Yksityisen turvallisuusalan digitalisaatio Suomessa: tulevaisuuskuva vuoteen 2025

Pasi Vallin

2018 Laurea

Laurea-ammattikorkeakoulu

Yksityisen turvallisuusalan digitalisaatio Suomessa: tulevaisuuskuva vuoteen 2025

Pasi Vallin
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Joulukuu, 2018

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusalan koulutusohjelma
Tradenomi (AMK)

Pasi Vallin

Yksityisen turvallisuusalan digitalisaatio Suomessa: tulevaisuuskuva vuoteen 2025

Vuosi 2018 Sivumäärä 52

Opinnäytteen tavoitteena on tuottaa yritykselle X tietoa, ennakoimalla digitalisaation mahdollisia tulevaisuuksia yksityisellä turvallisuusalalla. Opinnäytetyön tutkimustehtävänä on tutkia miten digitalisaatio mahdollisesti vaikuttaa Suomessa yksityiseen turvallisuusalaan tulevaisuudessa. Tutkimuskysymyksenä ovat: mitä todennäköisiä vaihtoehtoja tulevaisuus sisältää ja mihin vaihtoehtoon tulisi pyrkiä?

Tutkimusotteena on ennakointi, joka on tulevaisuudentutkimuksen käytännön ilmentymä. Opinnäytetyön tietoperusta on kerätty kirjoista, aikaisemmista tutkimuksista ja muista julkaisuista. Uutta tietoa on hankittu Delfoi-menetelmällä ja tulevaisuuspyörällä, tiedonlähteenä on käytetty aiheen asiantuntijoita. Tutkimuksen johtopäätöksiä ja olettamuksia mallinnetaan skenaarioilla, jotka tarjoavat mahdollisia tulevaisuuspolkuja yksityisen turvallisuusalan digitalisaation tilaan vuonna 2025.

Digitalisaatioon, ja ilmiön kehitykseen liittyvää kirjallisuutta, tutkimuksia, artikkeleita ja sähköisiälähteitä on runsaasti. Turvallisuusalaan keskittyvää materiaalia aiheesta on kuitenkin hankala löytää. Työn kannalta tärkeitä lähteitä olivat Laurea-ammattikorkeakoulu julkaisema tutkimus tulevaisuuden muutosvoimien vaikutuksesta turvallisuusalaan, sekä Valtiovarainministeriön julkaisu digitalisaation ja robotisaation mahdollisuuksista.

Tärkeä osa tutkimuksesta oli Delfoi-menetelmän mukaisesti suoritettu tiedon hankinta. Prosessi eteni kaksi kierroksisella haastatteluilla, kysymyspatteristojen avulla. Haastateltavina olivat neljä aiheen asiantuntijaa. Ensimmäisen kierroksen jälkeen kysymyksiä muokattiin palautteen mukaisesti, jonka jälkeen suoritettiin toinen haastattelukierros. Lopputuloksena oli asiantuntijoiden konsensus.

Toinen käytetty metodi oli tulevaisuuspyörä. Tulevaisuuspyörän avulla tunnistettiin aivoriihimäisesti pyörän keskelle määritellyn aiheen ympärille teemoja, pyörän ulkokehälle tunnistettiin trendejä, tapahtumia, päätöksiä, heikon signaalin vaikutuksia yhteiskunnan tai organisaation toimintaan. Tulevaisuuspyörän tavoitteena oli järjestellä, ymmärtää ja täsmentää erilaista tulevaisuutta koskevia näkemyksiä ja niiden mahdollisia vaikutuksia.

Vanhan ja uuden tiedon perusteella on luotu kolme erilaista skenaariota, eli tulevaisuuspolkua. Skenaariot mallintavat yksityisen turvallisuusalan digitalisaation mahdollisia tulevaisuuksia vuoden 2025 Suomessa. Tietoperusta ja tutkimus tukee digitalisaatiolle myönteisempien skenaarioiden toteutumista, kielteisin skenaario vaatisi vakavien riskien toteutumista. Digitalisaatio tehostaa ja luo uusia palvelu- ja liiketoimintamalleja. Työpaikkoja poistuu suorittavalta tasolta, mutta asiantuntijoille syntyy lisää työpaikkoja. Uhat myös monipuolistuvat ja monimutkaistuvat, aktiivinen riskienhallinta on erittäin tärkeää. Ilmiön ymmärtämistä syvemmin vaatii lisätutkimusta. Yksi tutkittava aihe olisi tulevaisuuden koulutustarpeet. Tällöin pystyttäisiin vastamaan proaktiivisesti työelämän osaamisen muuttuviin tarpeisiin.

Asiasanat: automatisaatio, digitalisaatio, esineiden Internet, megatrendi, robotisaatio, Smart city, yksityinen turvallisuusala

Laurea University of Applied Sciences **Abstract**
Degree Programme in Security Management
Bachelor´s Degree

Pasi Vallin

Digitalization of the Private Security Industry in Finland: Future Scenarios for 2025

Year 2018 Pages 52

The objective of the thesis is to provide information for company X, by foreseeing the possible futures of the Finnish private security sector digitalization. The mission of the thesis is to research how digitalization possibly affects the private security sector in the future. The research question answers the question of: what probable alternates the future contains and what the desirable outcome is.

The method of the thesis is foresight, which is a practical manifestation of futures studies. The framework off the thesis covers theories on past studies. The conclusions and presumptions of the study are modeled with scenarios, that show some possible future trails for the state of digitalization of the private security sector in 2025.

Important sources for the thesis were a Laurea University of Applied Sciences published study about the driving forces of the future in the security field, and the Ministry of Finances study about the possibilities of digitalization and robotization.

The Delphoi technique was exploited to gather data. The process involved two rounds of interviews, with readymade questions. Four experts working in the private security sector participated in the interviews. After the first round the questions were modified to the feedback of the experts. The process continued with the second round of interviews, after which there was a consensus on the subject matter.

Other method used to gather information was the Futures Wheel. A group brainstorming session was organized, where the subject matter was in the middle of the Futures Wheel and the purpose was to identify themes around the middle subject. On the next level of the wheel, around the themes, trends, events, decisions, and the weak signals´ impact on society and organizations were identified. The Futures Wheel is used to sort, understand and clarify the different views of the future and their impacts.

Three different scenarios, also called trails of the future, were crafted. The purpose was to model the possible state of the digitalization of the Finnish private sector in the year 2025. The framework of the thesis and the research support more digitalization positive trails of the future. The negative trail would need many of the identified risks to take place. Digitalization will result in optimizing and creating new services and business models. Some security guard jobs will be lost, but specialist jobs will be created. Threats will diversify and become more complicated, and as a result risk management will be very important. To better understand the matter of the thesis, there should be more specific research done. For example, by focusing on future needs of education, concerning the digitalization of the private security sector.

Keywords: automatization, digitalization, Internet of Things, megatrend, private security sector, robotization, Smart city

Sisällys

1 Johdanto

Digitalisaatio, pysäyttämätön megatrendi. Edellisen lauseen toteamus vaikuttaa olevan tosiasia, jota on hankala uskottavasti kyseenalaistaa. Digitalisaatio, ja siihen liittyvät muut ilmiöt kuten robotisaatio ja automatisaatio eivät ole taivaasta yhtäkkiä pudonneita ilmiöitä, vaan ovat kehittyneet vuosikymmeniä. Palvelut sähköistyvät vauhdilla, se on ollut trendi jo pitkään. Olin lapsena usein äitini mukana pankissa käymässä, koska piti asioida pankkivirkailijan luona, jotta sai maksettua laskut. Itse en ole koskaan maksanut laskuja pankissa, vaan sähköisesti Internetin kautta. Oheinen esimerkki havainnollistaa minkälaisia muutoksia digitalisaatio on lyhyessä ajassa mahdollistanut. Palvelujen sähköistyminen ei ole päättynyt, vaan jatkuu vielä pitkään.

On puhuttu, että lähitulevaisuudessa tapahtuu niin kutsuttu digiloikka, joka vaikuttaa elämäämme huomattavasti enemmän kuin aikaisemmat digitalisaation edistysaskeleet. Taustalla on toimintaympäristön kehittyminen digitalisaatiolle entistä suotuisammaksi, sekä teknologinen kehittyminen. Palvelujen, tuotteiden ja työn digitalisaatio kiihtyy ennen näkemättömän kiivaaksi. Kukaan ei voi tietää faktana, miltä tulevaisuus näyttää, mutta asiaa voi tutkia tieteellisillä menetelmillä. Tutkimuksen perusteella pystytään jossain määrin ennakoimaan tulevaisuutta. Ennakoimisen tarkkuuteen vaikuttaa käytettävissä oleva tietoperusta, on tärkeätä tunnistaa oikeat tiedonkeruumenetelmät ja tiedonkeruun kohteet, eli alan asiantuntijat.

Yksityinen turvallisuusala on ollut hyvässä nosteessa. Alalla liikkuu enemmän rahaa kuin koskaan, ja trendi on edelleen ylöspäin. Työntekijöiden määrä on kasvanut samaa tahtia, tämä koskee niin toimihenkilöitä kuin suorittavan työn tekijöitä, eli vartijoita, järjestyksenvalvojia, asentajia ja niin edelleen. Digitalisaatio on tähän mennessä tukenut liikevaihdon ja työntekijöiden määrän kasvua. Yleisesti on ollut kuitenkin esillä, että digitalisaation eteneminen aiheuttaa isoja muutoksia työvoimantarpeeseen. Toimintaympäristön muutokset vaikuttavat luonnollisesti myös yksityiseen turvallisuusalaan, joten on arvokasta ennakoida tulevaa tunnistaakseen mahdollisimman hyvin tuleva suunta. Tutkimukseen perustava arvio tulevaisuudesta voi auttaa tekemään oikeita päätöksiä nykyisyydessä.

Alun alkaen vartiointiliikkeet suorittivat vartiointia tekemällä kierroksia jalan ja autolla. Teknologian kehityksen myötä syntyivät erilaiset järjestelmät, kuten rikosilmoitin- ja kamerajärjestelmät. Nämä synnyttivät alalle uusia palveluita, tuotteita ja toimintoja. Syntyi esimerkiksi turvallisuusalan yritysten pyörittämät hälytyskeskukset, jotka muistuttavat varsinkin teknisesti hätäkeskuksia. Niissä valvotaan muun muassa murto-, palo-, ja ryöstöhälytyksiä. Digitalisaatio on jo mahdollistanut uudenlaista liiketoimintaa, sekä luonut uusia sidosryhmiä. Tulevaisuudessa otetaan uusi askel tai loikka, mutta mihin se vie?

2 Tutkimuksen lähtökohdat: tarve, tavoite ja tutkimuskysymys

Opinnäytetyön toimeksiantaja haluaa tarjota asiakkailleen digitalisaation mahdollistamia uusia palveluja. Digitalisaation mahdollistamista ratkaisuista tulee tunnistaa ne mitkä aidosti tuovat lisäarvoa asiakkaille ja toimeksiantajani liiketoiminnalle. Tarpeena on ymmärtää digitalisaatio ilmiönä paremmin, sekä ennakoida ilmiön vaikutusta yksityiseen turvallisuusalaan tulevaisuudessa.

Opinnäytteen tavoitteena on tuottaa yritykselle X tietoa ennakoimalla digitalisaation mahdollisia tulevaisuuksia yksityisellä turvallisuusalalla. Tiedon ei tässä tapauksessa ole tarkoitus olla faktatietoa, koska tulevaisuudentutkimus ei ole missään nimessä eksaktia tiedettä. Tulevaisuudenkuvien tulee olla mahdollisia ja perustua olemassa olevaan tietoon tai tutkimukseen.

Digitalisaatio ei ole varsinaisesti uusi asia, mutta ilmiön vaikutukset näkyvät ennustusten mukaan usealla alalla lähitulevaisuudessa entistä radikaalimmin. Opinnäytetyöni tutkimustehtävänä on tutkia miten ilmiö mahdollisesti vaikuttaa Suomessa yksityiseen turvallisuusalaan lähitulevaisuudessa. Tutkimuskysymyksenä on: mitä todennäköisiä vaihtoehtoja tulevaisuus sisältää ja mihin vaihtoehtoon tulisi pyrkiä?

2.1 Toimeksiantaja organisaation esittely

Toimeksiantajana on suomalainen, vain Suomessa liiketoimintaa harjoittava turvallisuusalan yritys. Toimeksiantajani edustajan pyynnöstä yrityksen nimeä ei opinnäytetyössäni mainita. Yritys on aikaisemmin ollut osa suurta, kymmenissä maissa toimivaa monialaista konsernia. Itsenäistyminen itsenäiseksi toimijaksi ilman emoyrityksen ohjausta ja tukea on ollut haastavaa. Tapahtuma on kuitenkin mahdollistanut oman vision toteuttamisen itsenäisen turvallisuusalan toimijana.

Toimeksiantajallani on tavoitteena erottautua positiivisesti muista alan toimijoista, ja lisätä tunnettavuuttaan. Tämä on tärkeää varsinkin nyt, kun takana ei ole enää emoyrityksen brändiä ja myyntiorganisaatiota. Yritys näkee jättimäisen potentiaalin digitalisaatiossa, ja uskoo kyseisen megatrendin mullistavan turvallisuusalaa. Ilmiön onnistunut hyödyntäminen auttaa yrityksen tavoitteiden saavutuksessa, tuoden kilpailuetua.

Visiona on olla uuden teknologian mahdollistamien palveluiden uran uurtajana omalla alallaan. Toimeksiantajani organisaatiossa on projekteja käynnissä liittyen palveluiden digitalisoimiseen. Yritys tarjoaa tällä hetkellä asiakkaille alan palveluita laidasta laitaan, esimerkiksi vartiointia, asiantuntijapalveluita ja turvallisuustekniikan ratkaisuja.

Yrityksellä on paljon sidosryhmiä, mukaan lukien alihankkijoita, sekä yritys tekee itse myös alihankkijana töitä. Suomen kokoisessa maassa yhteistyökumppaniverkosto on tärkeä, kun tavoitteena on pystyä tarjoamaan palveluja joka kolkkaan. Digitalisaatio voi poistaa välimatkan

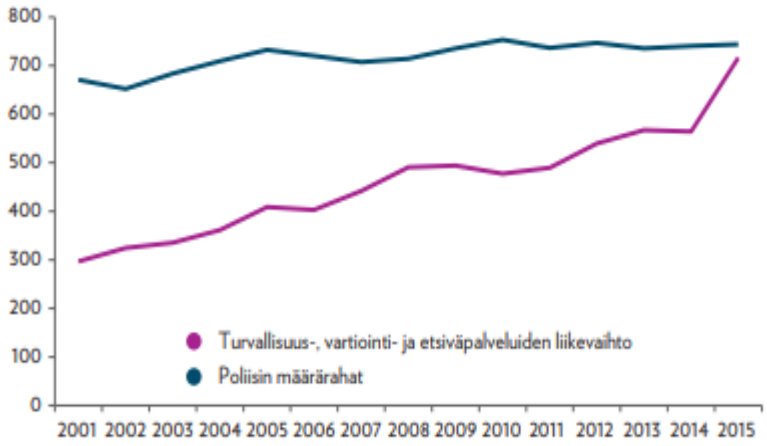
merkityksen palveluntuotannossa, mutta iso osa turvallisuusalan palveluista vaatii ainakin vielä fyysisen käymisen tiloissa.

2.2 Toimintaympäristö

Suomen nykyinen hallitus, eli Sipilän ensimmäinen, on määritellyt toteutettavaksi viisi kärkihanketta. Yksi hankkeista on teemalla ”Digitalisaatio, kokeilut ja normien purkaminen”. Sipilän hallitusohjelman 2025-tavoitteissa visioidaan, että Suomi olisi ottanut tuottavuusloikan julkisissa palveluissa ja yksityisellä sektorilla tarttumalla digitalisaation mahdollisuuksiin ja purkamalla turhaa sääntelyä ja byrokratiaa. Suomen ketterää uudistumista tuetaan luottamukseen, vuorovaikutukseen ja kokeilujen hyödyntämiseen perustuvalla johtamiskulttuurilla. Rakennetaan digitaalisen liiketoiminnan kasvuympäristö. Luodaan suotuisa toimintaympäristön digitaalisille palveluille ja uusille liiketoimintamalleille. Luodaan innovaatio- ja palveluiden syntymistä tukeva säädös- ja T&K-ympäristö. Hyödynnetään massadataa ja robotisaatio uuden liiketoiminnan ja toimintatapojen luomiseksi. Varmistetaan tietoturva. Päätoimiksi luetellaan esineiden internetin edistäminen, liikenteen digitaalisten palveluiden kasvuympäristö luominen, luottamusta lisäävän tietoturvastrategian, sekä robotiikan- ja massadatan toimintaohjelman toimeenpaneminen. Hallitusohjelman käytännön toteutuksen pitäisi mahdollistaa sopivan alustan niin kutsutulle digiloikalle. (Valtioneuvosto 2017.)

Tarkasteltaessa viimeisen sadan vuoden muutoksia yksityisen turvallisuusalan näkökulmasta, on muutos ollut suurta. Tarkastelujakson alkupuolella olivat tekniset apuvälineet vähissä, lähinnä lukkoja ja kaltereita. Vasta 1900- luvun jälkimmäisellä puoliskolla alkoi ilmestyä yleiseen käyttöön soveltuvia, huomattavasti turvallisuutta lisänneitä teknisiä ratkaisuja. Markkinoille tulivat esimerkiksi valvontakamerat, erilaiset sensorit, hälytysvalvonta hälytyskeskuksista käsin. Nyt toimintaympäristö, sekä teknologian eteneminen alkaa olemaan kypsä uudelle aikakaudelle.

Palkansaajien tutkimuslaitoksen raportti poliisien resursseista on käyttänyt yksityistä turvallisuusalaa verrokkina. Raportissa muun muassa kuvataan yksityisen turvallisuusalan liikevaihdon kasvua vuodesta 2001 vuoteen 2015 (Kuvio 1). Tarkastelujakson aikana liikevaihto on tuplaantunut, ja on juuri ohittamassa poliisien määrärahan määrää, joka on ollut lähes vakio. Kasvutrendi on jatkunut jo pitkään, eikä sen pysähtymistä ole näkyvissä lähitulevaisuudessa. (Kari 2017, 56.)



Kuvio 1: Poliisin määrärahat verrattuna yksityisen turvallisuusalan yritysten yhteenlaskettuun liikevaihtoon (milj. €) 2001-2015 (Kari 2017, 57)

Samassa raportissa käsitellään myös vartijoiksi hyväksyttyjen ja järjestyksenvalvojakortin haltijoiden määrää (Taulukko 1). Kuvio 1 havaittu liikevaihdon kasvu on tähän mennessä korreloinut jokseenkin vartijoiksi hyväksyttyjen määrän kanssa, liikevaihdon kasvu on ollut hieman nopeampaa. Sama koskee myös järjestyksenvalvojakorttien haltijoita.

	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Vartijoiksi hyväksytyt	11 573	11 513	11 737	12 220	12 508	12 969	13 704	14 186	14 545	14 909	15 393
Järjestyksenvalvoja-kortin haltijat	40 461	47 170	47 170	52 891	51 950	51 988	53 490	51 308	50 223	50 605	52 652

Taulukko 1: Vartijoiksi hyväksyttyjen henkilöiden ja järjestyksenvalvojakortin haltijoiden lukumäärät 2003-2013 (Kari 2017, 56)

Tähän mennessä alan liikevaihdon kasvu on myös tuonut lisää työpaikkoja (Kuvio 1; Taulukko 1). Tulevat digitalisaation tuomat toimintaympäristön muutokset saattavat muuttaa tämän trendin. Turvallisuusala on perinteisesti tarjonnut runsaasti myös matalamman koulutuksen työpaikkoja. Yleinen käsitys on, että digitalisaation luomat uudet työntehtävät syntyvät pääosin korkeampaa koulutusta vaativiin tehtäviin (Palvelualojen työnantajat PALTA ry 2016, 42).

Toimintaympäristön muutoksista huolimatta, monet turvallisuusalan yritykset ovat toimineet hyvin samanlaisella liiketoimintamallilla koko elinikänsä, ei ole koettu tarvetta muuhun. Ala on vuosien saatossa teknistynyt, mutta radikaaleimmat muutokset ovat todennäköisesti edessäpäin. Ennen on pärjätty vartija ja auto periaatteella, ja vielä on pieniä paikallisia yrityksiä, jotka toimivat edellä mainitulla konseptilla. Toimintaa tukemaan on tullut monenlaista tekniikka. Tekniikka on tuonut erilaisia palveluita, joilla asiakkaille tuotetaan lisäarvoa, mutta

ydinliiketoiminta on pysynyt samana. Tulevaisuudessa, myös turvallisuusalalla, pitää valmistautua radikaaleihin liiketoiminta muutoksiin toimintaympäristön muuttuessa. Digitalisaatio on todennäköisesti vaikutuksiltaan isoin megatrendi, joka tullee muuttamaan toimintaympäristöä rajusti. Radikaalisti muuttuvan toimintaympäristön myötä, Innovatiivisilla ratkaisuilla on mahdollista pienemälläkin pääomalla uusien yritysten haastaa isoja markkinajohtajia (Linz, Müller-Stewens & Zimmerman 2017, 1).

Yksityiseltä turvallisuusalalta löytyy hyvin monella eri konseptilla toimivia toimijoita, osa uskoo vanhoihin toimintamalleihin ja osa modernimpiin. Perinteisesti pienemmät alan yritykset seuraavat kehityksen perässä, koska heillä ei ole resursseja tuotekehitykseen. Pienemmät yleensä toimivatkin alueilla, joihin isot eivät ole laajentaneet. Pienempiä alan yrityksiä on määrällisesti useita, mutta käytännössä kolme isoa yritystä pitävät hallussaan Suomen yksityisen turvallisuusalan markkinat. Nämä kolme ovat suuruusjärjestyksessä Securitas Oy, AVARN Security Oy ja Prevent 360 Turvallisuuspalvelut Oy. Näistä kaksi jälkimmäistä ovat tämän opinnäytetyön luomisen aikana ilmoittaneet yhdistyvänsä.

Suomen toiseksi isomman yksityisen turvallisuusalan yrityksen, eli AVARNin, toimitusjohtaja Juha Murtopuron uskoo, että tekniikan kehittyessä yhteistyökumppanit ja kilpailijat ovat entistä monialaisempia. Pelkällä perinteisellä vartioinnilla ja rikosilmoitin- ja kiinteistöhälytysjärjestelmien hälytysvalvonnalla ei pärjätä uudessa toimintaympäristössä. Pitää pystyä havainnoimaan entistä tarkemmin ja laaja-alaisemmin uusia mahdollisuuksia kilpailuedun saavuttamiseksi. Hän uskoo teknologian tuovan uusia mahdollisuuksia Tärkeä yhteistyökumppani voi löytyä täysin eri alalta. (Lahtinen 2016, 24 – 25.)

Murtopuro kertoo, että tällä hetkellä 70 prosenttia heidän yrityksen kuluista on palkkoja. Hänen mukaansa kulurakenne tulee muuttumaan huomattavasti teknologian kehityksen myötä. joten teknologian avulla työtä voidaan kehittää ja tehostaa merkittävästi. Voi päätellä, että Murtopuro uskoo alan palkkakulujen jatkossa ainakin prosentuaalisesti pienentymään digitalisaation etenemisen johdosta. Toisin sanoen hän uskoo, että perinteisten vartijoiden tuottamat palvelut ainakin osin siirtyvät teknisten järjestelmien harteille. Tämä muuttaisi alaa huomattavasti, ala ei enää työllistäisi niin paljoa vartijoita ja alalle jäävien työnkuviin tulisi isojakin muutoksia. (Lahtinen 2016, 24 – 25.)

Murtopuro uskoo, että muitten alojen, kuten vähittäiskaupan digitalisaatio näkyy myös turvallisuusalalla. Kivijalkakauppojen vähentyessä, niin vähenee myös tarve vartioinnille. Verkkokaupatkin tarvitsevat turvallisuutta, mutta sitä ei tuoteta perinteisellä vartioinnilla. Ennen vartijan piti olla fyysisesti läsnä, niin nyt ja tulevaisuudessa toimenpiteitä voi suorittaa etänä. Murtopuro arvioi myös, että julkisella puolella siirrytään aina vain enemmän käyttämään yksityisen puolen palveluita. (Lahtinen 2016, 24 – 25.)

2.3 Opinnäytetyön rajaus

Digitalisaatio ilmiönä koskettaa käytännössä kaikkia aloja, opinnäytetyöni rajoittuu yksityiseen turvallisuusalaan. Näkökulmana on toimeksiantajani liiketoiminta, johon kuuluu yksityisen turvallisuusalan luvanvarainen toiminta, turvallisuusasiantuntijapalveluita, järjestelmäasennuksia, sekä etähallintaa. Viranomaisten, armeijan ja tuomioistuimen näkökulma on rajattu pois, vaikkakin viranomaislähteitä käytetään hyödyksi.

Työni koskee vain Suomen yksityistä turvallisuusalaa. Suomi ei kuitenkaan ole erakoitunut saari, varsinkaan digitalisaation suhteen, osa tietoperustasta on ulkomaalaisista lähteistä. Digitalisaatio on globaali megatrendi, joka yleistasolla vaikuttaa saman suuntaisesti maasta riippumatta. Jokaisella maalla on kuitenkin omat ominaispiirteensä, jotka vaikuttavat myös siihen miten globaalitkin megatrendit kyseisessä maassa ilmentyvät.

Suomen yksityinen turvallisuusala on suurilta osin markkinaosuuksien suhteen muutaman ison toimijan hallussa. Opinnäytetyöni näkökulma keskittyy isoihin toimijoihin. Digitalisaatio tulee vaikuttamaan myös alan pieniin ja keskisuuriin yrityksiin, näitä ei ole rajattu täysin pois työstäni. Digitalisaatio mahdollisesti myös osittain tasoittaa pelikenttää. Digitalisaatio voi jatkossa mahdollistaa laajemman, laadukkaan palvelukokonaisuuden pienemmillä resursseilla.

Työn ei ole tarkoitus syventyä tarkasti esittelemään erilaisia tulevia yksittäisiä teknologisia ratkaisuja, vaan tutkia digitalisaatiota ilmiönä yksityisen turvallisuusalan näkökulmasta. Digitalisaatio ja ilmiöön liittyvät toimintaympäristön muutokset tulevat vaikuttamaan kiihtyvällä tahdilla kaikkiin aloihin. Ilmiön ymmärtäminen on tärkeää, jotta osataan ennakoida oikeat, liiketaloudellisesti kannattavat trendit. Tällöin pystytään tarjoamaan moderneja, lisäarvoa tuovia, digitalisaation mahdollistamia palveluita.

3 Tutkimuksen tietoperusta

Tutkimuksen aikana olen tutustunut ja hyödyntänyt useita lähteitä, joista muodostuivat työni teoreettinen viitekehys, eli tietoperusta. Tutkimukseni aihe ja tavoitteet määrittelivät, minkälaista tietoa lähdin etsimään. Itse opinnäytteen ja tutkimuksen tekemisen tietoperustana käytin Laurean suosittelemia teoksia, sekä tulevaisuuden tutkimukseen keskittyviä teoksia.

Digitalisaatioon liittyvää kirjallisuutta, tutkimuksia, artikkeleita ja sähköisiälähteitä on runsaasti, mutta turvallisuusalaan keskittyvää materiaalia vähän. Ilahduttavasti kuitenkin suomalaiset organisaatiot ovat kunnostautuneet tällä saralla, työni kannalta tärkeitä lähteitä ovat Laurea-ammattikorkeakoulussa ja Valtiovarainministeriössä tehdyt julkaisut aiheesta.

Omaan näkemykseeni liittyy paljon muitakin dokumentteja kuin opinnäytetyössä mainitut. Normaalisti tutkimuksessa tutkijan on tarkoitus olla objektiivinen, jottei tutkimustulokset oli-

sivat mitenkään riippuvaisia tutkijasta. Tulevaisuudentutkimuksessa tutkijan persoona on kuitenkin läsnä, varsinkin käytettäessä kertomuksellisia skenaarioita tutkimuksen tuloksena. Pyrin perustamaan skenaariot parhaani mukaan opinnäytetyössä esiteltyyn tietoperustaan ja tutkimukseen.

3.1 Keskeiset käsitteet

Tässä luvussa on esiteltynä opinnäytetyön kannalta keskeisimmät käsitteet, sekä niiden taustaa ja ilmentymiä yhteiskunnassa. Opinnäytetyössä on useita muitakin käsitteitä, joista osa on sanoina tuoreita. Pyrin avaamaan näitä muitakin käsitteitä mahdollisuuksien mukaan itse tekstissä, eli siinä kohtaa missä käsite esiintyy.

Digitalisaatio, megatrendit sekä Smart City ovat kaikki käsitteenä yleistyneet vasta 2000- luvulla. Aikaisemmin ei ole ollut tarvetta, eikä juurikaan mahdollisuutta kehittää edellä mainittuja käsitteitä. Nyt teknologia, sekä yhteiskunnan kehitys ovat siinä pisteessä, että kyseiset käsitteet ovat tarpeellisia ja ajankohtaisia. Lähes kaikissa käytössä olleissa lähteissä mainitaan kunkin käsitteen kohdalla, että niiden määritelmistä ei ole olemassa edes asiantuntijoitten kesken konsensusta.

Automaatio tulee kreikankielisestä sanasta automatos, joka tarkoittaa itsetoimivaa. Automaatiossa toiminta tapahtuu ilman ihmisen ohjaavaa tai suorittavaa osuutta. Automaatti on automaattisesti eli itsestään toimiva kone tai laite. Automaatio käsitetään usein vain teollisuuden koneistojen ja prosessien automaatioksi, mutta itsestään toimivia laitteita ja järjestelmiä on myös kodeissa, liikenteessä, maanviljelyssä, luonnossa - miltei kaikkialla. **Automatisaatio** on automaation yleistymistä, leviämistä. (Suomen automaatioseura ry, 2013.)

Digitalisaatio on digitaalisten teknologioiden yleistymistä arkielämän toiminnoissa. Tämän ilmiön kehitys mahdollistaa yhä vaativampien tehtävien siirtämisen tekoälylle, koneille. Digitalisaation kehittyminen lähentää virtuaalisen ja fyysisen maailman toisiinsa, niin ettei rajoja pian enää ole. Digitalisaatio koskettaa jokaista yritystä toimialasta riippumatta. (Ilmarinen & Koskela 2015, 9 – 13.)

Miksi digitalisaatiolla tullee olemaan isommat vaikutukset kuin millään aikaisemmalla ilmiöllä, kuten globalisaatiolle tai suurimmilla lamoillakaan? Koska digitalisaatio poistaa esteet tavoittavaa ihmisiä, jolloin palvelut, työnteko ja moni muu asia on paikasta ja ajasta riippumatonta. Työnkuvat muuttuvat, osa ammateista häviää ja tilalle tulee uusia. (Bonnet, McAfee & Westerman 2014, 1 – 7.)

Internet of Things, lyhennettynä IoT, suomennettu välillä esineiden Internetiksi on määritelty Sanastokeskus TSK Ry:n toimesta, Internetiksi, johon kytketään laajamittaisesti laitteita ja muita esineitä, jotta niitä voisi ohjata ja jotta ne voisivat olla vuorovaikutuksessa keskenään. Esine, kuten auto, sähkölaite tai ruokatavara, voi liittyä suoraan internetiin sellaisen

tietokoneena toimivan komponentin avulla, jolla on IP-osoite. Komponentti voi olla esimerkiksi anturi, RFID- tai WLAN-siru. Toisinaan riittää, että esineellä on jokin tunniste, kuten postipaketin lähetystunnus tai ajoneuvon rekisterinumerosta muokattu yksilöllinen tunniste, jonka avulla esine voidaan tunnistaa internetissä. Esineen ei silloin tarvitse kytkeytyä suoraan internetiin. Esineiden internetiä käytetään esimerkiksi energia- ja kuljetusalalla. Energiayhtiöt ovat antaneet kuluttajille älykkäitä sähkömittareita, joilla kuluttajat saavat tosiaikaista tietoa kulutuksesta ja energiayhtiöt voivat etälukea mittareita. Esineiden internetiä voi hyödyntää myös logistiikassa, jolloin esimerkiksi ruokatavara voi mitata ympäristönsä lämpötilaa jakeluketjussa, ja hälyttää, jos lämpötila ylittää tai alittaa tietyn rajan. (Sanastokeskus TSK Ry 2017.)

Megatrendi sana esiintyi ensimmäisen kerran 1980-luvulla. Täten kyseisen käsitteen määritelmä ei ole vielä täysin vakiintunut, on osittain tulkinta kysymys, milloin voidaan puhua megatrendistä. Yleisimmän tulkinnan mukaan on kolme kohtaa, jotta voidaan puhua megatrendistä. Ensinnäkin ilmiön pitää olla globaali, määritelmä täyttyy, vaikka ilmiö esiintyisi eri alueilla hieman eri muodossa. Maailma on laaja, ja eri alueilla on omat tapansa ja kulttuurinsa, joten globaalitkin ilmiöt saavat erilaisia vaikutteita alueesta riippuen. Myös alueen kehityksen taso vaikuttaa miten ilmiö, esimerkiksi digitalisaatio esiintyy alueella. Toiseksi vaaditaan, että ilmiöllä on huomattavat vaikutukset ekonomisesti, sekä vaikutusten pitää olla kestävät ja jatkuvat. Tällä rajataan pois hetken kestävät muoti-ilmiöt. Kolmanneksi megatrendin tulee olla käänteentekevä, sen pitää muuttaa ihmisten elämää vapaa-ajalla, työssä ja muuttaa näkökulmaamme, miten käsittelemme elämää. (Singh 2012, 4.)

Maaseudulta muutto kaupunkeihin on megatrendi, on arvioitu, että vuonna 2040 kolme neljästä ihmisestä asuu kaupungeissa (Dameri & Rosenthal-Sabroux 2014, 90). Ilmiön voi mielestäni selittää tarvittaessa yksinkertaisesti: Ihmiset menevät sinne missä on palveluita ja monipuolisesti mahdollisuuksia, niin työelämän kuin harrastusten suhteen. Smart City on yksi vetovoimaa lisäävä konsepti, harvaan asutuille aluille ei ole mahdollista viedä niitä ratkaisuja, joita kaupunkeihin nyt ja lähitulevaisuudessa rakennetaan. Vaikka digitalisaatio ja teknologian kehitys vähentää välimatkojen merkitystä, niin kaikkea ei voida tuoda suoraan kotiin.

Nykyiset ja tulevat megatrendit eivät ole ensimmäisiä, ihmisten elämäntyyliä muuttaneita muutoksia on ollut useita. Viime vuosituhannen loppupuolella alkoi teollistuminen, josta jatkumona saapuivat automatisointi ja globalisaatio. Teknologian kehittyminen on ollut avain asemassa näissä muutoksia ja näin on jatkossakin. Internetin yleistymisen jälkeen digitalisaatio toden teolla syntyi ja on nyt räjähtämäisillään siten, että moni asia muuttuu pysyvästi. Innovaatio ja digitalisaatio ovat jo muuttaneet monen valtion visiota omasta tulevaisuudestaan, duunariyhteiskunnasta siirrytään digipohjaiseen. Tästä hyvänä esimerkkinä on Viro, jota Ross kuvailee maaksi, jonka koko talous pohjautuu sähköisiin palveluihin. (Ross 2016, 4.)

Robotiikalla perinteisesti tarkoitetaan tietokoneohjattuja työkappaleita tai työvälineitä käsitteleviä yleiskäyttöisiä laitetta. Yleiskäyttöisyydellä tarkoitetaan liikkeiden ohjelmoitavuutta ja mahdollisuutta käyttää samaa laitetta useisiin käyttötarkoituksiin. Robotin liikkeet tuotetaan yleensä sähköisten toimilaitteiden avulla, mutta ne voivat olla myös pneumaattisia tai hydraulisia. Nykyisin roboteiksi nimetään fyysiseltä rakenteeltaan monenlaisia ohjelmallisesti liikkuvia laitteita, joihin usein liittyy ympäristön havainnointia ja sen mukaan toimimista – on olemassa erilaisia liikkuvia robotteja kuten automaattisesti ohjautuvia lennokkeja ja autoja. **Robotisaatio** on robottien, robotiikan yleistymistä ja leviämistä. (Salmi 2014.)

Smart city on visio kaupungeista, joissa pitkälle viety digitalisaatio parantaa ihmisten elämää, myös turvallisuuden näkökulmasta. Nykyajan kaupungit toimivat monella tasolla teknologian avustamana, myös yksilötasolla elämä on täynnä teknologiaa. Teknologia tukee meidän liikkumista, työtä, vapaa-aikaa, lähes kaikkea. Silti isoimmissakin, hienoimmissakin metropoleissa teknologia on vielä tyhmää, älytöntä, varsinkin verrattuna siihen mitä jo lähitulevaisuus tuo tullessaan. Ei ole olemassa konsensusta yksityiskohdista asian parissa työskentelevillä visionääreillä, mutta siitä ollaan samaa mieltä, että teknologia tulee jatkossa suunnitella tukemaan holistisesti ihmiskunnan kehitystä. Yksinkertaisuudessaan tavoitteena on tehdä kaikki paremmin, tehokkaammin ja älykkäämmin. Nykyinen teknologinen kehitys on avustanut ihmiskuntaa monella eri tavalla, mutta voi sanoa, että älyn kanssa ollaan vielä ensiaskelissa. Tällä hetkellä teknologiset välineet suorittavat asioita sokeasti, keinoälyä ei vielä aktiivisesti näe esimerkiksi kaupunkikuvassa. (Stimmel 2015, 18.)

Smart City käsitteenä on tuore, mutta ei niin tuore mitä voisi helposti luulla. Asiaa tutkinut Annalisa Cocchia löysi useita tutkimuksia Smart Cityn teemoista, jotka olivat noin kaksikymmentä vuotta vanhoja (Dameri & Rosenthal-Sabroux 2014, 2). Teemat olivat näissä tutkimuksissa teknologian ja varsinkin informaatioteknologian käyttäminen elämänlaadun parantamiseksi urbaaneissa miljöissä. Kuitenkin vasta lähivuosina keskustelu näistä teemoista, ja käsite Smart city on todella noussut suosioon. Tähän on useita syitä, kuten mobiililaitteiden yleistyminen ja kehitys, internetin leviäminen joka puolelle, kaupunkien kasvaminen usealla eri tavalla, tarve suojata elin oloja saasteilta ja saada energiankäyttö hallintaan.

Osa akateemikoista tulkitsee Smart City käsitteen sisältävän myös kaupungin kulttuurisen tason. Tätä perustellaan, että ollakseen Smart City, tarvitsee kaupunki erittäin laajaa älypääomaa. Tähän sisältyy kaupungin tarjoamat kulttuuriset palvelut, koulutus ja asukkaitten koulutuksen taso. Varsinkin liiketalouden toimijat tulkitsevat Smart Cityn tarkoittavan puhtaasti teknologiaan liittyvää edistyksellisyyttä. Opinnäytteeni näkökulma on yhtenäinen liiketalouden tulkinnan kanssa. (Dameri & Rosenthal-Sabroux 2014, 6.)

Yksityinen turvallisuusala on laajan määrittelyn mukaan elinkeinotoiminta, joka liittyy jollakin tavoin turvallisuudella harjoitettavaan liiketoimintaan. Matthys (2010) sijoittaa yksityiseen turva-alaan kaikki toimijat, jotka hankaloittavat rikosten tekemistä etu- tai jälkikäteen tai vaikuttavat positiivisesti asiakkaan rikostorjuntaan. Mandelin (2002) mukaan kriteereitä on kaksi: omistus ja kontrolli ovat selkeästi irti valtiosta ja palvelu on selkeästi sidoksissa turvallisuustoimintaan. Alaan voidaan määritellä kuuluvan seuraavat toiminnot: vartioimisliike-, yksityisetsivä-, järjestyksenvalvonta ja turvatarkastustoiminta, turvasuojaustoiminta, turvallisuustekniikka ja -teknologia, turvallisuusasiantuntija- ja koulutuspalvelut. (Paasonen & Huumonen 2011,13; Laitinen, Manninen & Meristö 2014, 14 – 15.)

Yksityistä turvallisuusalaa koskeva kotimainen tutkimus on vähäistä, ala ei ole kiinnostanut tukijoita. Yksi syy on, että turvallisuusalaa on vaikea määritellä, haasteena on alan kansainvälisyys ja monipuolisuus. Kehitys on kuitenkin kulkemassa kohti kokonaisvaltaisempia ratkaisuja ja teknologioiden monikäyttöisyyttä. Myös erilaiset oheistehtävät ja monipalvelutehtävät lisääntyvät alalla. (Paasonen & Huumonen 2011, 10-14; Laitinen ym. 2014, 14 – 15.)

Turvallisuusala on segmentoitunut käyttäjäsektoreittain (Tiilikainen 2006). Näitä ovat finanssiala, julkiset palvelut, kaupan ala, teollisuus ja palvelut, logistiikka- ja kuljetusala, palontorjunta sekä kansallinen turvallisuus. Teollisuudessa turvallisuus korostuu prosessi-, energia- ja elintarviketeollisuudessa. Julkisten palveluiden suurin käyttäjäsektori on sosiaali- ja terveyspalvelut, mutta myös koulujen ja kuntien turvallisuuskysymykset nousevat esiin. Turvallisuuspalveluja voidaan tarjota myös netissä. Esimerkkeinä toimivat erilaiset palvelukeskukset ja neuvontapalvelut, etävalvonta sekä pääkäyttäjäpalvelut, Myös huolto-, koulutus- ja ASP-palveluita voidaan tarjota netin yli. (Laitinen ym. 2014, 14 – 15.)

3.2 Digitalisaatio ilmiönä Suomessa ja muualla

Suomalainen yhteiskunta on maailmanlaajuisesti hyvissä asemissa olemaan digitalisaation aallon harjalla. Tästä on indikaattorina esimerkiksi se, että Suomi on vuoden 2011 tilastojen mukaan maailman prosentuaalisesti viidenneksi eniten Internettiä käyttävä maa, 82,6 prosentilla suomalaisista on oma Internetyhteys käytettävissä. Muut viiden parhaan joukossa olevat maat ovat Tanska, Alankomaat, Ruotsi ja Islanti, joten myös Suomen lähellä on muita maita, joissa tilanne on myös todella hyvä. Suomen tilannetta on auttanut hallituksen tuki, hallitus on julistanut Internetin käyttömahdollisuuden olevan perusihmisoikeus. Tämä ei ole itsestäänselvyys edes kaikissa länsimaissa, esimerkiksi Yhdysvalloissa alkuperäisväestöä edustavien intiaanien joukossa alle kymmenellä prosentilla on oma Internetyhteys käytettävissään. (De Kare-Silver 2011, 125 – 126.)

Sähköisten palveluitten kasvu on ollut hurjaa. Vuonna 2014 on tilastoitu, että Yhdistyneessä Kuningaskunnassa noin sata miljardia puntaa, eli 7,2 prosenttia bruttokansantuotteesta muodostuu sähköisistä palveluista. Kasvua kuvaa hyvin se, että vuoden 2004 vastaavassa tilastossa

lukua ei edes mainita, koska se ei ole ollut merkityksellinen. On hyvin todennäköistä, että kasvu jatkuu trendin mukaisesti voimakkaasti, joten voidaan todeta, että tulevaisuus on digitaalinen. (De Kare-Silver 2011, 142.)

On olemassa digitalisaatioon perustuva liiketoimintamallin, jonka avulla vanha palvelu voidaan digitalisoida. Tavoitteena on vanhan palvelun tai tuotteen tuominen tarjolle digitaalisesti. Tällä on tarkoitus tehostaa toimintaa, alentaa kustannuksia ja vähentää välikäsiä. Palvelut ja tuotteet saadaan myös potentiaalisesti useamman ulottuville digitalisaation avulla. Samalla kun organisaatio vastaa kysymykseen, miten digitalisaatio onnistuu, on mahdollista tunnistaa uusia, innovatiivisia mahdollisuuksia. Tämä liiketoimintamalli alkoi kehittymään 1990-luvulla Internetin yleistyessä ympäri maailman. Ensimmäisten joukossa oli nykyään Microsoftin omistama Hotmail palvelu, joka tarjosi ja tarjoaa edelleen sähköpostipalveluita. Sähköposteilla osittain syrjäytettiin postitse lähetettävät kirjeet, eli vanha palvelutuote korvattiin digitalisoinnin avulla. Hotmailin liiketoimintamalli myös eroaa siitä, miten postipalvelut toimivat, eli heidän palvelunsa käyttö ei automaattisesti maksa mitään käyttäjälleen. Tätä vastoin tietyt ominaisuudet saa käyttöön maksamalla rahaa, he käyttävät niin kutsuttua freemium liiketoimintamallia. Freemiumia ei käytännössä ollut olemassa ennen digitalisaatiota, sen periaate on, että perusominaisuudet ovat ilmaisia, mutta lisäominaisuudet ovat maksullisia. Digitalisaation on levinnyt tämän jälkeen monelle eri toimialalle, ja tämä kehitys jatkuu edelleen. (Frankenberg, Gassman & Csik 2014, 133 – 136, 165.)

Digitalisaatio tuo eittämättä paljon hyvää mukanaan, mutta on tärkeää muistaa sen tuomat riskit. Jo nyt on tehty sähköisiä hyökkäyksiä, joilla on ollut huomattavia seuraamuksia, tulevaisuudessa vaarat kasvavat entisestään. Vuonna 2006 Saudi Aramcon toimitiloihin Saudi Arabiassa kohdistettiin onnistunut terroristinen hyökkäys, Saudi Aramco on yksi maailman arvokkaimmista yrityksistä. Saudi Aramcon arvoksi on arvioitu reilusti yli triljoonaa dollaria, joka on esimeriksi enemmän kuin Applen arvo. Saudi Aramcon kautta hallitaan Saudi-Arabian öljyimperiumia, sen vastuulla on lähes 90 prosenttia koko Saudi-Arabian tuloista. Onnistuneen fyysisen hyökkäyksen jälkeen yritys toimi reaktiivisesti, panostaen huomattavasti fyysisen turvallisuuden parantamiseen. Jälkeenpäin voi todeta, että heidän olisi pitänyt proaktiivisesti lähteä rakentamaan kattavaa turvallisuussuunnitelmaa, jolloin riskit olisi tunnistettu kattavammin. Tämä kostautui vuonna 2012, jolloin heihin kohdistettiin erittäin vakava kyberhyökkäys. Hyökkäys tehtiin viruksen avulla, eli koodiriveillä, sekä yksittäisen lahjotun työntekijän avustuksella. Työntekijä latasi yrityksen verkossa olleeseen tietokoneeseen USB-muistitikulla viruksen, tästä virus lähti leviämään nopeasti. Tavoitteena oli yrityksen toiminnan pysäyttäminen, jonka vaikutukset olisivat olleet suuret. Jos Saudi Aramcon öljyntuotanto olisi pysähtynyt, se olisi vaikuttanut maailman laajuisesti öljyn hintaan. Tämä ei täysin onnistunut, tuotanto ei missään vaiheessa pysähtynyt, mutta hyökkäys haittaisi huomattavasti yrityksen toimintaa. Lopulta kolmannes yrityksen verkossa olleista koneista jouduttiin korvaamaan, eli

noin 30000 konetta. Teon taustalla on arveltu olevan Iranin valtio, eli koodirivejä käytettiin aseena valtioiden välillä. (Ross 2016, 121 - 124.)

On tutkittu, että jo nyt kyberhyökkäykset aiheuttavat maailmanlaajuisesti yli 400 miljardin dollarin kustannukset vuosittain. Hyökkäysten torjuntaan käytettävät resurssit ovat nousseet vuoden 2000 tasosta, eli 3,5 miljardista dollarista noin 175 miljardiin dollariin vuosittain. Tämä luku tulee ainoastaan kasvamaan, alalla on valtava potentiaali. Tätä tukee esimerkiksi se, että maailmalla oli vuonna 2015 16 miljardia laitetta, jotka pystyvät olemaan verkossa, on arvioitu, että vuonna 2020 laitteita on käytössä jo 40 miljardia. On arvioitu, että vuonna 2020 Internet of Thingsin, eli esineiden Internetin vaikutus globaaleihin markkinoihin on vuositasolla 19 triljoonaa dollaria. Summan hahmottamiseksi kerrottakoon, että koko maailman bruttokansantuote on vuositasolla yhteensä hieman yli 100 triljoonaa dollaria. Potentiaalisesti kaikki laitteet, jotka ovat verkossa, ovat alttiita kyberhyökkäyksille. Niitä voi vahingoittaa, tai niitä voi käyttää hyväksi isommissa hyökkäyksissä. (Ross 2016, 134.)

Mielenkiintoinen ajatus on myös se, että mitä enemmän käytämme digitalisaation mahdollistamia palveluita ja tuotteita, sitä enemmän olemme niistä riippuvaisia. Digitalisaation myötä osa tietotaidosta häviää, tai osaajien määrä ainakin supistuu. CIA:n kyberturvallisuuden asiantuntija Jim Gosler toteaa, että esimeriksi GPS järjestelmän yleistettyä, pidetään sen toimivuutta itsestäänselvyytenä. Hän väittää, että esimerkiksi heidän laivastossaan ei enää opeteta, eikä täten osata navigoida tähtien asentojen perusteella. (Ross 2016, 136.)

Digitalisaation tuottaa todella paljon dataa. Olemme siinä pisteessä, että varsinkin länsimaissa lähes kaikilla ovat älypuhelimet käytössä. Puhelin kykenee tuottamaan meistä yksityiskohtaista dataa: missä liikumme, tallentamaan keskusteluitamme ja videota, mitä haemme Internetistä, kenen kanssa olemme tekemisissä, sen kautta voi tallentaa lähes kaiken. Isommassa kuvassa voi todeta, että vuonna 2015 tilastoitiin joka minuutti lähetettävän 204 miljoonaa sähköpostia, 2,4 miljoonaa päivitystä Facebookkiin, 72 tunnin verran videota ladataan Youtubeen ja 216000 kuvaa ladataan Instagrammiin. Tämä luku kasvaa 50% per vuosi. Digitaalisesti dataa on siis saatavilla valtavia määriä, on Big Dataa, sekä yksittäiseen ihmiseen yksilöitävää tietoa. Vuonna 2000 noin 25 prosenttia datasta tallennettiin digitaalisesti, jo vuonna 2007 luku oli 94%. Tieto on valtaa, joten se on haluttua. Digitaalisesti saatavilla olevaa tietoa voi vuotaa nopeasti isoja määriä, tämä tuottaa isoja haasteita turvallisuudelle. (Ross 2016, 154 – 155.)

Opinnäytetyön tekijä on toiminut turvallisuusalalla lähes koko työuransa, tullen alalle juuri kun siirtyminen analogisesta digitaaliseen teknologiaan alkoi. Digitalisaatio kehitti jo tällöin alaa, tuoden lisäarvoa asiakkaille. Esimerkiksi aikaisemmin yleisesti käytettiin kamerajärjestelmän tuottaman datan tallentamiseen VHS-kasetteja, järjestelmät olivat täysin analogisia.

Tämä oli aikaa ja tilaa vievää, sekä tiedon etsiminen oli kaikkea muuta kuin helppoa. VHS-kasetteja ja laitteistoa oli nurkat täynnä. VHS-kasetteja piti aika ajoin käsin vaihtaa laitteisiin, muuten tallentaminen keskeytyi. Tiedonsiirtäminen vaati käytännössä VHS-kasetin fyysisesti kuljettamista toiseen paikkaan. Nopeassa tahdissa järjestelmiä digitalisoitiin, materiaali tallentui ykkösinä ja nollina tietokoneen kovalevylle. Materiaalia oli paljon helpompi hallitta, selata, tallentaa ja kopioida. Tällöin myös kamerajärjestelmien etävalvonta- ja hallinta helpottui huomattavasti, datan pystyi esimerkiksi siirtämään suoraan yksityisen turvallisuusalan hälytyskeskukseen. Tietoturvallisuuden merkitys kasvoi, ja kasvaa edelleen.

Ei ole mahdollista, että Suomen valtio pystyisi turvaamaan kaiken digitaalisen toiminnan, joten itsenäisillä toimijoilla on vastuu suojata oma toimintansa. Yksityisellä turvallisuusalalla on iso mahdollisuus olla mukana tässä toiminnassa. Tietoturvayritykset luonnollisesti ovat tärkeässä osassa, mutta he eivät pysty toimittamaan kaiken kattavia turvallisuusratkaisuja.

3.3 Digitalisaatiosta tehty aikaisempi tutkimus

Oxfordin yliopiston Frey & Benedict (2013) suorittivat tutkimuksen, jonka tavoitteena oli arvioida digitalisaation mahdollistaman automatisoinnin vaikutukset perinteisiin ammatteihin. Tutkimuksessa todetaan, että robotiikka yleistyy koska tekniikka, kuten sensorit ovat jo hyvin kehittyneitä ja kehittyvät edelleen, sekä hinnat laskevat kiihtyvällä vauhdilla. Nämä trendit johtavat siihen, että robotiikka yleistyy hyvin monella alalla, täten monesti korvaten ihmisen työn suorittajana. Teollisuusrobottien myynnin määrä kasvoi vuonna 2011 40 prosenttia verrattuna edelliseen vuoteen. Kotitalouksissa robottien määrä on kasvanut muutaman vuoden ajan noin 20 prosentin vuosi vauhtia, kyseisiin robotteihin lasketaan esimerkiksi ruohon leikkuu- ja siivousrobotit. Kaupallisten robottien joukkoon on jo nyt tulossa robotteja, jotka pystyvät tekemään ruokaa, siivoamaan yritysten tiloja ja avustaa vanhusten hoidossa. On vain ajan kysymys, milloin robotiikan kehitys on siinä pisteessä, että myös osa vartijan työtehtävistä automatisoidaan tavalla tai toisella. (Frey & Benedict 2013, 20 – 22.)

Edellisessä kappaleessa mainitun tutkimuksen osana oli myös tilastojen avulla laskettu todennäköisyys eri ammattinimikkeiden töiden siirtymiselle robottien tehtäviksi. Tilastoina on käytetty Yhdysvaltojen viranomaisten julkaisemia tilastoja, joten tutkimus ei täysin päde Suomen markkinoille. Suomi ja Yhdysvallat ovat kuitenkin kehittyneitä länsimaita, joten tutkimustulokset antavat hyvin osviittaa Suomenkin tilanteeseen. Laskukaavan perusteella ammattinimikkeille annettiin arvo nollasta ykköseen, nollan edustaessa alaa, jota ei voi automatisoida ja ykkösen edustaessa alaa, joka on täysin automatisoitavissa. Tietoturva-asiantuntija sai arvon 0.21, turvatekniikan asentaja arvon 0.82 ja vartija arvon 0.84 (Frey & Benedict 2013, 67). Tämän tutkimuksen perusteella tietoturva tulee tarjoamaan nyt ja jatkossa töitä ihmisille, vain pieni osa työtehtävistä on jossain määrin automatisoitavissa lähitulevaisuudessa. Sitä vastoin yksityisen turvallisuusalan perinteiset suorittavan tason työtehtävät tulevat kokemaan

ison muutoksen. Suurin osa vartijan ja turvatekniikan asentajan tehtävistä on tulosten mukaan lähitulevaisuudessa korvattavissa digitalisaation mahdollistamilla ratkaisuilla.

Huoltovarmuuskeskus julkaisi vuonna 2018 tutkimuksen nimeltä ”Huoltovarmuuden Skenaariot 2030”. Huoltovarmuuskeskus kertoo, että ennakoinnista on tullut tärkeä osa huoltovarmuustyötä ja, että skenaariotarkastelut ovat hyvä ennakoinnin työkalu. Työ muodostui asiantuntijoiden haastatteluista ja neljästä työpajasta. Työn tuloksena oli viisi erilaista skenaarioita, joista tämän opinnäytteen tarpeisiin on skenaario 4, eli ”teknologinen maailman järjestys” mielenkiintoisin. Skenaario on teemoitettu vuosilukujen mukaan, ”2018 – 2021 Vanhat rakenteet romahtavat”, ”2022 – 2026 Teknologia tehostaa, puhdistaa ja polarisoi” ja ”2026 – 2030 Uusi kaupunkien ja yritysten globaali teknologiamarkkinatalous. Tässä skenaariossa digitalisaatio etenee vauhdilla. (Huoltovarmuuskeskus 2018.)

Skenaarion ensimmäisessä vaiheessa teknologiakehityksen ja digitalisaation vauhti kiihtyy entistään. Robotiikan ja tekoälyn kehitys vähentää työvoiman tarvetta lähes kaikilla toimialoilla ja työvoiman hinnan merkitys laskee. Tieto on valtaa ja globaalit teknologiayritykset omistavat paljon valtaa, valtioitten valta vähenee. Rakenteet ja toimijat verkostoituvat, jolloin yleistyy hajautetut toimintamallit. Julkisia palveluja yksityistetään, joka olisi varmasti yksityiselle turvallisuusalalle liiketoiminnallisesti positiivinen mahdollisuus. Myös kaupungistuminen nopeutuu entisestään, eli maaseutu kuihtuu vieläkin nopeammin. Luonnollisesti myös digitalisaation tuomat palvelut ovat parhaiten saatavilla kaupungeissa, joista kehkeytyy Smart City konseptin mukaisia. Skenaariossa siirrettäessä eteenpäin tulevaisuuteen kasvaa alueelliset erot entisestään, eli digitalisaation onnistujilla ja epäonnistujilla on hyvin erilaiset tavat elää. Skenaarion loppu puolella valtiot ovat menettäneet entisestään valtaa. Samalla digitalisaatio ja robotisaatio integroituu lähes kaikkeen, seurauksena syntyy ylivoimaiseen päätöksentekoon pystyvä tekoäly. Lopputulos on teknologinen maailman järjestys. (Huoltovarmuuskeskus 2018.)

Huoltovarmuuskeskuksen tutkimus on opinnäytetyön kannalta hyödyllinen tietolähde. Sen näkökulma on eri, mutta varsinkin edellä mainittu skenaario kuvailee pääpiirteittäin mitä hyvin mahdollisesti tapahtuu, jos digitalisaatio etenee vauhdilla. Tutkimusmenetelmät ovat suurin piirtein samat kuin omassa tutkimuksessani, mutta resurssit ovat huomattavasti isommat. Tutkimukseen on osallistunut useita kymmeniä asiantuntijoita, joka nostaa ennakoinnin reliabiliteetin tasoa verrattuna pienempään otantaan. Skenaarion toteutuessa visioidusti, tietäisi se yksityiselle turvallisuusalalle kovaa kysyntää. Valtiot menettäisivät kovasti valtaa, joka siirtyisi globaaleille yrityksille, tällöin myös moni valtion toiminta yksityistettäisiin. Ei välttämättä ole suotuisa tulevaisuuspolku yhteiskunnallisesti, että valtio ei enää kykenisi huolehtimaan kansalaistensa turvallisuudesta, vaan se olisi yritysten tehtävä. Mahdollinen tulevaisuus se varmasti on, tälläkin hetkellä on trendinä yksityistää palveluita.

3.4 Yksityisen turvallisuusalan tulevaisuudesta tehty aikaisempi tutkimus

Teknologian tutkimuskeskus VTT julkaisi vuonna 2010 raportin turvallisuusalan liiketoiminnan kasvualueista ja mahdollisuuksista Suomessa. Raportissa ei käytetä kertaakaan sanaa digitalisaatio, joka kuvastuu hyvin kyseisen ilmiön ja termin nopeaa kehittymistä, sekä yleistymistä. Raporttia varten luotiin myös kolme erilaista skenaariota, jotka perustuivat kirjallisuuteen, asiantuntijahaastatteluihin ja kahteen workshoppiin. Tavoitteena oli kartoittaa alan tulevaisuuden näkymiä. Kahdessa näistä skenaarioista tunnistettiin turvallisuusjärjestelmien kehitys kasvun moottorina. Positiivisimmassa skenaariossa nostettiin menestyksen takuuksi muun muassa asiantuntija-analyysit ja pitkälle asiakasräätälöidyt erikoisjärjestelmät. Digitalisaation tuomat mahdollisuudet on raportissa osittain tunnistettu, mutta niitä ei ole nostettu erityiseen asemaan, vaan on luotettu muihinkin teemoihin. (Kupi ym. 2010, 101 – 106.)

Vuonna 2012 Laurea-ammattikorkeakoulu suoritti kartoitusta ja arviointia koskien turvallisuusalaa. Osana työtä suoritettiin kysely koskien alan yleisiä tulevia muutostekijöitä. Kyselyyn osallistui turvallisuusalan asiantuntijoita, YAMK-opiskelijoita sekä koulun- ja työelämän edustajia. Kyselyssä osallistujat arvioivat vaikutusta asteikolla 1 – 5, jossa 1 tarkoittaa täysin eri mieltä ja 5 täysin samaa mieltä. Tulokset on kerätty taulukkoon 2. (Laitinen ym. 2014, 30.)

Yleiset muutostekijät	Keski-arvo
1. Tärkein turvallisuusalaan vaikuttava megatrendi on kaupungistuminen.	2,58
2. Ilmaston muutos vaikuttaa merkittävästi turvallisuuteen pitkällä aikavälillä.	3,49
3. Suomi säilyy turvallisuuden kehtona.	2,71
4. Järjestäytynyt rikollisuus on tulevaisuuden merkittävin uhka.	3,26
5. Teknologian kehittyminen avaa aivan uusia mahdollisuuksia turvallisuuden parantamiseen.	4,24
6. Biotunnisteet ovat uusi mahdollisuus rikollisuuteen.	3,29
7. Yksityisen ja julkisen sektorin yhteistyö on avain menestykseen.	4,18
8. Yksityisyyden suoja on tieturvallisuuden tärkein osa-alue.	3,26
9. Teknologian kehitys määrittää turvallisuusalan tulevaisuuden mahdollisuudet.	3,08
10. Sosiaalinen media tekee kaiken julkiseksi vähentäen samalla tietoturvatarvetta.	2,05
11. Pakolais- ja muuttovirrat lisäävät merkittävästi turvallisuusriskejä.	3,58

Taulukko 2: Yleiset muutostekijät turvallisuusalalla (Laitinen ym. 2014, 31)

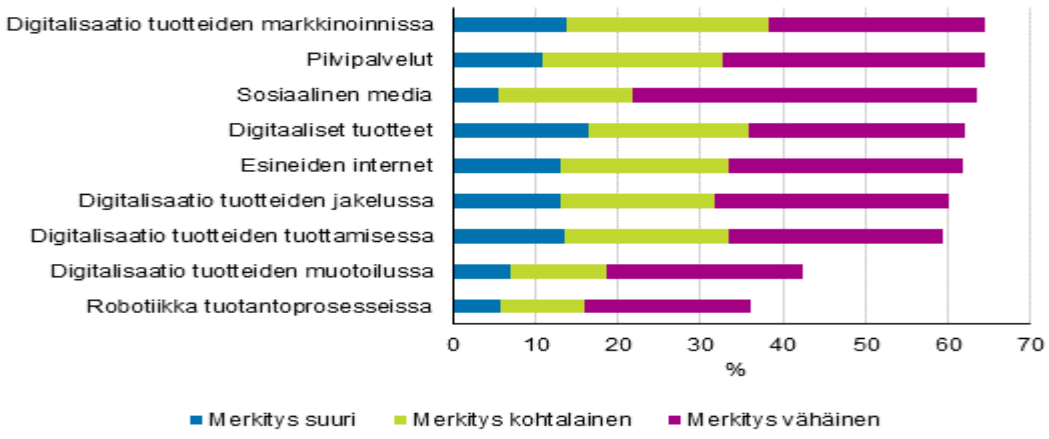
Merkittävämmäksi muutostekijäksi tunnistettiin: ”Teknologian kehittyminen avaa aivan uusia mahdollisuuksia turvallisuuden parantamiseen.”, pistein 4,24 (Taulukko 2). Tulos henkii sitä, että teknologiaan luotetaan uusien palvelujen moottorina. Vaikkakin samassa kyselyssä väittämä ”Teknologian kehitys määrittää turvallisuusalan tulevaisuuden mahdollisuudet” saa pisteitä hieman heikommin, eli 3,08. Voi olla, että määrittää sanaa pidettiin niin vahvana, että se hieman alensi pistemäärää. Vaikka teknologian uskotaan vahvasti, niin ehkä ei oltu valmiita ajattelemaan, että sen kehitys määrittäisi koko alan tulevaisuuden mahdollisuuksia.

Samassa tutkimuksessa kartoitettiin turva-alan opiskelijoilta kyselyn avulla osaamistarpeet. Vastauksista ilmenee, että uusien teknologioiden omaksuminen koettiin hyvin tärkeäksi. Koettiin, että piti olla moniosaaja, joka osaa hallita kokonaisuuksia. Huomion arvoista on myös, että opiskelijat tunnistavat turvallisuusalan tutkimistyön, kehitystrendien seurannan ja ennakoinnin tärkeäksi. Tieto seuraavasta kehityksen askeleesta, tai edes sivistynyt arvaus on monen onnistuneen päätöksen taustalla. (Laitinen ym. 2014, 37.)

3.5 Digitalisaation nykyinen merkitys suomalaisille yrityksille

Suomen Tilastokeskus julkaisee erilaisia tilastoja tutkimustensa pohjalta. Yksi näistä tutkimuksista on joka toinen vuosi toteutettava yritysten innovaatiotoiminta -tutkimus, se on osa Eurostatin koordinoimaa, kaikissa EU:n jäsenmaissa toteutettavaa yhteishanketta Community Innovation Survey (CIS). Tuoreimmassa innovaatiotutkimuksessa oli ensimmäistä kertaa tutkimuksen kohteena digitalisaation merkitys yritysten liiketoiminnassa. Tiedot on kerätty vähintään kymmenen henkilöä työllistäviltä yrityksiltä teollisuudessa, kaivostoiminnassa ja louhinnassa, sähkö-, kaasu- ja lämpöhuollossa ja vesi- ja jätehuollossa sekä valituilla palvelualoilla. Tiedot on kerätty kaikilta vähintään 250 henkilöä työllistäviltä yrityksiltä, 10–249 henkilöä työllistävistä yrityksistä on poimittu otos. Yrityksillä on lakiin kirjattu velvoite osallistua Suomen Tilastokeskuksen tekemiin tutkimuksiin. Valitettavasti turvallisuusala ei ole edustettuna tutkimuksessa, mutta tutkimus antaa kokonaiskuvaa Suomen tilanteesta. Vastaukset on kerätty vuosina 2012-2014. (Suomen virallinen tilasto 2014.)

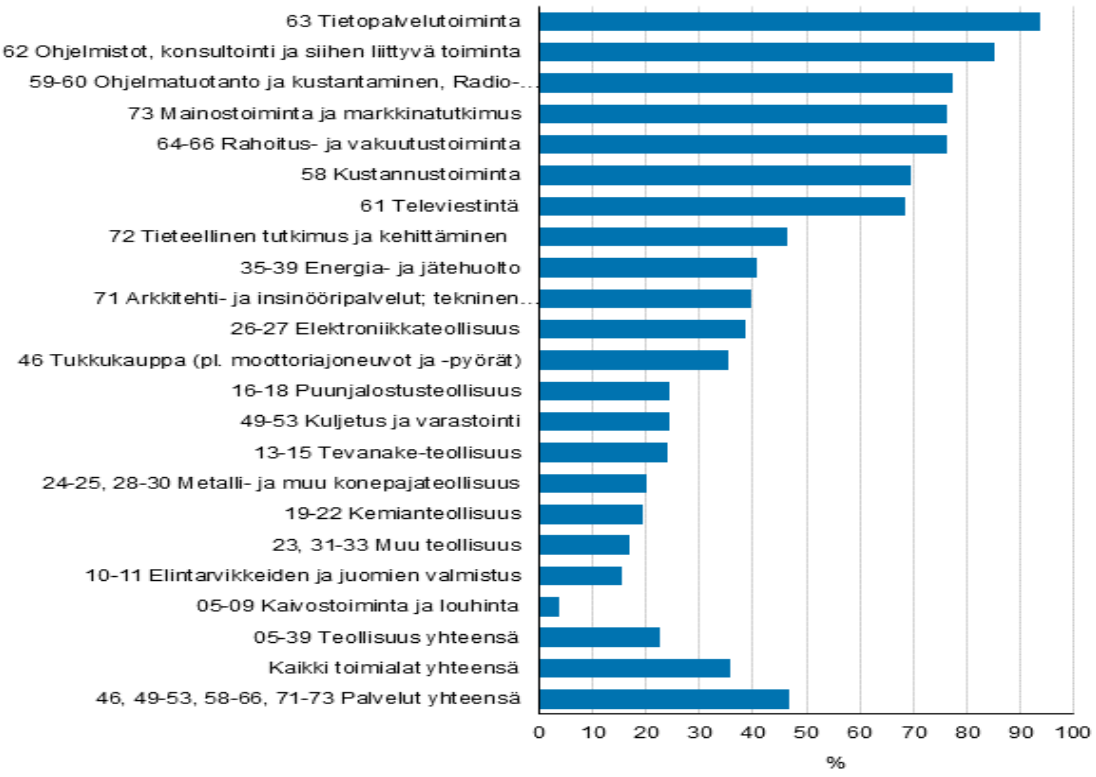
Osana tutkimusta yritykset arvioivat digitalisaation eri muotojen merkitystä heidän liiketoimintaansa, prosentuaalisesti enemmistönä oli vähäinen tai olematon merkitys (Kuvio 2). Kyseessä oli ensimmäinen kerta, kun Suomen Tilastokeskus suoritti kyselyn, joten ei ole olemassa historiatietoa mihin verrata kehitystä. Digitalisaation ollessa megatrendi, on kuitenkin selvää, että suunta on kasvava.



Kuvio 2: Digitalisaation merkitys yrityksen liiketoiminnassa 2012–2014, osuus yrityksistä (Suomen virallinen tilasto 2014, 7)

Kuviosta 2 voi todeta, että digitalisaatiolla suuri merkitys vain pienelle vähemmistölle yrityksistä. Toisaalta yli puolet yrityksistä kokevat, että digitalisaatiolla on vähintään vähäinen merkitys heidän liiketoiminnalleen. Kuvio 3 selventää yritysten alan vaikutusta tuloksiin. Siitä selviää, että alojen kesken on hyvin suurta vaihtelua, miten digitalisaation koetaan vaikuttavan liiketoimintaan. Vain muutama prosentti kaivoistoiminnan tai louhinnan yrityksistä koki digitalisaatiolle olevan vähintään kohtalaista merkitystä heidän liiketoimintaansa. Toisessa ääripäässä on tietopalvelutoiminta, kyseisen alan yrityksistä yli 90 prosenttia koki digitalisaatiolla olevan vähintään kohtalaista merkitystä heidän liiketoimintaansa.

Vaikka digitalisaatio koskettaa kaikkia, niin vaikuttaa siltä, että moni aloista ei koe sen vaikutuksia liiketoiminnassaan. Osassa teknistenkin alojen yrityksistä yli puolet kokevat digitalisaatiolla olevan korkeintaan vähäinen merkitys heidän toimintaansa (Kuvio 3). Kyseessä voi olla osittain myös tulkinta ja ymmärrys ongelma, koettiinko esimerkiksi robotit, automatisaatio, tietokonesovellukset osaksi digitalisaatiota.



Kuvio 3: Digitalisaation merkitys yrityksen liiketoiminnassa merkitykseltään suureksi tai kohtalaiseksi arvioineet toimialoittain 2012–2014, osuus yrityksistä (Suomen virallinen tilasto 2014, 7)

Tutkimuksessa oli mukana useita aloja, mutta ei yksityinen turvallisuusala (Kuvio 3). Yksityistä turvallisuusalalle on hankala löytää tutkimuksesta sopivaa verrokkia, mukana oli use-

ampi palveluala, mutta ne eivät kuitenkin luonteeltaan hieman erilaisia. Mukana ollut vakuutusala liittyy riskienhallintaan, mutta sen käytännön ilmentymä on täysin erilainen kuin yksityisellä turvallisuusalalla. Tutkimuksessa mukana olleista palvelualan yrityksistä lähes puolet koko digitalisaation vähintään kohtalaisen tärkeäksi. Yksityinen turvallisuusala on teknisempi kuin moni muu palveluala, joten on todennäköisestä, että alan yrityksistä iso osa pitää digitalisaatiota tärkeänä.

3.6 Valtiovarainministeriön näkemys digitalisaation tulevaisuudesta

Valtiovarainministeriön laajassa tutkimuksessa digitalisaation ja robotisaation mahdollisuuksista Andersson ym. (2017, 5) mainitsevat, että olemme siirtymässä kiihtyvää vauhtia teknologiassa ICT-aikakaudesta uudenlaiseen yhteiskuntaan, jossa keinoäly ja robotiikka tarjoavat huimia uusia mahdollisuuksia koko kansakunnan palveluiden toteuttamiseen. Tässä muutoksessa keskiössä on asiakas, eli kansalainen – ei teknologia. Tässä mielestäni on kiteytettynä hyvä ohjenuora, joka pitäisi muistaa kaikilla aloilla. Andersson ym. (2017, 5) jatkavat, että siirtyminen digitaalisten palvelujen varaan tekee meidät entistä haavoittuvaisimmiksi erilaisille häiriöille ja uusille uhkille. Tällöin riskienhallinnan merkitys korostuu, jotta toiminnan jatkuvuus on mahdollisimman varmalla pohjalla.

Dataa tuotetaan tulevaisuudessa vielä huomattavasti isompia määriä, tästä vastaa osaltaan Internet of Thingsin laajeneminen entistä useampaan laitteeseen. Henkilötietojen käsittelyn merkitys kasvaa. Toiminta myös automatisoituu, keinoäly pystyy yhä monimutkaisempiin asioihin. Tämä johtaa jossain vaiheessa itsenäisesti toimivaan robotteihin. Tutkimuksessa ennustetaan, että vuoteen 2030 mennessä olemme kehittäneet teknologiaa ja palveluita enemmän kuin koko PC- ja ICT-teknologian nykyisen 30-vuotisen historian aikana (Andersson ym. 2017, 12 – 13, 17 – 18.)

Kyberrikollisuus kehittyy, minkä vuoksi varautuminen ja ennakointi korostuva. Uhkana on esimerkiksi automatisoitujen tai etäohjattujen robottien kaappaaminen. Nostan tämän uhkan esiin, koska tulevaisuudentutkijat uskovat, että ihmiskunnassa käynnistyy uusi vaihe, johon liittyy se, että kaikki mikä voidaan robotisoida, robotisoidaan. Tästä seuraavan vaiheen uskotaan tuovan mukanaan jo teknologian ja älyn yhdistämät erikokoiset robotit, jotka ovat kykeneviä korjaamaan ja tuottamaan itse itseään – sekä toimimaan autonomisesti. Se milloin seuraava ja sitä seuraava vaihe toteutuu ei ole tiedossa, mutta Googlen keinoälyn kehittämisestä vastaaja johtaja Ray Kurzwell uskoo, että tietokoneäly saavuttaa ihmisen älyn jo vuonna 2020. (Andersson ym. 2017, 20 – 21, 36 – 37, 46 - 47.)

Mikä on ihmisen rooli robotisoituvassa maailmassa? Tämä on hyvä kysymys, jos teknologia kehittyy niin pitkälle mitä on visioitu. Tähän saakka teknologiset murrokset ovat tuottaneet uutta työtä, mutta ehkä tämä on se kerta, kun niin ei käykään. On toivottavaa, että kappa-

leen edellä mainittuun kysymykseen vastataan hyvissä ajoin. Ihmiskunnan pitää olla varautunut, jos tiedossa on monelle suuri elämäntapamuutos. Arviot työpaikkojen korvautumisesta roboteilla vaihtelevat suuresti, esimerkiksi EVA (2016) arvioi 7 % työpaikoista korvautuvan pian roboteilla, Bank of England (2015) arvio vuorostaan on 50%. Professori Richard Floridan tutkimuksen mukaan tulevaisuudessa jokainen tehtävä pitää tehdä luovaksi, muuten sillä ei ole tulevaisuutta. Roolijako olisi ainakin jonkin aikaa, että ihminen luo ja kone suorittaa. Vastuu pitää aina olla ihmisellä, koneen ollessa renki. (Andersson ym. 2017, 58.)

Andersson ym. (2017, 99 – 100) kehottavat siirtymään teknologiakeskeisyydestä ihmiskeskeisyyteen. Ihmisten luottamusta teknologian kehitykseen pitää pystyä vahvistamaan, kehityksen pitää olla eettistä ja ihmisten koulutukseen pitää panostaa, jotta osaaminen on riittävällä tasolla. Ei ole varaa siihen, että iso osa kokisi tippuneensa kehityksestä, eikä ymmärrä uutta maailmaa.

Internet-verkkoa ei alun alkaen suunniteltu tietoturvallisuuden näkökulmasta, kuten ei montaa muutakaan teknologian osa-aluetta. Andersson ym. (2017, 100 – 101) näkevät, että tästä lähtien tietoturvallisuus tulisi toteuttaa siten, että se on sisäänrakennettu osaksi kaikkea toimintaa. Käsitteet ”security by design”, henkilötietojen käsittelyssä ”privacy by design” sekä robotisaatiossa ”safe by design” muodostavat ne keskeiset toimintamallit, joiden pohjalta nykyiset palvelut ja toiminta tulisi suunnitella. Loppukäyttäjän tulisi pystyä luottamaan siihen, että palvelut ovat turvallisia.

Tulevaisuuden turvallisuusjohtamiseen kuuluu entistä tärkeämpänä toimintaympäristön muutosten ymmärtäminen ja ennakoiminen. Esimerkiksi miten digitalisaatio, seuraavan sukupolven ICT-ratkaisut, keinoäly ja robotisaatio vaikuttavat organisaation toimintaan, sekä miten varmistua turvallisuudesta. Andersson ym. (201,7 108 – 109) uskovat, että keskeisin seuraavien vuosien aikana kehitettävä osa-alue ja tarvittava kyvykkyys on riskienhallinta. Riskien ollessa hallittuja, niitä on mahdollista ottaa tietoisesti.

4 Tutkimuksen luonne ja menetelmät

Opinnäytetyöni on ennakoivaa laadullista tulevaisuudentutkimista. Ennakointi liittyy läheisesti tulevaisuustutkimukseen, sitä voi kuvailla tulevaisuudentutkimuksen käytännön ilmentymänä (Moilanen, Ojasalo & Ritalahti 2009, 80). Tulevaisuustutkimus ja sen menetelmät ovat lähtöisin armeijan tarpeista, josta se on levinnyt eteenpäin myös liiketoimintaan.

Kvalitatiivinen, eli laadullinen tutkimusotte soveltuu hyvin, kun ilmiöstä halutaan saada syvällinen näkemys, luodaan uusia teorioita ja hypoteeseja, käytetään mixed-tutkimusstrategiaa ja halutaan luoda ilmiöstä hyvä kuvaus (Kananen (2012, 24). Tulevaisuudentutkimus ja ennakointi soveltuvat hyvin megatrendien tutkimiseen, jota digitalisaatio eittämättä edustaa (Moilanen ym. 2009, 80 - 81).

Opinnäytetyön tietoperustan kirjallisuuskatsauksen analysointitapa on aineistolähtöinen sisältöanalyysi. Tietoperustan ja tutkimuskysymysten avulla on tunnistettu muut tarpeelliset tiedonkeruumenetelmät. Tutkimuksen uusi tieto on kerätty Delfoi-menetelmällä ja tulevaisuuspyörällä. Tutkimuksen johtopäätöksiä ja olettamuksia mallinnetaan kolmella erilaisella tulevaisuusskenaariolla. Skenaarioitten kertomukset ovat sidoksissa tietoperustaan ja tutkimuksen tuloksiin.

4.1 Tulevaisuudentutkimus ja ennakointi

Tulevaisuudentutkijat puhuvat tulevaisuuden visioimisesta näkemystietona. Sillä tarkoitetaan sellaista tietoa, joka yhdistää tietoja menneisyydestä ja nykyisyydestä käsitykseemme yhteiskunnallisen, taloudellisen ja teknologisen kehityksen luonteesta ja tuottaa näkemystä tulevaisuuden yhteiskunnasta. Hekään eivät väitä tietävänsä tulevaisuutta, vaan myöntävät ettei kukaan ihminen voi sitä tietää. Heidän tavoitteensa on antaa perusteltuja näkökulmia sille, mitä tulevaisuus voi olla (Wilenius 2015, 15).

Tulevaisuudentutkimus tieteellisesti on suhteellisen tuore asia, osittain tämän takia sen arvoa on kyseenalaistettu. On selvää, että tulevaisuudesta faktatiedon saaminen olisi erittäin arvokasta, mutta nykytietämyksen mukaan se ei ole yksinkertaisesti mahdollista. Tulevaisuudentutkijaan saatetaan suhtautua huijarina, ennustajatätinä, mutta monet tahot ovat kokeneet saavansa lisäarvoa tieteellisesti esitettyihin arvioihin tulevaisuudesta. On selvää, että tulevaisuutta ei voi mitata, laskea tai havainnoida, eli määrällisen tutkimus ei onnistu. Vaikkakin voi argumentoida, että tulevaisuuden tapahtumat voi laskea matemaattisesti, mutta tiettävästi siihen ei kukaan ihminen, eikä myöskään kone tällä hetkellä pysty. Historian kautta saa tilastoja, joiden avulla voi laskea todennäköisyyksiä tietyille tapahtumille, mutta varsinaisesti tulevaisen visiointiin tämä materiaali ei anna selviä vastauksia. Tulevaisuudentutkimuksen metodit ovatkin usein perinteisten laadullisten tutkimuksen mukaisia, joista osaa on modifioitu palvelemaan nimenomaisesti tulevaisuudentutkimusta. (Wilenius 2015, 18 – 25.)

Ennakoinnin avulla ei voi tehdä eksaktia tiedettä, mutta se voi silti tuottaa arvokasta tietoa. Esimerkiksi Nokian kohtalo maailman suurimmasta matkapuhelinvalmistajasta lähes täydelliseen epäonnistumiseen olisi voitu välttää panostamalla ennakointiin. Nokian epäonnistumisessa iso elementti oli väärien valintojen tekemisissä, koska tulevaisuuden vaatimuksia ei ymmärretty, ainakaan niin hyvin kuin moni kilpailija.

4.2 Kirjallisuuskatsaus

Maailma on pullollaan kirjallista ainestoa, mutta kelpaako mikä tahansa tutkimuksen lähdemateriaalina? Kananen (2008, 81 – 82) toteaa, että periaatteessa mikä tahansa tutkittavaan ilmiöön liittyvä kirjallinen dokumentaatio voi toimia aineistona. Avainasemassa on aineiston luotettavuus, jonka toteaminen on välillä haastavaa. Viralliset dokumentitkin voivat olla hyvin

värittyneitä, riippuen näkökulmasta, esimerkiksi jatkosodan syttymistä koskeva materiaali on hyvin erilaista venäläisten kirjoittamana, verrattuna suomalaisten dokumentteihin.

Tutkimuksen luotettavuutta voi mitata monella eri tavalla, unohtamatta maalaisjärkeä. Vertaisarvioitua dokumentointia on usein pidetty luotettavana, hyvänä tiedonlähteenä. Ei kuitenkaan pidä erehtyä ajattelemaan, että vertaisarvioinninkaan läpi käynyt tutkimus olisi automaattisesti hyvä, tai edes kovin luotettava. Vertaisarvioinnissa on useita vikoja, sen onnistuminen riippuu siitä, ketkä vertaisarvioinnin suorittavat. Koulutetuillakin ihmisillä on kuitenkin erilaisia mielipiteitä, motivaatiota, näkökulmia, uskomuksia. Vioistaan huolimatta vertaisarviointi on kuitenkin käytetyin tapa tieteessä varmistaa tutkimuksen luotettavuus, sille ei ole tunnistettu selkeästi parempaa vaihtoehtoa. (Smith 2006.)

Kerättyä kirjallista aineistoa voi analysoida monella eri tavalla. Ei ole tarkoituksenmukaista tutkimukseen kopioida tietoperustana käytettyä lähdettä sanasta sanaan, vaan lähde pitää pystyä tiivistämään, jotta se palvelee tutkimuksen tarpeita. Aineistolähtöinen sisältöanalyysi pelkistetään esimerkiksi tiivistämällä tai pilkkomalla osiin. Sisältöanalyysiä voi tarvittaessa jatkaa esimerkiksi ryhmittelemällä ja laskemalla asiasanojen esiintymistiheys, jolloin voidaan myös luoda määrällistä aineistoa. (Moilanen ym. 2009, 124 – 125.)

4.3 Delfoi-menetelmä

Delfoi-menetelmän nimi perustuu antiikin Kreikan mytologiaan ja historiaan. Delfoi oli antiikin Kreikassa kaupunki ja kaupunkivaltio, jota pidettiin tulevaisuuskeskuksena. Siellä toimi Apollo-jumalan ennustuksia välittävät Pythiaat, eli Delfoin oraakkelit. He olivat transsitilassa sekavia puhuvia naisia, joita papit tulkitsivat. Apollo oli taruston mukaan ylijumala Zeusin poika, jota pidettiin myös ennustustaidon jumalana. Oraakkeleilla oli symbolinen arvovalta, mutta todellisuudessa asiantuntijoina toimivat papit, jotka laativat lausunnon tietoa hakeneelle. Papit olivat oppineita, mutta tulevaisuuteen he tai oraakkelit tuskin näkivät. Käytännössä heidän onnistumisensa ja sitä myötä maine perustui moniselitteisiin vastauksiin. Esimerkkinä tästä on kertomus, jossa Lydian kuningas Croesus kysyi mitä tapahtuu, jos hän hyökkää Persiaan. Hän sai vastaukseksi, että tällöin suuri kuningaskunta tuhoutuu. Croesus armeijoineen hyökkäsi, jolloin Persia tuhosi hänen valtakuntansa. (Bergman, Kuusi & Salminen 2013, 248.)

Delfoi-menetelmän peruselementit, sekä sen tarkoitus ennakoinnin tiedonkeruumenetelmänä on laajasti dokumentoitu, mutta menetelmää on määritelty monin eri tavoin. Yksi tunnetuimmista määritelmistä on Linstone & Turoffin 1975 kirjoittama: ”Delfoi-tekniikkaa voidaan luonnehtia ryhmän kommunikaatioprosessin strukturointimenetelmäksi, jonka tarkoituksena on auttaa yksilöiden muodostamaa ryhmää kokonaisuutena käsittelemään mutkikasta ongelmaa”. Menetelmä perustuu asiantuntijoiden mielipiteisiin, mutta kuka kelpuutetaan asiantuntijaksi?

Tämä on jäänyt hyvin pitkältä tutkimuksen vetäjän tulkittavaksi. Loveridge et al. (1995) tekivät eksperttien asiantuntemukseen perustuneen tutkimuksen, johon määriteltiin korkea asiantuntemus seuraavasti: ”Olet aiheen asiantuntija siinä mielessä, että tunnet useimmat puolesta ja vastaan esitetty argumentit koskien aiheen kannalta olennaisia kiistakysymyksiä, olet lukenut asiasta ja olet muodostanut siitä jonkinlaisen mielipiteen.”. (Bergman ym. 2013, 249, 251.)

Modernin tulevaisuudentutkimuksen Delfoi-menetelmä pohjautuu 1950-luvulla suoritettuihin salaisiin sotilasteknologiaa koskeneisiin tutkimuksiin. 1960-luvulla menetelmää käytettiin erityisesti teknologian tulevan kehityksen ennakoimisessa. Menetelmän suosio hiipui 1970-luvun aikana, koska sitä kohtaan kohdistettiin runsaasti kritiikkiä. Menetelmän kritisoitiin vaativan liikaa aikaa ja rahaa, sekä tulokset pidettiin usein epäluotettavina. Menetelmä kuitenkin saavutti uuden arvostuksen OECD-maissa 1990-luvulla, koska Japanissa oli tehty menetelmän avulla menestyneitä tutkimuksia koskien teknologian kehitystä. Näissä tutkimuksissa Delfoi-menetelmä oli toteutettu survey-tyyppisenä, johon osallistui tuhansia asiantuntijoita. 2000-luvulla suuntana on kuitenkin ollut pienempien paneeleitten käyttö, enää ei olla koettu, että iso osallistuja määrä hyödyttäisi tiedonkeruuta. Pienempiä paneeleita on perusteltu sillä, että niissä korostuu asiantuntijoiden argumentit, jotka ovat laadullisesti arvokkaita. (Bergman ym. 2013, 249 - 263.)

Delfoi-menetelmä on hyvin skaalautuva, se voidaan toteuttaa muutaman asiantuntijan haastattelututkimuksena, tai tuhansien survey-tutkimuksena. Haastattelu on soveltuvampi laadulliseen tutkimukseen, haastatteluilla on myös helpompi ja nopeampi saavuttaa vuorovaikutus. Menetelmä perustuu kolmeen eri peruselementtiin. Ensimmäinen on asiantuntijoiden anonymiteetti, tällä pyritään siihen, että henkilöiden asemat eivät vaikuttaisi tilanteeseen, vaan keskiössä olisivat heidän argumenttinsa ja arvionsa. Ennen kyselylomakkeita jaettiin tai postitettiin asiantuntijoille, nykyään kyselylomake tyyppiset Delfoi-menetelmän tiedonkeruut ovat siirtyneet Internettiin. Haastattelutyyppiset Delfoi-menetelmää käyttävät tutkimukset ovat myös lisääntyneet, mutta näissäkin digitalisaatio tarjoaa tehokkaita ratkaisuja, kuten Skype. Toinen peruselementti on, että menetelmään sisältyy useampia kierroksia tai jatkuva vuorovaikutteinen kommentointi rajattuina aikoina. Kierrosten aikana asiantuntijat voivat mahdollisesti tutustua toistensa vastauksiin, muuttaa vastauksiaan, sekä tiedonkerääjä voi muuttaa kysymysten asettelua. Kolmas peruselementti on asiantuntijoiden saama palaute, jonka tavoite on lisätä menetelmän vuorovaikutteisuutta. Palaute voi olla määrällistä tai laadullista tietoa muitten asiantuntijoiden vastauksista, tai tutkimuksen tekijän antamaa vapaata palautetta. (Bergman ym. 2013, 248 – 263.)

Delfoi-menetelmän vuorovaikutteisuus ja palautteen antaminen on perustunut siihen, että perinteisesti menetelmän lopputuloksena oli tarkoitus saada asiantuntijoiden konsensus. Mielipi-

teiden yksimielisyys saavutettiin peräkkäisillä kyselyillä ja kontrolloidulla palautteella. Konsensuksen hakemista on perusteltu sillä, että arvioiden laatu paranee asiantuntijan voidessa muuttaa mielipidettään toisilta asiantuntijoilta saadun palautteen pohjalta. Nykyään suunta on kuitenkin ollut siihen, että konsensusta ei tarvitse saavuttaa, vaan arvostetaan myös eri suuntaisia argumentteja ja visioita. (Bergman ym. 2013, 252 – 253.)

4.4 Tulevaisuuspyörä

Tulevaisuuspyörä on Jerome Glennin 1970-luvulla kehittämä strukturoitu, aivoriihityyppinen menetelmä. Siinä etsitään pyörän keskiössä olevan aiheen ympärille kehäksi teemoja, teemojen avulla tunnistetaan tärkeän trendin, tapahtuman, päätöksen tai heikon signaalin ensimmäisen, toisen ja kolmannen vaiheen vaikutuksia yhteiskunnan tai organisaation toimintaan, arvoihin ja niin edelleen. Tulevaisuuspyörän avulla voidaan järjestellä, ymmärtää ja täsmentää erilaisia tulevaisuutta koskevia näkemyksiä ja niiden mahdollisia vaikutuksia. (Bergman ym. 2013, 333.)

Tulevaisuuspyörä voidaan lukea käsitekarttamenetelmäksi, sen avulla tutkittava asia voidaan purkaa osatekijöihinsä. Menetelmän toisessa vaiheessa voidaan analysoida ja arvioida miten erilaiset tunnistetut asiat vaikuttavat kuhunkin osatekijään. Tulevaisuuspyörää on käytetty varsinkin erilaisten megatrendin analysointiin, ymmärtämiseen ja ennakointiin. Tulevaisuuspyörää voidaan käyttää myös kehittämistyössä, jolloin tulevaisuuspyörästä valitaan osa-alue, jota lähdetään kehittämään. (Nurmi 2004.)

Tulevaisuuspyörän työstäminen lähtee sopivan ryhmän kokoamisella, ryhmä tarvitsee vetäjän, joka johtaa ja ylläpitää prosessia. Normaalisti vetäjä myös esittelee tutkittavan asian tai teeman, jonka ympärille tulevaisuuspyörää aletaan luomaan. Vetäjä aloittaa keskustelun kertomalla oman näkemyksensä tutkittavasta teemasta. Seuraavaksi ryhmän jäsenet kertovat oman näkemyksensä, tai edetään suoraan keskusteluun aiheesta. Keskustelussa esille tulleet osateemat otetaan ylös ja niiden joukosta valitaan tulevaisuuspyörälle vietävät aiheet. Seuraavaksi käsitellään jokainen tulevaisuuspyörälle viety osateema erikseen. Osateemat auttavat keskiössä olevan teeman pilkkomista osiin, jolloin sen vaikutuksia on helpompi käsitellä. Pääteema on keskiössä, osateemat seuraavalla kehällä ja uloimmalla kehällä tulevat vaikutukset. Toisiinsa liittyvät vaikutukset yhdistetään nuolilla. Tuloksena on eräänlainen käsitekartta. (Majavesi 2010, 7 – 8.)

4.5 Skenaariot

Bergman ym. (2013, 330) määrittelevät tulevaisuudentutkimuksen näkökulmasta Skenaarion: ”Tulevaisuuspolku, joka muodostuu valintatilanteista korostaen ajallisesti peräkkäisistä, mahdollisten tulevaisuudenkuvien sarjasta. Tulevaisuuspolku esitetään usein kertomuksena, joka voidaan ymmärtää tulevaisuuden tekemisen yhdeksi käsikirjoitukseksi. Skenaario sisältää tyy-

pillisesti kuvauksen toimijoista, toiminnoista sekä kuvauksen päätöksenteon ja seurausten tapahtumaketjusta. Skenaarioiden laadintaprosessi sisältää kvalitatiivisia, että kvantitatiivisia menetelmiä tai niiden yhdistelmiä."

Skenaariomenetelmää käyttävä tulevaisuudentutkija tutkii nykyhetkeä, siinä vallitsevia virtauksia ja etsii myös heikkoja signaaleja. Hän käyttää hyväkseen eri tieteiden tutkimustuloksia ja laatii niiden ja oman näkemyksensä ja kuvittelukykynsä pohjalta oman skenaarionsa tulevaisuudesta. Skenaariotutkija tuottaa kuvauksia siitä, mikä on tulevaisuudessa mahdollista, mikä on ehdollisesti mahdollista, mikä todennäköistä ja mikä toivottavaa tai kartettavaa. Tärkeää on kuitenkin, että polku tulevaan tästä hetkestä on johdonmukainen ja mahdollinen. Skenaariotyöskentelyn tavoitteena on kerätä ja jäsentää tietoa, joka mahdollisimman kattavasti auttaa ymmärtämään tulevaa toimintaympäristöä ja sen asettamia ehtoja organisaation toiminnalle ja tavoitteenasettelulle (Meristö 1991, 19).

Skenaariot kuuluvat olennaisena osana moderniin tulevaisuudentutkimukseen. Ne auttavat kuvittelemaan mikä on mahdollista, sekä analysoimaan, mikä on todennäköistä. Skenaariot toimivat perustana valittaessa haluttavaa ja toteutettavaa tulevaisuutta. Skenaarioista saatavaa hyötyä on vaikea arvioida ja lähes mahdotonta mitata. (Bergman ym. 2013, 179, 182.)

Skenaarioitten ominaispiirteisiin kuuluu muun muassa, että laaditut skenaariot ovat mahdollisia, mutta eivät välttämättä todennäköisiä tulevaisuuksia. Aikajänne ulottuu pidemmälle tulevaisuuteen kuin tavanomaisen strategisen suunnittelun, mieluiten tuplaten pidemmälle. Skenaariot tavalla tai toisella käsittelevät tulevaisuuden epävarmuutta, vaikka eivät poista sitä. (Bergman ym. 2013, 182.)

5 Tutkimuksen kulku ja tulokset

Varsinaisesti opinnäytetyön tutkimuksellinen osuus alkoi kirjallisuuskatsauksella kerätyllä tietoperustalla. Kappaleessa kolme on käsitelty kyseinen tietoperusta. Tietoperusta ja tutkimuskysymykset johtivat muiden tutkimusmenetelmien valintaan.

Delfoi-menetelmä käynnistyi tunnistamalla yhdessä opinnäytetyön toimeksiantajan kanssa useamman aiheen asiantuntija, joista neljää haastateltiin opinnäytetyötä varten. Haastatelluista kaksi työskentelee yksityisellä turvallisuusalalla hälytys- ja etävalvonnan asiantuntijoina, yksi on hälytyskeskuksen työntekijä sekä opiskelee ammattikorkeakoulussa turvallisuusalaa, ja yksi on etähallinnan asiantuntija. Haastatteluja varten luotiin kysymyspatteristo. Haastattelut tallennettiin äänitiedostoiksi, jotka litteroitiin. Litteroinnista kirjoitettiin tiivistelmät, joiden avulla luotiin ensimmäisen ja toisen kierroksen, sekä konsensuksen tulokset ja analyysit opinnäytetyöhön.

Prosessi eteni kaksi kierroksisella haastatteluilla, kysymyspatteristojen avulla (Liite 1; Liite 2). Haastattelut suoritettiin siten, että haastattelin jokaisen asiantuntijan yksitellen. Delfoi-

menetelmän yksi perusperiaate on se, että siihen osallistuvat asiantuntijat ovat toisilleen anonyymeja. Ensimmäisen kierroksen jälkeen kysymyksiä muokattiin palautteen mukaisesti, jonka jälkeen suoritettiin toinen haastattelukierros. Toisen kierroksen aikana saavutettiin työn kannalta riittävä konsensus. Kolmas kierros olisi voinut vielä vahvistaa tuloksia, mutta lopputulos tuskin olisi ollut olennaisesti erilainen. Haastattelut suoritettiin vuoden 2018 kesän ja syksyn aikana.

Seuraavaksi laadittiin tulevaisuuspyörä (Kuvio 5), se on laadittu aivoriihimäisen työskentelyn avulla. Siihen osallistui neljä turvallisuusalan asiantuntijaa. Osa oli mukana edellisessä luvussa käsitellyn Delfoi-menetelmän haastatteluissa, osa ei. Delfoi-menetelmän haastattelut suoritettiin ennen tulevaisuuspyörää.

Viimeisessä vaiheessa laadittiin skenaariot, eli tulevaisuuspolut. Tukena käytettiin opinnäytetyössä esiteltyä tietoperustaa, sekä Delfoi-menetelmän ja tulevaisuuspyörän tuloksia. Skenaarioilla pyrittiin myös tuomaan arvoa opintyöni toimeksiantajalle ja vastaamaan tutkimuskysymykseen.

5.1 Kaksi kierroksisella Delfoi-menetelmällä isojen linjojen tunnistamista

Ensimmäinen kierros. Tulokset on käsitelty liitteen 1 kysymysjärjestyksen mukaisesti seuraavissa kappaleissa, jokaisen kappaleen käsittäessä yhden kysymyksen aihealueen.

Yksityisen turvallisuusalan nähtiin kasvavan nyt ja tulevaisuudessa teknisempään suuntaan, eli digitalisaation etenemiseen uskotaan. Palvelut siirtyvät verkkoon, henkikohtainen palvelu vähenee, mutta asiakkaat pääsevät tietoihinsa käsiksi milloin vain, mistä vain. Tekoäly tulee tehostamaan työskentelyä, ihmisten toimiessa taustalla valmiina reagoimaan poikkeamiin. Osa uskoi myös kasvuun viranomaispuolen tehtävien yksityistämisen kautta, esimerkiksi muualla maailmassa on yksityisiä vankiloita. Esille nostettiin myös muuttoliike, esimerkiksi muutama vuosi sitten koettu niin kutsuttu pakolaisaalto työllisti vastaanottokeskuksiin satoja vartijoita. Kommentointiin myös, että tulevaisuuden kasvuun liittyvät prosessit ovat jo jossain määrin käynnissä, esimerkiksi ensimmäiset aitoa lisäarvoa tuottavat koneälyllä toimivat ratkaisut ovat jo tuotannossa. Käyttö on vielä vähäistä, mutta vastaavien ratkaisujen yleistyminen tulevaisuudessa on lähes varmaa.

Alan digitalisaation ei uskottu ainakaan lähitulevaisuudessa vähentävän työvoiman tarvetta. Palvelujen digitalisoituminen voi kyllä sinänsä vähentää nopeastikin työvoiman tarvetta, mutta sen kompensoi tekniikan ja palveluiden halpeneminen. Tämä taas mahdollistaa yksityisen turvallisuusalan palveluiden tulevan saataville paljon suuremmalla osalla kuin nykyään. Palvelut myös kehittyvät, jolloin voi syntyä uusia asiakassegmenttejä. Yksityinen turvallisuusala tunnetaan hyvin pitkälti vartiointialana, joka työllistää vartijoita. Tulevaisuudessa ammattititteli ja työnkuvat voivat olla monipuolisempia.

Vartijoiden ja järjestyksenvalvojien työkuvan uskotaan kehittyvän siinä mielessä vaativammaksi, että tarvitaan lisää tietoja ja taitoja. Esimeriksi mainittiin, että nykyään on olemassa vartijan tehtäviä, joihin vaaditaan myös hoiva-alan koulutus. Tästä jatkumona voi ilmaantua tehtäviä, joihin vaaditaan joku teknisempi koulutus vartijakoulutuksen lisäksi. Digitalisaatio tulee siirtämään joitakin rutiiniprosesseja ihmiseltä koneille, mutta poikkeamien ratkaisuun tarvitaan ihmisiä. Osa tulevista ratkaisuista voivat vaatia syvempää tieto tekniikasta, varsinkin häiriötilanteissa.

Asiantuntijoiden vastaukset omien työnkuvien muutoksista erosivat luonnollisesti toisistaan, koska henkilöt työskentelevät eri tehtävissä. Vastauksista ilmeni, että osalla työnkuva oli jo muuttunut, esimerkiksi kuvavalvonta on kehittynyt huimasti, jonka johdosta on tuotteistettu uusia palveluita. Ainoastaan hälytyskeskuspäivystäjänä työskentelevä uskoi, että hänen työtehtävistä iso osa automatisoidaan. Hänkään ei kuitenkaan uskonut siihen, että koko työtehtävä lakkaisi olemasta. Asiakasmäärät nousevat ja datan määrä kasvaa, jolloin poikkeamien määrä nousee ja tällöin tarvitaan edelleen ihmistä. Hän oli myös sitä mieltä, että on tiettyjä työtehtäviä, joita ei ainakaan lähitulevaisuudessa voida automatisoida.

Digitalisaation uskottiin tuovan uusia vakavia uhkia. Internet of Thingsiä pidettiin erityisen haasteellisena, koska silloin kaikki laitteistot ovat verkossa. Todettiinkin, että tulevaisuudessa murtoja ei suoriteta sorkkaraudoilla vaan hakkeroimalla. Uhat koskettavat myös suoraan yksityisen turvallisuusalan toimintaa, jos toiminta on käytännössä erilaisten järjestelmien varassa. Järjestelmän pettäessä palvelua ei voida tuottaa, tai tietomurron yhteydessä järjestelmästä voidaan saada sensitiivistä tietoa. Eräs haastateltava nosti esimerkiksi lähinnä ulkomailla tapahtuneet poliisiasemien ja sairaaloitten järjestelmien kaappaukset, joiden johdosta viranomaiset ovat joutuneet suorittamaan rikollisille maksuja, jotta järjestelmät on saatu takaisin hallintaan. Hän piti huolestuttavana, että turvallisuutta valvova viranomainen ei ole pystynyt riittävästi varautumaan nykypäivän haasteisiin edes nyt, kun tulevaisuudessa uhat tulevat vain lisääntymään. Taustalla voi olla myös se, että uusin teknologia halutaan nopeasti käyttöön, eikä riskejä kartoiteta.

Vapaassa kommentoinnissa tuotiin esille varautumisen tärkeyttä, kuten korkeamman standardin suojautumista kohteisiin, joihin ennen riitti kevyemmät ratkaisut. Suojautumisen tulisi aina perustua realistiseen riskiarviointiin. Tulevaisuudessa, digitalisaation myötä realistiseksi riskeiksi nousee asioita, joita nykyään ei voi pitää realistisena. Useampi kommentoi myös koulutuksen tarvetta, kommenttien perusteella toiselle haastattelukierroksille lisättiin koulutuksesta oman kysymyksenä.

Osallistujat antoivat kritiikkiä koskien kysymyksissä käytettyä epämääräistä ajankohtaa, eli tulevaisuutta. Se antoi liian suuren tulkinnanvaran ja vaati tarkempaa selvitystä, tarkoite-

taanko tilannetta muutaman vuoden päästä, vai paljon pidempää aikaväliä. Valtiovarainministeriön tutkimuksessa ”Pilkahduksia tulevaisuuteen – digitalisaation ja robotisaation mahdollisuudet” käytettiin robotisaation visiointiin vuotta 2025, se tuntui sopivalta vuodelta mihin ankkuroida myös opinnäytetyön tutkimus (Valtiovarainministeriö 2017, 45, 52, 59). Palautteen perusteella muokattiin kysymyksiä Delfoin toiselle kierrokselle, sekä ankkuroitiin vuosi 2025 skenaarioiden tapahtuma vuodeksi.

Toinen kierros ja konsensus. Tulokset on käsitelty liitteen 2 kysymysjärjestyksessä.

Ensimmäisellä kierrokselle argumentit, sekä arvioit, olivat valmiiksi jo hyvinkin saman suuntaisia. Osallistujille kerrottiin muiden vastauksista, sekä miksi toisella kierroksella oli kysymysten asettelua hieman muuttunut. Konsensus oli jo riittävä, joten ei ollut tarpeen enempää haastateltavia ohjata. Toisen kierroksen arvo oli oikeastaan siinä, että se vahvisti ensimmäisen kierroksen näkemyksiä, vaikka kysymysten asettelu oli hieman erilainen. Nykymuotoisessa Delfoi-menetelmässä ei myöskään pidetä täydellisen konsensuksen syntymistä tärkeänä ennakoinnin luotettavuuden kannalta, joten siihen pyrkiminen ei ollut tarpeellista muotoseikkojenkaan takia.

Haastateltava kuvasivat vuoden 2025 yksityisen turvallisuusalan tärkeiksi teemoja digitalisaation johdannaisiksi, kuten koneälyn ja robotiikan edelleen eteenpäin kehittymisen. Kaupungit alkavat muistuttaa enemmän Smart City vision mukaisia ympäristöjä. Yksityinen turvallisuusala on näkyvämmin mukana yhä useamman elämässä, koska he käyttävät yritysten tuottamia palveluja. Asiantuntijoilla ei ollut mainittavia mielipide eroja, kaikki uskoivat digitalisaation etenemiseen. Poliittisia suuntia tai muuta toimintaympäristöön liittyviä suuntauksia ei juurikaan mainittu.

Yksityisen turvallisuusalan liikevaihdon trendi on ollut useita vuosia nousussa, haastateltavat uskovat digitalisaation nopeuttavan tätä trendiä entisestään. Vastaukset olivat hyvin samansuuntaisia kuin ensimmäisen kierroksen vastaavaan kysymykseen. Palvelut kehittyvät, asiakasmäärä nousee, ala teknistyy. Työntekijöidenkin määrä voi vuonna 2025 olla kaiken kaikkiaan nykytilaan verrattuna huomattavasti suurempi, mutta työnkuva on monella eri kuin tämän hetken vartijalla.

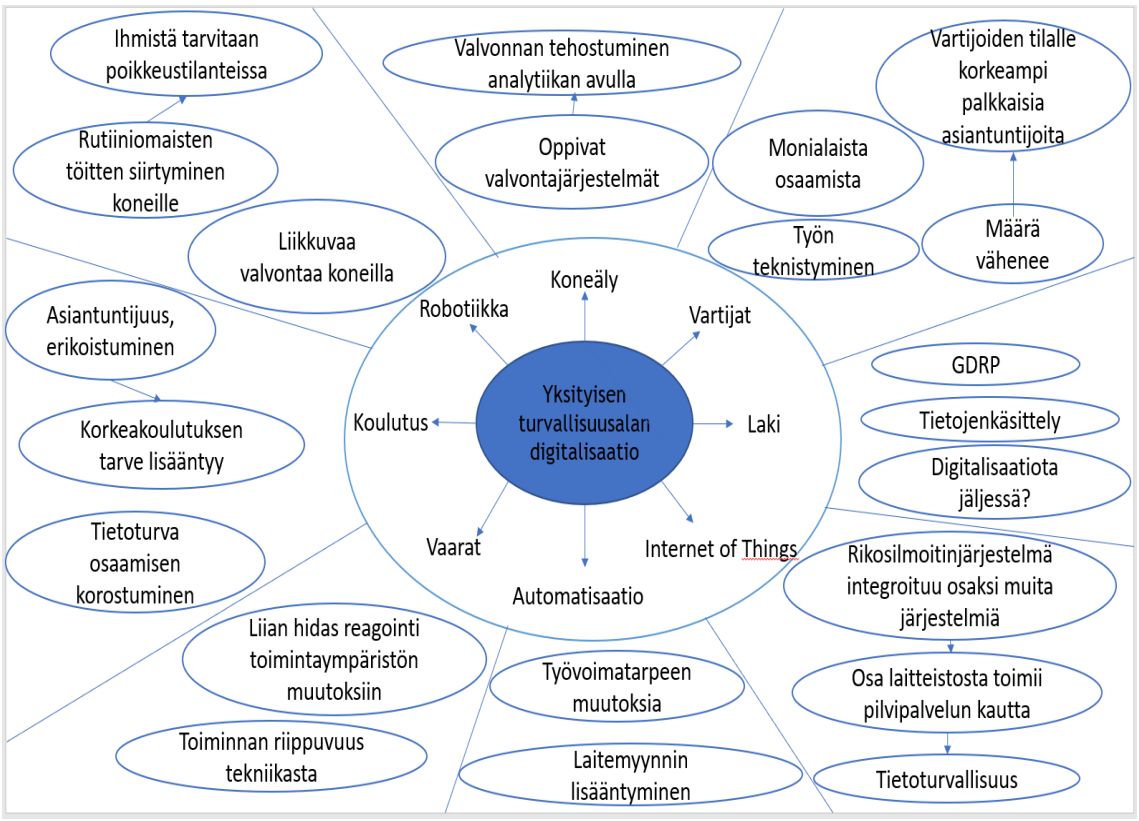
Ammatillisesti haastateltavat uskoivat pääsääntöisesti, että ammattinimike on vaihtunut ja työnkuva muuttunut. Jatkuvan kouluttautumisen tarve lisääntyy, sekä muun tiedonkeruun, jotta pysyy ajan tasalla alan kehityksessä. Vastaukset vahvistivat ensimmäisen kierroksen tuloksia.

Vartijoiden ja järjestyksenvalvojien työnkuvaa, sekä vuoden 2025 yksityisen turvallisuusalojen huomattavimmat uhkia koskievien kysymyksien vastaukset olivat myös hyvin linjassa ensimmäisen kierroksen vastauksiin. Sanavalinnat ja painotukset hieman erosivat, mutta lopputulos oli käytännössä sama. Vuoden 2025 käyttäminen kiintopisteenä ei tuonut lisäarvoa.

Vuoteen 2025 mennessä uskottiin turvallisuusalan asiantuntijakoulutuksen tarpeen kasvavan. Nykyään on olemassa turvallisuusalan tradenomi ammattikorkeakoulututkinto, jatkossa voi olla tarvetta turvallisuusalan opintojen suuntautumisvaihtoehdon tuomista esimerkiksi insinööreille. Turvallisuusalan käyttämän järjestelmät monimutkaistuvat ja osaamaton käyttäjä on turvallisuusriski. Tarvitaan koulutuksia, joissa pureudutaan syvemmällä tiettyihin osa-alueisiin. Kaikkea ei voi yksi ihminen osata, vaan on hyvä erikoistua. Yritysten sisäiset koulutuskanavat nousevat entistä tärkeimmiksi, mutta yhteiskunnan pitää tarjota koulutuksia, joista saa sopivat lähtökohdat kehittymiseen.

5.2 Tulevaisuuspyörällä visioita tulevaisuuden mahdollisuuksista ja uhkista

Tulevaisuuspyörän (Kuvio 4) rakentaminen perustui ilmiön yksityisen turvallisuusalan digitalisaation ympärille. Seuraavalle kehälle nostettiin teemat robotiikka, koneäly, vartijat, laki, Internet Of Things, automatisaatio, vaarat ja koulutus. Nämä teemat nähtiin aiheen kannalta tärkeimmiksi.



Kuvio 4: Tulevaisuuspyörä

Jokaisesta teemasta käytiin oma keskustelunsa, keskusteluiden perusteella tunnistettiin uloimmalle kehälle tulevaisuuden trendejä, tapahtumia ja muita asioita. Valmiin tulevaisuuspyörän taustalla on paljon keskustelua. Tulevaisuuspyörän hahmottamisen helpottamiseksi on jokaiseen teemaan liittyvästä keskustelusta luotu opinnäytetyöhön tiivistelmä. Tarkoituksena on auttaa ymmärtämään teemojen taustat, sekä miksi ne on koettu tärkeäksi.

Koneäly

Koneälystä turvallisuusalan näkökulmasta nostettiin tärkeäksi asiaksi oppivat valvontajärjestelmät. Nykyteknologia on siinä pisteessä, että esimerkiksi valvontakamerajärjestelmää voi opettaa tunnistamaan haluttuja objekteja. Nyt on jo tuotannossa järjestelmiä, jotka voivat esimerkiksi antaa hälytyksen, jos työmaalla on henkilö ilman kypärää, tai kauppakeskuksessa järjestelmä havaitsee aseen.

Käytännössä tarvitaan tarpeeksi tarkka kamera ja valvontaohjelmisto. Ohjelmistolle opetetaan esimerkki kuvien kautta tunnistettavia objekteja, kunnes se oppii tunnistamaan objekteja automaattisesti. Järjestelmät ovat jo nyt itseoppivia, kun ohjelmistolle on syötetty tarpeeksi dataa, se osaa itse kysyä käyttäjältä onko kuvassa esimerkiksi kypärä ja osoittaa objektin tarkan sijainnin. Tulevaisuudessa erilaisia järjestelmiä voi opettaa tunnistamaan lähes mitä vain, sekä niiden autonomiset oppimiskyvyt paranevat.

Digitalisaation etenemisen tuloksena on valvonnan tehostuminen automatisoidun analytiikan avulla. Tällä hetkellä esimerkiksi hävikin torjunta kameravalvonnalla on täysin manuaalista työtä, teho on täysin riippuvainen kameratarkkailijan taidosta ja motivaatiosta. Manuaalinen kameravalvonta on siinäkin mielessä tehotonta, että yksittäinen ihminen ei kykene seuraamaan kovin montaa kameraa tai kohdetta kerralla. Koneälyllä toimiva järjestelmä pystyy seuraamaan yhtä aikaa kaikkea mihin sillä on näkyvyys, ja se kykenee siihen ilman taukoja. Tulevaisuudessa koneälyn tekemät poikkeamahavainnot mahdollistivat paljon tehokkaamman ja nopeamman reagoinnin.

Vartijat

Vartijoiden työnkuvan visioitiin teknistyvän, kaikkia tai lähes kaikkia työtehtäviä digitalisaatio tullee muokkaamaan. Koneäly, robotiikka, automatisaatio ja IoT tulevat tehostamaan vartijan työskentelyä, tai tietyissä tehtävissä korvaamaan. Esimerkkinä tehostamisesta on teknisten-järjestelmien antamat hälytykset, jotka vaativat nykytilassa lähes aina ihmisen paikan päälle lähettämistä. Iso osa hälytyksistä on turhia, ja aiheuttavat asiakkaille kustannuksia, ollen myös vartioimisliikkeelle ongelma, koska vaativat vaihtelevan määrän resursseja, tuottavat reklamaatioita ja asiakastyytyväisyyden tippumista. Tulevaisuudessa digitalisaation tuomilla ratkaisuilla valtaosassa hälytyksistä ei tarvitse enää lähettää vartijaa paikalle, vaan turhat hälytykset pystytään seulomaan pois.

Vartijoiden määrällinen tarve tulee laskemaan, mutta ammattitaidon vaatimukset nousemaan. Alalle jääville tämä voi näkyä positiivisena palkkakehityksenä ja vastuun lisääntymisenä. Nykyisten vartijan perustaitojen osaamisen ei tarve ei häviä, mutta tarvitaan myös laajempaa teknistä osaamista ja lain tuntemusta.

Osa työtehtävistä saattaa siirtyä etätyöskentelyksi, ja mahdollisesti asiantuntijatyöksi. Palkkakulurakenne muuttuu työntekijöiden määrän vähentyessä, mutta teknisten laitteiston lisääntyessä.

Laki

Lakien säätäjät reagoivat muuttuvaan toimintaympäristöön, välillä suhteellisen pitkällä viiveellä. Digitalisaation kehitys voi jossain vaiheessa olla niin nopeaa, että syntyy lain kannalta hankalia tilanteita. Todennäköisesti kehityksen myötä syntyy liiketoimintaa, joka nojaa täysin uuteen teknologiaan. Tämä uusi teknologia voi olla kiisteltyä, ja on mahdollista, että liiketoiminnalta menee pohja, jos lain säätäjät päätyvät sääntelemään rajusti toimintaa. Esimerkkinä yksityinen pysäköinninvalvonta, joiden toiminta olisi mahdollisesti täysin lakannut, jos korkein oikeus olisi todennut toiminnan laittomaksi. Korkein oikeus totesi toiminnan kuitenkin lailliseksi, jolloin lain säätäjät ilmoittivat, että toimintaa säätelevä laki laaditaan pikaisesti. Lakia ei ole tätä kirjoittaessa edelleenkään laadittu.

Tulevaisuudessa dataa on saatavilla suuria määriä, yksityinen turvallisuusala pystyisi tehostamaan toimintaansa datan avulla, mutta voi olla, että laki ja lain tulkinta estää osan toiminnasta. Ei olla kaukana, että koneäly pystyy valvontakameroiden avulla tunnistamaan kauppaan tulevan tutun näpistelijän automaattisesti. Tulevaisuuspyörään osallistuneet asiantuntijat pystyivät perustelamaan tämän lailliseksi, sekä myös laittomaksi, virallista oikeuslaitoksen lain tulkintaa ei ole vielä tehty.

Keskustelussa nousi esille myös GDPR, eli General Data Protection Regulation, joka Suomeksi tunnetaan nimellä EU:n yleinen tietosuoja-asetus. Kyseinen asetus on hyvin ajankohtainen kirjoitushetkellä, ja se on aiheuttanut monessa organisaatioissa toimenpiteitä. Tulevaisuudessa asetus voi kokea muutoksia, mutta kyseinen asetus tai sen seuraaja on todennäköisesti aina ajankohtainen yksityisellä turvallisuusalalla. Alalla käsitellään monenlaisia henkilörekistereitä, tulevaisuudessa kirjo ja määrä kasvaa entisestään.

Internet Of Things

Esineiden Internet koettiin suuren mahdollisuuden lisäksi myös suurena uhkana turvallisuuden kannalta. Tulevaisuudessa lähes kaikki laitteet omaavat verkko-ominaisuuksia, kahvinkeittimestä autoon. Yksityisellä turvallisuusalalla tämä merkitsee esimerkiksi mahdollisuuksia käyttää rikosilmoitinjärjestelmän osana vaikkapa liikkeentunnistavaa lamppua, tai lähes mitä vain

sensoria. Tällä hetkellä rikosilmoitinjärjestelmän ilmaisimet ovat vain siihen käyttöön soveltuvia, jotka pitää erikseen asentaa.

Visioitiin myös, että vuonna 2025 tai aikaisemminkin ei tarvitse välttämättä edes asentaa itse kohteeseen rikosilmoitinjärjestelmän keskusta. Järjestelmä voi toimia pilvipalvelun kautta ja sitä hallitaan etänä. Palvelun käyttöönotto vaatisi vain sopivaa esineiden Internetin ekosysteemiä kohteessa, ekosysteemi voisi toimia sensoreina pilvessä toimivalla rikosilmoitinpalvelulle. Sama järjestelmä voi havaita myös muita vaaroja, kuten vuotoja, lämpötilan vaihteluita, riippuen käytettävissä olevista laitteista.

Tämä kaikki vaatii ensiluokkaista tietoturvallisuutta. Tulevaisuuden ammattirikolliset eivät käytä sorkkarautaa vaan tietokonetta, kännykkää ja vastaavia teknisiä välineitä. Ennen, ja varmasti jatkossakin löytyy haavoittuvaisuuksia, joten on panostettava laadukkaaseen riskienhallintaan.

Automatisaatio

Digitalisaation eteneminen tulee vahvistamaan automatisaatiota myös turvallisuusalalla, koneäly, robotiikka ja Internet of Things ovat kaikki osia automatisoinnin edistymisessä. Turvallisuusalan luonne palvelualana on tähän mennessä pitänyt automatisoinnin määrän vähäisenä, sopivaa teknologiaa ei ole ollut käytettävissä. Teollisuudessa automatisointi on ollut arkipäivää jo vuosikymmeninä, nykyään löytyy jo täysin automatisoitua tehtaita, joissa ihminen toimii työnvalvojana. Todennäköisesti yksityisellä turvallisuusalalla käy teknologian kehittyessä kuten teollisuudessa, vartijat siirtyvät enemmän työn tekemisestä järjestelmien valvojiksi, jotka puuttuvat asioihin vasta kun havaitaan poikkeamia.

Tulevaisuuspyörään osallistuneet asiantuntijat uskovat, että vuonna 2025 osa vartijoiden ja yksityisen turvallisuusalan toimihenkilöidenkin tehtävistä on automatisoitu, mutta osaan automatisointi ei vaikuta. Hälytystenkäsittely ja -tarkastaminen tulee osittain automatisoitumaan eri järjestelmien yhteistyön avulla. Visioitiin, että jonkin laitteen havaitessa valvotussa kohteessa poikkeaman, voi konenäöllä varustettu älykäslaite analysoida automaattisesti mikä oli poikkeaman aiheuttaja. Tällöin järjestelmä joko päättää, että poikkeama vaatii ihmisen suorittaman tarkastuksen, korjaa tilanteen itse tai kuittaa sen pois aiheettomana. Nykytila on se, että hälytyksen tullessa sen käsittelee hälytyskeskuspäivystäjä, joka lähettää paikalle piirivartijan, koska hälytyskeskuspäivystäjällä ei ole näköyhteyttä kohteelle, eikä hän voi mitenkään tietää onko hälytys aiheeton vai ei. Toimihenkilöiden töistä osa asiakkaiden yhteydenpidosta voidaan siirtää siinä mielessä automatisoiduksi, että asiakas itse nettipohjaisenpalvelun kautta käsittelee asiakkuuttaan. Asiantuntijan töistä esimerkiksi osa kartoituksista ja dokumenttien laatimisesta siirtyy automatisoidun palvelun kautta tehtäväksi. Laitteet- ja ohjelmistot kehittyvät, jolloin myynti painottuu niiden myymiseen, työvoimaa myydään vähemmän.

Vaarat

Digitalisaation myötä toimintaympäristö voi muuttua hyvin nopeasti, eli jos ei ole ajan tasalla niin on vaarana menettää markkina-asemansa. Suomalaisittain Nokian kohtalo on monella hyvin muistissa, jos ei tarjoa sitä mitä markkinat haluavat ja saavat kilpailijalta, niin koko liiketoiminta voi murentua nopeasti. Oman alan kilpailijoiden lisäksi pitää pystyä tarkkailemaan muuta kehitystä, esimerkiksi asiakkaiden tarpeet turvallisuuden palveluitten suhteen voi muuttua heidän alansa muuttuessa. Myös yhteiskunnan muut muutokset voivat vaikuttaa, kuten lakimuutokset tai kokonaan uudet lait.

Toiminnan teknistyessä lisääntyy riippuvuus teknologiasta, mahdolliset häiriöt voivat lamaannuttaa koko toiminnan. Jatkuvuussunnittelu on tärkeässä osassa, jotta häiriöiden vaikutus voidaan minimoida. Tulisi myös pitää muistissa miten asiat hoidettiin ennen, jottei käy niin kuin USA:n armeijan laivastolle, jossa havahduttiin siihen, ettei enää osata suunnistaa manuaalisesti tähtien avulla. Pahimmillaan tilanne olisi ollut se, että navigointijärjestelmien pettäessä ei olisi osattu määritellä sijaintia tai miten päästä määränpäähän. Ratkaisuna oli vanhojen taitojen opettamisen takaisin ottaminen koulutukseen.

Digitalisaatio aiheuttaa varmasti monia haasteita yksityisen turvallisuusalan toimijoille, ehkä jopa korostuneemmin kuin monella muulla alalla. Toimintaympäristön muutosten aktiivinen havainnointi ja riittävä varautuminen minimoi vaarojen muuttumista toteutuneiksi riskeiksi. Jatkuvuussunnittelussa tulee muistaa, että hyvin tehty suunnittelu on lähes arvotonta, jos sen toteuttamiseen ei ole valmiuksia. Monesti paperille laaditaan suunnitelma, mutta tarvittavat tahot eivät siihen tutustu, eivätkä harjoittele.

Koulutus

Digitalisaation vaatimiin koulutusmuutoksiin reagoidaan todennäköisesti jälkikädessä, eli siinä vaiheessa, kun osaajia olisi jo pidemmän aikaa tarvittu. Teknistyminen tuo alalle entistä enemmän ihmisiä, joiden tausta ja koulutus ei suoraan ole liittynyt turvallisuusalaan. Järjestelmäasiantuntijat, asentajat ja tuotekehittelijät tulevat nykyään koulutuksista, joissa turvallisuusalan näkökulmaa ei välttämättä käsitellä juurikaan.

Tulevaisuuspyörään osallistuneet visioivat, että vuonna 2025 on turvallisuusalan perus- sekä korkeakoulututkintoja, joissa pääpainona on erikoistuminen. Jatkossa kokonaisuudet voivat olla niin monimutkaisia, että tarvitaan koulutuksia, joissa ollaan syvennetty tiettyihin osa-alueisiin. Samaan aikaan tarvitaan esimerkiksi ITC-alan koulutuksia, joissa erikoistutaan turvallisuusalan tarpeisiin.

Tällä hetkellä koulutuksen näkökulmasta kynnys työllistyä vartijaksi on suhteellisen matala, väliaikaisen vartijakortin saa 40 tunnin koulutuksella ja vakinainen vartijakortti edellyttää 80

tuntia lisäkoulutusta. Voi olla, että tulevaisuudessakin kynnystä pidetään matalana, mutta tiettyihin tehtäviin vaadittaisiin lakisääteisestikin erillinen koulutus.

Robotiikka

Työryhmä visioi, että vuonna 2025 robotiikka on tuonut yksityiselle turvallisuusalalle toimivia ratkaisuja tehostamaan ihmisten työskentelyä. Valvonta ja avustavat tehtävät ovat sellaisia, joita koneet voivat suorittaa teknologian kehittyessä. Droneilla voisi jo nyt valvoa soveltuvia ulkoalueita, kuten tehdasalueita ja vastaavia. Kaupunki ympäristössä kameralla varustetun dronen käyttäminen ei todennäköisesti tule kuitenkaan olemaan helppoa, nykyisen lain puitteissa ehkä jopa mahdotonta.

Tulevaisuudessa, kun teknologia ja toimintaympäristö ovat kehittyneet, voi iso osa tarkastus-, sekä avaus- ja sulkukierroksista olla robottien ja automatiikan suorittamia. Turvatarkastukset siirtyvät myös täysin koneellisiksi, jolloin turvatarkastajien tarve muuttuu radikaalisti.

Robotit pystyvät tulevaisuudessa suorittamaan myös palvelutoimintaa, kuten opastamista. Vartijoiden, järjestyksenvalvojien ja turvatarkastajien ammatteihin kuuluu myös tietyissä tilanteissa henkilön koskemattomuuden loukkaaminen laillisesti. Tilanteita ovat esimerkiksi poisto, kiinniotto ja ensiapu. Näissä tilanteissa vastuuta tuskin vielä vuonna 2025 voidaan siirtää roboteille, teknologian rajoitteiden lisäksi kyseessä on iso periaatteellinen päätös. Tuskin pitkään aikaan tulemme näkemään tilannetta, jossa hyväksyttäisiin automatisoidun robotin käyttämät voimakeinot ihmistä kohtaan.

5.3 Tutkimustulosten mallintaminen skenaarioilla

Opinnäytetyössä olevat kolme skenaariota ovat opinnäytetyön tekijän luomia kertomuksia, tulevaisuuspolkuja. Kertomukset mallintavat tutkimuksen johtopäätöksiä ja olettamuksia. Jokaisella skenaariolla on oma lähtökohtansa, jonka näkökulmasta kertomus etenee käyttäen tutkimuksista saatua tietoa ja opinnäytetyön tietoperustaa.

Vuosi 2025 — yksityinen turvallisuusala pysähtyneisyyden tilassa kertoo tilanteesta, jossa riskienhallintaa ei ole tehty laadukkaasti, riskit ovat toteutuneet. Uuden teknologian käytettävyys ja saatavuus on ollut tärkeintä, turvallisuudesta on tingitty. Ei ole kyseenalaistettu kaikkea sitä informaatiota ja oikeuksia, joita annetaan palveluntuottajille. Jo nykyäänkin annetaan kaikennäköisille ohjelmistoille ja palveluille voimakkaita oikeuksia käyttää tietoja. Samoin tietoja jaetaan hyvin vapaasti eri tahoille, kuten digitaalisesti siirretään tietoja pilvipalveluihin. Vaarana on, että palveluntuottajalla on suoraan taka-ajatuksia tiedon hyödyntämiseksi jopa laittomin keinoin, tai heidän tietosuoja ei ole riittävä, jolloin jaetut tiedot voivat vuotaa täysin asiattomille tahoille.

Vuosi 2025 — yksityinen turvallisuusala on digitalisaatio ja ihmisiä kertoo tilanteesta, jossa digitalisaatio on edennyt tasapainoisesti. Digitalisaation suhteen on ollut onnistumisia ja epäonnistumisia. Riskienhallintaan on panostettu, mutta varautumisesta huolimatta joitakin epätoivottua tapahtumia on tapahtunut. Vuonna 2025 on syntynyt eräänlainen balanssi digitalisaation ja perinteisten palveluiden välille. Yhteiskunnan näkökulma on, että kaikkea ei rakenneta digitalisaation varaan. Digitalisaation mahdollistamat edistykset pidetään hyvänä renkinä, mutta ei päästetä isännän asemaan.

Vuosi 2025 — digitalisoitu yksityinen turvallisuusala kertoo tilanteesta, jossa digitalisoituminen on edennyt nopeasti, mutta hallitusti. Digitalisaation eteneminen on kokonaisuudessaan tarkasti suunniteltu, sekä toteutettu. Riskeihin on varauduttu laadukkaasti, epätoivotut tapahtumat eivät ole päässeet yllättämään. Digitalisaation mahdollistamat palvelut on kehitetty yhdessä asiakkaitten kanssa, muuttuva toimintaympäristö on huomioitu. Liiketoiminnan ja organisaatioiden näkökulmasta digitalisaatio on ollut menestys. Yksittäisen ihmisen näkökulmasta tilanne voi olla kuitenkin hyvin haasteellinen.

5.3.1 Vuosi 2025 — yksityinen turvallisuusala pysähtyneisyyden tilassa

Digitalisaatio megatrendinä on epäonnistunut, koska ilmiö ei edennyt lainkaan niin nopeasti kuin vielä 2010-luvulla visioitiin, ilmiö kohtasi kriittisiä esteitä. Kokeiluja tehtiin, mutta suurin osa digitalisaation perustuneista palveluista ja tuotteista kuihtui, koska asiakkaat eivät todellisuudessa tarvinneet niitä, tai niissä oli pahoja puutteita. Myös yksityinen turvallisuusala meni teknologia edellä, kehitellen kaikennäköistä mitä vain pystyi uudella teknologialle tekemään. Asiakkaitten tarpeita ei kartoitettu, harvalle uudelle ratkaisulle oli oikeasti tarvetta ja kysyntää. Tekemisestä tuli liian teknologia riippuvaista. Ratkaisut olivat myös niin teknisiä, että harva ymmärsi niitä syvemmin. Koulutus ei pysynyt perässä. Yksityisten turvallisuusalan yritysten piti sisäisesti kouluttaa lähes kaikki, mikä liittyi digitalisaation mahdollistamiin ratkaisuihin. Tähän yrityksillä ei ollut aikaa, eikä kouluttajia, koska osaajat olivat kiinni omissa töissään.

Henkilöstökuluja yritettiin myös karsia liian rivakasti, vartijoita ja toimihenkilöitä irtisanottiin. Perinteisten palvelujen tilalle tulleet sähköiset palvelut jättivät asiakkaat ilman aitoa kontaktia ja usein myös tarvitsemaansa palvelua. Osa vartijoiden työstä oli teoriassa korvattu koneälyllä ja roboteilla. Käytännössä ratkaisut olivat puolivillaisia, joista harva toimi kuten piti. Esimerkiksi oli tapaus missä yksityisen turvallisuusalan hälytyskeskus sai kohteelta palohälytyksen, kohteella oli useita erilaisia ilmaisimia ja myös etäkäytössä olevat kamerat. Hälytyskeskuspäivystäjä olisi heti todennut, että kohteella on akuutti tilanne päällä. Hälytyskeskuksen käytössä ollut vikaantunut koneäly kuitenkin hylkäsi hälytyksen aiheettomana, ilman että olisi pyytänyt ihmistä varmistamaan tapausta.

Uusia tuotteita otettiin myös liian nopeasti tuotantoon, kartoittamatta uhkia, vaaroja ja riskejä. Esimerkiksi kehitettiin koneälyllä toimiva kamerajärjestelmä, järjestelmä pystyi itsenäisesti keräämään ja käyttämään dataa. Järjestelmä alkoi automaattisesti tunnistamaan yksittäisiä ihmisiä, sekä profiloimaan ihmisiä ulkoisten ominaisuuksien perusteella. Järjestelmän asiakkaaksi tuli eräs kauppaketju, joka syötti omien asiakkaiden tiedot järjestelmään, siten että kamerat tunnistivat henkilön. Tämän avulla he seurasivat asiakkaitten ostokäyttäytymistä kaupassa, sivutuotteena myös tutut näpistelijät olivat järjestelmän automaattisessa valvonnassa. Uutismedia sai tästä tiedon, jonka jälkeen siitä tuli iso uutisaihe. Tapaus meni viranomaiskäsittelyyn, jonka lopputuloksena järjestelmä todettiin laittomaksi. Järjestelmästä vastuussa ollut yksityisen turvallisuusalan yritys sai isot sanktiot. Lain muutokset ovat mahdollisia, mutta hitaita, ilman muutoksia vastaavaa palvelua ei saa tarjota.

Esineiden Internettiin liitetty rikosilmoitinjärjestelmä tuntui aluksi hyvältä ja helpolta, sen kautta pystyi esimerkiksi kotiasiakas säätelemään lukituksia, valoja, kodin lämpötilaa ja niin edelleen. Hakkerit kuitenkin löysivät niistä nopeasti haavoittuvaisuuksia, jolloin kodin järjestelmiä pystyi kaappaamaan toiselta puolelta maapalloa. Osa hakkereista teki täysin huvikseen ilkivaltaa, osa suunnitelmallisia rikoksia. Etähallintaan otetulla järjestelmällä sai lukot auki ja hälyttimet pois päältä. Vuonna 2025 on palattu vanhoihin, paikallisiin järjestelmiin, joita valvovat ihmiset. Luottamuksen puutteen vuoksi moni organisaatio hoitaa turvallisuutensa kaikki osa-alueet itsenäisesti, eivätkä ulkoista yksityisen turvallisuusalan yrityksille.

Ihmisten luottamus yksityisen turvallisuusalan digitalisaation myötä tulleisiin palveluihin on heikkoa. Suurin osa käytössä olevista palveluista ja tuotteista ovat samoja, mitä oli jo 2010-luvulla. Yksityistäminen trendinä on myös pysähtynyt, koska päättäjät eivät luota yksityisen turvallisuusalan laatuun. Yksityinen turvallisuusala työllistää jonkin verran vähemmän ihmisiä, mitä 2010-luvulla. Kehitystyö on aloitettava uudestaan, eri lähestymistavalla.

5.3.2 Vuosi 2025 — yksityinen turvallisuusala on digitalisaatiota ja ihmisiä

Vuonna 2025 ihmiset ovat tottuneita digitaalisten palveluiden käyttäjiä, tämä pätee korkean elintason maihin, kuten Suomeen. Digitalisaation suhteen on ollut epäonnistumisia, sekä onnistumisia, mutta virheistä on opittu ja palveluihin luotetaan. Yksityisellä turvallisuusalla menee hyvin, alan liikevaihto on kasvanut vuosi vuodelta, sekä ala työllistää joka vuosi enemmän ihmisiä.

Digitalisaatio on yksityisellä turvallisuusalalla valjastettu tukemaan ihmisten toimintaa. Vartijoiden määrä on hienoisessa laskussa, verrattuna huippuvuosiin. Määrän lasku johtuu digitalisaation tuomasta tehostamisesta, sekä toimintaympäristön muutoksista. Esimerkiksi kivijalkakauppojen määrä on vähentynyt, kauppaa käydään digitaalisesti, jolloin vähittäiskaupan vartiointipalveluiden tarve on vähentynyt huomattavasti. Yksityisen turvallisuusalan asiakaskunta

on kuitenkin hyvin laajaa, digitalisaation tuoma tehostaminen ja kehitys ovat tuoneet monenlaisia palveluita yhä useamman ulottuville. Yksityistäminen on myös jatkunut, esimerkiksi vankilat pyörivät turvallisuusalan yritysten pyörittäminä.

Alalle on syntynyt uutta liiketoimintaa. Uusi liiketoiminta perustuu lähinnä asiantuntijoiden kehittämiin ja ylläpitämiin moderneihin ratkaisuihin. Vanhat ja uudet palvelut, sekä alan toimijat tukevat toistensa onnistumista. Alan arvostus on nousussa, koska ihmiset tuntevat yksityisen turvallisuusalan tekevän töitä yleisenkin turvallisuuden puolesta. Toisaalta osa taas kokee, että turvallisuudesta on tullut rahalla ostettavaa, eikä valtion vastuulla oleva perustehtävä.

Vanhatkin yksityisen turvallisuusalan yritykset ovat joutuneet uudistumaan, kaikki eivät ole siihen pystyneet. Jokaisen toimijan tulee pystyä tuottamaan osa palveluista digitaalisena, vaikka ydintoiminta pyörisi edelleen vanhalla liiketoimintamallilla ja konseptilla. Verkostoituminen eri alan toimijoiden kanssa on tärkeää, asiakkaalle voidaan tarjota verkostojen avulla monipuolisia palveluita. Toimintaympäristön muutokset ovat tuoneet uusia vaatimuksia, jokaisen alan toimijan pitää täyttää tiukat lain vaatimukset esimerkiksi henkilötietojen ja tietoturvallisuuden suhteen. Muutokset ovat tuoneet lisää vaatimuksia myös turvallisuusalan koulutuksiin, vartijoiltakin vaaditaan syvempää tietämystä. Koulut ovat muokanneet koulutustarjontaansa tarpeen mukaiseksi, sekä yrityksillä on omia sisäisiäkoulutuksia riittävillä resursseilla toteutettuna.

Asiantuntijoille on töitä, riskienhallinnan ja jatkuvuuden arvo on ymmärretty. Moneen koulutukseen sisältyy vuonna 2025 turvallisuuteen liittyviä opintoja. Palvelut suunnitellaan security by design periaatteella, eikä niin, että turvallisuus ajatellaan jälkikäteen. Riskienhallinnasta on tullut insinööritoimiston tapaista työtä. Riskienhallinnan asiantuntijatiimit koostuvat monen alan ihmisistä, riskienhallinnan prosesseihin keskittyneiden toimiessa tiiminvetäjinä. Koneäly tukee työskentelyä, se käsittelee isoa määrä dataa, sekä antaa ehdotuksia. Digitalisaatio ihmisten tukena on pääsääntöisesti nostanut ihmisten elämänlaatua Suomessa vuonna 2025.

5.3.3 Vuosi 2025 — digitalisoitu yksityinen turvallisuusala

Inhimillinen osuus turvallisuudesta on pyritty eliminoimaan. Historiallisesti useimmiten heikoin lenkki on ollut ihminen, kun jokin huomattava riski on toteutunut. Digitalisaation myötä turvallisuuttamme valvoo koneäly algoritmeillaan, robotit ja erilaiset muut verkottuneet laitteet. Kehitys on ollut hurjaa, mainittavia vastoinkäymisiä ei ole ollut. Riskit on tunnistettu ja hallittu, yksityiseen turvallisuusalaan luotetaan. Viranomaiset keskittyvät vakavaan rikollisuuteen, useat muut tehtävät ovat yksityistetty.

Vartijoiden määrä on vähentynyt huippuvuosista huomattavasti. Palvelut pyörivät digitalisaation mahdollistaman ekosysteemin avulla. Koneäly on ihmistä huomattavasti älykkäämpi ja tehokkaampi. Oppiva koneäly pyörittää monia yksityisen turvallisuusalan palveluita, sekä itsenäisesti kehittää niitä, ihmisten toimiessa varmistajina. Riskienhallintakin on pitkälti automatisoitua, asiantuntijoiden toimiessa taustalla. Koneäly toimii jo lähes isäntänä, robottien ollessa renkinä. Ihmisten osuus on muuttumassa epäselväksi.

Pitkään alalla uraa tehneiden on ollut hankala työllistyä uusiin tehtäviin, moni on jäänyt työttömiksi. Ylipäätään yhä harvempi tekee töitä, yhteiskunta pyörii koneälyn, robottien ja automatisoinnin avulla tehokkaasti. Työttömien tuet ovat parantuneet, mutta toimettomuus aiheuttaa epätyytyväisyyttä. Johtajille, huippuosaajille, sekä joidenkin alojen asiantuntijoille ja työntekijöille riittää vielä töitä.

Yksityisen turvallisuusalan nopea digitalisoituminen on karsinut vanhoja toimijoita alalta. Lähes kaikki pienemmät ovat joutuneet lopettamaan. Pienille, vanhoille yrityksille nopeat toimintaympäristön muutokset ovat olleet liian isoja, ne eivät ole pysyneet kehityksessä mukana. Muutamat pienemmät ovat osanneet uudistua riittävästi, nämä yritykset ovat löytäneet oman paikkansa markkinoilta. Isot yritykset ovat vahvistaneet asemiaan, sekä alalle on tullut uusia yrityksiä uudenlaisilla palvelu- ja liiketoimintamalleilla.

Koulutus on hyvin pitkälti digitalisoitunut, sekä opintojen sisällöt ovat entistä teknisempiä. Yleisopinnot muodostavat pienen osan kokonaisuudesta, erikoistuminen aloitetaan lähes heti. Vartijaksikaan ei voi enää kouluttautua lyhyillä kursseilla, vaan pitää käydä pidempi koulutus. Vartijakoulutukseenkin sisältyy erikoistuminen, erikoistuminen määrää sen minkä tyyppiseen työhön todennäköisesti työllistyy.

Katukuvassa näkyy erilaisia automatisoituja robotteja tekemässä manuaalista työtä. Robotit tarkkailevat myös turvallisuuspoikkeamia, sekä puuttuvat niihin. Harvemmin tarvitaan ihmistä paikalle, roboteilla on jopa oikeus pysäyttää rikoksesta epäilty ihminen tietyillä lievemmillä keinoilla. Asiakaspalvelu, ja lähes kaikki muukin asiointi toimii digitaalisesti ja automatisoidusti. Ihmiskontaktit ovat vähentyneet. Ero maaseudun ja Smart City tyyppisten kaupunkien välillä on iso. Maaseudun palvelut ovat hyvin karsittuja, joka johtaa entistä ripeämpään kaupungistumiseen. Digitalisaatio pitkälle vietynä tuo tiettyä helppoutta, mutta moni joutuu miettimään oman elämäntapansa uusiksi, kun töitä ei ole enää kaikille halukkaille.

6 Johtopäätökset ja pohdinta

Tutkimus toi esiin hyödyllistä tietoa ja näkemystä yksityisen turvallisuusalan digitalisaatiosta, sekä sen kehityssuunnista. Tutkimusmenetelmät olivat onnistuneita, niiden avulla hankittiin myös uutta tietoa. Opinnäytetyön tuloksena on runsaasti tietoa tutkittavasta ilmiöstä, tulos

palvelee toimeksiantajan asettamia tavoitteita. Skenaariot vahvistavat toimeksiantajan mahdollisuuksia tehdä oikeita päätöksiä.

Opinnäytetyön tutkimuskysymykset olivat: mitä todennäköisiä vaihtoehtoja tulevaisuus sisältää, sekä mihin vaihtoehtoon tulisi pyrkiä? Opinnäytetyössä esitetyt skenaariot tuovat vastauksia tutkimuskysymyksiin. Toimeksiantajan liiketoiminnan kannalta kummatkin digitalisaatiolle positiiviset skenaariot ovat toivottavia lopputuloksia. Yhteiskunnallisesti toivottavin skenaario on: yksityinen turvallisuusala on digitalisaatio ja ihmisiä, koska digitalisaation etenemisestä huolimatta ihmiset eivät jää toimettomiksi. Skenaariossa digitalisaatio tukee ihmisten toimintaa, muttei korvaa ihmistä yhteiskunnan pyörittäjänä, kuten kolmannessa skenaariossa lähes käy. Skenaarion yksityinen turvallisuusala pysähtyneisyyden tilassa toteutuminen olisi opinnäytetyön toimeksiantajalle erittäin haitallista, eli tämä mahdollinen tulevaisuus pitää välttää. Toteutuessaan liiketoiminta kärsisi, toiminta saattaisi jopa lakata. Skenaarion toteutuminen vaatisi suuria epäonnistumisia laajalti, myös valtioiden tasolla.

Luonteeltaan tulevaisuustutkimus on suurelta osalta näkemyksellistä tietoa, eli mielipiteitä. On hyvin mahdollista, että mikään tulevaisuuspoluista ei tule toteutumaan. Tämä ei merkitse, että tutkimus olisi epäonnistunut, vaan epävarmuus on osa tulevaisuudentutkimuksen luonnetta. Opinnäytetyön tietoperusta ja työtä varten tehty tutkimus kuitenkin luovat uskottavia ja mahdollisia tulevaisuuskuvia siitä, miltä vuoden 2025 Suomen digitalisoitunut yksityinen turvallisuusala voisi näyttää. Luotettavuutta lisää se, että lähteestä riippumatta visio tulevaisuuden kehityksestä oli hyvin samansuuntainen. Selkeästi ristiriitaista tietoa tai mielipidettä ei löytynyt opinnäytetyön tietoperustasta, tai työtä varten tehdystä uudesta tutkimuksesta.

Opinnäytetyön tutkimuksen perusteella, on todennäköistä, että monet vartijan suorittamat toimenpiteet korvataan digitalisaation mahdollistamilla ratkaisuilla vuoteen 2025 mennessä. Yksilön osaamisen vaatimukset nousevat, vartijalta jatkossa vaaditaan syvempää asiantuntemusta ja erikoistumista. Ammattinimekkeiden rajat hämärtyvät, esimerkiksi vartija, turvallisuusasiantuntija ja turvatekniikanasentaja voivat olla sama henkilö, jolla on tarvittava asiantuntijuus. Toisaalta monimutkaisemmat projektit ja järjestelmät tulevat vaatimaan entistä syvempää asiantuntemusta.

Teknologian kehityksen tahti tulee kiihtymään, ja näemme uusia palveluja monipuolisesti. Yksityisen turvallisuusalan tarjoamat ratkaisut kehittyvät ja muuttuvat digitalisaation myötä. Asiakkaat eivät tarvitse useampaa erilaista järjestelmää, vaan kaikki toimivat Internet Of Thingsin kautta yhdessä, osana samaa digitaalista ekosysteemiä. Järjestelmien keskuksia ei tarvitse enää asentaa kohteille, vaan toiminta perustuu pilvipalveluihin.

Yksityisen turvallisuusalan kasvu jatkuu, tätä tukee asiakaskunnan laajeneminen yleisesti, sekä yksityistäminen. Lähitulevaisuudessa suorittavan työn työtekijöiden määrä kasvaa edel-

leen, kunnes lähtee digitalisaation kehittymisen myötä laskuun. On todennäköistä, että jo lähitulevaisuudessa syntyy yksityiselle turvallisuusalalle täysin digitalisaatioon nojaavia liiketoimintamalleja. Digitalisaatio tehostaa vanhoja ja luo uusia palvelumalleja. Vuoteen 2025 mennessä työpaikkoja poistuu suorittavalta tasolta, mutta asiantuntijoille syntyy työpaikkoja.

Turvallisuuden kannalta digitalisaatio on suuri haaste, on tärkeää tunnistaa ja minimoida riskit ajoissa. Riskienhallinnan tulee olla laadukasta, jotta voidaan ottaa harkittuja ja hallittuja riskejä. On selvää, että myös rikosten tekijät käyttävät digitalisaatiota hyödyksi ja rikollisuudenmuodot kehittyvät. Vaarana on, että edetään liian nopeasti turvallisuutta huomioimatta, tällöin riskien toteutumisen mahdollisuudet kasvavat huomattavasti.

Yritysten pitää pystyä hyväksikäyttämään digitalisaatiolle suotuisa toimintaympäristö, ja tehdä asiakastarpeita kuunnellen kehitystyötä. Yksityisellä turvallisuusalalla on omat haasteensa sovittaa yhteen yksityisyyden suoja ja digitalisaation mahdollistamat palvelut. On tärkeää ymmärtää toimintaympäristön uhat, sekä mahdollisuudet. Mahdollisuuksia digitalisaatio tulee tuomaan runsaasti. Kaiken mahdollisen digitalisoiminen ei pitäisi olla tavoite, vaan pitää tehdä ihmislähtöisiä ratkaisuja, jotka parantavat elämäämme.

6.1 Jatkotutkimus

Tutkittavasta ilmiöstä olisi mahdollista tehdä myös määrällinen tutkimus, jonka ei välttämättä tarvitsisi olla tulevaisuudentutkimus. Näkökulmana esimerkiksi digitalisaation tuomat hyödyt ja uhat turvallisuusalalle. Tutkittavaa dataa löytyy todennäköisesti valmiista tilastoista, mutta hyödyllisen uuden tiedon kerääminen toisi tutkimukselle lisäarvoa.

Yksityisen turvallisuusalan toimijoita hyödyttäisi syvempi tutkimus tulevista asiakastarpeista. Digitalisaatio tulee mahdollistamaan monen muotoisia palveluita, olisi tärkeää yhdessä asiakkaiden kanssa arvioida minkä tyyppiset palvelut parhaiten palvelisivat heidän toimintaansa jatkossa. On tärkeää tunnistaa ajoissa muuttuvan toimintaympäristön uhat ja mahdollisuudet, jotta ymmärretään mitä asiakkaat tarvitsevat ja mistä ovat valmiita maksamaan.

Tulevaisuuden koulutustarpeet yksityisellä turvallisuusalla olisi myös hyödyllinen aihe uudelle tutkimukselle. Tutkimusta ei tarvitse sidota digitalisaation, vaan käsitellä yleisesti. Välillä kuulee koulutuksista kritiikkinä, että opetus ei ole ajantasaista, joten olisi hyvä olla proaktiivinen. Työelämää voitaisiin palvella entistä paremmin, jos osataan ennakoida muuttuvia koulutustarpeita.

6.2 Oman työn arviointi

Omasta ja toimeksiantajan mielestä tutkimukseni onnistui tuottamaan uutta tietoa, jota toimeksiantaja pystyy hyödyntämään. Toimeksiantaja oli tiiviisti mukana tutkimuksen toteutta-

misessa. Työn tavoitteet ja prosessi olivat yhdessä suunniteltu, sekä tutkimukseen osallistuneet asiantuntijat tulivat lähinnä toimeksiantajan kautta. Opinnäytetyössä on myös osatuotoksia, kuten tulevaisuuspyörä, jota on helppo käsitellä yrityksen kehittämistyön apuvälineenä. Jokaisen käyttämäni tutkimusmenetelmän tulokset voi halutessaan käsitellä erillisenä, jos esimerkiksi skenaarioitten kertomuksellinen ote epäilyttää.

Saavutin itselleni asettamani tavoitteet, opin aiheesta ja siihen liittyvistä asioista lisää, sekä myös tutkimuksellisuudesta. Aikataulun kanssa oli haasteita, eli työ venyi. Viivästyksestä oli sovittu yhdessä toimeksiantajan kanssa. Prosessi lähti käyntiin maalikuussa 2017 ja lopullinen tulos oli valmis joulukuussa 2018. Opinnäytetyön suunnitelman mukaan työn piti olla valmis viimeistään joulukuussa 2017. Syitä venymiselle oli useampia, yksi niistä oli, että lähdin haalimaan tietoa liikaa. Lopullisesta työstä on esimerkiksi poistettu osio, jossa olisi käyty läpi yleisesti tulossa olevia digitalisaation mahdollistamia ratkaisuja, jotka liittyvät yksityiseen turvallisuusalaan. Osion tarkoitus oli tunnistaa heikkoja signaaleja, joista voi tulla tulevaisuuden trendi. Luin kymmeniä artikkeleita ja laadin raakaversion tietoperustaksi opinnäytetyöhön. Koin kuitenkin, ettei osio palvele tarkoitusta, vaan heikentää lopputulosta. Opinnäytetyötä ei kannata laajentaa liikaa, vaan pitää fokus tavoitteissa.

Ylimääräisen vuoden aikana on tapahtunut muutoksia toimintaympäristössä, sekä toimeksiantajani organisaatiossa. Työni on kuitenkin edelleen toimeksiantajalleni hyödyllinen, sen arvo ei ole alentunut viivästyksestä huolimatta. Opinnäytetyössäni todennäköisesti näkyy tietty kokemattomuus tulevaisuudentutkimuksen tekemisestä, mutta myös innostus ja mielenkiinto tutkittavaan aiheeseen.

Lähteet

Painetut

Bergman, T., Kuusi, O. & Salminen, H. 2013. Miten tutkimme tulevaisuuksia? 3. painos. Helsinki: Tulevaisuuden tutkimuksen seura.

Bonnet, D., McAfee, A. & Westerman, G. 2014. Leading digital: turning technology into business transformation. Boston: Harvard Business Review Press.

Dameri, R. & Rosenthal-Sabroux, C. 2014. Smart city: how to create public and economic value with high technology in urban space. New York: Springer.

De Kare-Silver, M. 2011. e-shock 2020: how the digital technology revolution is changing business and all our lives. Basingstoke: Macmillan.

Frankenberg, K., Gassmaan, O. & Csik, M. 2014 The business model navigator: 55 models that will revolutionise your business. Harlow: Pearson.

Huoltovarmuuskeskus. 2018. Huoltovarmuuden skenaariot 2030. Helsinki: Huoltovarmuuskeskus.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15., uudistettu painos. Helsinki: Tammi.

Kananen, J. 2012. Kehittämistutkimus opinnäytetyönä: kehittämistutkimuksen kirjoittamisen käytännön opas. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, J. 2008. Kvali: kvalitatiivisen tutkimuksen teoria ja käytänteet. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kupi, E., Kortelainen, H., Lanne, M., Palomäki, K., Murtonen, M., Toivonen, S., Heikkilä, A., Uusitalo, T., Wuoristo, T., Rajala, A. & Multanen, A. 2010. Turvallisuusalan liiketoiminnan kasvualueet ja mahdollisuudet Suomessa. Espoo: VTT.

Lahtinen, T. 2016. Uudet toimintamallit luovat kasvua. Turvallisuus & Riskienhallinta, 24 – 25, 6/2016.

Linz, C., Müller-Stewens, G. & Zimmermann, A. 2017. Radical business model transformation: gaining the competitive edge in disruptive world. London: Kogan Page Limited.

Meristö, T. 1991. Skenaariotyöskentely yrityksen johtamisessa. Helsinki: Tulevaisuuden tutkimuksen seura.

Moilanen, T., Ojasalo, K. & Ritalahti, J. 2009. Kehittämistyön menetelmät: uudenlaista osaamista liiketoimintaan. Helsinki: WSOYpro.

Rodriguerz-Bolivan, M. 2015. Transforming city governments for successful smart cities. New York: Springer.

Ross, A. 2016. The industries of the the future. Lontoo: Simon & Schuster.
Singh, S. 2012. New mega trends: implications for our future lives. Basingstoke: Palgrave Macmillan.

Stimmel, C. 2015. Building smart cities: analytics, ICT, and design thinking. Boca Raton: Taylor & Francis, CRC Press.

Wilenius, M. 2015. Tulevaisuuskirja: metodi seuraavan aikakauden ymmärtämiseen. 2. painos. Helsinki: Otava.

Sähköiset

Andersson, C., Kärki, T., Linturi, R., Limnel, J., Lähteenmäki, I., Rousku, K & Strenfors. S. 2017. Pilkahduksia tulevaisuuteen – digitalisaation ja robotisaation mahdollisuudet. Viitattu 6.5.2017. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79260/Pilkahduksia_tulevaisuuteen.pdf?sequence=1

Frey, B. & Osborne, M. 2013. The future of employment: how susceptible are jobs to computerization? Viitattu 24.11.2018. https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf

Kari, M. 2017. Tarkastelu sisäministeriön ja poliisin resurssien ja poliisitoimen palvelujen laadun tasosta ja kehityksestä. Helsinki: Palkansaajien tutkimuslaitos. Viitattu 17.12.2018. http://www.labour.fi/tutkimusjulkaisut/raportteja/raportteja-35/

Laitinen, J., Manninen, A. & Meristö, T. 2014. Tulevaisuus turvassa! Tulevaisuuden muutosvoimat ja niiden vaikutus turvallisuusalaan ja sen osaamistarpeisiin. Viitattu 25.11.2018 http://www.theseus.fi/bitstream/handle/10024/114765/Laurea%20julkaisut%2023.pdf?sequence=1&isAllowed=y

Nurmi, T. 2004. Tulevaisuudentutkimus tiedonalana. TOPI – Tulevaisuudentutkimuksen oppimateriaalit. Viitattu 10.10.2018. https://tulevaisuus.fi/menetelmat/skenaariotyoskentelynsovelluksia/osallistavat-menetelmat/tulevaisuuspyora-verstastyoskentelyssa/

Majavesi, M. 2010. Ennakointimenetelmiä. Viitattu 5.10.2018. http://www.pilkahdus.fi/sites/default/files/51_ennakointimenetelmia.pdf

Palvelualojen työnantajat PALTA ry. 2016. Digitalisaatio palvelualoissa – Pysyykö Suomi mukana digikehityksessä? Viitattu 22.7.2018. https://www.palta.fi/wp-content/uploads/2016/11/Digitalisaatio-palvelualoilla-Pysyyk%C3%B6-Suomi-mukana-digikehityksess%C3%A4_FINAL.pdf

Poliisi. 2018. Yksityinen turvallisuusala ja lupaviranomaiset. Viitattu 25.4.2018. https://www.poliisi.fi/luvat/yksityinen_turvallisuusala

Salmi, T. 2014. Robotiikka – monien mahdollisuuksien tekniikkaa. Viitattu 25.11.2018. https://www.vtt.fi/Impulssi/Pages/Robotiikka-%E2%80%93-monien-mahdollisuuksien-tekniikkaa.aspx

Sanastokeskus TSK Ry. 2017. Tietotekniikan termitalkoot. Viitattu 25.11.2018. http://www.tsk.fi/tsk/termitalkoot/fi/node/266

Smith, R. 2006. Peer review: a flawed process at the hearth of science and journals. Viitattu 1.12.2018. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1420798/

Suomen Automaatioseura Ry. 2013. Automaation määritelmä. Viitattu 25.4.2018. http://www.automaatioseura.fi/component/content/article/5

Suomen virallinen tilasto (SVT). 2014. Digitalisaatio yritysten liiketoiminnassa 2012–2014. Helsinki: Tilastokeskus. Viitattu: 25.11.2018. http://www.stat.fi/til/inn/2014/inn_2014_2016-06-02_kat_007_fi.html

Valtioneuvosto. 2017. Digitalisaatio, kokeilut ja normien purkaminen. Viitattu 10.4.2018. http://valtioneuvosto.fi/hallitusohjelman-toteutus/digitalisaatio

Kuviot

Taulukot

Liitteet

Liite 1: Delfoi-menetelmän haastattelukysymykset, ensimmäinen kierros

Mitkä ovat mielestäsi ne teemat, jotka ajavat yksityisen turvallisuusalan kasvua

a.) nyt
b.) tulevaisuudessa

Yksityisen turvallisuusalan liikevaihto, sekä työntekijöiden määrä ovat kasvaneet tasaisen vahvasti vuosien ajan. Miten koet digitalisaation vaikuttavan tähän tulevaisuudessa?

Miten näet digitalisaation vaikuttavan vartijoitten ja järjestyksenvalvojien työnkuvaan tulevaisuudessa?

Miten visioit digitalisaation muuttavan omaa työnkuvaasi tulevaisuudessa?

Näetkö digitalisaation kehityksen tuovan huomattavia uhkia yksityisille turvallisuusalan yrityksille?

Vapaa kommentti aiheesta

Liite 2: Delfoi-menetelmän haastattelukysymykset, toinen kierros

Mitkä teemat uskot olevan tärkeitä vuonna 2025 yksityisen turvallisuusalan näkökulmasta?

Peilaten nykyhetkeä vuoteen 2025, miten uskot liikevaihdon, sekä työntekijöiden määrän kehittyvän.

Missä näet itsesi ammatillisesti olevan vuonna 2025?

Kuvaile vuoden 2025 vartijoiden ja järjestyksenvalvojien työnkuvaa.

Mitkä uskot olevan vuonna 2025 huomattavimmat uhat ja haasteet yksityisylle turvallisuusalalle?

Visioi vuonna 2025 järjestettäviä turvallisuusalan koulutuksia.