Hoivarobottien kyberturvauhkien kartoitus hoivarobotiikan asiantuntijoiden näkökulmasta

Marina Järvinen

2021 Laurea

Laurea-ammattikorkeakoulu

Hoivarobottien kyberturvauhkien kartoitus hoivarobotiikan asiantuntijoiden näkökulmasta

Marina Järvinen

Tietojenkäsittely

Opinnäytetyö

Joulukuu, 2021

Laurea-ammattikorkeakoulu **Tiivistelmä**

Tietojenkäsittely

Tradenomi AMK

Marina Järvinen

Hoivarobottien kyberturvauhkien kartoitus hoivarobotiikan asiantuntijoiden näkökulmasta

Vuosi 2021 Sivumäärä 54

Hoivarobotit ovat robotteja, jotka pystyvät itsenäisesti tai puoliautomaattisesti suorittamaan fyysiseen tai henkiseen hoitoon liittyviä tehtäviä kotona, palvelutalossa tai hoivalaitoksessa. Hoivaroboteilla on potentiaalia ratkaista useita väestön ikääntymiseen liittyviä haasteita. Kääntöpuolena hoivarobotit kärsivät vastaavista kyberturvaongelmista, joista tietokoneet ovat kärsineet jo vuosikymmeninen ajan. Hoivarobotteihin liittyviä kyberturvauhkia on tutkittu huomattavasti vähemmän, kuin esimerkiksi teollisiin ympäristöihin tarkoitettujen robottien kyberturvaa. Tämän tutkimuksen tarkoituksena oli kartoittaa hoivarobotteihin liittyviä kyberturvauhkia hoivarobotiikan asiantuntijoiden näkökulmasta.

Tutkimus toteutettiin laadullisena tutkimuksena ja tiedonkeruumenetelmänä käytettiin teemahaastattelua. Tutkimukseen osallistui 6 hoivarobotiikan asiantuntijaa, jotka valittiin harkinnanvaraisesti tarkoituksenmukaisuusperusteella. Haastatteluissa käytettiin tietoperustaan perustuvaa puolistrukturoitua teemahaastattelurunkoa. Haastatteluissa kerätty aineisto litteroitiin ja analysoitiin ensin teorialähtöisellä sisällön analyysillä, jonka jälkeen jäljelle jäänyt aineisto analysoitiin aineistolähtöisellä sisällön analyysillä.

Asiantuntijoiden näkemys hoivarobottien kyberturvauhkista oli, että hoivarobotiikan käyttöön liittyy samat riskit ja uhkat kuin muiden IT-laitteiden tai robottien käyttöön, jonka lisäksi uusien ominaisuuksien, kuten tekoälyn ja koneoppimisen koettiin luovan lisää mahdollisuuksia kyberrikollisuudelle. Verkkoon kytkettävyys ja verkkojen turvallisuus olivat asiantuntijoiden näkemyksen mukaan hoivarobotiikan kyberturvallisuuden toteutumisen kannalta avainasemassa. Tässä tutkimuksessa asiantuntijat korostivat myös kyberrikollisuuden taustalla vaikuttavia inhimillisiä tekijöitä, joita ei aiemmissa tutkimuksissa liioin käsitelty.

Hoivarobotteihin kohdistuvan kyberrikollisuuden motiivien ja siitä saavutettujen mahdollisten hyötyjen tutkimiseen tulisi kiinnittää huomiota, jotta hoivarobotteihin kohdistuvien uhkien todennäköisyys voitaisiin selvittää. Kyberturvallisuus on kilpajuoksua kyberrikollisuutta vastaan, ja tasapainon löytämistä sen välillä millaiset riskit ovat hyväksyttäviä, ja miltä on suojauduttava. Tulevaisuudessa tulisi myös selvittää, millainen palveluekosysteemi takaisi hoivarobottien turvallisuuden koko elinkaaren ajaksi; suunnittelu- ja kehitysvaiheessa, käyttöönotossa ja -opastuksessa, ylläpidossa ja laitteiden uusiokäytössä. Toisaalta tulee myös ottaa huomioon miten uudet robottien avulla tehtävät toimintamallit sietävät vikatilanteita, ja miten kriittiset palvelut voidaan turvata kyberturvauhkan toteutuessa.

Asiasanat: kyberturva, hoivarobotti, SHAPES

Laurea University of Applied Sciences

Business information technology

Bachelor's Thesis

Marina Järvinen

Abstract

Exploring care robots' cyber security threats from the point of view of the specialist in care robotics

Year 2021 Pages 54

Care robots are robots that can perform tasks related to physical or mental care, such as assisting in daily tasks, rehabilitation, or mental care, independently or semi-automatically. Care robots can be used in home care, in a nursing home or other care facility. Care robots have the potential to solve several challenges related to an aging population. But care robots suffer from similar cyber security issues that computers have been suffering from for decades. Also, cyber security threats related to care robots have been studied much less than the cyber security of robots intended for industrial environments. The purpose of this study was to map cyber security threats related to care robots from the perspective of care robotics specialists.

The study was conducted with a qualitative approach utilizing thematic interviews. A purposive sample of 6 specialists in care robotics took part in the study. A semi-structured thematic interview guide, based on literature view of previous studies, was used to facilitate the conversations at the interviews. All interviews were first transcribed verbatim, then analyzed by deductive content analysis, after which the remaining material was analyzed by inductive content analysis.

Cyber security threats of care robots according to the interviewed specialists were associated with the same risks and threats as the use of other IT devices or robots supporting the results of previous research. Most potential threats were considered to be remote access of care robots, espionage and eavesdropping. Network connectivity was seen as the main interface to the realization of cybersecurity threats in care robotics. New features such as artificial intelligence and machine learning were considered to create more opportunities for new threats. In this study, experts also highlighted the underlying human factors behind cybercrime, which were not addressed in previous studies.

According to the results of this study, more studies exploring the motives for cybercrime against care robots and the potential benefits derived from it is needed in order to determine the likelihood of the realization of threats to care robots are needed. Cyber security is a race against cybercrime and finding a balance between significant and acceptable risks. In future, a service ecosystem should be developed which guarantee the safety of care robots throughout their life cycle: during the design and development phase, deployment and user guidance, maintenance and reuse of the robot. Additionally, it is important to take into account how new robust operating models can withstand failures and how critical services can be secured in the event of a cyber security threat.

Keywords: care robots, cybersecurity, SHAPES

Sisällys

1 Johdanto

Väestön ikääntyessä vanhustenhoiva kohtaa uusia haasteita, kun hoidon kysyntä kasvaa. 80 vuotta täyttäneiden osuus Euroopassa oli vuonna 2016 27 miljoonaa, ja määrän odotetaan yli kaksinkertaistuvan vuoteen 2080 mennessä. Iso osa ikääntyneistä asuu kotona, ja tarvittavan avun ja hoidon ollessa saatavilla, suurin osa iäkkäistä haluaa asua kotona niin kauan kuin mahdollista. Vaikka ihmiset elävät terveempinä entistä vanhemmiksi, tarkoittaa väestön ikääntyminen myös hoidon kysynnän lisääntymistä, kun fyysisiin, kognitiivisiin ja muistiin liittyviin tarpeisiin tarvittava tuki lisääntyy. (Van Aerschot & Parviainen, 2020.)

Hoivarobotit ovat robotteja, jotka pystyvät itsenäisesti tai puoliautomaattisesti suorittamaan fyysiseen tai henkiseen hoitoon liittyviä tehtäviä, kuten auttamaan päivittäisissä tehtävissä, kuntoutuksessa tai henkisessä hoidossa. Hoivarobotteja voidaan käyttää henkilön hoitamisessa kotona, palvelutalossa tai hoivalaitoksessa. Niiden avulla voidaan myös helpottaa hoitajien työtä ja yhteistyötä kodin ja hoidon välillä esimerkiksi etäyhteyksien avulla. (Van Aerschot & Parviainen, 2020; Särkikoski ym. 2020, 278.)

Hoivarobotteihin ja niiden mukanaan tuomiin uhkiin ja mahdollisuuksiin liittyy paljon odotuksia ja ennakkoluuloja. Roboteilla on potentiaalia helpottaa arkea, luoda turvallisuuden tunnetta sekä toimittaa erilaisia tehtäviä, mutta kääntöpuolena ne kärsivät vastaavista kyberturvaongelmista, joista tietokoneet ovat kärsineet jo vuosikymmeninen ajan (Lera, Llamas, Guerrero & Olivera, 2017). Palvelu- ja hoivarobotteihin liittyviä kyberturvauhkia on tutkittu huomattavasti vähemmän, kuin esimerkiksi teollisiin ympäristöihin tarkoitettujen robottien kyberturvaa (Lera ym. 2017; Fosch-Villaronga & Mahlerb, 2021).

Tämän tutkimuksen tarkoitus on laadullisen tutkimuksen kautta tuoda esiin hoivarobotiikan asiantuntijoiden tämänhetkinen näkemys hoivarobottien kyberturvasta ja niiden käyttöön liittyvistä todellisista kyberturvauhkista, ja vastata tutkimuskysymykseen; ”Mitä kyberturvauhkia hoivarobotteihin kohdistuu?” Uhkien kartoituksen tavoite on lisätä tietoutta, johon perustuen sekä palveluntarjoajat että loppukäyttäjät voivat helpommin kriittisesti arvioida millaisia uhkia laitteiden käyttöön liittyy ja millaisia riskejä he ovat valmiita ottamaan.

Tämä tutkimus liittyy Euroopan Unionin Horisontti2020-ohjelman rahoittamaan, vuonna 2019 käynnistyneeseen SHAPES-hankkeeseen (Smart and Healthy Ageing through People Engaging in Supportive Systems), jossa eettinen osaaminen on yksi Laurea AMK:n vastuualueista. Hankkeen tavoitteena on kehittää digitaalista palveluekosysteemiä tukemaan ikääntyvien ihmisten hyvinvointia, ja siten heidän mahdollisuuksiaan elää hyvää elämää kotona tai kodinomaisessa ympäristössä. (Laurea Ammattikorkeakoulu, 2019.)

2 Tietoperusta

2.1 Digitalisaatio kehityksen mahdollistajana

Digitalisaatio tarkoittaa digitaalisten teknologioiden yleistymistä, ja sen voidaan katsoa alkaneen 1970-luvulta, kun mikropiireistä tuli kohtuuhintaisia ja ne tulivat kuluttajatuotteisiin. Tietotekniikka on yleistynyt arkielämän toiminnoissamme 1980-luvulta lähtien, kun tietotekniikka mahdollisti tietokoneiden välisen tiedonlevityksen, ja kotitietokoneiden käyttö alkoi yleistyä. (Marttinen 2018, 141.) Erilaiset laitteet ja järjestelmät ovat enenevissä määrin yhteydessä verkkoon, ja laitteiden ja järjestelmien käyttämää ja keräämää dataa säilytetään digitaalisessa muodossa verkossa. Tietotekniikan ja teknologian kehitys on mahdollistanut täysin uudenlaisia digitaalisia palveluja. Kehitys on ollut nopeaa, ja jatkuu edelleen. Tänään digitaaliset palvelut, internet ja internetiin kytköksissä olevat laitteet ovat meille arkipäivää, ja uusille sukupolville ne ovat jo itsestäänselvyys (Sosiaali- ja terveysministeriö 2016).

Suomi on kuulunut maailmanlaajuisesti digitalisaation hyödyntämisen edelläkävijöihin. Sosiaali- ja terveydenhuollon alta on esimerkiksi helppo nostaa esiin esimerkkejä digitalisaation kehityksen tuomista hyödyistä. Alan ammattilaiset käyttävät digitaalisia palveluita työssään päivittäin, kun paperien käsittelyn sijaan asiakas- ja potilastyössä tarvittavat järjestelmät mahdollistavat tietojen saatavuuden digitaalisesti. Digitaaliset palvelut ovat mahdollistaneet myös, että kansalaisilla on enenevästi pääsy omiin terveys- ja hyvinvointitietoihin, joka helpottaa kommunikaatiota kansalaisten ja palvelun tuottajien välillä. (Sosiaali- ja terveysministeriö 2019.) Digitalisaatio on mahdollistanut kommunikaation ja informaatioteknologian huiman kehityksen. Kehitys puolestaan mahdollistaa liiketoimien ja palvelujen kehittämisen uudenlaisella tavalla, jolloin liiketoimien ja palvelujen laatu ja tehokkuus paranee.

Sosiaali- ja terveysministeriön (2016) julkaisun mukaan Valtiovarainministeriön määrittelee digitalisaation seuraavasti:

> ”Digitalisaatio on sekä toimintatapojen uudistamista, sisäisten prosessien digitalisointia että palveluiden sähköistämistä. Kyse on isosta oivalluksesta, miten omaa toimintaa voidaan muuttaa jopa radikaalisti toisenlaiseksi tietotekniikan avulla.” (Sosiaali- ja terveysministeriö 2016.)

Digitalisaatiossa merkittävyyden puolesta puhuu myös se, että käyttäjälähtöisiä digitaalisia julkisia palveluja pidetään yhtenä Suomen kilpailukyvyn edellytyksenä (Sosiaali- ja terveysministeriö 2016). Jopa hallitusohjelmassa on asetettu tavoitteeksi nostaa julkisen sektorin teknologia- ja digitalisaatiokyvykkyyttä sekä kehittää julkisen ja yksityisen sektorin yhteistyötä. Tavoite on, että Suomi tunnettaisiin edelläkävijänä, jossa digitalisaation ja

teknisen kehityksen tuomia mahdollisuuksia kehitetään ja otetaan käyttöön yli hallinto- ja toimialarajojen. (Valtiovarainministeriö 2021.)

Digitalisaatiota voidaan siis oikeutetusti pitää yhtenä yhteiskunnan kehityksen mahdollistajana, ja se onkin viime vuosikymmenten aikana muuttanut maailmaa nopeasti ja tulee tulevaisuudessa muuttamaan maailmaa yhä enemmän. Digitalisaatio on yksi keskeinen tekijä myös robotiikan, ja siten myös hoivarobottien kehityksen taustalla. Tulee kuitenkin muistaa, että vaikka digitalisaatiota hyödyntämällä voidaan kehittää uusia ja innovatiivisia ratkaisuja, liittyy kehitykseen myös haasteita. Haasteet voivat liittyvät mm. yksityisyyden ja turvallisuuden takaamiseen sekä etiikkaan, joita ei automatisaation, tehokkuuden ja uutuuden viehätyksessä tule unohtaa.

2.2 Hoivarobotit ja niiden käyttömahdollisuudet

80 vuotta täyttäneiden osuus Euroopassa oli vuonna 2016 27 miljoonaa, ja määrän odotetaan yli kaksinkertaistuvan vuoteen 2080 mennessä. Iso osa ikääntyneistä asuu kotona, ja tarvittavan avun ja hoidon ollessa saatavilla, suurin osa iäkkäistä haluaa asua kotona niin kauan kuin mahdollista. Vaikka ihmiset elävät terveempinä entistä vanhemmiksi, tarkoittaa väestön ikääntyminen myös hoidon kysynnän lisääntymistä, kun fyysisiin, kognitiivisiin ja muistiin liittyviin tarpeisiin tarvittava tuki lisääntyy. Hoivarobotteja on kehitetty jo 1990-luvulta lähtien, ja niiden on ennustettu olevan mahdollinen ratkaisu mm. vanhushoivan haasteisiin. (Van Aerschot & Parviainen, 2020.)

Hoivarobotiikkaa voidaan kehittää helpottamaan tai jopa korvaamaan hoitajien tekemää työtä myös muilla sektoreilla kuin vanhustenhoivassa. Tämä tutkimus liittyy Euroopan Unionin Horisontti2020-ohjelman rahoittamaan, vuonna 2019 käynnistyneeseen SHAPES-hankkeeseen (Smart and Healthy Ageing through People Engaging in Supportive Systems). Hankkeen tavoitteena on kehittää digitaalista palveluekosysteemiä tukemaan ikääntyvien ihmisten hyvinvointia, ja siten heidän mahdollisuuksiaan elää hyvää elämää kotona tai kodinomaisessa ympäristössä. (Laurea Ammattikorkeakoulu, 2019.) Tässä työssä tullaan keskittymään hoivarobotiikkaan lähinnä vanhustenhoivan näkökulmasta.

2.2.1 Hoivarobotin määritelmä

Robotilla tarkoitetaan uudelleen ohjelmoitavaa mekatronista laitetta, joka vaikuttaa ympäristöönsä sensoreiden ja toimilaitteiden avulla (Särkikoski, Turja & Parviainen 2020, 280). Tyypillisesti robotit jaetaan teollisuus- ja palvelurobotteihin riippuen siitä, käytetäänkö niitä teollisuuden hyödyksi vai suoritetaanko niillä ihmisille hyödyllisiä tehtäviä (Fosch-Villaronga & Mahlerb, 2021).

Hoivarobotit ovat robotteja, jotka pystyvät itsenäisesti tai puoliautomaattisesti suorittamaan fyysiseen tai henkiseen hoitoon liittyviä tehtäviä, kuten auttamaan päivittäisissä tehtävissä, kuntoutuksessa tai henkisessä hoidossa. Hoivarobotteja voidaan käyttää henkilön hoitamisessa kotona, palvelutalossa tai hoivalaitoksessa. Niiden avulla voidaan helpottaa hoitajien työtä ja yhteistyötä kodin ja hoidon välillä mm. etäyhteyksien avulla. (Van Aerschot & Parviainen, 2020; Särkikoski ym. 2020, 278.)

Useissa alan artikkeleissa puhutaan sekä palveluroboteista, sosiaalisista roboteista että hoivaroboteista samassa yhteydessä. Palvelurobotti on robotti, joka pystyy osittain tai täysin itsenäisesti suorittamaan ihmisen hyvinvoinnin tai ympäristön kannalta hyödyllisiä palveluita. Sosiaalinen robotti on robotti, joka täydentää, lisää tai korvaa ihmisen sosiaalista vuorovaikutusta. (Särkikoski ym. 2020, 280-281.) Erilaisia robotteja voi usein ohjelmoimalla muokata erilaisiin käyttötarkoituksiin, joten robottikohtaisesti ei välttämättä ei ole täysin yksiselitteisesti määriteltävissä onko robotti hoivarobotti muun kuin käyttötarkoituksen tai käyttöympäristön perusteella (Fosch-Villaronga & Mahlerb, 2021). Näin ollen, jos robottia käytetään esim. lasten, vanhusten ja vammaisten hoidossa, on kyseessä hoivarobotti, vaikka sama robotti voitaisiin ohjelmoida toisaalla toimittamaan esimerkiksi aulavirkailijan työtä. Sosiaalinen robotti voidaan myös nähdä hoivarobottina, mikäli sen käyttötarkoitus liittyy henkiseen hoitoon.

2.2.2 Hoivarobottien ominaisuudet ja käyttökohteet

Jotta voidaan kartoittaa ne hoitotarpeet, joita hoivaroboteilla voidaan ratkaista, on Parviaisen ja Van Aerschotin (2020) mukaan ymmärrettävä yleisimmät hoidon tarpeet. Yleensä vanhemman henkilön riippuvuustaso arvioidaan sen mukaan, onko hän kykenevä selviytymään päivittäisestä elämästä ja niistä tehtävistä, joita päivittäisessä elämässä esiintyy. Näitä tehtäviä ovat mm. perusterveydenhuollon perustehtävät, joihin kuuluvat syöminen, peseytyminen, pukeutuminen, wc-käynnit, liikkuminen ja siistiytyminen, sekä henkilökohtaiseen autonomiaan liittyvät tehtävät, kuten talouden hallinta, kuljetusten hoitaminen, ostokset, aterioiden valmistaminen, puhelimen tai muiden viestintälaitteiden käyttö, lääkkeiden hallinta ja kotityöt. (Van Aerschot & Parviainen, 2020.)

Hoivaroboteilla on potentiaalia auttaa päivittäisessä toiminnassa, tarjota seuraa ja turvallisuuden tunnetta. Robotteja pyritään kehittämään ja tuomaan markkinoille, ja hoivarobotteja on kokeiltu Suomessa mm. vanhustenhoidossa (Schönberg, 2017) sekä muistisairaiden hoidossa (Helsingin Kaupunki, 2020). Toistaiseksi ei ole kuitenkaan onnistuttu kehittämään hoivan käyttöön tarkoitettua robottia, joka voisi kokonaan korvata ihmisen työn ikääntyneiden auttamisessa heidän jokapäiväisessä toiminnassaan. Valvontalaitteet, automaattiset lääkeannostelijat, robottilemmikit, matkapuhelinten läsnäololaitteet ja sairaalalogistiikka ovat jo käytössä, mutta ne kykenevät vain yksinkertaisiin puhekielisiin

vuorovaikutuksiin tai vaatimattomiin toistuviin tehtäviin, eivät tilannetajua vaativaan päivittäiseen toimintaan. (Van Aerschot & Parviainen, 2020.)

Kokonaisvaltaisen, kaikenkattavan monitoimirobotin suunnittelu ja kehitys on osoittautunut vaikeaksi. Hoivarobotit joita tällä hetkellä kehitetään ovat ennemmin suunniteltu toteuttamaan muutamia tiettyjä tehtäviä, kuin kokonaisvaltaista hoitoa. Van Aerschot ja Parviainen (2020) jakaa hoivarobotit kahteen kategoriaan: tehokkaisiin (tai utilitaristisiin) ja affektiivisiin (tai sosiaalisiin) niiden suunnittelustrategian mukaan (Sullins 2009). Robottien jakaminen tehokkaan suunnittelun tuotteisiin ja affektiivisen suunnittelun tuotteisiin on hyvin karkeaa, koska monet hoivarobotit edustavat näiden kahden välimaastoa. Toinen mahdollinen jako olisi jakaa robotit ns. ”älyttömiin” ja ”älyllisiin” laitteisiin, jossa tehokkaan suunnittelun robotit kuuluvat ensimmäiseen kategoriaan, ja sosiaaliset toiseen. Tämäkään jako ei kuitenkaan ole täysin yleispätevä, joten hoivarobottikohtaisten erojen esiintuomiseksi käytetään tässä työssä mm. Van Aerschotin ja Parviaisen käyttämää jakoa. Jako on hyödyllinen, jotta voidaan ymmärtää erot erilaisten hoivarobottien ominaisuuksien ja käyttötarkoituksien välillä. Erilaiset ominaisuudet ja käyttötarkoitukset vaikuttavat esimerkiksi laitteiden riskiprofiiliin, joten niillä on selkeitä eroja kyberturvallisuuden näkökulmasta.

2.2.3 Tehokkaan suunnittelun tuotteet

Tehokkaan suunnittelun on tarkoitus tuottaa robotteja, jotka voivat tehdä sellaisia tehtäviä, jotka eivät vaadi esimerkiksi harkintakykyä ja tilannetajua, tai muita ihmisen sosiaalisia tai käytännön taitoja. Tehokkaassa suunnittelussa hoito nähdään sarjana aktiviteetteja tai instrumentaalisia tehtäviä, jotka ovat korvattavissa teknologisilla ratkaisuilla ja robottilaitteilla kustannusten leikkaamiseksi, tehokkuuden lisäämiseksi sekä ajan ja ihmisen työvoiman säästämiseksi. (Van Aerschot & Parviainen, 2020.)

Robotit, jotka on suunniteltu työkaluiksi ja laitteiksi ihmisen toiminnan automatisoimiseksi, noudattavat tehokkaan suunnittelun mallia. Tämän suunnittelustrategian tavoitteena on kehittää robotteja, jotka ovat mahdollisimman itsenäisiä ja korvaavat ihmisen avun jonkin tietyn tehtävän osalta. Tällaisia tehtäviä ovat mm. kodin puhtaana pitäminen (robottipölynimuri), lääkkeiden toimittaminen (lääkkeiden annostelurobotti) ja auttaminen raskaiden taakkojen nostamisessa ja siirtämisessä (puettava ulkoinen tukiranka eli exoskeleton), liikkumisen tukeminen (robottikävelijä) tai syömisen avustaminen (ruokintarobotti). (Sullins 2009.) Esimerkiksi ruokintarobotin (esim. Obi-robotin) idea on, että henkilö, joka ei itse kykene syömään ei tarvitse ihmisen apua syömiseen, koska robotti ruokkii ruokaa henkilön suuhun (Van Aerschot & Parviainen, 2020). Toinen vastaava esimerkki tehokkaan suunnittelun mallista on ruotsalaisten kehittämä Poseidon-suihkurobotti, jonka tehtävä on helpottaa apua tarvitsevan ihmisen peseytymistä (Robotics Care, 2021).

2.2.4 Affektiivisen suunnittelun tuotteet

Affektiivisella ohjelmoinnilla tarkoitetaan koneen toiminnallista muotoilua ja ohjelmointia siten, että se vetoaa käyttäjän tunteisiin herättämällä esimerkiksi empatian kokemuksia (Särkikoski ym. 2020, 277.) Affektiivisen suunnittelun ensisijainen tavoite on kehittää interaktiivisia robotteja, jotka voisivat toimia seuralaisina ja sosiaalisina kumppaneina. Affektiivinen suunnittelustrategia perustuu näkemykseen, jonka mukaan ihminen on luonnostaan sosiaalinen olento, ja pyrkii vastaamaan ihmisten sosiaalisiin tarpeisiin ja lieventämään yksinäisyyttä tai sosiaalista eristäytymistä. Esimerkkejä mm. ikääntyneiden ihmisten hoitamiseen käytetyistä sosiaalisista roboteista ovat lemmikkimäinen robotti Paro ja pieni humanoidi NAO / Zora. Paro on interaktiivinen hylkeen näköinen robotti, jota käytetään enimmäkseen terapeuttisena välineenä ahdistuksen, masennuksen ja levottomuuden lievittämiseksi muistihäiriöpotilailla. NAO / Zora-robottia voidaan käyttää vanhusten hoidossa esimerkiksi liikunnan avustamiseen, musiikin soittamiseen, tanssiliikkeiden näyttämiseen, tarinoiden kertomiseen sekä muisti- ja arvauspelien pelaamiseen (Van Aerschot & Parviainen, 2020.)

2.2.5 Hoivarobotit osana terveydenhuollon toimintaympäristöä

Hoivarobotteja ja muuta hoivateknologiaa suunnitellaan avuksi päivittäisiin toimiin kuten siivoamiseen, syömiseen, pukeutumiseen, peseytymiseen, kognitiivisten kykyjen harjoittamiseen sekä sosiaalisen kanssakäymisen tueksi, seuraksi ja viihdyttäjiksi. Edellä mainittujen ominaisuuksien ja käyttötarkoitusten lisäksi niitä suunnitellaan tukemaan hoivaa ja hoitoa etäyhteyksin. Tällä hetkellä odotuksia ladataan robotteihin, jotka kykenisivät omatoimisina ja monitoimisina apureina suorittamaan ihmisten tekemiä tehtäviä. (Särkikoski ym. 2020, 115-116.) Toistaiseksi hoivan robotisaatio on kuitenkin varhaisessa vaiheessa, ja robotteja käytetään hoivatyössä hyvin vähän, eikä niitä juuri ole vielä käytössä kodeissa tai kotihoidossa. (Särkikoski ym. 2020, 115-116; Van Aerschot & Parviainen, 2020.)

Kun hoivarobotteja kehitetään terveydenhuollon (kuten vanhusten hoivan) tarpeisiin, on yksi suurimmista ongelmista kehittyneiden robottiraajojen puute. Kehittyneiden robottiraajojen puutteen takia on vaikea kehittää robotteja, jotka sopisivat esimerkiksi pukeutumisessa, peseytymisessä tai wc-käynneissä avustamiseen. Kun terveysteknologialle asetettuja tiukkoja turvallisuuskriteerejä sovelletaan hoivarobotiikkaan, on suunnittelijoiden tähän asti täytynyt kehittää joko tehokkaan suunnittelun mallin mukaisia, tai affektiivisen suunnittelun mallin mukaisia robotteja, jotka keskittyvät yksinkertaiseen toimintaan, kuten viihdyttämiseen tai tietyn yksinkertaisen hoitotyön helpottamiseen. (Van Aerschot & Parviainen, 2020.)

Hoivarobotiikan kehittämiseen liittyy myös robotiikan eettisyyteen liittyviä huolia, jotka korostuvat terveydenhuollon alalla. Särkikosken ym. (2020, 115) teoksessa pohditaan mm. sitä, vapauttaisivatko robotit hoitajien ja omaisten aikaa käytännöllisten toimien ja tehtävien

hoitamisesta inhimilliseen kohtaamiseen ja vuorovaikutukseen, vai kävisikö niin että robotit korvaisivat ihmiskontakteja ja inhimillistä vuorovaikutusta. Van Aerschot & Parviainen (2020) artikkelista ilmenee huolenaihe siitä, minkälaisia todellisia hyötyjä viihdyttävät sosiaalirobotit, jotka eivät suorita fyysisiä ja konkreettisia hoitotehtäviä tarjoavat, verrattuna paljon halvempaan nykyiseen jo käytössä olevaan tekniikkaan. Huolen taustalla on ajatus siitä, että hoivarobotteja kehittävät yritykset lisäävät pääasiassa terveydenhuollon kustannuksia ja elektroniikkaromua tarjoamatta todellisia ratkaisuja ikääntyneiden hoitotarpeisiin. Lisäksi tutkimus nostaa esiin kysymyksen siitä, onko hoivarobotiikan kehityksen taustalla pääasiallinen tavoite löytää terveydenhuollon ekosysteemiin eettisesti ja sosiaalisesti kestäviä ratkaisuja, jotka parantavat hyvinvointia, laadukasta hoitoa ja ikääntyneiden tasa-arvoa, vai tuottaa hyödykkeitä hoivarobottien muodossa niille, joilla on varaa niitä ostaa.

Hoivarobotiikan turvallisuus on eettisyyden lisäksi hoivarobottien kehitykseen liittyvä osa-alue, johon liittyy erityispiirteitä terveydenhuollon toimintaympäristössä. Terveydenhuollon toimintaympäristö asettaa erityisvaatimuksia robottien fyysisen toimintakyvyn lisäksi niiden kyberturvallisuudelle koska terveydenhuoltoala on sektorina haavoittuvaisempi kyberhyökkäyksille. Kyberturvalla on iso rooli hoivarobotiikkaan ja hoidon turvallisuuteen liittyvissä oikeudellisissa kysymyksissä. Kyberturvallisuudella sosiaali- ja terveydenhuollossa turvataan hoidon ja palvelun laadukkuutta ja tehokkuutta. Tietoturvallisuus ja tietosuoja liittyvät kiinteästi kyberturvallisuuden kokonaisuuteen. (Sosiaali- ja terveysministeriö, 2019.)

2.2.6 Robotiikan etiikka – Roboetiikka

Etiikka tutkii oikeaa ja väärää sekä hyvää ja pahaa, ja on yksi käytännöllisen filosofian perinteisistä osa-alueista. Käytännöllisyys viittaa toimintaan, jota ihmiset tekevät yhdessä ja yksin, toisilleen ja itselleen, yksityisesti tai osana laajempaa ryhmää tai instituutiota. Etiikka käsittelee hyvää ja pahaa, arvoja ja normeja, oikeuksia ja velvollisuuksia (Malkavaara 2020), ja sitä, onko jokin teko moraalisesti oikein tai väärin (Noponen 2020.) Etiikkaa ohjaa meitä ajattelemaan, tekemään valintoja sekä arvioimaan omaa ja muiden toimintaa, ja sitä tulisi soveltaa kaikkeen tekemiseen, jotta voimme punnita mitä haluamme ja mitä emme halua tehdä.

Teknologian kehittyessä robottien toiminta kehittyy, robotit yleistyvät ja ne vaikuttavat enenevissä määrin elämäämme, joten eettisen ajattelun tulisi kattaa oman toimintamme lisäksi myös robottien kautta suoritettujen toimien arviointia. Teknologian kehittyessä on tärkeää pystyä hallitsemaan kehityksen suunta myös eettisestä näkökulmasta. Roboetiikka on moderni monitieteinen tutkimusala, joka tutkii ja yrittää ymmärtää ja säännellä robotiikkatekniikan, erityisesti älykkäiden ja autonomisten robottien aiheuttamia eettisiä

vaikutuksia ja seurauksia yhteiskunnassamme. Roboetiikan ensisijaisena tavoitteena on ohjata robottien moraalista suunnittelua, kehitystä ja käyttöä ihmiskunnan eduksi. (Tzafestas 2018.)

Tutkijat eri tieteenaloilta, kuten robotiikka, tietojenkäsittelytiede, tietotekniikka, automaatio, filosofia, laki, psykologia jne. ovat yrittäneet vastata robottitekniikan kehittämistä ja käyttöä koskeviin eettisiin kysymyksiin jo vuosikymmenten ajan. Tazafestas (2018) listaa eettisiksi perusongelmiksi mm. robottien kaksoiskäytön (eettinen ja epäeettinen käyttö), pyrkimyksen robottien antropomorfismiin eli inhimillistämiseen, sekä robotiikan vaikutuksen varallisuuden ja vallan oikeudenmukaiseen jakautumiseen. Kuten edellä jo mainittiin, on robotiikkaan liittyvässä eettisessä keskustelussa otettu kantaa myös mm. ekologisiin kysymyksiin (kuten energiankulutukseen ja elektroniseen jätteeseen), hoitorobotiikkaan liittyvään politiikkaan, hoivarobotiikan kehityksen taustalla vaikuttaviin taloudellisiin motiiveihin, sekä hoivarobotiikkaan ja hoidon turvallisuuteen liittyviin oikeudellisiin kysymyksiin. (Van Aerschot & Parviainen, 2020.)

Erityisen tärkeitä ovat kuitenkin eettiset kysymykset, jotka koskevat niitä robotiikan alueita, jotka ovat suoraan vuorovaikutuksessa ihmisten kanssa, kuten erilaiset hoiva- ja apurobotit. (Tzafestas 2018.) Vanhusten hoitoon liittyvässä robotiikassa suurimpia eettisiä huolenaiheita ovat mm. ihmisarvoon, itsenäisyyteen ja yksityisyyteen, sekä perustavanlaatuisiin kysymyksiin kuten hoitoarvoihin, tarkkaavaisuuteen, vastuullisuuteen, osaamiseen ja vastavuoroisuuteen liittyvät eettiset kysymykset (Van Aerschot & Parviainen, 2020). Saisiko nostamiseen tarkoitettu robotti ihmisen kokemaan kontrollin menettämistä ja tuntemaan olonsa esineellistetyksi? Vaarantaako monitoroiva robotiikka ihmisten yksityisyyden? Liittyykö sosiaalisiin robotteihin iäkkäitä ihmisiä infantilisoivia piirteitä, kun robotit simuloivat kiinnostusta ja vastavuoroisuutta ja saavat siten ihmisen luulemaan, että robotti kykenee inhimillisiin tunteisiin? (Särkikoski ym. 2020, 139-140.) Vanhusten hoidon lisäksi erityispiirteitä hoivarobotiikan etiikkaan tuo kognitiivisiin häiriöihin, dementiaan ja vammaisuuteen liittyvien haavoittuvuuksien erityispiirteet. (Van Aerschot & Parviainen, 2020.)

Eettiset arvot vaikuttavat vahvasti myös laitteiden turvallisuuden kehittämiseen. Eettiset arvot yhdessä mm. tietosuojaan ja tuoteturvallisuuteen liittyvien lakien ja säädösten kanssa ohjaavat kyberturvallisuuden suunnittelua ja toteutusta. Kyberturvallisuus ja etiikka liittyvät vahvasti toisiinsa, koska kyberturvaan liittyy eettisiä arvokonflikteja, ja puutteellinen kyberturva voi johtaa tilanteeseen, jossa eettisiä arvoja ei kunnioiteta. Eettinen arvokonflikti hoivarobotin turvallisuuden näkökulmasta on esimerkiksi se, että liian vähäinen panostus kyberturvaan on pahimmillaan uhka ihmisen fyysiselle turvallisuudelle, yksityisyydelle, ja ihmisarvolle, kun taas liian suuri panostus kyberturvallisuuteen on ristiriidassa mm. itsemääräämisoikeuden ja vapauden kanssa.

2.3 Kyberturvallisuus ja tietoturvallisuus

Verkkoon kytköksissä olevien laitteiden, järjestelmien ja datan suojaamisen ja turvallisuuden varmistamiseksi tarvitaan sekä tietoturvaa, että kyberturvaa. Kyberturva ja tietoturva ovat termejä, jotka helposti sekoitetaan keskenään. Molempien on tarkoitus taata turvallisuus verkossa ja digitaalisissa ympäristöissä, mutta niiden toiminnan tavoitetiloilla on selvä ero. Tässä luvussa pyrin selventämään mitä kyberturva ja tietoturva ovat, ja miksi ne ovat tärkeitä erityisesti terveydenhoitoalan ja hoivarobottien näkökulmasta.

2.3.1 Tietoturva

Tietoturvallisuus on laaja käsite, jolla tarkoitetaan tiedon saatavuuden, eheyden ja luottamuksellisuuden takaamista (Rousku 2014, 47). Turvallisuuskomitean (2018) laatiman sanaston mukaan tietoturvan määritelmä on: ”järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus”. Tietoturvaan kuuluu mm. tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Käytännön järjestelyjä, joilla tietoturvallinen ympäristö luodaan ovat esimerkiksi kulunvalvonta, tilojen lukitus, asiakirjojen turvallinen säilytys ja hävitys, tietojen salaus ja varmuuskopiointi sekä palomuurin, virustorjuntaohjelman ja varmenteiden käyttö. (Turvallisuuskomitea, 2018.)

2.3.2 Luottamuksellisuus

Luottamuksellisuudella tarkoitetaan sitä, että jos tieto on luokiteltua tai muuten salassa pidettävää, sen voivat saada käyttöönsä vain ne, joilla on tiedonsaanti- tai käyttöoikeus. Luottamuksen säilymisellä pyritään takaamaan, että sivullisilla ole pääsyä edellä mainittuihin tietoihin. (Rousku 2014, 47; Turvallisuuskomitea, 2018.) Luottamuksellisuus voidaan toteuttaa käyttöoikeuksien hallinnalla. Käyttöoikeuksien hallinta käytännössä voi olla esimerkiksi, että käyttäjille annetaan järjestelmiin vain sellaiset oikeudet, jotka ovat tarpeen tehtävien hoitamisen kannata, ja järjestelmien käyttö edellyttää autentikointia. (Rousku 2014, 47.)

2.3.3 Eheys

Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa (Turvallisuuskomitea, 2018), ja että tietoa saavat muuttaa vain sellaiset henkilöt, joilla on siihen tarvittavat käyttöoikeudet (Rousku 2014, 49). Mitä kriittisemmästä järjestelmästä on kysymys, sitä tärkeämpää on tietojen eheyden säilyminen, ja kyky palauttaa hallitsemattomasti muuttuneet tiedot. Kyberturvallisuuden näkökulmasta mm. henkilö- ja väestötiedot, terveydenhoitoon liittyvät tiedot, julkishallinnon johtamisen järjestelmät, pankkijärjestelmät, verotus, maanomistus- ja kiinteistötiedot sekä vakuutustiedot ovat sellaisia järjestelmiä ja tietoja, jotka eivät saa muuttua hallitsemattomasti ja jotka pitää kaikissa olosuhteissa olla palautettavissa, jos eheys on vaarantunut (Rousku 2014, 48-49).

2.3.4 Saatavuus

Saatavuudella tarkoittaan, että tieto on saatavissa ja hyödynnettävissä silloin kuin sitä tarvitaan (Turvallisuuskomitea, 2018) palvelussa tai ICT-järjestelmässä toiminnolta edellyttämässä vasteajassa (Rousku 2014, 50). Käytännössä yhteiskunnan digitalisoituminen on johtanut siihen, että palveluita pyritään pitämään toiminnassa sadan prosentin vasteajalla, pois lukien pakolliset huoltokatkot (Rousku 2014, 50).

2.3.5 Haavoittuvuus

Järjestelmissä voi olla haavoittuvuuksia, joiden takia tietoturva vaarantuu. Haavoittuvuus on järjestelmässä oleva vika, joka mahdollistaa järjestelmän käyttämisen tavalla, jota varten sitä ei ole suunniteltu (Rousku 2014, 53). Haavoittuvuuksia voi olla tietojärjestelmissä, prosesseissa ja ihmisen toiminnassa. Haavoittuvuudet kattavat kaikki ne heikkoudet, jotka mahdollistavat vahingon toteutumisen tai jota voidaan käyttää vahingon aiheuttamisessa. (Turvallisuuskomitea 2018.)

2.3.6 Kyberturvallisuus

Tietoturvan ja kyberturvan suurin ero on, että tietoturva keskittyy tietojen luottamuksellisuuden, eheyden ja saatavuuden takaamiseen, kun taas kyberturva kattaa huomattavasti laajemman kokonaisuuden. Turvallisuuskomitean (2018) sanaston mukaan kybertuvallisuus tarkoittaa tavoitetilaa, ”jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan”. Kybertoimintaympäristöllä tarkoitetaan yhdestä tai useammasta digitaalisesta tietojärjestelmästä muodostuvaa toimintaympäristöä jolle tunnusomaista on tietoverkkojen (etenkin internetin) käyttö datan ja informaation varastointiin, muokkaamiseen ja siirtoon. Verkkojen lisäksi ympäristöön kuuluvat datan ja informaation käsittelyyn liittyvät fyysiset rakenteet. (Rousku 2014, 56-57; Turvallisuuskomitea 2018.)

Kyberturvallisuuden vaarantuminen johtuu usein tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä (Turvallisuuskomitea 2018). Useimmat toteutuneet kyberhyökkäykset tehdään internetin kautta, ja niiden avulla on päästy heikentämään tietoturvallisuutta esimerkiksi tietoja muuttamalla (eheyden vaarantuminen), vuotamalla tietoja (yksityisyyden suojan ja tietosuojan vaarantuminen) sekä heikennetty palvelujen käytettävyyttä esimerkiksi palvelunestohyökkäyksillä (saatavuuden vaarantuminen). (Rousku 2014, 57.)

2.3.7 Kyberrikollisuus

Kyberrikollisuus on rikollisuutta, joka muodostuu viestintäverkkoja ja tietojärjestelmiä hyödyntäen tehdyistä sekä niihin kohdistuvista rikoksista. Kyberrikollisuuden vaikutukset

kohdistuvat tietojärjestelmien kautta niin valtioihin, yksityisiin kansalaisiin kuin organisaatioiden toimintaan. Kyberrikoksia ovat mm. tietojen kalastelu, identiteettivarkaudet ja palvelunestohyökkäykset. Henkilöä, joka tunkeutuu tai vaikuttaa tietoverkkoon, tietojärjestelmään tai niiden sisältämään tietoon ja käyttää ohjelmaa, palvelua tai muuta resurssia luvattomasti, kutsutaan hakkeriksi. Vihamielinen hakkeri saattaa esimerkiksi tuhota tietojärjestelmästä tietoja tai käyttää järjestelmää omiin tarkoituksiinsa. (Turvallisuuskomitea 2018.)

2.3.8 Kyberturva sosiaali- ja terveydenhuollon alalla

Digitalisaatio ja teknologian nopea kehitys ovat mahdollistaneet että sosiaali- ja terveydenhuollon asiakas- ja potilastyöhön tarvittavat tiedot ovat saatavilla digitaalisesti. Alan ammattilaiset käyttävät digitaalisia palveluita työssään päivittäin. Palveluiden toteutuksessa merkittävässä roolissa ovat tieto- ja viestintäteknologia, kuten mobiiliteknologiaan, pilvipalveluihin, tekoälytoimintaan, IoT (Internet of things) ja ICMT1 (Information, Communication and Medical Technology) -teknologia. Tietojärjestelmien käytöllä tavoitellaan potilaiden ja asiakkaiden etua hoidon ja palvelun laadun sekä tehokkuuden paranemisella. (Sosiaali- ja terveysministeriö, 2019.)

Sosiaali- ja terveydenhuollossa käsitellään paljon asiakas- ja henkilötietoja, sekä asiakkaisiin liittyvää arkaluonteista dataa, jonka vuoksi on kiinnitettävä erityistä huomiota tietojen luottamuksellisuuden suojaamiseen yksityisyyden takaamiseksi. Asiakaspalvelu ja potilaan hoito perustuvat tietoihin, joiden on oltava oikeita ja yhdistettävissä oikeaan potilaaseen. Tietojen tulee myös olla saatavilla silloin kun niitä tarvitaan, joten turvallisuudessa korostuvat myös tietojen eheys ja saatavuus. (Sosiaali- ja terveysministeriö, 2019.)

Tietoliikenne vaatii tietoverkkoja, joten verkkojen turvallisuus ja niiden turvallinen käyttö on myös olennainen osa kyberturvallisuuden toteutumista. Suurin osa sosiaali- ja terveydenhuollon järjestelmien välisestä tietoliikenteestä tapahtuu erillisissä verkoissa, ja on siten valvottua ja suojattua. Osa pienistä toimialan toimijoista käyttää palveluita kuitenkin julkisen verkon kautta, mikä altistaa erilaisille julkisen verkon häiriöille. Myös esimerkiksi Omakanta-palvelu, jossa terveydenhuollon asiakkaat voivat nähdä itseään koskevia tietoja omilla välineillään ja omissa ympäristöissään, toimii julkisten verkkojen kautta. Julkisissa verkoissa ja tietoturvallisesti harjaantumattomissa käyttäjissä on suurempi riski, että arkaluontoisia tietoja saattaa vuotaa julkisuuteen käyttäjien omien toimenpiteiden kautta. (Sosiaali- ja terveysministeriö, 2019.)

Sosiaali- ja terveydenhuoltoon kohdistuu kyberuhkia päivittäin. Teknologian nopea kehitys on lisännyt haasteita tuottaa palveluita tietoturvallisesti ja vaatimusten mukaisesti. Kyberhyökkäykset ovat tapahtuneet kuitenkin yleensä joko julkisen verkon puolella tai paikallisissa järjestelmissä, jolloin ne eivät ole merkittävästi vaikuttaneet järjestelmien

kriittisiin palveluihin. Hyökkäykset ovat usein olleet palvelunestohyökkäyksiä suoraan esimerkiksi Kanta-palveluita vastaan tai verkon kriittisiä palveluita, kuten Väestörekisterikeskuksen palveluja vastaan. Kyberrikolliset ovat erityisesti vuosina 2016–2018 suosineet myös tiedostoja salaavia kiristyshaittaohjelmia. Lisäksi sosiaali- ja terveydenhuollon organisaatioissa on kohdattu henkilöstön sähköpostin kautta tulevia tietojenkalasteluyrityksiä. (Sosiaali- ja terveysministeriö, 2019.)

Hoivateknologian yleistyminen ja erilaisten ohjelmistoja sisältävien laitteiden lisääntyminen voi aiheuttaa lisää haavoittuvuuksia kyberturvaan. Ohjelmistoista paljastuu usein virheitä eli haavoittuvuuksia, joiden hyväksikäyttö voi vaarantaa kyberturvan ja laitteiden oikeanlaisen käytön. Laitteet vaativat päivityksiä virheiden ja haavoittuvuuksien korjaamiseksi. Esimerkiksi sairaalaympäristöissä on käytössä erilaisia lääkinnällisiä laitteita, joihin valmistajalla on pääsy etäyhteyksien kautta mm. ylläpitotoimien suorittamiseksi. Lisääntyvien laitteiden käytössä piilee myös riski, että käytettävyydeltään kankeat ohjelmistot voivat houkutella laitteiden käyttäjiä kiertämään tietoteknisiä suojausmekanismeja. Käyttäjät saattavat esimerkiksi jättää oletussalasanat vaihtamatta, tai käyttää järjestelmiä samalla käyttäjätunnuksella. (Sosiaali- ja terveysministeriö, 2019.)

Hoivarobottien on ennustettu olevan potentiaalien ratkaisu mm. vanhustenhoivan haasteisiin väestön ikääntyessä, mutta käytännössä hoivarobottien käyttöönotot tarkoittavat lisääntyvää määrää laitteita jo ennestään kyberturvan näkökulmasta erityispiirteitä sisältävään toimintaympäristöön. Lisääntyvä määrä laitteita tarkoittaa lisääntynyttä määrää ohjelmistoja, joissa voi olla haavoittuvuuksia. Lisäksi lisääntyvä määrä laitteita tarkoittaa entistä useampaa verkkoon kytköksissä olevaa laitetta, ja lisääntyvää määrää loppukäyttäjiä. Loppukäyttäjien digitaidot, tieto ja toiminta voi olla puutteellista kyberturvallisuuden ja tietoturvallisuuden näkökulmasta. Käytännössä hoivarobottien käyttöön liittyy toimintaympäristön kyberturvan kannalta vähintään samat riskit kuin edellä mainittuihin lääkinnällisen laitteen luokituksen omaaviin laitteisiin. Toimintaympäristön lisäksi uhkia voi kohdistua myös suoraan laitteisiin ja niiden loppukäyttäjiin. Lisäksi erilaisten laitteiden käyttö osana sosiaali- ja terveydenhuoltoa kodeissa ja kodinomaisissa ympäristössä luo kyberturvan toteutumiseen uusia ulottuvuuksia.

2.4 Hoivarobottien kyberturva

Roboteilla on potentiaalia helpottaa arkea, luoda turvallisuuden tunnetta sekä toimittaa erilaisia tehtäviä, mutta kääntöpuolena ne kärsivät vastaavista kyberturvaongelmista, joista tietokoneet ovat kärsineet jo vuosikymmeninen ajan. Robotit pystyvät tunnistamaan, käsittelemään ja tallentamaan ympäröivää maailmaa, ja ne keräävät jatkuvasti dataa. (Lera, Llamas, Guerrero & Olivera, 2017.) Robottien toiminta (kuten navigointi, puhe, objektien tunnistus jne.) vaatii raskasta laskentaa, joka on mahdollistettu pilvipalvelujen avulla.

Toisiinsa kytkettyjen järjestelmien ja laitteiden määrän lisääntyessä lisääntyy myös mahdollisuus, että järjestelmät sisältävät haavoittuvuuksia, ja haitallisten hyökkäysten riski kasvaa. (Fosch-Villaronga & Mahlerb, 2021.)

Kyberturva hoivarobottien näkökulmasta on hankala käsite, koska kuten aiemmin jo mainittiin, ei ole täysin yksiselitteisesti määriteltävissä onko robotti hoivarobotti muun kuin käyttötarkoituksen tai käyttöympäristön perusteella. Hoivarobotti on kuitenkin robotti siinä missä muutkin, jolloin sen turvallisuuteen voi kohdistua laajalti erilaisia uhkia. Uhkat voivat kohdistua mm. suoraan robottiin, sen sisältämään ja keräämään dataan, sekä loppukäyttäjän henkiseen että fyysiseen terveyteen.

2.4.1 Tulkinnanvaraisuuden ongelma

Hoivarobottien kyberturvaan liittyvästä lakiperustasta on ilmestynyt tieteellinen artikkeli alkuvuodesta 2021. Fosch-Villarongan ja Mahlerbin (2021) artikkelista “Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots.” käy ilmi muun muassa, että EU:n lainsäädännössä ei ole selkeää hoivarobottien kyberturvaa koskevaa sääntelyä, vaikka hoivarobotit ovat suorassa yhteydessä heikommassa asemassa olevien kanssa, kuten lasten, vanhusten ja vammaisten kanssa. Useasta palvelu- ja hoivarobotteja koskevasta artikkelista käy lisäksi ilmi, että palvelu- ja hoivarobotteihin liittyviä kyberturvauhkia on tutkittu huomattavasti vähemmän, kuin esimerkiksi teollisiin ympäristöihin tarkoitettujen robottien kyberturvaa (Lera, Llamas, Guerrero, & Olivera, 2017; Fosch-Villaronga & Mahlerb, 2021). Selkeän määrittelyn puuttuminen johtaa monimutkaiseen tilanteeseen, jossa hoivarobottien kyberturvallisuuteen liittyviä velvoitteita ja vastuita voidaan tulkita monin eri tavoin.

Erilaiset tuoteturvallisuuteen liittyvät säädökset eivät suoraan ota kantaa, mutta voivat vaikuttaa robottien kyberturvallisuuteen. Tietyillä aloilla on myös alakohtaisesti sääntelyä erilaisten tuotteiden yleiseen turvallisuuteen liittyen (mm. radiolaitteet, lääketieteelliset laitteet, lelut jne.). Robottien näkökulmasta on usein kuitenkin epäselvää, miten erilaiset robotit voidaan luokitella, koska luokittelu riippuu niiden käyttötarkoituksesta. Asiaa hankaloittaa entisestään teollisuuden pyrkimys luoda uusia välituoteryhmiä, kuten esimerkiksi ”henkilökohtainen hoito”, johon lääkinnällisten laitteiden sääntely ei päde, vaikka robotit on kehitetty hoivan tarkoituksiin. Eurooppalaiset kuluttajajärjestöt ovat arvostelleet tuotelainsäädännössä vallitsevaa turvallisuuskäsitettä vanhentuneeksi, koska se ei kata tuotteiden liitettävyyteen ja hakkerointiin liittyviä turvallisuusriskejä. Kyberturvallisuuden sääntelyä hankaloittaa myös se, että kyberturvallisuuteen liittyvät uhkat muuttuvat jatkuvasti; uusia laitteita ja niiden liitettävyyttä kehitetään, olemassa olevat ohjelmistot vanhenevat ja toimintaympäristö muuttuu. (Fosch-Villaronga & Mahlerb, 2021.)

Edellä mainittujen lisäksi on muitakin yleisiä lakeja ja säädöksiä, jotka osittain koskevat myös hoivarobottien kyberturvaa. Koska kyberturva kattaa myös tietoturvan, on yksi esimerkki tällaisesta säädöksestä GDPR (General Data Protection Regulation), jonka mukaan henkilökohtaisia tietoja sisältävät ja käsittelevät laitteet ja ohjelmistot ovat velvoitettuja toteuttamaan asianmukaiset toimenpiteet asiaankuuluvan turvallisuuden tason varmistamiseksi. (Fosch-Villaronga & Mahlerb, 2021.)

Vastuu hoivarobottien kyberturvaan liittyen voi hämärtyä, koska hoivarobottien kyberturvallisuuden toteutumista eivät ohjaa mitkään yleispätevät lait tai säädökset. On huolestuttavaa, että hoivarobottien kyberturvaa koskeva sääntely on osittain puutteellista sekä tulkinnanvaraista, ottaen huomioon hoivarobottien toimintaympäristön ja käyttötarkoituksen. Loppukäyttäjillä on toki mahdollisuus arvioida, millaisia riskejä he ovat turvallisuuden suhteen valmiita ottamaan. Arviointia vaikeuttaa kuitenkin se, että usein loppukäyttäjillä ei ole tarvittavaa tietoa ja taitoa arvioida laitteiden turvallisuutta, eikä valmistaja ole velvollinen kertomaan niistä. Jos ihmisten hoivassa otetaan enenevissä määrin käyttöön hoivarobotteja, kuka kantaa vastuun kyberturvallisuuden toteutumisesta?

2.4.2 Hoivarobotin kyberturva käytännössä

Lera ym. (2017) jakavat tutkimuksessaan kyberturvan kahteen osa-alueeseen: turvallisuus ja yksityisyys. Ihmiset ovat usein huolissaan uhkista, joita hakkeroidut robotit voivat aiheuttaa fyysiselle omaisuudelle tai koskemattomuudelle. Kotona käytettävien hoivarobottien osalta fyysisiä turvallisuusongelmia ovat mm. niiden mahdollisuus vahingoitta arvokasta omaisuutta tai pikkulapsia (törmäily, tuhopoltto jne.). Hakkeroidut robotit voivat myös vuotaa yksityistä ja arkaluonteista tietoa käyttäjistään, jolloin käyttäjän yksityisyys vaarantuu.

Leran ym. (2017) mukaan robotteihin kohdistuvilla kyberturvauhkilla voi olla kolme syytä: luonnolliset syyt (kuten luonnonkatastrofit), vahinko (inhimillinen erehdys), tai ulkopuolinen hyökkäys, joista voi aiheutua fyysisiä tai virtuaalisia vahinkoja. Fyysisiä vahinkoja ovat laitteen tuhoutuminen kokonaan tai osittain (häiriö), tai laitteen odottamaton käyttäytyminen. Virtuaalisiin vahinkoihin kuuluu lähinnä ohjelmistoihin liittyvät vahingot, jotka vaikuttavat laitteen normaaliin toimintaan virtuaalisella tavalla, esim. robotin keräämään, tallentamaan tai lähettämään dataan.

Kyberturvauhkat voivat aiheuttaa niin taloudellista, aineellista kuin psyykkistä vahinkoa loppukäyttäjille (robotin kanssa vuorovaikutuksessa olevat ihmiset), yrityskäyttäjille (yrityksille, jotka käyttävät robottia tiettyyn tehtävään), valmistajille ja myyjille, sekä kehittäjille. Kyberturvauhkat vaikuttavat eri toimijoihin eri tavoin. Esimerkiksi palvelurobotiikan ja hoivarobotiikan loppukäyttäjät ovat yleensä enemmän huolissaan yksityisyydestä, kun taas yrityskäyttäjät ovat enemmän huolissaan yrityksen maineesta. Loppukäyttäjät ovat myös enemmän huolissaan taloudellisista vahingoista, joita robotit voivat

aiheuttaa heidän omaisuudelleen, kun taas yrityskäyttäjät ovat enemmän huolissaan mahdollisista oikeusjutuista. (Lera ym. 2017.)

Robotin rakentaminen on teknisesti erittäin haastavaa monin tavoin. Fosch-Villarongan ja Mahlerbin (2021) mukaan ei olisi yllättävää, jos valmistajat keskittyvät ensisijaisesti robottien toimintojen kehittämiseen, kuin niiden turvaamiseen kaikilta kyberhyökkäyksiltä. Kilpailupaineet markkinoilla ovat kovat, ja voivat vaikuttaa negatiivisesti laitteiden kyberturvaan, koska kilpailupaineet painostavat valmistajia nopeaan markkinoille tuloon, jolloin tuotteiden turvallisuus pyritään turvaamaan vasta myöhemmin.

Kyberturvallisuuden lisääminen aiheuttaa myös kuluja valmistajille. Kyberturvauhkat eivät yleensä vaikuta suoraan valmistajaan, joten ne eivät siten välttämättä ole valmistajan prioriteetti. Fosch-Villarongan ja Mahlerbin (2021) mukaan on väitteitä, joiden mukaan kuluttajat jättävät usein tietoturvaongelmat huomiotta, ja arvostavat enemmän käytettävyyttä, toiminnallisuutta ja kilpailukykyisiä hintoja. Näin ollen kysynnässä ei niinkään vaikuta laitteiden kyberturva, eikä kysynnän laatu siten kannusta valmistajia panostamaan kyberturvan toteutumiseen.

Käytännössä kyberturvan toteutuminen edellyttää ennakointia ja riskien tunnistamista. Toisaalta investoimalla kyberturvallisuuteen tekniikan suunnittelusta lähtien voitaisiin edistää turvallisempaa tekniikkaa, josta voi olla hyötyä sekä käyttäjille että valmistajille pitkällä aikavälillä. Fosch-Villarongan ja Mahlerbin (2021) mukaan tutkimukset osoittavat, että kuluttajat ovat halukkaita priorisoimaan ja maksamaan enemmän turvallisuudesta ostaessaan verkkoon kytkettyjä tuotteita, jos turvallisuuden tasosta viestitään selkeästi. Selkeä viestintä on avainasemassa, koska käytännön tasolla ei ole selvää, osaavatko robottien hankkijat arvioida robottien kyberturvan tasoa. On lähes mahdoton erottaa ne robotit, joilla on korkea kyberturvallisuus roboteista, joilla ei ole optimaalista kyberturvallisuutta, jos kyberturvan tasosta ei viestitä selkeästi. Loppukäyttäjälle olisi hyödyllistä, jos turvallisuustaso välitetään ymmärrettävällä tavalla, kuten sertifikaatilla. (Fosch-Villarongan & Mahlerbin, 2021.)

2.4.3 Esimerkkejä hoivarobottien kyberturvauhkista

Erilaiset robotit, kuten palvelurobotit, sosiaaliset robotit ja hoivarobotit, herättävät huolia yksityisyydestä ja turvallisuudesta. Huoli on ymmärrettävää koska robotit ovat usein varustettuja kyvyllä aistia, käsitellä ja tallentaa ympäröivää maailmaa. Leran ym. (2017) mukaan sisäisten kameroiden, mikrofonien, kaiuttimien ja mobiililaitteiden ansiosta kaikki kauko-ohjattavat, langattomat, Wi-Fi:iin kytköksissä olevat robotit voivat olla riski käyttäjilleen, koska ulkopuolinen taho voi päästä käsiksi laitteisiin verkon kautta.

Huolenaihe on erityisen suuri roboteilla, jotka käyttävät kameroita esimerkiksi käyttäjien tunnistamiseen. Kotiympäristössä robotit voivat kuunnella keskusteluja tai ottaa kuvia

henkilökohtaisista tiedoista tai käyttäjästä. Julkisiin tiloihin sijoitetut robotit voivat mm. kerätä dataa ihmisten kiinnostuksen kohteista, nauhoittaa keskusteluja ja kloonata tunnistusmenetelmiä. (Lera ym. 2017.) Hyökkäykset voivat olla erityisen petollisia, koska loppukäyttäjän voi olla vaikeaa huomata, jos robottiin on hyökätty. Hyökkäyksen voi huomata esimerkiksi siitä, että robotti ei toimi normaalilla tavalla. On kuitenkin mahdollista että hyökkäyksen kohteena oleva robotti toimii myös täysin normaalisti, jolloin voi olla mahdotonta huomata, että siihen on hyökätty. (Lera ym. 2017; Fosch-Villaronga & Mahlerb, 2021.)

Fosch-Villaronga ja Mahlerb (2021) esittävät artikkelissaan käytännön esimerkin hyökkäyksestä hoivarobottiin. Esimerkkitapauksessa lähtökohtana on, että yksinelävällä vanhuksella on hoivarobotti kotonaan. Hoivarobotin tehtävä on mahdollistaa, että perheenjäsenet voivat etäyhteyden avulla valvoa vanhusta ja paikantaa hänet, mikäli hänen terveydentilansa heikkenee. Hoivarobotti on kytketty kodin langattomaan verkkoon, ja se on varustettu videokameralla, mikrofonilla ja kaiuttimella, jotta perhe voi näkö- ja ääniyhteydellä kommunikoida vanhuksen kanssa. Esimerkissä taloudellisesti motivoitunut hyökkääjä tunkeutuu kotiverkkoon, ja kaappaa robotin hallintaansa. Hyökkääjä pääsee näin tarkkailemaan vanhusta kameran ja mikrofonin kautta, ja voi mm. urkkia hänen tietojaan, kuten luottokorttitietoja, ja käyttää niitä omaksi hyödykseen. (Fosch-Villaronga & Mahlerb, 2021.)

Edellä mainittu esimerkki on vain yksi monista mahdollisista uhkaskenaarioista. Leran ym. (2017) mukaan on useita erilaisia tapoja hyökätä erilaisiin robotteihin, jotka pätevät myös hoivarobotteihin:

- ”Stealth attack”, on hyökkäys, jossa hyökkääjä pääsee manipuloimaan robotin sensorien toimintaa, ja siten aiheuttamaan esimerkiksi mobiilin robotin törmäämisen.
- ”Replay attack”, jossa on toinen tunnettu hyökkäys, jossa hyökkääjät pystyvät sieppaamaan järjestelmän viestinnän, ja manipuloimaan dataliikennettä, ja siten häiritsemään mm. sensorien toimintaa.
- ”False data injection”, on hyökkäys, jossa robotin käsittelemää dataa päästään muokkaamaan.
- ”Evesdropping”, eli salakuuntelu, on yksi yleisimmistä hyökkäyksistä robotteihin yksityisyyden näkökulmasta.
- ”Denial of Service” (palvelunestohyökkäys) on hyökkäys, jolla käytännössä lopetetaan robotin toiminta. DoS-hyökkäys ei välttämättä aiheuta suoraa vahinkoa itse laitteelle tai sen käyttäjälle, mutta estää robotin tarjoaman palvelun saannin.
- ”Remote access” on yksi vaarallisimmista hyökkäyksistä, jossa ulkopuolinen käyttäjä kaappaa laitteen, ja pystyy siten aiheuttamaan sekä yksityisyyteen että fyysiseen terveyteen liittyvää vahinkoa.

Erilaisiin robotteihin voi kohdistua erilaisia hyökkäyksiä riippuen siitä, missä ympäristössä robotit toimivat, ja mitä tehtäviä ne suorittavat.

2.4.4 Tehokkaan suunnittelun tuotteiden turvallisuusriskit

Tehokkaan suunnittelun tuottamat robotit ovat mahdollisimman itsenäisiä ja korvaavat ihmisen avun jonkin tietyn tehtävän osalta. Tällaisia tehtäviä ovat mm. kodin puhtaana pitäminen (robottipölynimuri), lääkkeiden annostelu (lääkkeiden annostelurobotti), auttaminen raskaiden taakkojen nostamisessa ja siirtämisessä (puettava exoskeleton), liikkumisen tukeminen (robottikävelijä) tai syömisen avustaminen (ruokintarobotti).

Maalaisjärjellä ajateltuna tällaisiin robotteihin kohdistuu enemmän fyysiseen turvallisuuteen liittyviä turvallisuusriskejä. Turvallisuuden takaamisen näkökulmasta on tärkeää, että tällaisten robottien hallinta säilyy kaikissa tilanteissa. Jos esimerkiksi liikkumisen tukemiseen käytettävä robottikävelijä hakkeroidaan, voidaan sen toimintaan vaikuttaa ulkopuolelta niin että se ei käyttäydykään odotetulla tavalla. Hakkeroitu robotti voi aiheuttaa esimerkiksi käyttäjän kaatumisen. Turvallisuusriskit eivät rajoitu kuitenkaan vain fyysiseen turvallisuuteen. Useita verkkoon kytköksissä olevia laitteita on onnistuttu hakkeroimaan, ja mm. LG:n robottipölynimureita on käytetty vakoiluun (Check Point 2017).

2.4.5 Affektiivisen suunnittelun tuotteiden turvallisuusriskit

Affektiivisen suunnittelun tuottamat robotit ovat usein interaktiivisia, ja toimivat seuralaisina ja sosiaalisina kumppaneina. Esimerkiksi Paro on interaktiivinen hylkeen näköinen robotti, jota käytetään enimmäkseen terapeuttisena välineenä ahdistuksen, masennuksen ja levottomuuden lievittämiseksi muistihäiriöpotilailla. Affektiivisen suunnittelun robotit sisältävät useimmiten sekä kameroita että mikrofoneja, joten jos turvallisuudesta ei ole huolehdittu asianmukaisella tavalla, voidaan hakkeroituja robotteja käyttää mm. vakoiluun ja salakuunteluun. Hakkeroitu robotti voi vaikuttaa siltä, että se toimii tarkoitetulla tavalla, ja koska tällaisille roboteille on tyypillistä vedota käyttäjän empatiakykyyn ja tunteisiin, ovat ne hakkeroituina mahdollisia välineitä myös tietojen kalasteluun ja manipulointiin. (Fosch-Villaronga & Mahlerb, 2021.)

3 Tutkimusmenetelmä

Tähän opinnäytetyöhön tutkimusmenetelmäksi valikoitui laadullinen tutkimus, koska laadullinen tutkimus on joustava tutkimustapa, joka mahdollistaa erilaisia lähestymis- ja analyysitapoja, ja tutkittavan asian tarkastelun tutkimuksen kohteena olevien henkilöiden näkökulmasta (Juhila 2021). Laadullinen tutkimus sopii hyvin tutkimusmenetelmäksi tutkimukseen, jonka tarkoitus on kartoittaa tutkimuksen kohteena olevien henkilöiden

(hoivarobotiikan asiantuntijoiden, kuten tutkijoiden ja hoivarobotiikan hankkeissa mukana olleiden, kehittäjien ja palveluntarjoajien) näkökulmaa siitä, mitä kyberturvauhkia hoivarobotteihin kohdistuu.

3.1 Tutkimukseen osallistujien valinta ja rekrytointi

Tässä tutkimuksessa haastateltavat valittiin harkinnanvaraisesti tarkoituksenmukaisuusperusteella. Toisin sanoen tutkimukseen valittiin henkilöitä, joilla on tietoa ja/tai kokemusta tutkittavasta ilmiöstä, tai edustavat jotain ryhmää, joka on tutkimuksen kannalta relevantti (Puusa & Juuti 2020, 84–85), eli haastateltaviksi kutsuttiin hoivarobotiikan asiantuntijoita, kuten tutkijoita, hoivarobotiikan hankkeissa mukana olleita, kehittäjiä ja palveluntarjoajia.

Asiantuntijoita lähestyttiin sähköpostitse, jonka yhteydessä kerrottiin mm. tutkimuksen tavoitteesta ja toteutuksesta. Haastattelukutsut liitteenä suomeksi ja englanniksi (Liite 1 & Liite 2). Haastattelukutsu lähetettiin ensin kaikille mahdollisille kotimaisille tahoille, joita internetin avulla löytyi, mutta vastausten vähyyden takia haastattelukutsua lähetettiin lisäksi ulkomaalaisille tahoille. Kun ensimmäiset haastateltavat löytyivät, käytettiin seuraavien osallistujien rekrytointiin lumipallo-otantaa, eli haastateltavilta pyydettiin kontakteja muihin tutkimukseen sopiviin henkilöihin.

3.2 Aineistonkeruu

Tutkimuksen aineistonkeruumenetelmäksi valikoitui haastattelu, jolla voidaan parhaiten selvittää tutkimuksen kohteena olevien henkilöiden omaa näkökulmaa. Haastattelutyypiksi valikoitui teemahaastattelu, koska se on vapaamuotoinen ja joustava haastattelumenetelmä. Teemahaastattelussa oletetaan, että tutkittavat ovat läpikäyneet tai kokeneet tietyn asian tai prosessin (Puusa & Juuti 2020, 112; Hirsjärvi & Hurme 2011, 47), jolloin voidaan olettaa, että haastattelun aihepiiri on haastateltavalle tuttu. Teemahaastattelussa ei ole tarkkoja kysymyksiä tai järjestystä, mutta haastattelun aihepiirit ovat kaikille haastateltaville samat (Hirsjärvi & hurme 2011, 47). Ennalta valittujen teemojen muodostama haastattelurunko antaa haastateltavalle vapauden kertoa kokemuksistaan ja ajatuksistaan laajemmin, ja mahdollistaa siten että haastattelusta saadaan laajasti sellaista ainesta, jota on myöhemmin mahdollista tulkita teorian avulla (Puusa & Juuti 2020, 112–113). Esihaastattelut ovat Hirsjärven (2011, 72) mukaan tärkeä osa teemahaastatteluja mutta mahdollisten tutkimukseen osallistuvien määrän vähyydestä johtuen varsinaisia esihaastatteluja ei toteutettu, vaan haastattelurunko (Liite 3) luotiin teoriaan perustuen ja sitä muokattiin paremmaksi ensimmäisen haastattelun perusteella. Lopulliset teemat muutettiin muotoon: hoivarobottien kyberturva tällä hetkellä, hoivarobottien mahdolliset kyberturvauhkat ja suurimmat riskit ja uhkat koskien hoivarobottien kyberturvallisuutta.

Osallistujien rekrytointihaasteiden vuoksi, tutkimukseen osallistumiskynnystä päätettiin madaltaa antamalla mahdolliselle haastateltavalle mahdollisuus valita yksilöhaastatteluun osallistuminen tai vastausten palauttaminen kirjallisesti tai äänitettyinä. Sekä kirjallisessa versiossa että suullisissa haastatteluissa haastateltaville kerrattiin aluksi tutkimuksen tavoite, haastatteluun osallistumisen vapaaehtoisuus sekä anonymiteettiin liittyvät seikat, ja pyydettiin lupa anonyymien kirjallisten vastausten ja litteroitujen haastattelujen säilyttämiseen. Haastatteluja kertyi yhteensä kuusi, joista yksi oli kirjallinen, ja viisi yksilöhaastatteluja. Yksilöhaastatteluista kaksi suoritettiin puhelimitse, ja kolme Microsoft Teamsin välityksellä.

Haastattelujen kestot vaihtelivat 35 - 75 minuutin välillä. Haastattelujen edetessä tutkimusaineistossa havaittiin saturaatiota, eli haastateltavien näkemykset toistivat aikaisempien haastattelujen näkemyksiä hoivarobottien kyberturvasta, eikä uusia näkökulmia noussut esiin.

3.3 Aineiston analyysi

Aineistoa kertyi kuudesta haastattelusta yhteensä 40 sivua fonttikoolla 10 ja rivivälillä 1,5. Aineisto analysoitiin sisällön analyysillä, tarkemmin teorialähtöisellä analyysillä. Teorialähtöisessä analyysissä aineiston analyysiä ohjaa valmis aikaisemman tiedon perusteella luotu teoria, kehys tai malli (Tuomi & Sarajärvi 2018, 110). Koska tässä tutkimuksessa pääasiallisena aineistonkeruu metodina oli teemahaastattelu, on aineiston hankinta ollut teorialähtöistä: tutkimuksen teoreettisen osuuden perusteella oli hahmotettu valmiiksi haastattelun teemat. Samaa logiikkaa noudattaen päätettiin myös analyysi tehdä teorialähtöisesti: haastattelujen teemat toimivat myös kategorioina joihin aineisto voidaan suhteuttaa.

Ennen aineiston analyysiä haastattelunauhat litteroitiin noudattamalla haastateltavien lausumia mahdollisimman uskollisesti, jonka jälkeen aineistoon tutustuttiin tarkasti ja luotiin analyysirunko, jossa yläluokat edustavat haastattelujen teemoja. Alkuperäisilmaukset korostettiin aineistosta eri värein, riippuen siitä mihin kategoriaan alkuperäisilmaisu kuului. Korostetut alkuperäisilmaukset siirrettiin omaan kategoriaansa analyysirungossa, jonka jälkeen alkuperäisilmaukset pelkistettiin. Pelkistetyille ilmauksille annettiin koodit, joiden perusteella muodostettiin alakategorioita. Taulukko 1 edustaa esimerkkiä aineiston teorialähtöisestä analyysistä.

Yläluokka	Alkuperäinen ilmaus	Pelkistetty ilmaus	Koodi	Alaluokka
Hoivarobottien kyberturva tällä hetkellä	A: Et nyt kun puhutaan ihan fyysisistä roboteista niin varmaan enemmänkin kiinnitetään huomiota siihen toiminnallisuuteen.	Ennemmin kehitetään toiminnallisuutta, kuin kyberturvaa.	Toiminnallisuus prioriteetti kehityksessä	Kyberturvan kehittäminen
	E: Tällä hetkellähän hoivarobotteja ei ihan hirveästi ole käytössä vielä.	Hoivarobotteja ei juuri ole käytössä.	Laitteiden käyttö vähäistä	Kyberturvan ajankohtaisuus
Hoivarobottien mahdolliset kyberturvauhkat	A: Uhka on tietysti se, että joku sitten vaikka hakkeroituisi ja kaappaisi ne robotit siitä hallintaansa, ja tekisi jotain mitä ei ole, tota niin niin, haluttu mitä ne tekee.	Hakkeroiminen ja laitteen hallinnan kaappaus on uhka.	Hallinnan kaappaus	”Remote Access”
	E: Teknisesti se *(salakuuntelu)* on mahdollinen uhka erityisesti sellaisessa tilanteessa, kun ne laitteet on alunperinkin rakennettu kuuntelemaan ympäristöään.	Salakuuntelu on teknisesti mahdollinen uhka, jos laite kuuntelee ympäristöään.	Salakuuntelu	”Evesdropping”
Suurimmat riskit ja uhkat koskien hoivarobottien kyberturvallisuutta	C: Tietysti sitten me tiedetään se että ihmisillä muisti ei ainakaan niin kun vanhetessa parane, tai tulee muita tämmöisiä asioita. Et kuka ottaa vastuun et siellä on oikeesti niin kun se tietoturva olemassa siellä vanhuksen kotona koska ei hän välttämättä osaa sitä päivittää.	Käyttäjän vanheneminen aiheuttaa muistin heikentymistä. Vastuu käyttäjän kodin tietoturvasta	Loppukäyttäjän vanheneminen Käyttäjän kodin tietoturva	Loppukäyttäjä Loppukäyttäjä

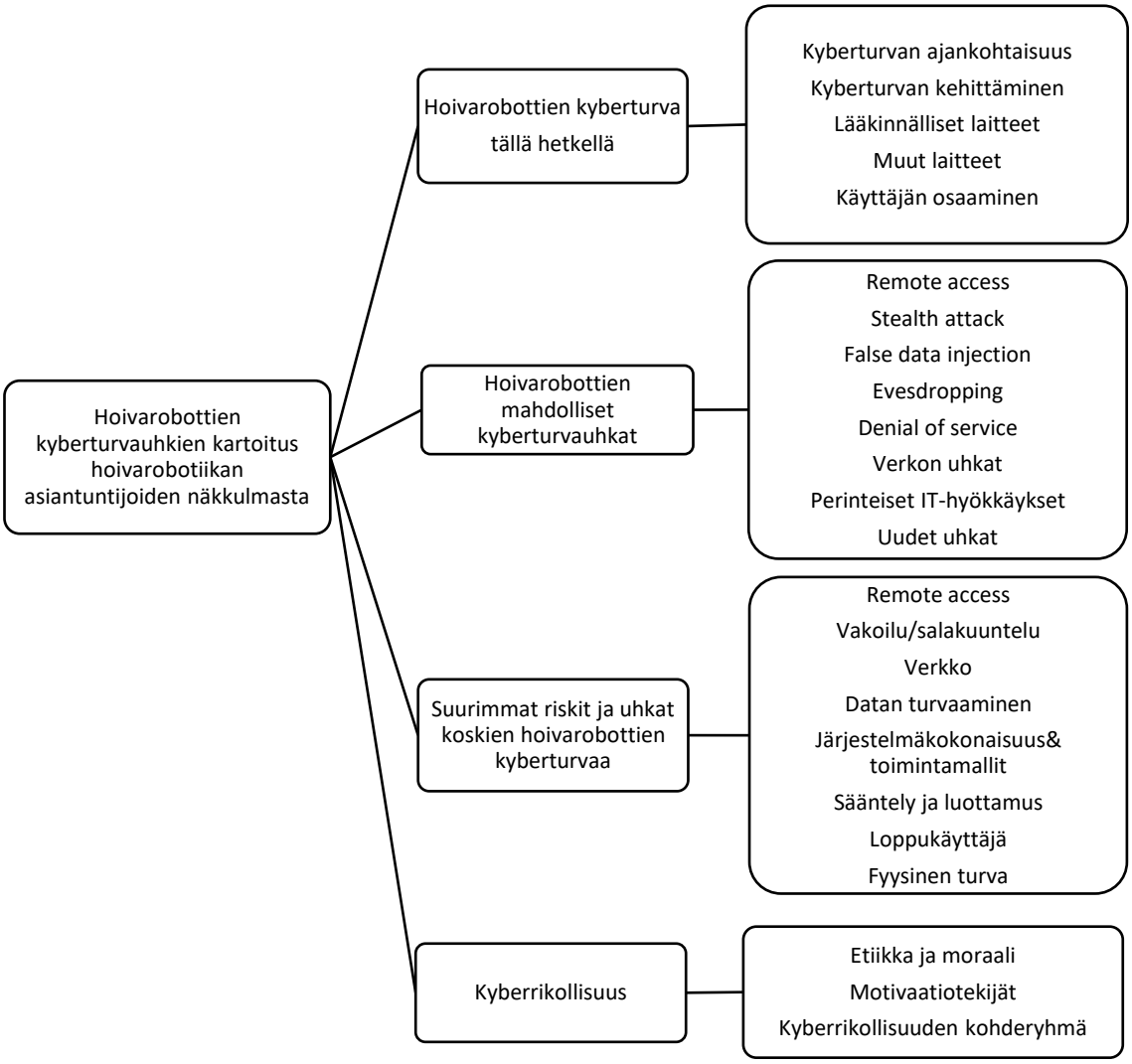
Taulukko 1: Esimerkki aineiston teorialähtöisestä analyysistä

Teorialähtöisen analyysin jälkeen jäljelle jäänyt aineisto analysoitiin aineistolähtöisellä sisällönanalyysillä (Tuomi & Sarajärvi 2018, 108), jotta aineistosta saatiin esiin tärkeimmät näkökulmat, jotka eivät sopineet yllä kuvattuun analyysirunkoon. Aineistolähtöinen analyysi poikkesi teorialähtöisestä niin että taulukossa ei ollut yläluokkia joihin aineisto istutetttiin, vaan yläluokat muodostuivat alkuperäisilmausten pelkistyksen, koodaamisen ja alaluokkiin jakamisen jälkeen alaluokkien perusteella.

4 Tulokset

4.1 Hoivarobotiikan asiantuntijoiden näkemys hoivarobottien kyberturvasta

Teorialähtöisesti hoivarobotiikan asiantuntijoiden näkemys hoivarobotiikan kyberturvasta jakautuu kolmeen kategoriaan; hoivarobotiikan kyberturva tällä hetkellä, hoivarobottien mahdolliset kyberturvauhkat ja suurimmat riskit ja uhkat koskien hoivarobottien kyberturvaa. Lisäksi aineistolähtöisessä analyysissä nousi esiin näkökulma kyberrikollisuudesta, joka on keskeisessä asemassa kyberturvallisuuden toteutumisessa (kuvio 1).



Kuvio 1: Hoivarobotiikan asiantuntijoiden näkemys hoivarobottien kyberturvasta

4.2 Hoivarobottien kyberturva tällä hetkellä

<u>Kyberturvan ajankohtaisuus</u>

Hoivarobotiikan asiantuntijat eivät olleet huolissaan hoivarobottien kybertuvasta tällä hetkellä, koska laitteita ei juurikaan ole käytössä tai markkinoilla saatavissa. Asiantuntijat eivät olleet kuulleet hoivarobotteihin kohdistuneista uhkista, eivätkä kokeneet, että aiheesta juurikaan puhuttaisi. Asiantuntijat kokivat kuitenkin, että hoivarobottien kyberturva on ajankohtainen aihe, koska hoivarobottien, kuten kaikkien muiden laitteiden käyttöön liittyy riskejä, ja hoivarobottien lisääntyessä myös kyberrikollisten kiinnostus hoivarobotteja kohtaan kasvaa. Tällä hetkellä koettiin kuitenkin todennäköisemmäksi, että kyberrikollisuus kohdistuu muihin laitteisiin, joita on jo enemmän käytössä.

”Tällä hetkellähän hoivarobotteja ei ihan hirveästi ole käytössä vielä. ” (E)

”Tässä vaiheessa uskoisin, että hoivarobottien käyttö on niin pientä, että ketään ei vielä oikein kiinnosta...” (A)

Kyberturvan kehittäminen

Asiantuntijat arvioivat, että tällä hetkellä hoivarobotteja suunniteltaessa ja kehitettäessä prioriteetti on toiminnallisuuden kehittäminen, ja hoivarobottien kyberturvaa koskevat aspektit jäävät siten vähemmälle huomiolle. Asiantuntijat toivat esiin huolen siitä, että kyberturvassa keskitytään dataan liittyviin uhkiin ja tietoturvaan, eikä oteta huomioon millaisia uhkia hoivarobotti voi aiheuttaa fyysiselle ympäristölle.

”Veikkaan että ei ole hirveästi siihen (kyberturvaan) kiinnitetty huomiota. Et nyt kun puhutaan ihan fyysisistä roboteista niin varmaan enemmänkin kiinnitetään huomiota siihen toiminnallisuuteen.” (A)

”Ne on niin uusia laitteita tyypillisesti kaikki vielä, ja ne on niin paljon tulossa, että, ja toisaalta että niissä on aika paljon, aika paljon pieniä yrityksiä, että tietoturva ei tyypillisesti oo ollu niissä semmoinen merkittävä osa sitä suunnittelua…” (E)

”Ja on keskitytty liian paljon, ei liian paljon, mutta on keskitytty niin kun tähän digitaaliseen uhkaan enemmän kuin siihen että tämmöinen fyysinen toimija, joka toimii jo osittain autonomisesti, niin tekisi jotakin.” (D)

Lääkinnälliset laitteet

Asiantuntijat pitivät kyberturvan toteutumista lääkinnällisten laitteiden osalta pakollisena, koska lääkinnällisten laitteiden regulaatio velvoittaa laitteen turvallisuudesta huolehtimisen. Lääkinnälliset laitteet ovat Valviran valvonnan alla. Ongelmalliseksi koettiin, että tällä hetkellä hoivarobotiikaksi voidaan laskea sekä tietynlaiset lääkinnälliset laitteet että tietyn tyyppinen hyvinvoinnin teknologia. Asiantuntijoiden näkemys oli, että mikään ei takaa että

laitteen turvallisuudesta olisi huolehdittu, jos sillä ei ole lääkinnällisen laitteen luokitusta, koska valvontaa ei ole.

”Jos ne ei ole lääkinnällisiä laitteita, eli valmistaja ilmoittaa sanallisen ilmoituksen tai käyttötarkoituksen mukaan, että onko ne lääkinnällisiä laitteita vai ei, ja jos niitä ei oo siihen käyttöön ilmoitettu, niin tota se voi olla sitten, että ei ole myöskään niin kun tämä kyberturva-asia kunnossa… se lääkinnällisen laitteen ikään kuin status velvoittaa näistä asioista huolehtimisen, ja Valvirahan sitä valvoo siis.” (B)

”Sillä puolella (lääkinnälliset laitteet) meillä on olemassa regulaatiota, muihin laitteisiinhan meillä ei käytännössä oo olemassa mitään regulaatiota, joka sanoo, että pitää olla tietoturvaa tai yhtään mitään.” (E)

Muut laitteet

Asiantuntijoiden mukaan tällä hetkellä koteihin ja kodinomaisiin ympäristöihin on saatavilla mm. telepreesensrobotteja, eli etäyhteysrobotteja, mutta ei tiedetä missä tai kuinka paljon niitä on käytössä. Asiantuntijoiden mukaan etäyhteysrobottien tietoturva on samaa tasoa kuin tyypillisten etäyhteyksien, eli niissä on pyritty perustason ratkaisuihin, ja niiden koetaan olevan alttiita kyberturvauhkille. Muiden kuin lääkinnällisten laitteiden turvallisuus oli asiantuntijoiden mukaan epävarmaa.

”Ja sitten vaikka etäyhteysrobotit, joka on sellanen epämääränen robottiluokka, mut nehän on verkossa, niissä on kamerat ja mikrofonit, niin ne on tuota, vaikka se on niinku laitteena, robottilaitteena se on niinku tosi yksinkertanen ku se on etäohjattu, niin siinä itessään ei oo minkäänlaista älykkyyttä. Se on hyvin altis sitten kyberturvauhkille.” (B)

*”Semmoinen joukko robotteja, joka tällä hetkellä on meillä kodeissa, tai jota on saatavilla myös kodinomaisiin ympäristöihin, on nämä erilaiset etäläsnäoloon liittyvät robotit kuten joku ******, ja muutama muu. Niin niissä, nehän tyypillisesti, niissä on sen lisäksi että ne tuo etäyhteyden, jonka tietoturva on sitä samaa tasoa kuin meidän tyypillisten etäyhteyksien, olkoot ne sitten videopuheluita Skypen yli, tai Zoomin tai jonkun muun yli, niissä on tyypillisesti taustalla joku videonjakosovellus, jo olemassa oleva… Eli ne ei ole niin kun korkean tietoturvan laitteita, mutta niissä on semmoinen perustason luottamuksellisuus, yleensä säilyy, mutta joihin on kyllä mahdollista siihen videoyhteyteen murtautua.” (E)*

Käyttäjän osaaminen

Käyttäjän osaaminen vaikuttaa tällä hetkellä mahdollisesti käytössä olevien hoivarobottien kyberturvan toteutumiseen kahdella tavoin. Asiantuntijoiden mukaan, jos laitteella ei ole lääkinnällisen laitteen luokitusta, on loppukäyttäjän käytännössä mahdotonta arvioida laitteen turvallisuuden tasoa. Käyttäjän osaaminen vaikuttaa asiantuntijoiden mukaan myös

laitteiden turvallisuuteen käytön aikana: robotteja on vaikea valmistaa turvallisiksi, jos niitä ei käytetä tiettyjen periaatteiden mukaisesti.

”Se robotti sinällään on vaikea niin kun rakentaa tietoturvalliseksi, jos sen robotin käyttäjä ei käytä sitä tiettyjen periaatteiden mukaisesti. Jotka voi olla toki kerrottu sille, mutta jos se silti tekee asioita, joita ei suositella, niin silloin sen tietoturvan taso voi olla täysin olematon.” (E)

”Sillä puolella (lääkinnälliset laitteet) meillä on olemassa regulaatiota, muihin laitteisiinhan meillä ei käytännössä oo olemassa mitään regulaatiota, joka sanoo, että pitää olla tietoturvaa tai yhtään mitään. Eli niinkun käyttäjä ei voi tietää yhtään mitään siitä, että onko sielä tietoturvaa eikä pysty millään tavalla oikeestaan arvioimaan, ellei hänellä oo asiantuntijatason tietoa minkä perusteella kysyä, ja sitten tulkita ne vastaukset.” (E)

4.3 Hoivarobottien mahdolliset kyberturvauhkat

Remote access

”Remote access”, eli laitteen hallinnan kaappaus on asiantuntijoiden mukaan yksi mahdollisista hoivarobotteihin kohdistuvista uhkista. Vaikka hallinnan kaappaus oli kaikkien asiantuntijoiden mielestä mahdollinen uhka, jakautuivat mielipiteet sen suhteen, onko uhka todennäköinen vai ei.

” Ne (hallinnan kaappaukset) on aivan mahdollisia, siis siinä mielessä, että ei taaskaan, siihen ei ole mitään estettä miksi näin ei voisi tapahtua.” (E)

” (”Remote access”) on ihan todellinen mahdollisuus, todennäkösyys on ehkä pieni…” (B)

Stealth attack

”Stealth attack”, eli hyökkäys, jossa hyökkääjä pääsee manipuloimaan robotin sensorien toimintaa, ja siten aiheuttamaan esimerkiksi mobiilin robotin törmäämisen, oli asiantuntijoiden mielestä edellisen tavoin mahdollinen uhka. Osa haastateltavista koki, että koska vastaavia hyökkäyksiä voidaan tehdä muihin liikkuviin robotteihin, voidaan niitä kohdistaa myös hoivarobotteihin, varsinkin jos robotti on huonosti suojattu. Osa asiantuntijoista koki että motivaatiota tällaisten hyökkäysten toteuttamiselle on vaikeaa keksiä.

”On todellisia ja todennäköisiä, ja muun muassa robottiautojen osaltahan tästä on nyt keskusteltu… Ja jos näihin autoihin voidaan hyökätä, ja saada se auto vaikka ajamaan johonkin rautatieasemalle, niin ilman muuta miksei sitten tämmöinen hoivarobotti….” (A)

”Joo, se (”Stealth attack”) on mahdollinen mutta toisaalta vielä tuntuu… tai no kauhee elää tällein pumpulissa, mutta ajatella että… että ketä se kiinnostaa, ja miksi joku sen tekis… Elikkä on mahdollinen mutta pidän sitä aika epätodennäköisenä” (D)

”Et jos me nähdään et me voidaan muita liikkuvia robotteja, olkoon vaikka näitä logistiikkarobotteja, tehdä niille vastaavia asioita. Se ei tarkoita, että kaikki, jokainen robotti olisi välttämättä altis sille, mutta esimerkiksi robotti, joka on konfiguroitu heikolla salasanalla tai muuta, joka on verkossa niin se on toki. Tai että on ”man in the middle”, että pystyy kaappaamaan viestinnän, eli pääsee sinne väliin johonkin, ja sillä tavalla pääsee sinne viestintään vaikuttamaan niin tottakai.” (E)

False data injection

Hyökkäyksiä, jossa robotin käsittelemää dataa päästään muokkaamaan pidettiin mahdollisena ja tietyissä tilanteissa jopa helppona toteuttaa. Asiantuntijat olivat yhtä mieltä siitä, että tällaisen uhkan toteutumisesta koituvat seuraukset voivat olla kriittisiä, mutta mielipiteet jakautuivat sen suhteen, onko uhka todennäköinen.

”Voi olla mahdollinen.” (B)

”Kaikkeen mihin me ihmiset ollaan lisätty sitä teknologiaa niin tota, ja tieto kulkee puoleen jos toiseen, ja samalla lailla kun jos lääkemääriin pääsee käsiksi niin kyllä sillä ihan varmasti saa niin kun hirvittävää jälkeä aikaan.” (C)

”Jos se on esim. lääkeannostelija robotti, jota terveyskeskuksessa hoitaja pystyy naputtelemalla tehdä jotain, muuttamaan lääkemääriä, niin silloinhan tämä on äärimmäisen helppoa, jos siihen joku pääsee puoleen väliin muuttamaan niitä lukuja mitä sinne kulkee.” (E)

Evesdropping

Salakuuntelu ja vakoilu robotin avulla nousivat haastatteluissa eniten esiin, ja niitä pidettiin mahdollisina ja todennäköisinä uhkina. Vastaavia hyökkäyksiä on tehty muihin robotteihin, joilla on mikrofonit ja kamerat, joten asiantuntijoiden mukaan on todennäköistä, että varsinkin huonosti suojattuja etäyhteysrobotteja voidaan käyttää vakoiluun, koska niiden turvallisuuden taso ei tällä hetkellä välttämättä ole riittävä.

”No se (salakuuntelu) on ehkä hiukan todennäköisempi kuin noi toiset, et jos koetaan et täntyyppisiä ois jonkun mielestä kiva harrastaa, tällasta salakuuntelua ja kalastelua. Et tää on kyllä siinä mielessä ihan realistinen keissi, että on kerran tehty ja on saatettu tehdä useampiakin. Et kaikki ei ehkä ole jääneet kiinni.” (B)

”Tämmöisten (etäyhteysrobottien) videonjakosovellusten turvallisuus on yleensä sellainen että, se on jonkunmoinen, mutta ne ei oo millään tavalla vahvasti autentikoituja, ellei niissä oo joku erillinen virtuaaliverkko, joka on suljettu ulkopuolisilta, jota yleensä ei koskaan ole. Eli käytännössä se tarkoittaa sitä, että ne on jollain tavalla salattuja ne videoyhteydet, mutta melko kevyesti sillä tavalla, jos on niin kun joku pahantekijä jolla on halua käyttää resursseja niin se pystyy sinne videoyhteyteen murtautumaan. Ne samat robotithan sitten myös tietysti liikkuu ja niitä voi yleensä etäohjata, niitten liikettä. Tyypillisesti ne on rakennettu sillä tavalla että, ja se että ne liikkuu jossain tilassa niin sehän periaatteessa mahdollistaa niitten käytön esimerkiksi vakoiluun.” (E)

Denial of service

Asiantuntijat puhuivat palvelunestohyökkäyksistä kahdesta ei näkökulmasta; hoivarobotteja voidaan käyttää palvelunestohyökkäysten toteutukseen ja palvelunestohyökkäyksillä voidaan estää robotin tarjoama palvelu. Palvelunestohyökkäykset koettiin mahdollisiksi uhkiksi molemmista näkökulmista, mutta asiantuntijat näkivät, että laitteet, jotka eivät ole yhteydessä verkkoon ovat palvelunestojen näkökulmasta turvallisia. Asiantuntijoiden näkemys oli, että jos laite ei ole kytköksissä verkkoon, ei esimerkiksi etäyhteyksien blokkaaminen välttämättä juurikaan vaikuta laitteen toimintaan. Verkottomia laitteita ei myöskään voi käyttää palvelunestohyökkäysten toteutukseen.

”Etäyhteyden voi tietysti palvelunestolla blokata.” (E)

”Voi olla aika katastrofaalista esimerkiksi, jos vanhuksen lääkitys perustuu siihen että sillä on se toimiva lääkeautomaatti tai lääkerobotti siellä kotona, niin sitten jos joku estää et sieltä ei tulekaan niitä lääkkeitä niin, niin sehän on todella paha juttu sitten.” (A)

” …tietyllä tavalla niin kun tieto lähtee ja tulee niin tota kyllähän niitäkin (hoivarobotteja) pystytään ihan varmasti samalla tavalla niinkun käyttämään… eli kyl mä nään et enenevissä määrin voi olla että niitäkin sitten käytetään hyväksi.” (C)

Verkon uhkat

Verkkoyhteydet altistavat hoivarobotteja erilaisille uhkille, ja asiantuntijat kokivat verkkojen olevan keskeisessä asemassa siinä kuinka turvallisia erilaiset laitteet ovat. Verkkoyhteyden tarve riippuu hoivarobottien käyttötarkoituksesta ja ominaisuuksista, ja mitä monimutkaisempia ja interaktiivisempia laitteita kehitetään, tulee verkkoyhteys olemaan entistä keskeisemmässä asemassa. Asiantuntijat kokivat, että mm. kaikkien edellä mainittujen uhkien toteutuminen on todennäköisempää, mikäli laite on kytköksissä verkkoon.

”Mitä monimutkaisempi, interaktiivisempi ja erityisesti verkkoon kytketty laite, niin se on alttiimpi erilaisille kyberturvauhkille, kuin yksinkertainen laite, joka ei ole verkossa, jossa

on vaan mekaanisia ominaisuuksia, eikä varsinaista sellaista prosessointiakaan kovin paljon itsessään." (B)

"Mutta sitten telepreesensrobotit puolestaan, että vaikka hoitaja tekee käyntejä kotihoidon asiakkaalla, ikäihmisen luona, telepreesensrobotilla, niin näissähän on sitten taas kamerat ja verkon yli liikkuu tietoa. Että siinä on sitten taas riskinsä." (D)

"Hoivarobotit ovat alttiimpia kuin perinteiset robotit, koska ne eivät toimi eristyksissä. Ne ovat yhteydessä ulkomaailmaan, eli Internetiin, useiden rajapintojen kautta, esim. Wifi, 3G, Bluetooth jne. Aina päällä oleva yhteys altistaa robotin verkkohyökkäyksille." (F)

Perinteiset IT-hyökkäykset

Hoivarobotit eroavat teknisesti hyvin vähän muista jo käytössä olevista roboteista ja IT-laitteista, jolloin hoivarobotteja koskee samat riskit kuin muita laitteita. Asiantuntijoiden mukaan perinteiset, puhtaasti tietokonepohjaiset IT-hyökkäykset ovat mahdollisia myös hoivarobotteihin, ja metodit hyökkäysten toteutukselle ovat samat kuin muillekin laitteille.

"Meillä alkaa olemaan niin paljon niitä laitteita jo muutenkin, että hoivarobotteja oikeastaan koskee ne samat riskit, kun näitä kaikkia laitteita… Et oikeastaan, hoivarobotit eroaa hyvin vähän mistä tahansa, tavallaan ne "attack methodit" on ihan samat, eli siis nämä tavat hyökätä on ihan samat hoivarobotteihin kuin moneen muuhun." (E)

"Hoivarobotteihin voi kohdistua kolmenlaisia uhkia. 1) Puhtaat tietokonepohjaiset tai perinteiset IT-hyökkäykset. Hoivarobotit käyttävät enemmän tai vähemmän erilaisia sovelluksia, joihin perinteiset uhkat voivat vaikuttaa, mm. puskurin ylivuodot, käyttöjärjestelmän, komentosarjan tai sovellusten haavoittuvuudet jne." (F)

Uudet uhkat

Asiantuntijat kokivat, että hoivarobotiikan kehitys tuo tullessaan myös uusia uhkia, kun hoivarobotteihin integroidaan uusia tekniikoita; esimerkiksi tekoälyn ja koneoppimisen käyttö hoivarobotiikassa luo mahdollisuuksia uusille hyökkäyksille. Asiantuntijat kokivat myös, että hoivarobottien kykyyn liikkua ympäristössään liittyy uusia riskejä, joita ei välttämättä vielä ole otettu huomioon. Hoivarobottien fyysiseen olemukseen liittyvät riskit ovat toistaiseksi pieniä koska roboteilla ei toistaiseksi ole kehittynyttä kykyä esim. manipuloida esineitä, mutta tulevaisuudessa kun fyysisyyteen liittyviä ominaisuuksia kehitetään, lisääntyy myös fyysisyyteen liittyvät riskit.

"Lopuksi hoitoroboteihin integroidut uudet tekniikat mm. koneoppiminen, vahvistusoppiminen jne. avaa oven uusille hyökkäyksille, joihin on puututtava." (F)

”Oletetaan et meillä on joku iso robotti, joka pystyy fyysisesti tekemään pahojaan siinä ympäristössä liikkumalla ja törmäilemällä asioihin, esimerkiksi, niin sen tyyppiset asiat on tietysti tavallaan uusia riskejä verrattuna mitä meillä on jo jossain määrin hyväksyttäviä riskejä”.

4.4 Suurimmat riskit ja uhkat koskien hoivarobottien kyberturvaa

Remote access

Asiantuntijat kokivat, että yksi suurimmista uhkista koskien hoivarobottien kyberturvaa on laitteiden hallinnan kaappaus. Laitteen kaappauksen kautta kyberrikollinen voi tehdä laitteella käytännössä kaikkia samoja asioita, joita käyttäjä itsekin pystyisi, eli mm. päästä käsiksi laitteen tietoihin ja vakoilla laitteen käyttäjää. Jos kyseessä on fyysisesti liikkuva laite, voi hyökkääjä laitteen kaappauksen kautta aiheuttaa myös fyysistä vahinkoa laitteen ympäristössä, tai jopa laitteen loppukäyttäjälle.

”Just nyt niin kun tässä ajassa… niin se on kyllä ehkä se suurin uhka, että ne jollakin lailla otetaan sitten hallintaan, että ne sitten liikkuu sinne minnekkä ei pitäisi liikkua taikka että se pysäytetään kokonaan.” (A)

”Kun hyökkäys (hallinnan kaappaus) on suoritettu, hän voi hallita robottia ja voi sitten vapaasti tarkkailla käyttäjää, ja etsiä tietoja, kuten luottokorttitietoja.” (F)

Vakoilu/salakuuntelu

Toinen uhka, jonka asiantuntijat kokivat erityisen suureksi riskiksi, oli vakoilu ja salakuuntelu. Hoivarobotin käyttö salakuunteluun tai salakatseluun nähtiin muita uhkia helpommaksi toteuttaa, sekä mahdolliseksi toteuttaa laajemmalle joukolle. Asiantuntijat kokivat, että vakoilusta ja salakuuntelusta saatavat hyödyt ovat tällä hetkellä rikollisen näkökulmasta ovat kaikkein suurimmat.

”Salakuuntelu ja salakatselu on luultavasti sen verran paljon helpompaa, eikä vaadi fyysistä läsnäoloa ja tämäntyyppistä, että sen tyyppinen riski on siinä mielessä todennäköisempi ja mahdollista tehdä laajemmalle joukolle, jos siihen on intressejä.” (E)

Verkko

Verkko, ja varsinkin etäyhteyksien turvallisuus oli asiantuntijoiden mukaan yksi merkittävimmistä riskeistä hoivarobottien kyberturvassa. Verkkoyhteys on usein se rajapinta, joka mahdollistaa hoivarobottien turvallisuuden vaarantumisen. Paikallisverkot nähtiin hiukan etäyhteyksiä turvallisempina, mutta asiantuntijat kokivat, että myös niihin on mahdollista

päästä käsiksi paikan päällä. Tämänhetkisten etäyhteyssovellusten tietototurvaa pidettiin yleisesti perustasoisena, jolloin erityisesti niiden hakkerointia pidettiin mahdollisena.

”Ensisijaisesti se etäyhteys ja sitä kautta sitten se et sinne ei tule sitä ylimäärästä niin kun porukkaa ketkä sinne ei kuulu.” (C)

”Eli se on just toi, että verkon kautta niin se on yks tosi kriittinen, et periaatteessa nekin, jotka ei ole verkossa, tai on ikään kuin vaan, tai siis ei oo niin kun Internetissä mutta on niin kun paikallisessa verkossa, niin periaatteessa näihinkin voi tietenkin jollain tavalla hakkeroitua siellä paikan päällä, semmoinen on mahdollista.” (B)

Datan turvaaminen

Asiantuntijat olivat huolissaan hoivarobottien keräämän datan turvallisuudesta. Esiin nousi erityisesti tietosuojan säilyminen pilvipalvelujen käyttöön liittyen. Asiantuntijat olivat huolissaan siitä, miten data pystytään turvaamaan niin että voidaan olla varmoja siitä, että sitä hyödynnetään, säilytetään ja että se hävitetään oikein, eivätkä väärät tahot pääse käsiksi dataan. Asiantuntijat nostivat esiin datan eheyden säilymiseen liittyvän huolen.

”Pilvipalveluitten käyttö näissä robotiikkajärjestelmissä… että tietosuojaa ei enää olekaan, että ei pysy se tietosuoja Euroopan unionin piirissä.” (B)

”Se aspekti siinä, että millä tavalla sitä niin kun oikeasti, kaikkea tätä datamassaa, tullaan niin kun käyttämään hyväksi. Koska nyt jo on ollut hyvin vakavia tietomurtoja.” (C)

Järjestelmäkokonaisuus & toimintamallit

Hoivarobotit saattavat olla osa suurempaa järjestelmää ja toimintamallia, jolloin häirintää voidaan kohdistaa johonkin muuhun järjestelmän osaan ja aiheuttaa siten myös hoivarobottien toiminnan häiriintyminen. Asiantuntijat kokivat toimintamallien muutokset riskitekijöiksi, koska kun toimintamallit suunnitellaan robottien avulla toteutettaviksi, voivat vahingot olla suuria, jos robotit jostain syystä eivät toimi. Paluu vanhaan toimintamalliin voi olla vaikeaa ja aikaa vievää. Hoivarobottien loppukäyttäjien näkökulmasta hoivarobotin toimintahäiriöt voivat olla erittäin kriittisiä, riippuen hoivarobottien avulla suoritettujen tehtävien kriittisyydestä. Asiantuntijat kokivat riskiksi myös sen, että järjestelmäkokonaisuudet ja hoivarobotit ovat alttiita sekä päivitys- että käyttöjärjestelmän haavoittuvuushyökkäyksille koko elinkaarensa ajan.

”Et enää ei riitä et me saadaan niin kun kytkettyä kaikki yhteen ja toimiin sulavasti yhden laitteen kautta, vaan se pitäisi niin kun miettiä kuinka haavoittuvainen se systeemi niin kun todellisuudessa voi olla.” (C)

”Jos toimintamalli on suunniteltu robottien avulla toteutettavaksi, mutta sitten robotit on pois pelistä niin se on iso ongelma muuttaa takaisin siihen niin sanottuun vanhaan malliin... Jos yhtäkkiä vaikka kaikki 300 robottia olisi yhtä aikaa pois pelistä jonkun kyberhyökkäyksen takia, niin mistä ihmeestä me kaivetaan hoitajat antamaan näille kolmellesadalle lääkkeet. Niin puhutaan aika isosta ongelmasta, tai valtavista ongelmista.” (D)

Sääntely ja luottamus

Kaikki hoivarobotiikkaan liittyvät riskit eivät koske pelkästään itse hoivarobotteja ja niiden käyttöä. Asiantuntijat kokivat, että tällä hetkellä, kun hoivarobottien kyberturvallisuutta koskevaa regulaatiota ei ole, korostuu turvallisuuden suhteen luottamus toimittajaan ja laitteen valmistajaan. Varsinkin palveluntarjonnan näkökulmaa edustaneet asiantuntijat kokivat, että tällä hetkellä täytyy vain luottaa siihen, että laitteen valmistaja on ottanut turvallisuuteen liittyvät näkökulmat huomioon, ja toteuttanut laitteet mahdollisimman turvallisiksi. Riskitekijäksi koettiin se, että muiden kuin lääkinnällisten laitteiden osalta ainoa tae laitteiden turvallisuudesta toimittajan lupaus.

”Niin tämä nyt on minusta niin kun meille (palveluntarjoajille) se suurin riski, että meidän täytyy luottaa toimittajaan, jos me jotakin hankitaan, että heillä nämä asiat on mietitty loppuun asti ja… ne on kunnossa.” (D)

Loppukäyttäjä

Asiantuntijoiden mukaan hoivarobottien loppukäyttäjiin liittyy turvallisuuden näkökulmasta riskitekijöitä. Asiantuntijat eivät olleet vakuuttuneita siitä, että loppukäyttäjät välttämättä huolehtivat oman kotinsa ja omien verkkojensa turvallisuudesta. Asiantuntijat eivät myöskään olleet vakuuttuneita siitä, että loppukäyttäjät toimivat tietoturvallisten periaatteiden mukaan. Kun hoivarobotiikan loppukäyttäjinä ovat vanhukset, nousi esiin myös huoli heidän mahdollisesti puutteellisista digitaidoistansa, sekä siitä että ihmisen muisti ja tietyt muut ominaisuudet eivät yleensä vanhemmiten parane. Asiantuntijoiden mukaan voi olla todennäköistä, että ihminen vanhetessaan ei välttämättä enää muista tai osaa käyttää laitetta, tai huolehtia tietoturvasta.

”Toisaalta käyttäjän pitää osata hoitaa oman kotinsa tietoturva, että langattomat verkot on suojattuja eikä avoimia, eli hoitaa niin kun omalta puoleltaan päivitykset ja muut ihan samalla tavalla kuin muissakin laitteissa. Et näistähän ei niin kun aina välttämättä huolehdita.” (B)

”Tietysti sitten me tiedetään, se että ihmisillä muisti ei ainakaan niin kun vanhetessa parane, tai tulee muita tämmöisiä asioita. Et kuka ottaa vastuun et siellä on oikeesti niin

kun se tietoturva olemassa siellä vanhuksen kotona koska ei hän välttämättä osaa sitä päivittää." (C)

Fyysinen turvallisuus

Asiantuntijat kokivat, että jos kyberrikollisella on tarpeeksi iso, esim. valtiontason insentiivi, aiheuttaa fyysistä vahinkoa, on se hoivarobotin kautta mahdollista. Asiantuntijat kokivat lisäksi, että robottien fyysisyyteen liittyvät riskit tulevat tulevaisuudessa kasvamaan, kun robottien fyysiset ominaisuudet, kuten esineiden manipulointikyky, paranee.

"Sitten jos meillä tulee tilanteita, jossa on hyvin suuri insentiivi, sanotaan niin kun valtiontason insentiivi vaikuttaa jonkun henkilön turvallisuuteen, siis aiheuttaa sille vamma tai jotain muuta, niin se on mahdollista tehdä hoivarobotin kautta. Tulevaisuudessa ku mennään, sanotaan kymmenen vuotta eteenpäin niin meillä luultavasti ne robotit pystyy paremmin enemmän manipuloimaan ja käsittelemään esineitä, niin se toki sitten lisää näitä uhkia." (E)

4.5 Kyberrikollisuus

Etiikka ja moraali

Asiantuntijoiden mielestä suomessa saatetaan suhtautua kyberrikollisuuteen sinisilmäisesti. Esiin nousivat näkökulmat siitä, että kyberrikollisuuteen suhtautumiseen vaikuttavat epätietoisuus siitä mitä kyberrikollisuuden saralla on jo nyt mahdollista tehdä. Suhtautumiseen vaikuttaa lisäksi se, että halutaan uskoa siihen että ihmiset toimivat eettisesti oikein eivätkä siten halua aiheuttaa pahaa toisille ihmisille, varsinkaan haavoittuvassa asemassa oleville.

"Siis varmaan niin kun tietyssä mittakaavassa ollaan aika turvallisilla vesillä, mutta että me ollaan tota suomessa aika liian sinisilmäisiä siihen että mitä kenties nyt jo niin kun pystytään tekemään." (C)

"Ehkä suurin osa ajattelisi, että kuka nyt haluaisi oikeesti semmosta pahaa tehä…" (D)

"Eikä niin kun tavallaan tota haluta ehkä niin kun uskoo siihen että, että tämmöiset asiat on välttämättä niin kun mahdollisia ja varsinkaan niin kun haavoittuvassa asemassa olevia, olevia kohtaan, oli ne sitten vanhuksia tai lapsia tai muita…" (C)

Motivaatiotekijät

Kyberrikollisuuden taustalla vaikuttavat motivaatiotekijät nousivat esiin kaikissa haastatteluissa useaan otteeseen. Asiantuntijat arvioivat usein erilaisia uhkia sen kautta,

mitkä motivaatiotekijät vaikuttavat rikollisen toimintaan, ja mitä hyötyjä rikollisen näkökulmasta on saavutettavissa tietyn uhkan toteutuessa. Asiantuntijoiden näkemys yleisesti oli se, että mikäli rikollisella on riittävän suuri motivaatio ja mahdollisuus käyttää resursseja, kasvavat todennäköisyydet erilaisten uhkien toteutumiselle. Tällä hetkellä koettiin kuitenkin, että hoivarobotiikka ei välttämättä vielä ole niin mehukas ympäristö, että se houkuttelisi kyberrikollisia, koska rikosten aiheuttamat vahingot ja hyödyt jäävät tällä hetkellä pieniksi. Asiantuntijoiden oli vaikea kuvitella miksi kukaan ylipäänsä haluaisi hyökätä laitteisiin, joiden on tarkoitus auttaa haavoittuvassa asemassa olevia, poissulkien tilanteet, joissa hoivarobotti on tarpeeksi merkittävällä henkilöllä.

”Mitä tää hyökkääjä, tai hyökkäyksen organisoija kuvittelee sillä saavuttavansa, niin se on ehkä niin kun vaikeempi hahmottaa…” (B)

”Meijän on helppo löytää mahdollisia tapoja, sanotaan että teknisesti mahdollisia tapoja tehdä asioita, jotka voi potentiaalisesti tapahtua on niin kun valtavan paljon. Mutta se että ne tapahtuisi, vaatii aina jonkun tahdon, eli ihmisen joka haluaa sitä hyödyntää. Ja kun näitä riskejä kartoitetaan tämmöisessä asiassa, niin se on olennainen dimensio siinä arviossa. Että mikä on sen riskin vakavuus on yksi dimensio, mut sen riskin todennäköisyyteen liittyy hirveen vahvasti sen jonkun toimijan motivaatio käyttää sitä jotain heikkoutta siinä kokonaisjärjestelmässä, oli se sitten tietoturvassa tai jossain muussa, niin hyväksi.” (E)

”Sitten jos meillä tulee tilanteita, jossa on hyvin suuri insentiivi, sanotaan niin kun valtiontason insentiivi, vaikuttaa jonkun henkilön turvallisuuteen, siis aiheuttaa sille vamma tai jotain muuta, niin se on mahdollista tehdä hoivarobotin kautta…” (E)

<u>Kyberrikollisuuden kehitys</u>

Asiantuntijat olivat tietoisia siitä, että kyberrikollisuutta tapahtuu tällä hetkellä erilaisissa konteksteissa. Vaikka hoivarobotiikkaa ei tällä hetkellä koettu erityisen ajankohtaiseksi kyberrikollisuuden kohteeksi, tulee asiantuntijoiden mielestä kuitenkin ottaa huomioon se, että siinä missä hoivarobotiikka kehittyy, kehittyy myös kyberrikollisuus.

”Et sitä mä en niinku vielä usko et hirveesti tässä vaiheessa joku hyökkäisi johonkin yksittäiseen robottiin… Valmistajat varmasti valmistautuvat näihin kyberhyökkäyksiin, mut sitten toisaalta ne jotka hyökkäyksiä tekevät niin nekin kehittyvät kokoajan paremmiksi ja paremmiksi.” (A)

”Tietoturva on käytännössä usein kilpajuoksua hyökkääjän ja puolustajan välillä.” (E)

5 Pohdinnat

5.1 Tulosten pohdinta

Asiantuntijoiden mukaan hoivarobottien kyberturvan tasosta tällä hetkellä ei tarvitse olla huolissaan, koska laitteita ei juurikaan ole käytössä tai markkinoilla saatavissa. Asiantuntijoiden näkemys laitteiden käytöstä tällä hetkellä tukee aiempia tutkimuksia, joissa on todettu, että hoivarobotteja ei juurikaan ole vielä käytössä, vaikka hoivarobotit ovat mahdollinen ratkaisu tulevaisuuden hoitajapulaan väestön ikääntyessä (Van Aerschot & Parviainen, 2020). Vaikka asiantuntijoiden näkemys oli, että kyberrikollisuus kohdistuu tällä hetkellä muihin laitteisiin, joita on jo enemmän käytössä, pitivät asiantutijat hoivarobottien kyberturvallisuutta tärkeänä ja ajankohtaisena aiheena. Hoivarobottien yleistyessä on todennäköistä, että myös kyberrikollisten kiinnostus hoivarobotteja kohtaan kasvaa.

Asiantuntijat nostivat esiin, että tällä hetkellä hoivarobottien kyberturvassa panostetaan enemmän dataan liittyviin uhkiin kuin fyysisyyteen liittyviin uhkiin. Vastaavaa ei aiemmissa tutkimuksissa esitetty. Yleisesti asiantuntijoiden näkemys oli kuitenkin linjassa mm. Fosch-Villarongan ja Mahlerbin (2021) artikkelin kanssa siitä, että hoivarobotiikan kehityksessä keskitytään enemmän toiminnallisuuden kuin turvallisuuden kehitykseen. Datan turvaamiseen panostaminen on ymmärrettävää koska sosiaali- ja terveydenhuollossa käsitellään paljon asiakas- ja henkilötietoja, sekä asiakkaisiin liittyvää arkaluonteista dataa, jonka vuoksi luottamuksellisuus, yksityisyys, tietojen eheys ja saavutettavuus on keskeisessä asemassa (Sosiaali- ja terveysministeriö, 2019). Fyysisyyteen liittyvät uhkat tulisi kuitenkin ottaa enenevästi huomioon, jotta ne eivät tulevaisuudessa muodostu ongelmaksi, kun hoivarobottien fyysiset ominaisuudet kehittyvät.

Asiantuntijat nostivat esiin laitteiden luokituksiin ja niiden käyttötarkoituksen tulkinnanvaraisuuteen liittyviä ongelmia, jotka olivat linjassa aiempien tutkimusten kanssa (Fosch-Villaronga & Mahlerb, 2021). Tällä hetkellä asiantuntijat kokivat, että lääkinnällisen laitteen luokituksen omaavien hoivarobottien turvallisuuteen voidaan luottaa, koska lääkinnälliset laitteet ovat Valviran valvonnan alaisia. Vaikka laitteella ei ole lääkinnällisen laitteen luokitusta voidaan sitä mahdollisesti kuitenkin käyttää hoivan tarkoituksiin, mutta tällöin ei ole mitään takeita siitä, miten kyseisen laitteen kyberturvasta on huolehdittu. Asiantuntijat nostivat esimerkeiksi erilaiset etäyhteysrobotit, joita on jo saatavilla koteihin ja kodinomaisiin ympäristöihin.

Selkeä viestintä hoivarobottien kyberturvan tasosta on keskeisessä asemassa kyberturvan toteutumisessa, koska käytännössä ei tällä hetkellä ole selvää, osaavatko robottien hankkijat arvioida robottien turvallisuuden tasoa (Fosch-Villarongan & Mahlerbin, 2021; Lera ym. 2017). Asiantuntijat tässä tutkimuksessa painottivat myös selkeän viestinnän merkitystä palveluntarjoajan, ja varsinkin loppukäyttäjän näkökulmasta; näiden tahojen tieto ja aiheen

ymmärrys eivät välttämättä riitä siihen, että he itse osaavat tehdä tietoon perustuvia ratkaisuja ja riskiarvioita laitteiden käyttöön liittyen.

Tuloksista kävi ilmi, että hoivarobotteihin kohdistuu käytännössä kaikki tämän työn tietoperustassa esiin tulleet uhkat aina perinteisistä IT-uhkista robottien fyysiseen olemukseen liittyviin uhkiin. Hoivarobotit eroavat teknisesti hyvin vähän muista jo käytössä olevista roboteista ja IT-laitteista, jolloin hyökkäykset ja niihin käytetyt menetelmät ovat teknisesti samat kuin muissa laitteissa. Asiantuntijoiden mahdollisiksi kokemat uhkat olivat näin ollen linjassa aiempien tutkimusten kanssa. Tässä tutkimuksessa asiantuntijat korostivat verkkojen turvallisuuden olevan keskeisessä asemassa siinä kuinka turvallisia erilaiset laitteet ovat, ja kokivat että uhkien toteutumisen todennäköisyys on suurempi, mikäli laite on kytköksissä verkkoon. Tämä näkemys on linjassa mm. Leran ym. (2017) ja Rouskun (2014, 57) esittämään näkemykseen siitä, että kaikki verkkoon kytköksissä olevat robotit voivat olla riski käyttäjilleen koska ulkopuolinen voi päästä laitteisiin käsiksi verkon kautta.

Hoivarobotiikan kehitys tuo tullessaan myös uusia uhkia, joita ei aikeisemmissa tutkimuksissa liioin tuotu esiin. Tässä tutkimuksessa asiantuntijat nostivat esiin, että uusien teknologioiden integroiminen, esimerkiksi pilvipalveluiden, tekoälyn ja koneoppimisen käyttö hoivarobotiikassa luo mahdollisuuksia uusille hyökkäyksille. Asiantuntijat korostivat lisäksi aiemmista tutkimuksista poiketen, että tulevaisuudessa fyysisyyteen liittyvät riskit nousevat kyberturvallisuudessa keskeisempään asemaan, kun hoivarobottien fyysisiä ominaisuuksia kehitetään.

Erityisen suuriksi riskeiksi asiantuntijat kokivat hoivarobottien hallinnan kaappauksen, sekä vakoilun ja salakuuntelun. Nämä uhkat koettiin muita uhkia helpommiksi toteuttaa, koska näistä on olemassa esimerkkitapauksia jo muilta robotiikan aloilta. Asiantuntijat kokivat, että vakoilusta ja salakuuntelusta saatavat hyödyt ovat tällä hetkellä rikollisen näkökulmasta kaikkein suurimmat.

Aiemmissa tutkimuksissa hoivarobottien kyberturvaa on käsitelty usein melko teknisestä näkökulmasta. Tässä tutkimuksessa nousi kuitenkin esiin, että kaikki hoivarobotiikan kyberturvaan liittyvät riskit eivät koske itse hoivarobotteja ja niiden käyttöä. Erityisesti asiantuntijat, jotka edustivat palveluntarjonnan näkökulmaa, painottivat hoivarobottien kyberturvallisuutta koskevan sääntelyn tarvetta. Riskitekijäksi koettiin se, että muiden kuin lääkinnällisten laitteiden osalta ainoa tae laitteiden turvallisuudesta on toimittajan lupaus.

Toinen suurimpiin riskeihin liittyvä näkökulma, joka oli linjassa Fosch-Villaronga & Mahlerbin (2021) näkökulman kanssa, oli toisiinsa kytkettyjen järjestelmien ja laitteiden määrän lisääntymiseen liittyvät riskit. Hoivarobotin ollessa osa suurempaa järjestelmää, voidaan häirintää kohdistaa johonkin muuhun järjestelmän osaan ja aiheuttaa siten myös hoivarobottien toiminnan häiriintyminen. Asiantuntijat tässä tutkimuksessa kokivat

toimintamallien muutokset riskitekijöiksi, koska jos tällä hetkellä hoitohenkilökunnan tekemä työ suunnitellaan laajemmin robottien avulla toteutettaviksi, voi paluu vanhaan toimintamalliin häiriötilanteessa olla vaikeaa varsinkaan nopealla aikataululla. Jos esimerkiksi 300 lääkeannostelurobottia asiakkaiden kotona jostain syystä lakkaa toimimasta kyberturvauhkan toteutumisen tuloksena, pitäisi kuitenkin pystyä takaamaan, että kaikki asiakkaat saavat lääkkeensä ajallaan ja oikeina annosteluina.

Hoivarobottien kehitystyötä edustaneet asiantutijat nostivat esiin myös sen, että laitteita on vaikea valmistaa turvallisiksi, jos niitä ei käytetä tiettyjen periaatteiden mukaisesti. Näkemys on linjassa aiempien tutkimusten kanssa (Lera ym, 2017; Fosch-Villarongan & Mahlerbin, 2021). Sosiaali- ja terveysministeriö (2019) toteaa myös, että mm. käytettävyydeltään kankeat ohjelmistot voivat houkutella laitteiden käyttäjiä kiertämään tietoteknisiä suojausmekanismeja, jolloin käyttäjät saattavat esimerkiksi jättää oletussalasanat vaihtamatta, tai käyttää järjestelmiä samalla käyttäjätunnuksella. Käyttäjän osaaminen on toisin sanoen myös keskeisessä asemassa käytössä olevien laitteiden kyberturvallisuuden toteutumisessa. Kun hoivarobotiikan loppukäyttäjinä ovat vanhukset, täytyy myös ottaa huomioon heidän mahdollisesti puutteelliset digitaidoistansa, sekä se, että ihmisten ominaisuudet, kuten muisti, eivät yleensä vanhemmiten parane.

Uudet näkökulmat, joihin aiemmissa tutkimuksissa ei liioin kiinnitetty huomiota liittyivät niihin inhimillisiin tekijöihin, jotka vaikuttavat sekä kyberturvallisuuteen suhtautumisessa että kyberturvauhkien toteutumisessa. Aiemmissa tutkimuksissa kyberturvaa on käsitelty teknisemmästä näkökulmasta, jolloin teon taustalla vaikuttava inhimillinen näkökulma kuten pahantekemisen tahto ja siitä saatava hyöty, ovat jääneet vähemmälle huomiolle.

Tässä tutkimuksessa asiantuntijat kokivat, että varsinkin Suomessa kyberrikollisuuteen saatetaan suhtautua liian sinisilmäisesti; halutaan uskoa siihen, että ihmiset toimivat eettisesti oikein eivätkä siten halua aiheuttaa pahaa toisille ihmisille, varsinkaan haavoittuvassa asemassa oleville. Tällainen ajattelu ei kuitenkaan poista sitä, että kyberrikollisuutta on olemassa, ja riittävän suuri motivaatio ja mahdollisuus käyttää resursseja kasvattaa todennäköisyyksiä erilaisten uhkien toteutumiselle. On myös todennäköistä, että hoivarobotiikan yleistyessä kyberturvauhkia tulee kohdistumaan enenevissä määrin. Kyberturvan kehitys on kilpajuoksua kyberrikollisuutta vastaan, jossa erilaisten riskianalyysien ja motivaatiotekijöiden tutkimisen avulla pystyttäisiin ymmärtämään rikollisuuden taustalla vaikuttavia tekijöitä paremmin, ja mahdollisesti kohdistamaan kyberturvallisuuden kehityksen resurssit todennäköisimpien uhkien torjumiseen.

5.2 Tutkimuksen toteutuksen pohdinta

5.2.1 Tutkimuksen luotettavuus

Tässä tutkimuksessa luotettavuutta mitattiin määrällisen tutkimuksen luotettavuustarkastelussa tyypillisten reliabiliteetin ja validiteetin avulla, jotka soveltuvat myös laadullisen tutkimuksen luotettavuuden arviointiin. Lisäksi luotettavuutta arvioitiin laadullisen tutkimuksen luotettavuuskriteerien, eli uskottavuuden ja siirrettävyyden avulla. Tutkimuksen luotettavuuteen on kiinnitetty huomiota tutkimuksen kaikissa vaiheissa.

5.2.2 Reliabiliteetti

Reliabiliteetilla tarkoitetaan luotettavuutta ja toistettavuutta, eli reliabiliteetti ilmaisee sen, miten luotettavasti ja toistettavasti käytetty mittari mittaa haluttua ilmiötä (Tilastokeskus 2021a). Käytännössä tutkimus ei saa sisältää sattumanvaraisia tuloksia, jotta tutkimus on luotettava ja toistettavissa.

Reliabiliteetin arviointi on osittain hankalaa, koska käsitteenä se sopii paremmin kvantitatiivisen tutkimuksen arviointiin. Toistettavuuden osalta voitaneen olettaa, että jos haastateltava vastasi haastattelukysymyksiin autenttisesti, vastaa hän niihin samalla tavalla, jos tutkimus toistetaan. Suullisten haastattelujen osalta voidaan olla varmoja siitä, että vastaukset ovat autenttisia koska haastateltavat eivät tienneet haastattelukysymyksiä etukäteen, eikä kahdenkeskeisessä haastattelutilanteessa ole ollut riskiä, että vastauksiin olisi vaikuttanut esimerkiksi ryhmäpaine tai muut ulkoiset tekijät. Haastattelutulosten luotettavuuden arviointi on kirjallisesti saatujen vastausten osalta hankalaa, koska vastauksista ei voi päätellä ovatko vastaukset täysin autenttisia.

5.2.3 Validiteetti

Validiteetti tarkoittaa tutkimuksen pätevyyttä ja ilmaisee sen, miten hyvin tutkimuksessa käytetty mittausmenetelmä mittaa juuri sitä tutkittavan ilmiön ominaisuutta, mitä on tarkoituskin mitata (Tilastokeskus 2021b).

Validiteetin arvioinnissa on punnittu, onko tutkimuksen kohderyhmä ja kysymykset oikeat tutkittavan ilmiön kannalta. Tutkimuksen tavoitteena oli kartoittaa hoivarobotiikan asiantuntijoiden näkemystä hoivarobottien kyberturvauhkista. Haastateltavat, eli tutkimuksen kohderyhmä valittiin harkinnanvaraisesti. Haastateltavien taustat tarkistettiin, jotta voitiin olla varmoja siitä, että he ovat toimineet asiantuntijatason tehtävissä hoivarobotiikan hankkeissa, hoivarobottien kehityksessä tai hoivarobotiikan palveluntarjonnassa. Haastattelun toteuttaminen teoriaan perustuvana teemahaastatteluna antoi haastateltaville laajan mahdollisuuden kertoa omat näkemyksensä teemoihin liittyvistä asioista.

5.2.4 Uskottavuus ja siirrettävyys

Laadullisen tutkimuksen luotettavuus ja uskottavuus herättävät helposti keskustelua, koska laadullinen tutkimus perustuu ihmisten subjektiivisten kokemusten ja näkemysten tarkasteluun. Haasteita luotettavuuden ja uskottavuuden näkökulmasta luo myös tutkijan asema ja tulkinnanvaraisuus, koska laadullisessa tutkimuksessa tutkijan ja tutkittavan suhde on vuorovaikutteinen, ja tarkasteltavana on tulkintaan ja ymmärtämiseen liittyviä prosesseja. (Puusa & Juuti 2020, 59–60.) Uskottavien päätelmien teko haastatteluista edellyttää, että haastattelut tallennetaan, jotta voidaan tehdä analyysi, joka perustuu objektiivisesti haastattelussa saatuun tietoon. Objektiivisuuden takaamiseksi haastatteluissa kiinnitettiin erityisesti huomiota siihen, että haastattelija ei ohjaa tutkittavien vastauksia. Jotta voitiin varmistua siitä, että haastattelija ja haastateltava varmasti kuitenkin puhuvat samasta asiasta, käytiin tutkimuksen kannalta keskeisimpien käsitteiden määritelmät läpi haastattelun alussa. Tutkittavaa pyrittiin haastattelun aikana ymmärtämään mahdollisimman hyvin, joten lisäkysymyksiä esitettiin tarvittaessa ymmärryksen saavuttamiseksi.

Tutkimusaineiston analyysi pyrittiin tekemään tulkitsemalla haastateltavien lausumia mahdollisimman totuudenmukaisesti ja objektiivisesti. Laadullisessa tutkimuksessa haastattelu ymmärretään kuitenkin vuorovaikutustilanteena, jossa haastattelijan merkitystä aineiston muotoutumiseen ei voi kokonaan koskaan poistaa (Juhila, 2021). Koska osa aineistosta saatiin kirjallisena, ei vuorovaikutusta erityisesti syntynyt, ja haastattelijan merkitys oli kirjallisesti saadussa aineistossa pienempi. Tutkimukseen uskottavuutta vahvistaa, että tutkimuksen kohderyhmä oli valittu tarkasti. Tutkimukseen osallistui 6 haastateltavaa, joten tutkimus olisi mahdollisesti hyötynyt suuremmasta otannasta, mutta jo tällä otannalla aineistossa havaittiin selkeää saturaatiota.

Tässä tutkimuksessa ei erityisemmin pyritty siirrettävyyteen, mutta koska tutkimuksen osallistujat on valittu tarkkoihin kriteereihin perustuen, voidaan olettaa, että heillä on kokemusta ja ensikäden tietoa tutkimuksen aihepiiristä. Haastatteluihin osallistuneet olivat lisäksi kiinnostuneita tutkimuksesta ja suhtautuivat siihen myönteisesti, joten aineiston kokoamista voidaan pitää tarkoituksenmukaisena, ja siten todennäköisenä että toinen tutkija voi päätyä samoihin päätelmiin.

5.2.5 Tutkimuksen eettisyys

Tutkimusetiikka on osa hyvää tieteellistä käytäntöä, ja siinä on kyse niistä toimintatavoista, joita tutkijan tulee noudattaa tuottaakseen kestävää tietoa ja kohdellakseen tutkimiansa ihmisiä hyvin (Vuori 2021). Tutkimuseettisen neuvottelukunnan (TENK 2019) mukaan kaikkia tutkijoita kaikilla tieteenaloilla Suomessa ohjaavat yleiset eettiset periaatteet, ja niitä on myös tässä tutkimuksessa noudatettu. Yleisiin eettisiin periaatteisiin kuuluu mm. tutkittavien henkilöiden ihmisarvon ja itsemääräämisoikeuden, ja muiden perustuslain (1999/731, 6–23 §)

mukaisien oikeuksien kunnioittaminen, sekä tutkimuksen toteutus siten, että tutkimuksesta ei aiheudu tutkittavina oleville ihmisille, yhteisöille tai muille tutkimuskohteille merkittäviä riskejä, vahinkoja tai haittoja. Tutkijan on erityisen tärkeää huolehtia tutkittavien oikeuksista, joihin kuuluu mm.:

- osallistumisen vapaaehtoisuus ja mahdollisuus kieltäytyä, keskeyttää tai peruuttaa osallistuminen, ja riittävä harkinta-aika osallistumispäätöksen tekoon
- oikeus saada tietoa tutkimuksen sisällöstä, henkilötietojen käsittelystä ja tutkimuksen käytännön toteutuksesta, mukaan lukien aineiston käsittelyn ja säilyttämisen elinkaari
- oikeus saada ymmärrettävä, totuudenmukainen ja realistinen kuva tutkimuksen tavoitteista sekä osallistumisesta mahdollisesti koituvista haitoista ja riskeistä

Tutkimuseettisen neuvottelukunnan (TENK 2019) ohjeistuksen mukaan tutkittavia on informoitava heidän henkilötietojensa käsittelystä ja oikeuksista tutkimuksen ja sen kohderyhmän kannalta käytännöllisellä ja luontevalla tavalla. Tämän tutkimuksen osalta mahdollisia haastateltavia lähestyttiin sähköpostitse, ja haastattelupyynnössä ilmoitettiin:

- tutkimuksen tarkoitus ja tavoitteet
- osallistujien pysyminen anonyymeinä ja kaikkien tietojen käsittely luottamuksellisesti
- tutkimuksen toteuttamisesta mainittiin, että haastattelut nauhoitetaan ja litteroidaan analyysiä varten
- mahdollisuus kysyä lisää tutkimuksesta, ja yhteystiedot

Kirjallisessa haastatteludokumentissa sekä suullisten haastattelujen alussa kerrattiin tutkimuksen tarkoitus ja tavoitteet, käytiin läpi haastattelun toteutus ja aineiston käsittely (mm. henkilötietojen poistaminen kirjallisista vastauksista ja litteroidusta aineistosta), sekä aineiston säilyttämisen elinkaari. Haastateltavalle annettiin mahdollisuus kysyä mahdollisia kysymyksiä ennen haastatteluun osallistumista. Suullisten haastattelujen alussa pyydettiin vielä erikseen haastateltavalta lupa haastattelun nauhoittamiseen, ja mainittiin että haastatteluun osallistuminen on vapaaehtoista ja haastattelun voi keskeyttää koska vain jos niin haluaa.

Anonymiteettia noudatettiin vaihtamalla kaikki henkilötiedot tunnistetiedoiksi litteroinnin yhteydessä. Litteroinnin jälkeen haastattelunauhoitteet hävitettiin. Litteroitu ja muu tekstimuotoinen aineisto säilytettiin tutkimuksen ajan, eli opinnäytetyön arviointiin asti. Opinnäytetyön arvioinnin jälkeen aineistot tuhottiin.

Tieteen näkökulmasta tutkimusetiikkaa noudatettiin mm. toteuttamalla litteroinnit noudattamalla haastateltavien lausumia mahdollisimman uskollisesti, jotta aineisto ei pääse vääristymään. Raportissa pyrittiin noudattamaan totuudenmukaisuutta kaikissa vaiheissa.

6 Johtopäätökset

Tutkimuksen tarkoituksena oli kartoittaa asiantuntijoiden näkökulmaa siitä, millaisia kyberturvaan liittyviä uhkia ja riskejä hoivarobotiikkaan liittyy. Tutkimus toteutettiin laadullisena teemahaastattelututkimuksena, joka tuotti rikkaan aineiston aiheesta.

Tämän tutkimuksen perusteella voidaan todeta, että hoivarobotiikan käyttöön liittyy samat riskit ja uhkat kuin muiden IT-laitteiden tai robottien käyttöön, mikä tukee aiempien tutkimusten tuloksia hoivarobottien kyberturvauhkista. Suurimmat uhkat liittyvät hoivarobottien hallinnan kaappaukseen, ja siihen että niitä voidaan käyttää vakoiluun ja salakuunteluun, mutta myös muut uhkat ovat mahdollisia. Lisäksi verkkoon kytkettävyys, ja uudet ominaisuudet kuten tekoäly ja koneoppiminen luo lisää mahdollisuuksia kyberrikollisuudelle. Tulevaisuudessa kun robottien fyysiset ominaisuudet, ja mm. esineiden manipulointikyky paranee, tulee fyysiseen ympäristöön liittyvät uhkat kasvamaan.

Vaikka hoivarobotit ovat käytännössä alttiita täysin samoille uhkille kuin muut jo käytössä olevat laitteet, on riski sille, että hoivarobotteihin kohdistuu kyberturvauhkia tilastollisesti pienempi, koska hoivarobotteja ei juurikaan ole. Tästä näkökulmasta voitaneen olettaa, että kyberrikollisuus kohdistuu tällä hetkellä ennemmin muihin laitteisiin. Tämän tutkimuksen mukaan tulevaisuudessa tilanne tulee kuitenkin muuttumaan, kun hoivarobotit kehittyvät ja niitä tuodaan enemmän markkinoille.

Tämän tutkimuksen mukaan hoivarobotiikka robottiluokkana on toistaiseksi hyvin epämääräinen, eikä tällä hetkellä ei ole olemassa sääntöjä tai regulaatioita, jotka erityisesti määräsivät, että hoivarobottien turvallisuuden tulee täyttää mitään vaatimuksia. Jos uusia laitteita, joilla ei ole lääkinnällisen laitteen luokitusta, otetaan käyttöön, tulee niiden kyberturvallisuuteen kiinnittää erityistä huomiota. Esimerkiksi jos telepreesenslaitteita ja muita etäyhteysrobotteja otetaan hoivan käyttöön, tulee olla erityisen tarkka niiden turvallisuuden suhteen, koska tässä tutkimuksessa haastateltujen asiantuntijoiden mukaan laitteissa ei tyypillisesti ole pyritty korkean tason tietoturvaan. Jos tällaisia laitteita käytetään hoivan tarkoitukseen, täytyy olla varmoja siitä, että yhteyksiin ei voi murtautua koska hoitajan ja asiakkaan välillä saatetaan käydä arkaluontoisia keskusteluja, tai muuta vastaavaa.

Aiempiin tutkimuksiin verrattuna tässä tutkimuksessa nousi esiin enemmän kyberturvan taustalla vaikuttaviin inhimillisiin tekijöihin liittyviä näkökulmia, ja että kyberturvallisuus on kilpajuoksua kyberrikollisuutta vastaan. Hoivarobottien käyttöönotossa ja niiden kyberturvallisuutta arvioitaessa tulee ottaa huomioon, että rikollisen toiminnan takana on yleensä jokin motiivi. Jos riskejä arvioidaan kapealla sektorilla (esim. mikä on pahin uhka mikä voi tapahtua?), eikä ajatella motiiveja tekojen taustalla, voidaan päätyä erikoisiin johtopäätöksiin siitä, että hoivarobotteja ei tulisi olla koska niille on mahdollista tapahtua

asioita, joita on käytännössä mahdotonta estää. Tätä logiikkaa käyttäen voitaisiin päätyä mm. johtopäätökseen, että autoja ei tulisi olla koska joku voi sabotoida autoa niin että se ei toimi kuten sen pitäisi, ja kuljettaja voi ajaa kolarin. Siksi motiivien ja rikollisuudella saavutettavien hyötyjen kartoitus on keskeisessä asemassa, jotta myös hoivarobotiikan suhteen päästään tasapainoon hyväksyttävien riskien ja vakavien riskien välillä.

6.1 Jatkotutkimusehdotukset

Asiantuntijat pohtivat tässä tutkimuksessa mahdollisia kyberturvauhkia usein sen kautta, millainen hyöty siitä on kyberrikolliselle. Asiantuntijat toivat esiin näkökulman siitä, että pitäisi ajatella kuten kyberrikollinen, jotta voitaisiin ymmärtää mitkä asiat motivoivat heitä rikolliseen toimintaan, ja millaisia hyötyjä toiminnasta voi olla. Hoivarobotteihin kohdistuvan kyberrikollisuuden motiivien ja mahdollisten hyötyjen kartoitus olisi aihe, jota voitaisiin jatkossa tutkia tarkemmin, ja mahdollisesti kehittää riskianalyysimalli, jonka perusteella hoivarobottien käyttöön liittyviä riskejä voitaisiin konkreettisesti arvioida eri ympäristöissä.

Toinen näkökulma, joka haastatteluissa nousi esiin mutta jätettiin tämän työn ulkopuolelle koska se ei suoranaisesti liittynyt tutkimuskysymykseen, oli hoivarobottien kyberturvaan liittyvän vastuun jakautuminen, kun hoivarobotteja otetaan enemmän käyttöön. Asiantuntijat pohtivat sitä, millainen konsepti tai kokonaisuus takaa laitteiden turvallisuuden ja ylläpidon laitteen koko elinkaaren ajaksi, ja miten vastuun tulisi jakautua eri tahojen välillä. Tätä näkökulmaa voitaisiin tutkia laajemmin, ja kartoittaa millainen palveluekosysteemi takaisi hoivarobottien turvallisuuden kehitysvaiheessa, käyttöönotossa ja ylläpidossa, ja mahdollistaisi sen, että loppukäyttäjät saavat tarvitsemansa opastuksen ja tuen hoivarobottien käyttöön liittyvissä asioissa.

Tässä tutkimuksessa nousi esiin myös asiantuntijoiden huoli siitä, miten laajempia toimintamalleja käytännössä voidaan toteuttaa turvallisesti hoivarobottien avulla toteutettavaksi. Jatkossa hoivarobottien käyttöönottoihin liittyen ja toimintamallien muutoksien osalta tulisi selvittää, millaisiin tilanteisiin voidaan joutua, jos kyberuhka toteutuu, ja miten robottien kautta hoidettavat palvelut näissä tilanteissa taataan.

Lähteet

Artikkelit

Fosch-Villaronga, E. & Mahlerb, T. 2021. Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. Computer law & security review, 41. Viitattu 3.5.2021. https://www.sciencedirect.com/science/article/pii/S0267364921000017

Lera, F., Llamas, C., Guerrero, Á., & Olivera V. 2017. Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety. Viitattu 07.07.2021. https://www.intechopen.com/books/robotics-legal-ethical-and-socioeconomic-impacts/cybersecurity-of-robotics-and-autonomous-systems-privacy-and-safety

Van Aerschot, L. & Parviainen, J. 2020. Robots responding to care needs? A multitasking care robot pursued for 25 years, available products offer simple entertainment and instrumental assistance. Ethics and Information Technology (22), 247–256. Viitattu 3.5.2021. https://link.springer.com/article/10.1007/s10676-020-09536-0

Tzafestas, S. 2018. Roboethics: Fundamental Concepts and Future Prospects. Information. Viitattu 06.07.2021. https://www.researchgate.net/publication/325884319_Roboethics_Fundamental_Concepts_and_Future_Prospects

Painetut

Hirsjärvi, S & Hurme, H. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. E-kirja. Helsinki: Gaudeamus.

Rousku, K. 2014. Kyberturvaopas - Tietoturvaa kotona ja työpaikalla. Helsinki: Talentum.

Tuomi, J. & Sarajärvi, A. 2018. Laadullinen tutkimus ja sisällönanalyysi, uudistettu laitos. Helsinki: Tammi.

Marttinen, J. 2018. Palvelukseen halutaan robotti. Tekoäly ja tulevaisuuden työelämä. Helsinki: Aula & Co

Sullins, J. P. (2009). Friends by design. A design philosophy for personal robotics technology. In P. E. Vermaas, et al. (Eds.), Philosophy and design from engineering to architecture (s. 143–157). Berlin: Springer Science and Business Media.

Särkikoski, T., Turja, T., & Parviainen, J. 2020. Robotin hoiviin? Yhteiskuntatieteen ja filosofian näkökulmia palvelurobotiikkaan. Tampere: Vastapaino.

Sähköiset

Check Point. 2017. HomeHack: How Hackers Could Have Taken Control of LG's IoT Home Appliances. Viitattu 14.7.2021. https://blog.checkpoint.com/2017/10/26/homehack-how-hackers-could-have-taken-control-of-lgs-iot-home-appliances/

Jokinen, A. 2021. Laadullisen tutkimuksen näkökulmat. Jaana Vuori (toim.) Laadullisen tutkimuksen verkkokäsikirja. Yhteiskuntatieteellinen tietoarkisto. Viitattu 07.09.2021. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/mita-on-laadullinen-tutkimus/laadullisen-tutkimuksen-nakokulmat/

Juhila, K. 2021. Laadullisen tutkimuksen ominaispiirteet. Teoksessa Jaana Vuori (toim.) Laadullisen tutkimuksen verkkokäsikirja. Yhteiskuntatieteellinen tietoarkisto. Viitattu 16.7.2021. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/mita-on-laadullinen-tutkimus/laadullisen-tutkimuksen-ominaispiirteet/

Laurea Ammattikorkeakoulu. 2019. Shapes hanke käynnistyy: digitaalisista palveluista haetaan ratkaisuja ikääntyvien hyvinvointiin. Viitattu 02.05.2021. https://www.laurea.fi/ajankohtaista/uutiset/shapes-hanke-kaynnistyy-digitaalisista-palveluista-haetaan-ratkaisuja-ikaantyvien-hyvinvointiin/

Malkavaara, M. 2020. Etiikan perusteita. Viitattu 07.07.2021. https://aoe.fi/api/download/etiikanperusteitalitteraatti-1608215915787.pdf

Noponen, N. 2020. Etiikan perusteet — perustellen. Viitattu 07.07.2021. https://aoe.fi/api/download/nnoponenetiikanperusteetperustellen3062020-1593550756115.pdf

Robotics Care. 2021. Om Poseidon. Viitattu 06.07.2021. http://roboticscare.com/poseidon/

Sosiaali- ja terveysministeriö. 2016. Digitalisaatio terveyden ja hyvinvoinnin tukena : Sosiaali- ja terveysministeriön digitalisaatiolinjaukset 2025. Viitattu 07.07.2021. https://verkkojulkaisut.valtioneuvosto.fi/stm/zine/2/cover

Sosiaali- ja terveysministeriö. 2019. Kyberturvallisuus Ohje sosiaali- ja terveydenhuollon toimijoille. Viitattu 06.07.2021. https://julkaisut.valtioneuvosto.fi/handle/10024/161683

TENK. 2019. Ihmiseen kohdistuvan tutkimuksen eettiset periaatteet ja ihmistieteiden eettinen ennakkoarviointi Suomessa. Tutkimuseettisen neuvottelukunnan ohje 2019. Viitattu

19.07.2021.
https://www.tenk.fi/sites/tenk.fi/files/Ihmistieteiden_eettisen_ennakkoarvioinnin_ohje_2019.pdf

Tilastokeskus. 2021a. Reliabiliteetti. Viitattu 07.09.2021.
https://www.stat.fi/meta/kas/reliabiliteetti.html

Tilastokeskus. 2021b. Validiteetti. Viitattu 07.09.2021.
https://www.stat.fi/meta/kas/validiteetti.html

Turvallisuuskomitea. 2018. Kyberturvallisuuden sanasto. Viitattu 07.07.2021.
https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Valtiovarainministeriö. 2021. Digitalisaation edistämisen ohjelma. Viitattu 07.07.2021.
https://vm.fi/digitalisaation-edistamisen-ohjelma

Vuori, J. 2021. Tutkimusetiikka ihmistieteissä. Teoksessa Jaana Vuori (toim.) Laadullisen tutkimuksen verkkokäsikirja. Yhteiskuntatieteellinen tietoarkisto. Viitattu 19.07.2021.
https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/tutkimusetiikka/tutkimusetiikka-ihmistieteissa/

Kuviot

Taulukot

Liitteet

Liite 1: Haastattelukutsu

Hei!

Olen tietojenkäsittelyn opiskelija Laurea AMK:sta ja teen opinnäytetyökseni tutkimuksen hoivarobotteihin liittyvistä kyberturvauhkista. Tutkimuksen tavoitteena on kartoittaa yleisellä tasolla hoivarobotiikan asiantuntijoiden, kuten tutkijoiden, palveluntarjoajien ja valmistajien näkökulmaa hoivarobottien käyttöön liittyvistä kyberturvauhkista. Tutkimus on osa Laurea AMK:n SHAPES-hanketta (Smart and Healthy Ageing through People Engaging in Supportive Systems), jonka tavoitteena on kehittää digitaalista palveluekosysteemiä tukemaan ikääntyvien ihmisten hyvinvointia, ja siten heidän mahdollisuuksiaan elää hyvää elämää kotona tai kodinomaisessa ympäristössä.

Etsin tutkimustani varten haastateltaviksi henkilöitä, jotka ovat tekemisissä hoivarobottien, tai hoivaroboteiksi sopivien robottien suunnittelun, valmistuksen, palveluntarjonnan tai hoivarobotteihin liittyvän hanketyön kanssa. Haastateltavat pysyvät anonyymeina ja kaikkia tietoja käsitellään luottamuksellisesti.

Haastattelu kestää enintään tunnin, ja se toteutetaan esisijaisesti vapaamuotoisena teemahaastatteluna etänä. Haastattelun ajankohta sovitaan yhdessä haastateltavan kanssa, ja haastattelut toteutetaan touko-syyskyyn aikana. Haastattelu nauhoitetaan, jotta haastattelun saattaminen tekstimuotoon yhteenvetoa varten olisi mahdollista. Jos haastatteluun osallistuminen ei onnistu, voi tutkimukseen osallistua myös vastaamalla haastattelukysymyksiin kirjallisesti tai äänittein.

Toivon, että pystyisitte tukemaan tutkimustani tulemalla haastateltavaksi. Jos Kerro kiinnostuksestasi lähettämällä minulle sähköpostia osoitteeseen marina.jarvinen@student.laurea.fi tai soittamalla/ lähettämällä viestiä numeroon *** *******. Vastaan myös mielelläni tutkimukseeni liittyviin kysymyksiin.

Ystävällisin terveisin,

Marina Järvinen

Opiskelija, Laurea AKM

Lisätietoa SHAPES.hankkeesta löydät mm. täältä: https://www.laurea.fi/en/current-topics/news/shapes-project-launched-harnessing-digital-services-to-support-the-well-being-of-ageing-individuals/

Liite 2: Interview request

Hello,

I am a computer science student at Laurea University of Applied Sciences, and I am doing my thesis research on cyber security threats related to care robots.
The aim of the research is to map, at a general level, the perspective of care robot experts, such as researchers, service providers and manufacturers, on cyber security threats related to the use of care robots.. The research is part of Laurea Universityv of Applied Sciences' SHAPES project (Smart and Healthy Aging through People Engaging in Supportive Systems), which aims to develop a digital service ecosystem to support the well-being of older people and thus their chances of living a good life at home or in a home like environment.

For the purpose of my research, I am looking for interviewees who are involved in the design, manufacture, service provision or project work related to care robots, or robots suitable as care robots. Interviewees remain anonymous and all information is treated confidentially.

The interview lasts up to an hour and is primarily conducted as a free-form thematic interview remotely. The time of the interview is agreed with the interviewee. The interview is recorded to allow the interview to be text-translated for summary. If you are unable to participate in the interview, you can also participate in the study by answering the interview questions in writing or by audio recording.

I hope you could support my research by participating in the interview. Let me know you interested by sending me an e-mail to marina.jarvinen@student.laurea.fi. I am also happy to answer any questions related to the research.

Thank you for your time,

Marina Järvinen

Student, Laurea AMK

More information about the SHAPES project can be found e.g. from here:
https://www.laurea.fi/en/current-topics/news/shapes-project-launched-harnessing-digital-services-to-support-the-well-being-of-ageing-individuals/

Liite 3: Haastattelurunko

Teema 1: Hoivarobottien kyberturva tällä hetkellä

Millainen käsitys hoivarobottien kyberturvasta tällä hetkellä?

Mitä kyberturvauhkia hoivarobotteihin kohdistuu tällä hetkellä?

Teema 2: Hoivarobottien mahdolliset kyberturvauhkat

Tuleeko mieleen muita hoivarobotteihin kohdistuvia kyberturvauhkia, joita ei vielä ole tullut esiin?

Näkemys mm. seuraavista:

”Stealth attack” & ”Replay attack”, ovat hyökkäyksiä, joissa hyökkääjä pääsee manipuloimaan/sieppaamaan järjestelmän viestinnän ja siten häiritsemään robotin sensorien toimintaa, ja siten aiheuttamaan esimerkiksi mobiilin robotin törmäämisen.

”False data injection”, on hyökkäys, jossa robotin käsittelemää dataa päästään muokkaamaan.

”Evesdropping”, on hyökkäys, jossa robottia käytetään salakuunteluun.

”Denial of Service” (palvelunestohyökkäys) on hyökkäys, jolla käytännössä lopetetaan robotin toiminta. DoS-hyökkäys ei välttämättä aiheuta suoraa vahinkoa itse laitteelle tai sen käyttäjälle, mutta estää robotin tarjoaman palvelun saannin.

”Remote access” on hyökkäys, jossa ulkopuolinen käyttäjä kaappaa laitteen, ja pystyy siten aiheuttamaan sekä yksityisyyteen että fyysiseen terveyteen liittyvää vahinkoa.

Teema 3: Merkittävimmät riskit

Mitkä ovat mielestäsi suurimmat uhkat tai riskit hoivarobottien kyberturvaan liittyen?