh ym., 2023; Harvey ym., 2023
WannaCry	Potilastiedot ja potilaskirjausjärjestelmät menetettiin, radiologiapalveluissa koettiin häiriöitä, poliklinikkakäyntejä peruutettiin, suunnitellut sairaalahoitojaksot ja päiväkirurgiset toimenpiteet keskeytyivät tai viivästyivät ja viideltä tartunnan saaneelta sairaalalta ambulanssit ohjattiin muihin sairaaloihin.	1 viikko	Ghafur ym., 2019; Kandasamy ym., 2022
The 2021 CVS Health Data Breach	Terveydenhuollon luottamuksen vähentyminen, tietoturvallisuuden vaarantuminen ja mahdollinen päätyminen kyberrikollisten käytettäväksi.	Tiedot ehtivät olla 2 päivää altistuneina väärinkäytölle	Prentosito ym., 2022
The 2018 SingHealth data breach	1,5 miljoonan potilaan terveystiedot varastettiin	-	Kandasamy ym., 2022
ACS level 1 traumacenter ransomware	Leikkaussalien käyttö vähentyi kliinisesti, taloudellisesti ja tilastollisesti merkitsevästi kyberhyökkäyksen aikana. Potilastiedot menetettiin kyberhyökkäyksen ajaksi ja sairaalan internetyhteys jouduttiin sulkemaan.	25 päivää	Tarka ym., 2023

Vaikutukset yksilöön

Kyberhyökkäyksistä kiristyshaittaohjelmat vaikuttivat yksilötasolla laajasti sekä yksittäisiin potilaisiin että hoitohenkilökuntaan. Potilastietojen menettämisestä kärsivät erityisesti syövän ja traumapotilaiden hoitoon keskittyneet yksiköt ja näiden erikoisalojen potilaat (Moore ym., 2023; Keogh ym., 2023; Harvey ym., 2023; Tarka ym., 2023). Näiden yksiköiden hoitopäätökset nojaavat aiempiin kuvantamistutkimuksiin ja potilastietoihin, jotka menetettiin kyberhyökkäyksen seurauksena. Kiireettömiä hoitokäyntejä peruttiin kyberhyökkäyksen vuoksi useassa sairaalassa (Van Boven ym., 2023; Ghafur ym., 2019; Moore ym., 2023; Keogh ym., 2023; Harvey ym., 2023). Perutuista hoitokäynneistä korostuivat syöpäpotilaiden hoitokäynnit, joita oli peruttu 139 potilaalta (Ghafur ym., 2019) ja 513 potilaan syöpähoito koki eri asteisia häiriöitä (Harvey ym., 2023). Yhdessä tutkimuksessa raportoitiin, että aivohalvauspotilaita oli jouduttu ohjaamaan lähialueen sairaaloihin kyberhyökkäyksen vuoksi. Aivohalvauspotilaiden hoito on erittäin aikakriittistä ja viivästyksillä voi olla negatiivisia vaikutuksia aivohalvauksesta selviämiseen. (Dameff ym., 2023.)

Vaikka tietomurroilla ei raportoitu yksilölle näkyviä vaikutuksia, tutkimuksessa tuotiin esiin luottamuksen kärsiminen terveydenhuollon palveluntuottajaan (Prentosito ym., 2022). Vaikka yksittäinen henkilö olisikin huolehtinut tietoturvallisuudesta, siitä ei ole hyötyä, jos terveydenhuollon organisaatio vuotaa tiedot kolmansille osapuolille. Potilastiedoilla raportoitiin olevan korkeampi arvo rikollisten silmissä kuin luottokorttitiedoilla (Kandasamy ym., 2022). Tietomurroilla voidaan tavoitella myös yksittäisen vaikutusvaltaisen henkilön potilastietoja. Esimerkiksi SingHealthin tietomurrossa varastettiin myös maan pääministerin potilastiedot (Ghafur ym., 2019).

Henkilökunnan koettiin kuormittuneen henkisesti kyberhyökkäysten seurauksena (Van Boven ym., 2023; Moore ym., 2023; Keogh ym., 2023; Harvey ym., 2023). COVID-19-pandemian jäljiltä henkilöstö oli jo valmiiksi kuormittunut, minkä vuoksi kyberhyökkäyksen luomat poikkeusolot loivat tilanteesta entistä haastavamman (Van Boven ym., 2023; Moore ym., 2023; Harvey ym., 2023). Yhdessä tutkimuksessa henkilöstö koki kyberhyökkäyksen tuomat vaikutukset jopa kuormittavammaksi kuin COVID-19-pandemian (Moore ym., 2023). Toisaalta sairaalan henkilökunnan toiminta koettiin joustavaksi, kekseliääksi ja ripeäksi, ja tällä nähtiin positiivista vaikutusta kyberhyökkäyksestä selviämiseen (Tarka ym., 2023; Van Boven ym., 2023; Moore ym., 2023; Keogh ym., 2023). Positiivisena vaikutuksena nähtiin

sairaalahierarkian tasoittuminen. Henkilökunnan koettiin tekevän tehokkaammin yhteistyötä kyberhyökkäyksen vaikutusten alla. (Tarka ym., 2023; Moore ym., 2023.)

Hoidon toteutuksen vaikutukset

Tietomurroilla ei raportoitu päivittäisen toiminnan vaikutuksia, kun taas kiristyshaittaohjelmien seurauksena sairaaloissa koettiin useita viikkoja tai kuukausia toiminnan häiriöitä. Tässä osassa käsitellään suurelta osin kiristyshaittaohjelmien tuomia vaikutuksia.

Kyberhyökkäyksen seurauksena organisaatiot joutuivat ryhtymään suojatoimenpiteisiin. Kymmenestä tutkimuksesta kuudessa mainittiin internet-yhteyden katkaiseminen joko kyberhyökkäysten seurauksena tai IT (information technology) -henkilöstön toteuttamana ennaltaehkäisevänä toimenpiteenä (Ghafur ym., 2019; Van Boven ym., 2023; Moore ym., 2023; Keogh ym., 2023; Harvey ym., 2023; Tarka ym., 2023). Conti-kyberhyökkäystä käsitelleet tutkimukset käsittelivät eri yksiköitä, mutta internet-yhteyden katkaiseminen oli valtakunnallinen päätös, joka vaikutti kaikkiin kyberhyökkäyksen vaikuttamiin sairaaloihin (Moore ym., 2023; Keogh ym., 2023; Harvey ym., 2023). Taulukossa viisi esitellyistä kyberhyökkäyksistä kolmessa katkaistiin koko sairaalan internet-yhteys. Internet-yhteyden katkaiseminen johti myös niiden ohjelmien menettämiseen, jotka eivät olleet kyberhyökkäyksen kohteena. Tällaisia ohjelmia olivat esimerkiksi kommunikaatiojärjestelmät. Kommunikaatiojärjestelmien, kuten sähköpostin, kaatumisesta selviämiseen vaikutti positiivisesti aiemmin mainittu henkilöstön nopea reagointi. Potilaiden hoitoon liittyviä viestejä välitettiin henkilökunnan henkilökohtaisilla älylaitteilla organisaation luvalla. (Moore ym., 2023; Keogh ym., 2023.)

Laboratoriokokeiden tilausjärjestelmien kaatuminen mainittiin viidessä tutkimuksessa. Järjestelmien kaatuminen oli vaatinut joko lisää henkilöstöä tai toimistohenkilökunnan siirtämistä toisiin tehtäviin, jotta laboratoriopyynnöt ja -tulokset saatiin välitettyä hoitohenkilökunnalle. Laboratoriojärjestelmien kaatumisen koettiin hidastaneen potilashoitoa. (Moore ym., 2023; Van Boven ym., 2023; Harvey ym., 2023; Tarka ym. 2023; Keogh ym., 2023.)

Potilastietojen menetyksellä koettiin olevan huomattavat vaikutukset potilashoitoon ja potilasturvallisuuteen. Yksittäisen potilaan hoidon lisäksi tietojen menetys johti potilaskarttojen menetykseen, minkä vuoksi oli ollut vaikea paikantaa yksittäisen potilaan sijainti osastoilla ja päivystyksissä. Syöpähoitoyksiköissä oli mahdotonta tietää, missä vaiheessa syövän hoito oli ja mikä olisi ollut seuraava syövän hoitoon tarkoitettu lääke- tai sädehoitoannos. Potilastietojen menetys raportoitiin kuudessa tutkimuksessa ja kyberhyökkäysten vaikutuksista tätä käsiteltiin tutkimuksissa eniten. (Ghafur ym., 2019; Kandasamy ym., 2022; Van Boven ym., 2023; Harvey ym., 2023; Tarka ym., 2023; Keogh ym., 2023.)

Taloudelliset vaikutukset

Valituissa tutkimuksissa käsiteltiin taloudellisia vaikutuksia hyvin vähän. Kiristyshaittaohjelmasta johtuvassa kyberhyökkäyksessä taloudelliseen vaikutukseen vaikuttaa se, maksetaanko lunnaita hyökkäävälle taholle. Kolmessa tutkimuksessa mainittiin taloudellisia vaikutuksia, jotka koostuivat menetetyistä poliklinikkakäynneistä, sairaalahoidoista, päivystyskäynneistä ja leikkaussalien käytöstä sekä turvallisuuden parantamisesta, vanhojen laitteiden korvaamisesta ja valvontainfrastruktuurin hankinnasta (Ghafur ym., 2019; Tarka ym., 2023; Keogh ym., 2023).

Kyberhyökkäyksen kustannukset vaihtelivat 6,9 miljoonasta eurosta (tutkimuksessa raportoitu summa 5,9 milj. puntaa) 100 miljoonaan euroon (Ghafur ym., 2019; Keogh ym., 2023). Summat vaikuttivat olevan yhteydessä kyberhyökkäysten vaikutusten kestoon. WannaCry-hyökkäyksen vaikutukset kestivät viikon ja aiheutunut kustannus oli 6,9 miljoonaa euroa (Ghafur ym., 2019), kun taas traumayksikön kyberhyökkäyksen arvioitiin kustantaneen 47 miljoona euroa (50 milj. dollaria) ja kyberhyökkäyksen vaikutusten raportoitiin jatkuneen 25 päivää (Tarka ym., 2023). Conti-kyberhyökkäys oli kaikista laajin ja pitkäkestoisin kyberhyökkäys, mikä näkyi myös suurimpana 100 miljoonan euron kustannuseränä (Keogh ym., 2023; Harvey ym., 2023). Conti-kyberhyökkäyksen kustannusten arvioitiin nousevan edelleen suuremmiksi, mahdollisesti yltäen vielä 500 miljoonan euron kustannuksiin (Harvey ym., 2023).

5.4 Kyberhyökkäyksiin varautuminen sosiaali- ja terveydenhuollossa

Varautuminen yksilötasolla

Kyberturvallisuutta sekä kyberhyökkäyssuunnitelmia tulisi harjoitella (Sullivan ym., 2023; Van Boven ym., 2023; Kandasamy ym., 2022; Keogh ym., 2023; Ghafur ym., 2019). Yhdessäkään tutkimuksessa ei mainittu henkilöstön harjoitelleen kyberhyökkäysten varalle, vaikka sairaaloilla olisikin käyttökatkosuunnitelmia. Yhdessä tutkimuksessa henkilöstön mainittiin kuitenkin harjoitelleen kyberturvallista käyttäytymistä ennen hyökkäystä. Henkilöstön huomioitiin olevan ensimmäinen linkki kyberturvallisuuspoikkeamien huomioimisessa, minkä vuoksi henkilöstöä kannustettiin ilmoittamaan epäilyttävästä toiminnasta, jotta mahdolliseen poikkeamaan voitaisiin reagoida nopeasti. (Van Boven ym., 2023.)

Kahdessa tutkimuksessa huomioitiin, ettei nuorempi sukupolvi hoitohenkilökunnassa ollut koskaan aikaisemmin kirjannut potilaskirjauksia paperille. Vanhemman henkilökunnan kokemus koettiin arvokkaaksi ja he opettivat nuorempia työntekijöitä (Tarka ym., 2023; Van Boven ym., 2023).

Varautuminen organisaatiossa

Kyberhyökkäyssuunnitelmat puuttuivat useasta sosiaali- ja terveydenhuollon organisaatiosta. Suunnitelmien puuttumisen todettiin pahentaneen kyberhyökkäyksen vaikutusta (Harvey ym., 2023; Keogh ym., 2023). Kymmenestä tutkimuksesta seitsemässä mainittiin kyberhyökkäysten varautumissuunnitelmien puuttuminen (Keogh ym., 2023; Harvey ym., 2023; Sullivan ym., 2023; Kandasamy ym., 2022; Prentosito ym., 2022; Ghafur ym., 2019; Moore ym., 2023). Yhdessä tutkimuksessa mainittiin sairaalalla olleen käyttökatkosuunnitelmia kyberhyökkäyksen varalle, mutta tässä ei huomioitu kuin yhden järjestelmän kaatuminen kerrallaan (Van Boven ym., 2023). Harveyn ym. tutkimuksessa (2023) tunnistettiin kaksi organisaatiota, joilla oli valmiussuunnitelma kyberhyökkäyksien varalle ja kahdeksalta puuttui suunnitelma kokonaan. Traumakeskukseen kohdistunut kyberhyökkäys oli ainoa, jossa sairaalalla oli ennen kyberhyökkäystä tehty hätävarmuuskopio kaikista potilastiedoista. Tällä todettiin olleen suuri positiivinen vaikutus kyberhyökkäyksestä toipumiseen. (Tarka ym., 2023.) Yhdessä Conti-kyberhyökkäyksen kohdanneessa sairaalassa

ICT-palveluilla oli viimeisen 7–15 vuorokauden varmuuskopio potilastiedoista, mutta näiden raportoitiin osoittautuneen hyödyttömiksi. Tutkimuksessa ei mainittu, miksi lyhyt varmuuskopio oli hyödytön. (Moore ym., 2023.)

Varmuuskopioiminen ja päätelaitteiden virusturvan päivitys olisivat yhdessä kaksi toimenpidettä, jolla parannettaisiin terveydenhuollon kyberturvallisuutta. Conti-kyberhyökkäyksen todettiin päässeen tartuttamaan päätelaitteita vanhojen Windows-järjestelmien vuoksi. Järjestelmäpäivityksien jäädessä jälkeen myös virusturva oli jäänyt päivittämättä. Organisaatiotasolla ei ollut kiinnitetty huomiota järjestelmien ajantasaisuuteen, mikä on voinut vaikuttaa kyberhyökkäyksen onnistumiseen. (Harvey ym., 2023; Moore ym., 2023.) Tietojärjestelmät ovat terveydenhuollossa keskimäärin vanhoja, minkä vuoksi niiden valmistajat eivät välttämättä enää päivitä niitä tai niiden tietoturvaa (Sullivan ym., 2023). Tietojärjestelmien päivittämättömyys todettiin kuudessa tutkimuksessa osasyynä kyberhyökkäyksen onnistumiseen (Harvey ym., 2023; Moore ym., 2023; Sullivan ym., 2023; Ghafur ym., 2019; Kandasamy ym., 2022; Van Boven ym., 2023).

Kyberhyökkäyksen kohdanneen sairaalan lisäksi poikkeustilanne vaikutti alueen lähisairaaloihin. Viidessä tutkimuksessa mainittiin, että ambulansseja ja potilaita oli jouduttu ohjaamaan lähisairaaloihin hoitoon kyberhyökkäyksen takia (Dameff ym., 2023; Ghafur ym., 2019; Keogh ym., 2023; Van Boven ym., 2023; Tarka ym., 2023). Tutkimuksessa raportoitiin lähisairaaloiden päivystysosaston potilasmäärän nousseen jopa 15 % kyberhyökkäyksen vaikutuksen aikana (Dameff ym., 2023). Organisaatiossa tunnistettiin tarve varautua myös muualla, kuin sairaalassa, johon hyökkäys kohdistui.

Varautumiseen tehdyt muutokset

Kahdessa tutkimuksessa mainittiin, että kyberhyökkäyksen seurauksena sairaalat loivat potilastiedoista ja henkilöstön yhteystiedoista hätävarmuuskopion (Keogh ym., 2023; Moore ym., 2023). Kahdessa muussakin tutkimuksessa tunnistettiin varmuuskopioiden tarve, mutta ei erikseen mainittu, oliko näin toimittu (Van Boven ym., 2023; Ghafur ym., 2019).

Henkilöstön lisäkoulutus kyberturvallisuusasioissa nähtiin useassa tutkimuksessa tärkeänä, mutta silti harvassa mainittiin kyberhyökkäyksen lisänneen koulutusta. Kolmessa tutkimuksessa mainittiin kyberhyökkäyksen jälkeen aloitetut henkilöstön koulutukset, jotka

tähtäävät tietojenkalastelun tunnistamiseen (Tarka ym., 2023; Van Boven ym., 2023; Kandasamy ym., 2022).

Kyberhyökkäysten jälkeen tutkimuksissa mainittiin sairaalojen luoneen kokemuksen pohjalta varautumisen muistilistoja ja ehdotuksia valmiussuunnitelmiin. Tutkimuksien pohjalta koottiin yhteen ehdotuksia varautumiseen ja ne on esitetty taulukossa 6a ja 6b.

Taulukko 6a. Ehdotukset sosiaali- ja terveydenhuollon valmiussuunnitelman luomiseksi

Ongelma	Varautuminen
Kommunikaatiojärjestelmien kaatuminen	Luodaan vakiotoimintamenettelyt, joilla annetaan ohjeita henkilökunnalle mahdollisen kyberhyökkäyksen aikana (Keogh ym., 2023)
	Vaihtoehtoiset turvalliset viestintä- ja sähköpostijärjestelmät tulisi tunnistaa etukäteen (Keogh ym., 2023; Tarka ym., 2023). Hyväksi koettuja järjestelmiä ovat olleet radiopuhelimet, tekstiviestit, henkilökohtaisten älypuhelimien viestisovellukset, faksilaitteet ja massaviestintäjärjestelmät (Van Boven ym., 2023).
	Tiimien johtajien tulisi perustaa turvalliset ryhmäviestintäjärjestelmät monitieteisille tiimeille (Keogh ym., 2023)
	Kaikille sairaalan palveluille tulisi olla hätäpuhelinjärjestelmä ja puhelinluettelo (Keogh ym., 2023)
	Koko henkilökunnan henkilökohtaisiin matkapuhelinnumeroihin tulisi olla pääsy (Keogh ym., 2023)
Potilastietojärjestelmän kaatuminen	Terveydenhuollon toimijalla tulisi olla valmiina paperikirjauslomakkeita (Van Boven ym., 2023)
	Paperilomakkeelle kirjaamista tulisi harjoitella etukäteen (Van Boven ym., 2023)
	Valmis taulukkotiedosto tulisi luoda potilaistiedoille turvalliseen ja vaikuttumattomaan tietokantaan (esim. Excel) (Tarka ym., 2023)
Potilastietojen menetys (myös kuvantamistutkimukset, sydänfilmit ja laboratorioarvot)	Yhteistyön kehittäminen toisiin terveydenhuollon toimijoihin, joiden potilastietojärjestelmät saattavat edelleen toimia (Keogh ym., 2023)
	Luodaan hätävarmuuskopio potilastiedoista ja henkilöstön yhteystiedoista (Keogh ym., 2023)
	Säännöllinen varmuuskopioiminen lisää varmuutta (Boven ym., 2023)
	Yhteistyön edistäminen apteekkien kanssa, joista on mahdollista saada tietoa esimerkiksi potilaan ajankohtaisista lääkityksistä (Tarka ym., 2023)

Taulukko 6b. Ehdotukset sosiaali- ja terveydenhuollon valmiussuunnitelman luomiseksi

Ongelma	Varautuminen
Julkinen viestintä	Standardoitu ja läpinäkyvä viestintä tulisi valmistella ja olla saatavilla kaikille (Keogh ym., 2023)
	Henkilöstöä tulisi tiedottaa asiasta ennen julkista viestintää (Van Boven ym., 2023)
Henkilökunnan jaksaminen	Etukäteen tulisi tehdä hyvinvointisuunnitelma, jolla voidaan hallita työntekijöille aiheutunutta kriisinaikaista stressiä (Keogh ym., 2023; Tarka ym. 2023).
	Sairaalan henkilökunnan tehtävien uudelleen sijoittamisen suunnittelu tulisi tehdä etukäteen ja tätä tulisi harjoitella (Van Boven ym., 2023)
Johtaminen	Johtoporras, hätätiimit ja vastuut tulisi olla jaettu etukäteen ja sisällytetty valmiussuunnitelmaan
	Keskeisillä paikoilla tulisi olla saatavilla valkotaulu, johon voi tarvittaessa piirtää tai kirjata vuodekartan potilaspaikoista (Tarka ym., 2023; Van Boven ym., 2023)
Potilaiden hoitoonohjaus	Potilaiden koordinoitu ohjaaminen muihin sairaaloihin akuutin vaiheen aikana on mahdollista, mutta tämän täytyy olla etukäteen suunniteltua ja tukea antavien sairaaloiden kanssa koordinoitua. Lähisairaaloissa voi olla vielä toimivat järjestelmät, mutta ne kuormittuvat normaalia isommasta potilasvolyymista (Dameff ym., 2023)
Henkilökunnan koulutus	Henkilökunnalle tulisi olla tarjolla tietoturvakoulutuksia (Van Boven ym., 2023)
	Henkilökunnan pitäisi vaihtaa salasanat säännöllisin väliajoin (Prentosito ym., 2022)
	Henkilökuntaa tulisi kannustaa ilmoittamaan epäilyttävästä toiminnasta (Van Boven ym., 2023)
	Kyberhyökkäyssuunnitelmaa tulisi myös säännöllisesti harjoitella (Sullivan ym., 2023; Van Boven ym., 2023)

6 Pohdinta

6.1 Tulosten tarkastelu

Tämä tutkielma tuotti tietoa kyberuhkista, jotka ovat kohdistuneet sosiaali- ja terveydenhuoltoon. Tutkielmassa todettiin, että maailmalla sosiaali- ja terveydenhuoltoa kohtaan on tehty useita kyberhyökkäyksiä. Kyberhyökkäyksiä on useaa eri luokkaa. Kyberhyökkäyksissä ei voida varautua vain yhden ohjelman hyökkäykseen tai yhden hyökkäysluokan tapahtumiseen. Viidestä käsitellystä kyberhyökkäyksestä kolme (60 %) olivat kiristyshaittaohjelmia. Myös kaikki tutkimuksissa salatut viisi kyberhyökkäystä olivat kiristyshaittaohjelmia. Kaikissa käsitellyissä tapauksissa kiristyshaittaohjelma oli päässyt terveydenhuollon järjestelmiin kalastelusähköpostien kautta (Kandasamy ym., 2022; Moore ym., 2023; Tarka ym., 2023). Harvey kollegoidensa kanssa totesi (2023), että jopa 72 %:ssa kiristyshaittatapahtumista varastetaan myös potilastietoja. Yksi kyberhyökkäys voi siis alkaa kalastelusta, tartuttaa työaseman kiristyshaittaohjelmalla ja varastaa potilastietoja samaan aikaan.

Kyberhyökkäyksillä on laaja-alaisia vaikutuksia sosiaali- ja terveydenhuoltoon ympäri maailmaa. Kyberhyökkäyksillä tunnistettiin tutkielmassa olevan vaikutuksia yksilöihin ja hoidon toteutukseen. Vaikutuksien laajuus ja kesto luovat sosiaali- ja terveydenhuollon organisaatioille tarpeen suunnata asiantuntijaosaamista varautumiseen. Valmiussuunnitelman kehittämisellä voidaan edistää sosiaali- ja terveydenhuollon kykyä jatkua keskeytyksettömänä kyberhyökkäyksestä huolimatta. Kirjallisuudessa tunnistettiin kyberhyökkäyksien luoneen erityisesti kiireettömän terveydenhuollon peruutuksia. Valmiussuunnitelman puuttuminen voi johtaa hoitovelan kasvamiseen. Suomessa yli 152 000 potilasta odotti kiireettömään erikoissairaanhoitoon vuonna 2022 (THL, 2022). Hoitovelan kasvattaminen johtaa taloudellisten kustannusten kasvuun entisestä enemmän, joten tämän voidaan ajatella painottavan valmiussuunnitelmien luomisen tärkeyttä.

Vaikka tietomurroilla ja tietovuodoilla ei välttämättä nähdä potilastyössä suoria vaikutuksia, näiden ennaltaehkäiseminen on tärkeää. Kirjallisuuden tietomurroissa potilaiden luottamuksesta puhuttiin enemmän menetettyjen asiakkaiden valossa (Prentosito ym., 2022), mutta esimerkiksi Suomen sosiaali- ja terveydenhuoltojärjestelmissä on hyvä pohtia luottamuksen säilymisen tärkeyttä yhteiskunnalle. Tietovuodoilla voi olla vaikutuksia kansan luottamuksessa terveydenhuoltoon. Tästä syystä on tärkeää luoda monitahoinen

valmiussuunnitelma, joka ottaa huomioon monipuoliset ja laajat kyberhyökkäysten seuraukset. Kirjallisuuskatsauksen tulosten pohjalta voidaan esittää toimenpiteet, jotka olisi hyvä huomioida kyberhyökkäyksiin varautumisessa sosiaali- ja terveydenhuollon organisaatiossa.

Kyberhyökkäys ei välttämättä kohdistunut kaikkiin käytettäviin ohjelmiin, mutta kyberhyökkäyksen leviämisen estämiseksi saatetaan joutua sulkemaan internet-yhteydet tai suurin osa päätelaitteista. Tähän tulisi kiinnittää huomiota valmiussuunnitelmien tekemisessä. Organisaation yksi helpoimmista tavoista nostaa kyberturvallisuutensa tasoa on pitää käyttöjärjestelmät ajan tasalla (Harvey ym., 2023; Moore ym., 2023). Käyttöjärjestelmäpäivityksissä korjataan myös virustorjunnan puutteita ja mitä kauemmin käyttöjärjestelmä on päivittämättä, sitä pidempään tiedostettu puute jää korjaamatta. Käyttöjärjestelmän päivittäminen on lopulta nopea ja vähän resursseja vaativa toimenpide, millä voidaan parantaa kyberturvallisuutta. Suomessa sosiaali- ja terveydenhuollossa on useita eri käyttöjärjestelmiä, mikä saattaisi rajoittaa kyberhyökkäyksen leviämistä useisiin terveydenhuollon yksiköihin. Tietojenkalastelulla voidaan kuitenkin tavoittaa useita järjestelmiä, joten tämä ei vähennä kyberhyökkäysten varautumisen tarvetta.

Sosiaali- ja terveydenhuollon järjestelmissä on mahdollista myös arvioida oman organisaation tietoturvallisuuden tasoa. Kandasamy kumppaneineen (2022) tuo esiin artikkelissaan haavoittuvaisuuden itsearvioimiskyselyn. Vulnerability Self-Assessment Questionnaire (VSAQ) luotiin mille tahansa terveydenhuollon organisaatiolle käytettäväksi, jotta Aasiassa voitaisiin parantaa kyberturvallisuutta terveydenhuollossa. Suomessakin voitaisiin hyödyntää vastaavia kyselyitä ja sosiaali- ja terveyshuollossa tulisi parantaa kyberturvallisuutta samankaltaisten systemaattisten itsearviointien avulla.

Kyberuhkiin varautuminen osoitettiin tutkielmassa tärkeäksi vaikutuksien minimoimiseksi. Kyberturvallisuuteen olisi ollut tärkeää keskittyä sosiaali- ja terveydenhuollon organisaatioissa jo 10 vuotta sitten, kun kyberhyökkäyksien määrän havaittiin nousseen. Europarlamentissa 14.12.2022 säädetyn NIS2-EU-direktiivin myötä tämä tulee pakolliseksi Euroopan unionin jäsenmaihin. NIS2-direktiiviä kutsutaan kyberturvallisuus- tai verkko- ja tietoturvadirektiiviksi, joka asettaa säädökset tietoturvavelvollisuuksista ja häiriöraportoinnista useille eri sektoreille. Direktiivin myötä eri yhteiskunnan kriittisille sektoreille ja monissa organisaatioissa tulee pakolliseksi kyberturvallisuutta parantavat riskienhallintavelvoitteet ja raportointivelvoitteet merkittävistä

kyberturvallisuuspoikkeamista. (Kyberturvallisuuskeskus, 2022.) Direktiivin luoma raportointivelvoite tulee kehittämään sosiaali- ja terveydenhuollon kyberturvallisuutta ja varautumista. Useassa tiedonhaussa poissuljetussa artikkelissa mainittiin sosiaali- ja terveydenhuollon kyberuhkien olevan haastavia tutkia. Tämän pohdittiin johtuvan siitä, että läheskään kaikkia kyberturvallisuuspoikkeamia ei ilmoiteta sosiaali- ja terveydenhuollon organisaatioissa. Raportointivelvoite voi luoda uusia mahdollisuuksia tutkimukselle ja varautumisen kehittämiselle, mikäli pienemmätkin kyberturvallisuuspoikkeamat tilastoidaan entistä useammin.

6.2 Tutkielman luotettavuuspohdinta

Tutkielman kirjallisuuskatsauksen tyypiksi valittiin kuvaileva kirjallisuuskatsaus. Kuvailevan kirjallisuuskatsauksen aineistot ovat laajoja ja aineiston valinta on hyvinkin vapaata metodisista säännöistä. Kun kyseessä oli vähän tutkittu ja yhteiskunnallisesti tuore aihe, kuten kyberhyökkäykset, tutkittavaa ilmiötä pystyttiin kuvaamaan laajasti kuvailevalla kirjallisuuskatsauksella. (Salminen, 2011.) Kuvailen kirjallisuuskatsauksen väljyys voi kuitenkin kokemattoman tutkijan käsissä heikentää luotettavuutta, mikäli tutkimusprosessia ei dokumentoida tai toteuteta oikein. Tutkielman kirjoittajalle tämä on ensimmäinen itsenäinen kirjallisuuskatsaus, joten tämä voidaan nähdä luottamusta heikentäväksi tekijäksi.

Tutkimuksia haettiin neljästä eri tietokannasta. Tietokannoiksi päädyttiin valitsemaan PubMed, CINAHL ja Cochrane, koska ne ovat lääketieteelliseen ja hoitotieteelliseen tietoon keskittyviä tietokantoja. Kyberhyökkäyksistä haluttiin löytää tietoa nimenomaan sosiaali- ja terveydenhuollon kontekstissa. Hakua täydentämään valittiin Scopus, koska se on monitieteellinen tietokanta. Scopus täydensi hakua sosiaalitieteiden ja tietojenkäsittelytieteen osalta. Kirjallisuushaun hakulausekkeen luomisen apuna käytettiin Turun yliopiston informaatikkoa, minkä voidaan ajatella tekevän tutkielmasta luotettavamman. (Pölkki ym., 2012.)

Tutkielman kirjallisuuden hakuprosessin luotettavuutta heikentää useat poissuljetut artikkelit, jotka eivät olleet saavutettavissa Turun yliopiston tunnuksilla haetuista tietokannoista. Katsaus ei tavoittanut kaikkia mahdollisia sosiaali- ja terveydenhuoltoon kohdistuneista kyberhyökkäyksistä julkaistuja tutkimuksia. On mahdollista, että tutkielmassa esiintyy tästä syystä julkaisuharhaa (Luoto, 2012).

Kirjallisuuden hakuprosessin suoritti vain yksi henkilö, vaikka yleisesti suositellaan kahden tutkijan osallistumista kirjallisuushakuun ja tutkimusten laadunarviointiin (Pölkki ym., 2012). Hakuprosessin suoritti vain yksi henkilö, koska tutkielman tarkoituksena oli harjoittaa kirjoittajaa kirjallisuuskatsauksen tutkimusmetodiikassa ja tutkimusten laadunarvioinnissa.

Tutkielmaan valitun aineiston laatu arvioitiin MMAT-työkalulla (Hong ym., 2018), mikä lisää tutkielman luotettavuutta. Tutkielmasta ei poissuljettu laadunarvioinnissa kirjallisuutta, mutta kaikki laadunarvioidut tutkimukset ylittivät 50 % laadunarvioinnin kriteereistä (Hotus n.d.). Tutkimusprosessissa sitouduttiin noudattamaan hyvän tieteellisen käytännön ohjetta (HTK-ohje) ja hyviä tieteellisiä menettelytapoja (Keski ym., 2023; Tutkimuseettinen neuvottelukunta [TENK], 2024).

Kaikki tutkielmaan valitut artikkelit olivat englannin kielellä kirjoitettuja. Tämä on voinut aiheuttaa kieliharhaa, mikä voi heikentää tutkielman luotettavuutta. Tutkielmaan valittu aineisto on pieni ja osa aineistosta käsitteli samaa kyberhyökkäystä, vaikkakin eri terveydenhuollon yksiköissä. Kaikkia tuloksia ei voi siis pitää aukottomina, vaikka ne ovatkin linjassa muun kirjallisuuden tulosten kanssa.

7 Johtopäätökset ja jatkotutkimusehdotukset

Tässä tutkielmassa todettiin kyberhyökkäyksien olevan terveydenhuollolle kasvava uhka ja niihin pitäisi suhtautua yhtä vakavasti kuin Kansallisen riskinarvion (Sisäministeriö, 2023) muihin osa-alueisiin. Sosiaali- ja terveyspalveluihin kohdistuneilla kyberhyökkäyksillä on ollut laaja-alaisia ja pitkäkestoisia vaikutuksia, joihin ei olla kirjallisuuden mukaan varauduttu tarpeeksi tai ollenkaan. Kyberhyökkäyksissä keskeisesti esiintyneitä vaikutuksia olivat potilastietojen menetys, laboratoriojärjestelmän kaatuminen, internet-yhteyden katkaiseminen, päivittäisten poliklinikkakäyntien ja kiireettömän leikkaustoiminnan vähentyminen sekä henkilökunnan uupuminen.

Varautumista tulisi parantaa kehittämällä kyberhyökkäykseen keskittyvä valmiussuunnitelma. Valmiussuunnitelman ei tulisi keskittyä vain IT-henkilöstön toimenpiteisiin kybertoimintaympäristössä, vaan tulisi luoda päivittäisten toimenpiteiden jatkumiseen keskittyvä suunnitelma. Kyberhyökkäysten valmiussuunnitelmaa tulisi harjoitella ja henkilöstön tulisi tietää, miten poikkeustilanteessa toimitaan. Harkittu suunnitelma ja henkilöstön osaaminen säilyttää sairaalojen toimintakyvyn parempana kyberhyökkäyksestä huolimatta. Tämä pitkällä aikavälillä vähentää kyberhyökkäyksen aiheuttamia kustannuksia, jos sen vuoksi ei jouduta perumaan kiireettömiä ajanvarauksia ja päiväkirurgisia leikkauksia. Syöpäosastoilla sekä neuro- ja ortopedisillä yksiköillä olisi hyvä olla omat valmiussuunnitelmat, jossa otettaisiin kantaa potilaiden hoitosuunnitelmiin ja kuvantamislaitteiden mahdollisiin ruuhkautumisiin.

Kyberhyökkäyksen valmiussuunnitelmassa täytyy huomioida laaja yhteistyö alueellisten sairaaloiden ja tiedotusvälineiden kesken, jotta potilaita pystytään tarvittaessa ohjaamaan tasaisesti muihin hoitopaikkoihin. Kyberhyökkäyksien tunnistettiin luovan ongelmia, johon löydettiin varautumisehdotuksia kuten potilastietojen varmuuskopioiminen.

Tässä tutkielmassa käytiin läpi kansainvälisesti vaikuttaneita kyberhyökkäyksiä. Maailmalla terveydenhuolto on järjestetty eri tavoilla, ja useiden maiden terveydenhuolto pohjautuu enemmän yksityisiin palveluihin ja terveysvakuutuksiin. Conti- ja WannaCry-kyberhyökkäykset kohdistuivat julkiseen terveydenhuoltoon, jotka voivat olla paremmin vertailtavissa Suomen sosiaali- ja terveydenhuoltoon. Lisätutkimusta tarvitaan Suomen sosiaali- ja terveyspalveluiden varautumisesta ja alttiudesta kyberhyökkäyksille. Kyberhyökkäyksen varalle kehitettävän valmiussuunnitelman sisältöön voidaan ottaa mallia

kirjallisuudesta, mutta tarvitaan eri terveydenhuollon yksiköiden ominaisuudet huomioon ottavaa tutkimusta sisällön luomisen tueksi.

Kirjallisuudessa tietomurtoja käsiteltiin huomattavasti vähemmän kuin kiristyshaittaohjelmia. Suomessa tapahtui 33 000 potilaan tietomurto, kun Vastaamo-nimiseen psykoterapiakeskukseen hyökättiin. Suomessa tapahtuneesta tietomurrosta ei löytynyt tutkimuskirjallisuutta tähän katsaukseen, vaikka tietomurto oli uhrimäärältään Suomen suurin. Tähän voi vaikuttaa Vastaamo-tietomurron ajankohtaisuus, sillä tietomurto tapahtui vuosina 2018–2019 ja oikeudenkäynnit olivat keväällä 2024 vielä kesken. (Mäntysalo, 2023.) Tietomurtojen aiheuttamia tunteita käsiteltiin vain yhdessä kirjallisuuskatsauksen tutkimuksessa ja nämä tulokset keskittyivät asiakkaiden tunteisiin organisaation näkökulmasta (Prentosito ym., 2022). Tietomurroista tarvitaan lisätutkimusta ja erityisesti uhrien näkökulmaa olisi hyvä kuvata tieteellisellä tutkimuksella. Tietomurroissa uhrimäärät voivat olla suuria. Tutkimusta uhrien tarvitsemasta psykososiaalisesta tuesta tarvitaan, jotta sosiaali- ja terveydenhuollon organisaatiot voivat varautua tuen tarjoamiseen.

Lähteet

Argaw, T., Troncoso-Pastoriza, T., Lacey, D., Florin, M., Calcavecchia, F., Anderson, D., Burleson, W., Vogel, J., 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). https://doi.org/10.1186/s12911-020-01161-7

Burns, N. & Grove, S. (2005). The practice of nursing research. Conduct, critique, and utilization. Elsevier Saunders. Fifth Edition, s. 715-719.

Choucri, N., Madnick, S., & Ferwerda, J. (2013). Institutions for Cyber Security: International Responses and Global Imperatives. Information Technology for Development, 20(2). https://is.muni.cz/el/fss/podzim2018/IRE107/um/11_institutions_for_cyber_security.pdf

Dameff, C., Tully, J., Chan, T., Castillo, E., Savage, S., Maysent, P., Hemmen, T., Clay, J. & Longhurst, C. (2023). Ransomware attack associated with disruptions at adjacent emergency departments in the US. JAMA network open, 6(5). https://doi.org/10.1001/jamanetworkopen.2023.12270

Elo, S. & Kyngäs, H. (2008). The qualitative content analysis process. Jan; Leading Global Nursing Research, 62(1). https://doi.org/10.1111/j.1365-2648.2007.04569.x

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. NPJ digital medicine, 2(1). https://doi.org/ 10.1038/s41746-019-0161-6

Harvey, H., Carroll, H., Murphy, V., Ballot, J., O'Grady, M., O'Hare, D., Lawler, G., Bennett, A., Connolly, M., Noone, E., Kelly, M., Bazin, A., Daly, A., Mulroe, E., McDermott, R. & O'Reilly, S. (2023). The impact of a national cyberattack affecting clinical trials: the cancer trials Ireland experience. JCO Clinical Cancer Informatics, 7. https://doi.org/10.1200/CCI.22.00149

Hong, Q. N., Fàbregues, S., Bartlett, G., Boardman, F., Cargo, M., Dagenais, P., Gagnon, M-P., Griffiths, F., Nicolau, B., O'Cathain, A., Rousseau, M-C., Vedel, I. & Pluye, P. (2018). The Mixed Methods Appraisal Tool (MMAT) version 2018 user guide. McGill, Department of family medicine.

Hotus. (n. d.). Tutkimustiedon laadun arvioiminen. Saatavilla 16.4.2024 https://hotus.fi/hoitosuositukset/laadinta/

Interpol. (2020). Preventing crime and protecting police: INTERPOL's COVID-19 Global Threat Assessment. International Criminal Police Organization. Saatavilla 20.2.2024 https://www.interpol.int/News-and-Events/News/2020/Preventing-crime-and-protecting-police-INTERPOL-s-COVID-19-global-threat-assessment

International Telecommunication Union [ITU]. (2007). Global Cybersecurity Agenda. Saatavilla 5.2.2024 https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

Jansson, S., & Sihvonen, T. (2018). Kyberturvallisuus valtiollisena toimintaympäristönä ja siihen kohdistuvat uhkat. Media & viestintä, 41(1). https://doi.org/10.23983/mv.69950

Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. (2022). Digital healthcare-cyberattacks in Asian organizations: an analysis of vulnerabilities, risks, nist perspectives, and recommendations. IEEE Access, 10. https://doi.org/10.1109/ACCESS.2022.3145372

Keski, R., Hämäläinen, K., Karhunen, M., Löfström, E., Näreaho, S., Varantola, K., Spoof, S-K., Tarkiainen, T., Kaila, E. & Aittasalo, M. (2023). Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. Tutkimuseettisen neuvottelukunnan HTK-ohje 2023. Saatavilla 16.4.2024 https://tenk.fi/sites/default/files/2023-03/HTK-ohje_2023.pdf

Keogh, R., Harvey, H., Brady, C., Hassett, E., Costelloe, S., O'Sullivan, M., Towey, M., O'Leary, M., Cahill, M., O'Riordan, A., Joyce, C., Moloney, G., Flavin, A., Bambury, R., Murray, D., Bennett, K., Mullooly, M. & O'Reilly, S. (2024). Dealing with digital paralysis: Surviving a cyberattack in a National Cancer center. Journal of Cancer Policy, 39(100466). https://doi.org/10.1016/j.jcpo.2023.100466

Kyberturvallisuuskeskus. (2020). Kyberturvallisuuden perussanasto. Saatavilla 20.2.2024 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/kyberturvallisuuden-perussanasto

Kyberturvallisuuskeskus. (2022). NIS2- Euroopan unionin kyberturvallisuusdirektiivi. Saatavilla 25.2.2024 https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & security, 105(102248). https://doi.org/10.1016/j.cose.2021.102248

Luoto, R. (2012). Julkaisuharha - lääketieteellisen tiedon akilleenkantapää. Duodecim, 128(5). Saatavilla 23.4.2024 https://www.duodecimlehti.fi/lehti/2012/5/duo10120

Moore, G., Khurshid, Z., McDonnell, T., Rogers, L., & Healy, O. (2023). A Resilient Workforce: patient safety and the workforce response to a cyber-attack on the ICT systems of the national health service in Ireland. BMC Health Services Research, 23(1). https://doi.org/10.1186/s12913-023-10076-8

Mäntysalo, J. (2023). Uhrimäärältään Suomen suurin rikosjutun epäilty saapuu oikeuden eteen - tässä viisi keskeistä kysymystä Vastaamo-tapauksesta. Yle. Saatavilla 17.4.2024 https://yle.fi/a/74-20019922

Ponemon institute. (2016). Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data. Ponemon, 6. Saatavilla 20.2.2024 https://www.ponemon.org/local/upload/file/Sixth%20Annual%20Patient%20Privacy%20%26%20Data%20Security%20Report%20FINAL%206.pdf

Prentosito, A., Skoczen, M., Kahrs, L. & Bhunia, S. (2022). Case Study on a Session Hijacking Attack: The 2021 CVS Health Data Breach. Springer International Publishing, 13475. https://doi.org/10.1007/978-3-031-14391-5_7

Puolustusministeriö. (2013). Suomen kyberturvallisuusstrategia 2013. Saatavilla 20.2.2024 https://www.defmin.fi/files/2347/Suomen_Kyberturvallisuusstrategia.pdf

Pölkki, T., Kanste, O., Elo, S., Kääriäinen, M., & Kyngäs, H. (2012). Järjestelmällisten kirjallisuuskatsausten metodologinen laatu: katsaus kansainvälisiin ja kansallisiin hoitotieteen julkaisuihin vuodelta 2009–2010. Hoitotiede, 24(4). https://journal.fi/hoitotiede/article/view/128257/77380

Radoniewicz, F. (2021). Cybersecurity in Poland. Legal aspects. Springer publishing. First Edition, s. 65-66

Riggi, J. (2020). Ramsomware Attacks on Hospitals Have Changed. American Hospital Assosiation. Saatavilla 30.3.2024 https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed

Sanastokeskus TSK ry, Huoltovarmuuskeskus & Turvallisuuskomitea. (2018). Kyberturvallisuuden sanasto. Saatavilla 3.3.2024 https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

Salminen, A. (2011). Mikä kirjallisuuskatsaus?: Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Opetusjulkaisuja, 6. https://urn.fi/URN:ISBN:978-952-476-349-3

Schjølberg, S. (2017). The History of Cybercrime (1976-2016). Cybercrime Research Institute. Volume 11, s. 1.

Sisäministeriö. (2023). Kansallinen riskinarvio 2023. Sisäministeriön julkaisuja, 4. Saatavilla 20.3.3024 https://julkaisut.valtioneuvosto.fi/handle/10024/164627

Sosiaali- ja terveysministeriö [STM]. (2024). Sosiaali- ja terveyspalvelut; sosiaalipalvelut & terveyspalvelut. Saatavilla 10.3.2024 https://stm.fi/sotepalvelut

Sosiaali- ja terveysministeriö [STM]. (2023). Sosiaali- ja terveyspalveluja koskeva lainsäädäntö. Saatavilla 20.3.2024 https://stm.fi/sotepalvelut/lainsaadanto

Sosiaali- ja terveysministeriö [STM]. (2008). Sosiaalitoimen valmiussuunnitteluopas. Sosiaali- ja terveysministeriön julkaisuja, 12. Saatavilla 26.4.4024 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/72006/Julkaisuja_2008_12_valmius suunnitteluopas_verkko.pdf?sequence=1&isAllowed=y

Sosiaali- ja terveysministeriö [STM]. (no date). Valmiusasiat sosiaali- ja terveysministeriössä. Saatavilla 26.4.4024 https://stm.fi/valmiusasiat

Sullivan, N., Tully, J., Dameff, C., Opara, C., Snead, M., & Selzer, J. (2023). A national survey of hospital cyber attack emergency operation preparedness. Disaster medicine and public health preparedness, 17. https://doi.org/10.1017/dmp.2022.283

Tarka, M., Blankstein, M., & Schottel, P. (2023). The crippling effects of a cyberattack at an academic level 1 trauma center: An orthopedic perspective. Injury, 54(4). https://doi.org/10.1016/j.injury.2023.02.022

Tutkimuseettinen neuvottelukunta [TENK]. (2024). Hyvä tieteellinen käytäntö (HTK). Saatavilla 26.4.4024 https://tenk.fi/fi/hyva-tieteellinen-kaytanto-htk

THL. (2022). Hoitovelka kiireettömään erikoissairaanhoitoon kasvoi edelleen elokuussa. Tilastoraportti 37/2022. Saatavilla 24.4.2024 https://www.julkari.fi/bitstream/handle/10024/145343/TR37_2022_ESH_hoitoonpaasy.pdf?sequence=1&isAllowed=y

Van Boven, L., Kusters, R., Tin, D., Van Osch, F., De Cauwer, H., Ketelings, L., Rao, M., Dameff, C. & Barten, D. (2023). Hacking acute care: a qualitative study on the health care impacts of ransomware attacks against hospitals. Annals of emergency medicine, 83(1). https://doi.org/10.1016/j.annemergmed.2023.04.025

WHO. (2020). WHO reports fivefold increase in cyber attacks, urges vigilance. World Health Organization. Saatavilla 20.2.2024 https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

Liitteet

Liite 1. Tiedonhaku ja sen tulokset

Tietokanta	Hakulauseke	Hakupäivä	Tulokset	Käytetyt rajaukset
Pubmed (lopullinen haku)	("cyber attack*" OR "cyber assault*"[tw] OR "cyber intrusion*" OR "cyber breach*" OR "cyber offence*" OR "digital attack*" OR "cybersecurity incident*" OR "information security breach*" OR "security breach*" OR "data breach*" OR malware* OR ransomware* OR phishing* OR "cybersecurity breach*") AND ("Delivery of Health Care"[Mesh] AND healthcare* OR "health care*" OR "medical care*" OR "health service*" OR "wellness service*" OR "health system*" OR "medical service*" OR "healthcare service*" OR "health maintenance*" OR "health provision*")	20.2.2024	187 tulosta	englanti ja suomi, vuosi 2007-nykyhetki
CINAHL (lopullinen haku)	("cyber attack*" OR "cyber assault* OR "cyber intrusion*" OR "cyber breach*" OR "cyber offence*" OR "digital attack*" OR "cybersecurity incident*" OR "information security breach*" OR "security breach*" OR "data breach*" OR malware* OR ransomware* OR phishing* OR "cybersecurity breach*") AND (MH "Health Care Delivery+") AND (healthcare* OR "health care*" OR "medical care*" OR "health service*" OR "wellness service*" OR "health system*" OR "medical service*" OR "healthcare service*" OR "health maintenance*" OR "health provision*")	20.2.2024	101 tulosta	Rajauksia ei tarvinnut käyttää, koska artikkelit alkoivat vuodesta 2011 ja kaikki artikkelit olivat englanniksi
Cochrane (lopullinen haku)	(cyber NEXT attack OR cyber NEXT assault OR cyber NEXT intrusion OR cyber NEXT breach OR cyber NEXT offence OR digital NEXT attack OR cybersecurity NEXT incident OR information NEXT security NEXT breach OR security NEXT breach OR data NEXT breach OR malware OR ransomware OR phishing OR cybersecurity NEXT breach) AND (health NEXT care NEXT delivery OR healthcare OR health NEXT care OR medical NEXT care OR health NEXT service OR wellness NEXT service OR health NEXT system OR medical NEXT service OR healthcare NEXT service OR health NEXT maintenance OR health NEXT provision)	20.2.2024	2 tulosta	Rajauksia ei tarvinnut käyttää, koska artikkelit alkoivat vuodesta 2011 ja kaikki artikkelit olivat englanniksi
Scopus (lopullinen haku)	("cyber attack*" OR "cyber assault*" OR "cyber intrusion*" OR "cyber breach*" OR "cyber offence*" OR "digital attack*" OR "cybersecurity incident*" OR "information security breach*" OR "security breach*" OR "data breach*" OR malware* OR ransomware* OR phishing* OR "cybersecurity breach*") AND ("health care delivery") OR healthcare* OR "health care*" OR "medical care*" OR "health service*" OR "wellness service*" OR "health system*" OR "medical service*" OR "healthcare service*" OR "health maintenance*" OR "health provision*")	20.2.2024	503 tulosta	englanti ja suomi, vuosi 2007-nykyhetki, keyword Health care

Liite 2. Valitut tutkimukset

Tutkimuksen tekijät, maa ja julkaisuvuosi	Tutkimuksen tavoite	1. Tutkimusmenetelmä 2. Aineistonkeruumenetelmä	1. Osallistujat 2. Otoskoko	Keskeiset tulokset
Moore, G., Khurshid, Z., McDonnell, T., Rogers, L., & Healy, O. **Irlanti 2023**	Tutkimuksessa kuvattiin terveyspalvelujen henkilöstön reagointia ICT-järjestelmien menetykseen. Tutkimuksessa tuodaan esiin myös riskinhallintatoimenpiteet, jotka otettiin käyttöön kyberhyökkäyksen hillitsemiseksi. Ensilinjan henkilöstön sitkeys tuodaan myös esiin, koska heidän toimintansa varmisti potilaiden turvallisen hoidon jatkumisen.	1. Monimenetelmätutkimus 2. Fokusryhmähaastattelut	1. 8 fokusryhmää muodostettiin henkilöstöstä, jotka työskentelivät kliinisissä, liiketoiminnan, tutkijan, hallinnon ja tietojärjestelmien rooleissa. 2. N=36	Kyberhyökkäyksen vaikutus vaihteli tulosyksikön mukaan. Vaikutuksiin oli iso merkitys sillä, kuinka laaja IT-tuki yksiköllä oli saatavilla. Henkilöstön koettiin reagoineen nopeasti ja sitkeästi, mutta toisaalta kyberhyökkäyksen aiheuttaman stressin arvioitiin olevan COVID-19-pandemiaa vakavampi.
Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A., & Aylin, P. **Englanti 2019**	Tutkimuksen tarkoitus oli tunnistaa vuonna 2017 tapahtuneen WannaCry-hyökkäyksen vaikutukset Kansalliseen terveyspalveluun (National Health Service, NHS). Tutkimuksessa pyrittiin tunnistamaan kiristyshaittaohjelmasan liittyvät peruuntuneet tapaamiset, kuolemat ja taloudelliset kustannukset.	1. Retrospektiivinen vaikutusanalyysi 2. Sairaalajaksojen tilastotietojen (Hospital Episodes Statistics, HES) systemaattinen analyysi	1. Sairaalatiedoista poimittiin peruutettujen avohoitotapaamisten määrä, vaikutukset kiireellisiin ja suunniteltuihin sairaalahoitoihin, päivystyskäynnit, kuolemat ja sairaalan taloustiedot. 2. N/A	Kyberhyökkäyksen kokonaiskustannukset olivat 5.9 miljoonaa puntaa. Tämä muodostui peruutetuista kiireettömistä sairaalakäynneistä ja kiireellisten vastaanottojen vähentymisestä, jotka yhdessä vähenivät normaaliin viikkoon verrattuna 6 %. Kuolleisuuteen kyberhyökkäyksellä ei ollut vaikutusta, mutta tämän tunnistettiin olevan huono mittari arvioimaan potilaille tulleita terveysvaikutuksia.
Prentosito, A., Skoczen, M., Kahrs, L. & Bhunia, S. **Yhdysvallat 2022**	Tapaustutkimuksen tarkoitus oli analysoida tietovuodon metodologiaa ja vaikutuksia sekä tarjota mahdollisia puolustusstrategioita tällaisia hyökkäyksiä vastaan.	1. Tapaustutkimus 2. CVS Healthin tietovuotoon liittyvät uutiset ja kirjallisuushaku	1. N/A 2. N/A	Tietovuoto tapahtui CVS Healthin kyberturvallisuuden laiminlyömisen vuoksi. Tämänkaltainen laaja tietovuoto voi aiheuttaa yritykselle negatiivisia vaikutuksia. Tietovuodosta koituu aina merkittäviä kustannuksia. Puolustukseksi ehdotetaan monivaiheista tunnistautumista, salasanasuojausta ja ennalta laadittua tapahtumavasteen suunnitelmaa.

Keogh, R., Harvey, H., Brady, C., Hassett, E., Costelloe, S., O'Sullivan, M., Towey, M., O'Leary, M., Cahill, M., O'Riordan, A., Joyce, C., Moloney, G., Flavin, A., Bambury, R., Murray, D., Bennett, K., Mullooly, M. & O'Reilly, S. **Englanti 2023**	Tutkimuksen tarkoitus oli arvioida kyberhyökkäyksen vaikutuksia ja seurauksia Irlannin syöpäkeskukseen.	1. Monimenetelmätutkimus 2. Syöpäkeskusten osastojen toimintalokit 120 päivän ajalta hyökkäyksen jälkeen ja kuukausia ennen	1. Kliiniset ja ei-kliiniset terveydenhuollon ammattilaiset, jotka olivat työskennelleet CUH:ssa kyberhyökkäysten aikana ja sairaalatiedoista poimittiin laboratoriopuutokset, uusien potilaiden lähetteet ja syövän hoidon aikamääreet. 2. N/A	Kyberhyökkäyksen ensimmäisenä päivä kaikki IT-järjestelmät suljettiin. Syövänhoidossa koettiin suuria vaikutuksia. Näytteenotto väheni huomattavasti, esimerkiksi radiologian kapasiteetti väheni 90 %. Syövänhoidon poliklinikkatoiminta väheni 50 %. Kaikki IT- toiminta toisten sairaalojen kanssa keskeytettiin.
Kandasamy, K., Srinivas, S., Achuthan, K., & Rangan, V. **Intia 2022**	Tutkimuksen tarkoituksena oli analysoida Aasian maiden terveydenhuoltoon kohdistuneita kyberhyökkäyksiä sekä terveydenhuollon heikkouksia ja riskejä kyberturvallisuudessa. Tutkimuksessa esitetään myös ehdotuksia kyberhyökkäyksien riskin pienentämiseksi.	1. Monimenetelmätutkimus 2. Kuvaileva kirjallisuuskatsaus ja kvantitatiivinen kyselytutkimus, jonka tilastollinen data tulkittiin käyttämällä Lawshen menetelmää	1. Asiantuntijat terveydenhuollon tietotekniikan alalta 2. N=5	Tuloksissa tunnistettiin viisi yleisintä kyberhyökkäystyyppiä Aasian terveydenhuoltoa kohtaan. Tutkijat onnistuivat tunnistamaan myös yleisimmät terveydenhuollon kyberturvallisuuden heikkoudet ja arvioi NIST-kehyksen sopivuutta Aasian terveydenhuollon palvelimiin. Tutkimuksen tuloksista luotiin terveydenhuollon organisaatioille kysely, millä voi arvioida omaa kyberturvan tasoa.
van Boven, L., Kusters, R., Tin, D., van Osch, F., De Cauwer, H., Ketelings, L., Rao, M., Dameff, C. & Barten, D. **Yhdysvallat 2023**	Tutkimuksen tavoitteena oli tutkia useiden suurten sairaaloihin kohdistuneiden kiristyshaittaohjelma-hyökkäysten akuuttia vaikutusta Euroopassa ja Yhdysvalloissa vuosien 2017 ja 2022 välillä	1. Laadullinen haastattelututkimus 2. Puolistrukturoidun haastattelupohja luotiin kirjallisuuskatsauksen ja kyberturvallisuusasiantuntijoiden konsultaation pohjalta	1. Hätätilanteissa toimivia terveydenhuollon tarjoajia ja tietotekniikkaan keskittyneitä henkilöitä 2. N=9	Haastattelujen pohjalta rakennettiin viisi teemaa; vaikutukset ja haasteet potilashoidon jatkuvuuden kannalta, haasteet toipumisprosessin aikana, henkilökohtaiset vaikutukset terveydenhuollon henkilöstöön, valmius ja tunnistetut opetukset sekä tulevat suositukset.
Dameff, C., Tully, J., Chan, T., Castillo, E., Savage, S., Maysent, P., Hemmen, T., Clay, J. & Longhurst, C. **Yhdysvallat 2023**	Tutkimus kuvasi viereisiin sairaaloihin kohdistuneita vaikutuksia, kun toisissa alueen sairaaloissa on kiristyshaittaohjelmasta johtuva kyberhyökkäys. Tutkimus raportoi potilasmääristä, operatiivisista ja toiminnallisista häiriöistä.	1. Retrospektiivinen kohorttitutkimus 2. Sähköisistä potilastiedoista käyttämällä rakenteellista kyselykieltä Clarity-tietokannan avulla	1. Päivystysosaston aikuis- ja lapsipotilaat kahdessa viereisessä sairaalassa tutkimusjakson aikana 2. N=19 857 potilastietoa	Hyökkäyksen ja sen jälkeisen vaiheen aikana havaittiin huomattavaa kasvua potilasmäärissä, ambulanssien saapumisissa ja odotusaikojen pitenemisessä, potilaissa, jotka lähtivät näkemättä, kokonaishoidon kestossa, hätäpalvelujen ohjauksessa ja akuutin aivohalvauksen hoidon mittareissa.

Tarka, M., Blankstein, M., & Schottel, P. **Alankomaat 2023**	Tutkimuksessa arvioitiin kyberhyökkäyksen vaikutusta korkean tason traumasairaalaan. Tutkimuksessa keskityttiin leikkaussalien toimintamäärän arvioimiseen ja esitetään konkreettisia ehdotuksia käyttökatkosta selviämiseksi.	1. Retrospektiivinen kohorttitutkimus 2. Sähköisistä leikkaussalin potilastiedoista	1. Arkiviikon kokonaisleikkausaika (TIRT) kyberhyökkäyksen aikana vertailtuna siihen, mitä kyseinen aika oli vuosi ennen ja vuosi sen jälkeen 2. Tutkimuksen ajanjakson aikana arkipäivinä tehty TIRT kaikista leikatuista potilaista	Leikkaussalin toiminta laski taloudellisesti, tilastollisesti ja kliinisesti merkittävästi kyberhyökkäyksen seurauksena. Henkilökunnalta onnistuttiin keräämään konkreettisia ehdotuksia kyberhyökkäyksen onnistumisista ja varautumisesta.
Harvey, H., Carroll, H., Murphy, V., Ballot, J., O'Grady, M., O'Hare, D., Lawler, G., Bennett, E., Connolly, M., Noone, E., Kelly, M., Bazin, A., Daly, A., Mulroe, E., McDermott, R. & O'Reilly, S. **Irlanti 2023**	Tutkimuksen tarkoituksena oli mitata hyökkäyksen vaikutusta Irlannin syövän kliinisen tutkimusverkon toimintaan. Tutkimus pyrki myös selvittämään miten vaikutuksia voisi ehkäistä.	1. Laadullinen kyselytutkimus 2. Kyselylomakkeista, jotka lähetettiin 4 viikkoa ennen kyberhyökkäystä, neljän viikon ajanjaksolla kyberhyökkäyksen alkamisesta ja seuraavien neljän viikon ajanjaksolla	1. Kliinisen tutkimuksen yksiköt CTI-verkostossa 2. N=18 yksikköä	Kyberhyökkäys aiheutti merkittäviä häiriöitä kliinisiin tutkimuksiin, mikä johti dramaattisiin laskuihin rekrytoinneissa ja haasteisiin potilasturvallisuuden ja tieteellisen integriteetin ylläpitämisessä. Vaikutukset vaihtelivat julkisten ja yksityisten sairaalojen välillä. Ehkäisemisessä korostettiin kyberturvallisuussuunnitelman tärkeyttä.
Sullivan, N., Tully, J., Dameff, C., Opara, C., Snead, M., & Selzer, J. **Yhdysvallat 2023**	Tutkimus pyrki selvittämään Yhdysvaltojen sairaalajärjestelmien valmiusasteen kyberhyökkäyksiä vastaan.	1. Määrällinen kyselytutkimus 2. Kyselylomakkeista, jotka lähetettiin University of California (UC) sairaalajärjestelmän hätätilanteidenhallinnan sähköpostilistalle	1. Sairaalojen hätätilanteista vastaavat henkilöt 2. N=57	Sairaaloiden hätätilanteista vastaavista henkilöistä suurin osa sisällyttivät kyberuhat HVA:han (hazard vulnerability analysis), mutta yli puolen kielsivät mainitsevansa kyberuhkia EOP:ssa (emergency operation plan). Vain yksi neljäsosa oli aktivoinut hätävasteen kyberturvallisuuspoikkeamassa.