Sari Valkama

KYBERRIKOKSISTA ILMOITTAMINEN POLIISILLE - KAUPUNKIEN JA POLIISIN VÄLINEN YHTEISTYÖ

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Valkama, Sari
Kyberrikoksista ilmoittaminen poliisille – Kaupunkien ja poliisin välinen yhteistyö
Jyväskylä: Jyväskylän yliopisto, 2019, 70 s.
Tietojenkäsittelytiede, pro gradu -tutkielma
Ohjaaja: Lehto, Martti

Kyberrikollisuus on yksi tämän päivän suurimpia ongelmia. Kyberrikollisuus on termi, joka määritellään eri tavoilla eri yhteyksissä, mutta sitä voidaan käyttää kuvaamaan laajasti erilaisia rikoksia, joissa käytetään tietoverkkoja hyödyksi suoraan tai epäsuorasti tai tietoverkot ovat suoria tai epäsuoria kohteita. Kyberrikokset saavat jatkuvasti uusia muotoja, mikä vaikeuttaa niiden tunnistamista ja niihin varautumista. Poliisi pitää Suomessa yllä kyberrikollisuuden tilannekuvaa ja sen ylläpitämisen kannalta olisi olennaista, että kyberrikoksista ilmoitettaisiin poliisille. Tällä hetkellä kuitenkin monet rikokset jäävät ilmoittamatta, mutta miksi? Sitä ei ole vielä oikeastaan tutkittu ja siitä lähdettiin tätä tukimusta tekemään. Tutkimusongelma voitiin tiivistää kysymykseen: Miksi kaikista kyberrikoksista ei ilmoiteta poliisille? Tutkimusmenetelmäksi valittiin tapaustutkimus ja tiedot kerättiin puolistrukturoiduin haastatteluin. Tutkimukseen saatiin mukaan yhdeksän kaupunkia eri puolilta Suomea. Haastatteluista löytyneet syyt voidaan tiivistää kahdeksi isommaksi kokonaisuudeksi. Kyberrikoksista ilmoittamisesta koetaan olevan enemmän haittaa kuin hyötyä ja kaikista kaupungeissa havaituista tapahtumista ei tule tietoa ilmoituksen tekemisestä päättäville tahoille asti. Haastatteluissa kerättiin myös käytännön kehitysehdotuksia poliisille. Tulosten mukaan laadittiin lista toimenpiteistä, joilla voisi olla mahdollista lisätä kyberrikosilmoitusten määrää.

Asiasanat: kyberrikos, kyberturvallisuus, rikosilmoitus, kunnat, poliisi

ABSTRACT

Valkama, Sari
Making a Report of an Offence to the Police - Municipalities and the Police Working Together
Jyväskylä: University of Jyväskylä, 2018, 70 pp.
Computer Science, Master's Thesis
Supervisor: Lehto, Martti

Cybercrime is one of the most common crime types nowadays and one that can potentially cause a lot of harm to both organizations and citizens. Cybercrime is tricky to define as the meaning can change depending on who's giving the definition. One of the many problems with cybercrime is that the cyber security scene is changing constantly with new types of threats and risks appearing almost daily. This is one of the reasons that make cybercrime difficult to counter. The police in Finland are maintaining a cybercrime related situational awareness so that it has capabilities to inform and warn organizations and citizens alike when needed. Therefore, the police want to get information about every cybercrime incident that is encountered. Unfortunately, the police are aware that only a fraction of cybercrimes are reported. There is an interest to know why and this is what this study aimed to do. The study problem can be summarized with one question: Why some of the cybercrimes are not reported to the Police? The study was conducted as a multi-case case study and the material was collected using semi-structural interviews. There were nine cities all around Finland that participated in this study. Reasons collected from the study can be combined in to two main reasons for not making reports of an offence to the police. Making a report is seen to cause more harm than good in several ways and decision-making people in the city organizations don't necessarily receive information about all the incidents detected in their organization. Interviewees were also asked if they had any suggestions to the police about how to make cybercrime reporting and handling easier. A list of possibly beneficial actions that aim at increasing amounts of reported cybercrime was formed according to the results.

Keywords: cybercrime, cyber security, report of an offence, municipalities, police

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Kyberrikollisuus on yksi tämän päivän uhista, jonka eri muodot koskettavat tavalla tai toisella lähes kaikkia ihmisiä, ellei yksityiselämässä niin ainakin työn puolella. Europolin (2018) IOCTA raportissa listatuista kyberrikollisuuden trendeistä kuten kiristyshaittaohjelmista (engl. ransomware), palvelunestohyökkäyksistä, skimmauslaitteista (engl. skimming device) ja käyttäjän manipulointi yrityksistä sähköpostitse on puhuttu julkisuudessa. Raportissa ennustetaan myös, että seuraavan viiden vuoden aikana kyberuhkien havaitsemisesta tulee aikaisempaa vaikeampaa (Europol, 2018). Internettiä hyödyntävät rikokset ovat kannattavampia kuin monet perinteisen rikollisuuden muodot (Europol, 2016) ja todennäköisyys joutua kyberrikoksen uhriksi on suurempi kuin perinteisen rikoksen uhriksi joutuminen (UNODC, 2013). Viestintäviraston (2018) julkaisemassa raportissa todettiin, että kohdistettujen, vakavampien, kyberhyökkäysten kohteina olivat Suomessa yleensä julkisen sektorin organisaatiot. Vaikka vakavia vahinkoja aiheuttavia kampanjoita on ollut liikkeellä, niin poliisille ilmoitettujen kyberrikosten määrä on pysynyt suurin piirtein samanlaisena kolmen viime vuoden aikana (Poliisin tilastotietojärjestelmä, 2018).

Kyberrikollisuus on käsite, jolla tarkoitetaan eri asioita riippuen määrittelijästä (UNODC, 2013). Kyberrikollisuus voi olla synonyymi tietoverkkorikoksille tai tietoverkkorikollisuus voidaan nähdä yhtenä kyberrikollisuuden muodoista (Sabillon ym., 2016). Kyberrikollisuus ei ole siis terminä kovinkaan yksinkertainen, eikä välttämättä yleisesti käytetty, kuten tuli ilmi tämän tutkimuksen aikana.

Sabillon ym. (2016) määrittelevät kyberrikollisuuden laajasti. Heidän mukaansa kyberrikoksella tarkoitetaan rikoksia, joiden toteutuksessa käytetään tai sen kohteena on tietotekninen laite sekä rikoksia, joissa toissijaisena kohteena tai toteutuksen apuvälineenä toimii tietotekniset laitteet (Sabillon ym., 2016). Kyberrikoksen kohteina voivat olla tieto (UNODC, 2013), tietoverkot tai järjestelmät (EU komissio, 2007). Esimerkkejä kyberrikoksista ovat tietomurrot, palvelunestohyökkäykset ja identiteettivarkaudet (Lehto ym., 2017).

Organisaatiot hallitsevat kyberuhkia erilaisin kyberturvallisuuden hallinnan keinoin. Kyberturvallisuuden hallinta on monimutkaista ja sitä on tutkittu

paljon akateemisissa tutkimuksissa. Kyberturvallisuuden ongelmallisemmiksi osoittautuneita osa-alueita ovat mm. kyberulottuvuuden nopeat muutokset (Lehto ym., 2017), riskien arviointi (Baskerville, 1991) kybertilannetietoisuuden onnistunut levittäminen organisaatioihin (Korpela, 2015) ja organisaatioiden työntekijöiden piittaamattomuus laadituista kyberturvallisuuden säännöistä (Moody, 2018).

Näiden tutkimusten ja niistä löydettyjen ongelmien kautta on muodostunut useita malleja ja standardeja kyberturvallisuuden hallintaan. Monet näistä malleista perustuvat jollakin lailla sykliseen ajatteluun, jossa ensiksi suunnitellaan, toteutetaan, tarkkaillaan ja sitten aloitetaan taas alusta. Tällaisia malleja ovat mm. Raggadin (2010) malli, NIST -kyberturvallisuuden hallintamalli (Huergo, 2018) sekä ISO 27001 standardin malli (Susanto, Almunawar ja Tuan, 2011).

NIST-kyberturvallisuuden hallintamallin keskiössä on viisi aktiviteettia, jotka kulkevat loputtomassa syklissä: Opi **tuntemaan** oma organisaatio, mitkä ovat sen kriittiset kohdat ja mitä riskejä on olemassa. Etsi keinot **suojella** organisaation kriittisimpiä toimintoja. Etsi tapoja, joilla voidaan **havainnoida** ja tunnistaa poikkeustilanteet. Etsi keinot, joilla voidaan **vastata** poikkeustilanteisiin. Laadi **palautumisen** vaiheen suunnitelmat, jotta organisaatiossa osataan toimia poikkeustilanteissa. (NIST, 2018; Huergo, 2018)

Organisaatiotason kybertilannetilannetietoisuuden ylläpito voidaan nähdä yhtenä välineenä NIST-kyberturvallisuuden hallintamallin tunnistamisen ja havainnoinnin vaiheissa. Kybertilannetietoisuuden tarkoituksena on havaita kyberympäristöön liittyviä ilmiöitä, ymmärtää niitä ja kehittää sen pohjalta ennusteita. (Franke, Brynielson, 2014; Tianfield, 2016) Valtakunnallinen tilannetietoisuuden ylläpito on myös osa Suomen kyberturvallisuusstrategiaa (Turvallisuuskomitea, 2013).

Erilaisilla poikkeustilanteiden palautumisen suunnitelmilla, kuten kriiseistä palautumisen ja toiminnan jatkuvuuden takaavilla suunnitelmilla voidaan nopeuttaa poikkeustilanteista palautumista ja vähentää niistä aiheutuvia vahinkoja (Botha ja Solms, 2004; Cerullo ja Cerullo, 2004; Raggad, 2010).

Poliisi on huomannut käytännön työssään, että kaikista organisaatioissa havistuista kyberrikoksista ei ilmoiteta eteenpäin (Piiroinen, 2018). Olisi kuitenkin tärkeää, että poliisi saisi näistä tiedot. Lehto ym. (2017) ovat tutkimuksessaan maininneet, että mahdollisimman monen kyberrikoksen ilmoittaminen viranomaisille, kuten poliisille, edesauttaa häiriötilanteiden hallintaa, selvittämistä ja analysointia sekä mahdollistaa paremman varautumisen niihin. KRP:n Timo Piiroinen (2019) toi esille myös sen, että mitä enemmän ilmoituksia tulee, sitä enemmän kerääntyy tietoja, joita voidaan käyttää hyväksi rikollisten löytämisessä. Näiden pohjalta kyberrikoksien ilmoittamista poliisille lähdettiin tutkimaan.

Tutkimusongelma muotoiltiin kysymykseksi: Miksi kaikista kyberrikoksista ei ilmoiteta poliisille? Tätä tutkimuskysymystä tuettiin neljällä alakysymyksellä: Miksi kyberrikoksista ilmoitetaan tai jätetään ilmoittamatta? Onko kaupungeilla olemassa olevaa suunnitelmaa kyberrikosten varalle? Onko

kaupunkien työntekijöillä tarpeeksi tietoa kyberrikoksista? Mitä poliisi voisi tehdä ilmoittamiskynnyksen madaltamiseksi? Näihin kaikkiin kysymyksiin pyrittiin löytämään vastaus.

Tutkimus rajattiin koskemaan julkisia organisaatioita ja niistä vielä isoja kaupunkeja Suomessa, jotta saataisiin isompi otanta samankaltaisia organisaatioita. Tutkimukseen saatiin yhdeksän kaupunkia eri puolilta Suomea.

Tutkimusmenetelmäksi valittiin tapaustutkimus, jossa yksi kaupunki ja sen kyberrikoksien ilmoittamisen prosessi muodostivat yhden tapauksen. Tiedonkeruu tehtiin puolistrukturoiduin haastatteluin, jotka toteutettiin sähköposti- ja puhelinhaastatteluina sekä niiden yhdistelmänä. Kaikki haastateltavat saivat määritellyt haastattelukysymykset aluksi sähköpostitse.

Litteroidut haastattelut tiivistettiin ja koodattiin, minkä jälkeen tapauksia verrattiin keskenään, jotta löydettiin yhteneväisyyksiä, eroja ja säännöllisyyksiä. Tuloksia lähdettiin analysoimaan näiden pohjalta.

Tutkimuksen tuloksista voidaan löytää kaksi isoa syytä sille, miksi kyberrikoksia jätetään ilmoittamatta. Ensimmäinen on se, että ilmoittamisesta koetaan olevan enemmän haittaa kuin hyötyä. Toisena oli, että kaupunkien johdossa olevat henkilöt eivät kuule kaikista organisaatiossa kohdatuista tapauksista. Näiden yläotsikoiden alle mahtui useampia syitä. Kyberrikoksista ilmoittamisen ongelmiksi koettiin poliisin pitkät vasteajat tehtyihin ilmoituksiin, haluttomuus kuormittaa poliisien tunnetusti rajallisia resursseja liian pieniksi tai liian suuriksi arvioiduilla tapauksilla ja ilmoittamisen vaivaan verrattuna liian pieneksi koettu hyöty kaupungille itselleen. Haastatelluista osa olivat huomanneet myös, että heille ei aina tule tietoa kaikista organisaatiossa havaituista tapauksista, koska vakavampia tapauksia ei tunnisteta, vaan ne usein poistetaan joko työntekijän itsensä tai IT-lähituen toimesta ja unohdetaan.

Tutkimuksessa kerättiin myös kehitysehdotuksia, joilla kaupunkien ja poliisin välistä yhteistyötä olisi mahdollista parantaa. Kehitysehdotuksissa nousi esiin kolme teemaa: poliisin vasteaikojen parantaminen, aikaisempaa laajempi ja syvällisempi kommunikaatio kaupunkien ja poliisin välillä sekä poliisin osallistuminen yleisen kybertietoisuuden levittämiseen.

Tutkimuksen tulosten ja kehitysehdotusten pohjalta valmistettiin lista toimenpiteistä, joilla poliisi voisi vaikuttaa kyberrikoksista tehtävien ilmoitusten määrään ja vastata tutkimusongelmaan. Tutkimuksen tuloksia voidaan käyttää hyödyksi myös lisätutkimuksia suunniteltaessa.

Tämä tutkimusraportti on jaettu seitsemään osaan johdanto mukaan lukien. Seuraavaksi käydään läpi tutkimuksen kannalta olennaista taustaa ja teoriaa. Kolmannessa luvussa käsitellään tutkimusmenetelmien ja työkalujen teoriapohjaa. Siinä käydään läpi myös menetelmien tunnettuja vahvuuksia ja heikkouksia. Neljännessä luvussa laaditaan tutkimusasetelma eli esitellään tutkimusongelma ja tutkimuksen toteutustavat. Viidennessä luvussa esitellään tutkimuksen tulokset. Kuudennessa luvussa esitetään tulosten pohjalta tehdyt analyysit. Luvussa seitsemän löytyy yhteenveto tutkimuksesta.

2 TAUSTA

Tässä luvussa esitellään tutkimuksen kannalta tärkeitä määritelmiä ja olennaisten ilmiöiden taustaa, nykytilaa ja tutkimusta. Tausta-aineistoa on etsitty erilaisten akateemisten artikkeleiden internethauista kuten Google Scholarista. Vaikka suurin osa tausta-aineistosta on e-artikkeleita ja muita internet julkaisuja, on mukana perinteistä kirjallisuuttakin. Näiden lisäksi haastateltiin taustaa varten Keskusrikospoliisin kyberrikostorjuntakeskuksen päällikköä Timo Piiroista.

Ensimmäisenä tässä osiossa käsitellään kyberrikoksen määritelmää ja esitellään ilmiötä. Sen jälkeen esitetään organisaatioiden kyberturvallisuuden hallintaa keskittyen toiminnan jatkuvuuden hallintaan, kyberrikoksista palautumiseen ja johtamiseen, mutta myös lyhyesti yleisestä prosessista. Tämän jälkeen esitellään kyberturvallisuuden hallintaan tarkoitettu NIST-malli lyhyesti. Sen lisäksi esitellään ja määritellään tilannetietoisuus sekä yleisesti että kyberturvallisuuden kontekstissa. Viimeiseksi kerrataan lyhyesti, miten nämä liittyvät toteutettavaan tutkimukseen.

2.1 Kyberrikollisuus

2.1.1 Määritelmiä

Kyberrikollisuus voidaan määritellä eri tavoin riippuen kontekstista ja käyttötarkoituksesta (UNODC, 2013). Yleisesti voidaan kuitenkin sanoa, että kyberrikollisuuden määritelmän täyttääkseen rikos joko toteutetaan käyttäen hyväksi tietoteknisiä laitteita, rikoksen kohteena voi olla tietotekninen laite tai tietotekniset laitteet voivat olla toissijaisia apuvälineitä tai kohteita. Kyberrikoksiksi voidaankin määritellä hyvin erilaisia rikoksia. (Sabillon ym., 2016) Kyberrikoksina voidaan nähdä tietojärjestelmiin kohdistuvat toimet, joilla pyritään vaikuttamaan järjestelmän ja sen tietojen luottamuksellisuuteen, saatavuuteen tai muuttumattomuuteen, mutta niihin voidaan lukea myös mm. identiteettivarkaudet, mak-

suvälinepetokset jne., joilla päästään käsiksi arkaluonteisiin tietoihin. (UNODC, 2013)

Suomalaisessa kirjallisuudessa käytetään ajoittain tietoverkkorikollisuus termiä kyberrikollisuuden synonyyminä (Nevalainen, 2018). Esimerkiksi Euroopan komission tiedonannossa tavoitteesta luoda yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi (EU komissio, 2007) tietoverkkorikoksiksi kutsutaan

> --rikoksia, jotka tehdään sähköisiä viestintäverkkoja ja tietojärjestelmiä hyödyntäen tai jotka kohdistuvat mainittuihin verkkoihin ja järjestelmiin. (KOM/2007/267/lopull.,2007, s.2)

Tämä määritelmä muistuttaa hyvin paljon aikaisemmin esitettyä YK:n kyberrikoksia (UNODC, 2013) koskevassa tutkimuksessa määriteltyä kyberrikos-termiä. Euroopan komission tiedonannossa tietoverkkorikokset jaetaan kolmeen alaryhmään. Nämä alaryhmät ovat perinteiset rikokset, joiden toteuttamisessa hyödynnetään sähköisiä viestintäverkkoja, laittoman sisällön julkaisemiseen sähköisessä verkossa ja pelkästään sähköisessä verkossa tapahtuvat rikokset. (EU komissio, 2007)

Vaikka osassa julkaisua kyber- ja tietoverkkorikollisuutta kohdellaan synonyymeinä, niin toisaalla tietoverkkorikollisuus nähdään yhtenä kyberrikollisuuden muodoista. Tietoverkkorikoksiin voidaan silloin luetella mm. tietomurrot, palvelunestohyökkäykset, laittomat tietosisällöt ja identiteettivarkaudet. (Lehto ym., 2017)

Kyberrikollisuus ei ole laaja-alaista ja monimutkaista pelkästään siksi, että termiä käytetään hyvin erilaisten rikosten yhteydessä ja siksi, että sillä voidaan tarkoittaa eri yhteydessä eri asioita, vaan myös siinä, että siihen syyllistyy hyvin erilaisia toimijoita erilaisin motiivein. (Sabillon ym., 2016) Erilaisten hakkerien lisäksi kyberrikollisuuteen syyllistyvät terroristit sekä valtiolliset tai valtioiden rahoittamat toimijat (UNDOC, 2013) sekä organisaation sisäiset toimijat kuten työntekijät (Keyser, 2017). Esimerkkinä valtiollisesta toiminnasta voidaan pitää tiedustelutoimintaa (Lehto ym., 2017).

Motiivit kyberrikoksien takana voivat olla moninaiset. Tavoitteena voi olla esimerkiksi hauskanpito, maineen luominen, oman asiansa ajaminen tai taloudellisten hyötyjen tavoittelu. (Sabillon ym., 2016)

Kyberrikoksien parissa toimivien kirjo on laaja mm. sen takia, että kyberrikoksien toteuttamiseen ei välttämättä tarvita paljoa tietoteknisiä taitoja (UNDOC, 2013). YK:n (UNDOC, 2013) raportin mukaan kuitenkin 80% kyberrikoksista on ainakin osittain organisoituneiden rikollisten tuotosta ja suurimman rikollisten ryhmän muodostaa alle 25-vuotiaat miehet. Vaikka kyberrikoksiin ei välttämättä tarvita suuria resurssimääriä ja taitoja, on olemassa toisenlaisiakin ryhmiä (UNDOC, 2013; Lehto ym., 2018). APT- hyökkäykset (engl. Advanced Persistent Threath) ovat kehittyneimpiä kyberrikoksen muotoja. Nämä liitetään usein valtiollisiin toimijoihin tai isoihin rikollisryhmiin niiden toteuttamiseen vaadittavien resurssimäärien takia. (Lehto ym., 2018)

2.1.2 Lainsäädäntö

Vaikka kyberrikollisuuden päälinjoista onkin YK:n (UNODC, 2013) raportin mukaan yhteneväinen näkemys, eroaa eri valtioiden lait kyberrikollisuuden yksityiskohdissa toisistaan. Kaikki valtiot eivät luokittele samoja ilmiöitä kyberrikoksiksi (UNODC, 2013).

Euroopan Unioni on yksi niistä alueista, jotka ovat viime vuosina keskittyneet kyberrikollisuuteen liittyvän lainsäädännön uudistamiseen ja kehittämiseen. (UNODC, 2013) Hyviä esimerkkejä tästä ovat Euroopan Unionin tietosuoja-asetus (2016) GDPR (engl. General Data Protection Regulation), joka keskittyy henkilötietojen suojaamiseen sekä NIS-direktiivi (engl. Network and Information Security directive), joka keskittyy tietoverkkojen suojaamiseen. (Viestintävirasto, 2018)

Euroopan Unioni tunnisti tietoverkkorikokset uhkaksi vuonna 2001 laaditussa Euroopan neuvoston tietoverkkorikollisuutta koskevassa yleissopimuksessaan (Euroopan neuvosto, 2001; Euroopan neuvosto, 2007). Vuonna 2007 annettiin Euroopan komission tiedonanto (EU komissio, 2007), joka määritteli EU:n tavoittelevan yleistä toimintalinjaa tietoverkkorikollisuuden torjumiseksi. Tietoverkkorikollisuuden yleissopimuksessa määritellään tietoverkkorikollisuudeksi laskettavat rikokset ja kansainvälisen yhteistyön periaatteet (Euroopan neuvosto, 2001; Euroopan neuvosto, 2007).

Euroopan unioniin kuuluvana maana Suomen kyberrikollisuus lainsäädäntöä säätelee suurelta osin nämä Euroopan Unionin linjaukset ja säädökset. Tuoreimpia säädöksiä tähän liittyen on Euroopan Unionin tietosuoja-asetus (GDPR), jonka voimaantulon siirtymäaika loppui toukokuussa 2018.

Kyberrikokset on määritelty suomen rikoslain (19.12.1889) uudemmassa luvussa 38 (21.4.1995/578) tieto- ja viestintä rikoksista ja osa luvussa 36, joka käsittelee petoksia. Suomen rikoslaissa (19.12.1889) rikoksiksi on määritelty:

1. Salassapitovelvollisuuden rikkominen
2. Viestintäsalaisuuden loukkaus tai sen yritys
3. Tietoliikenteen häirintä
4. Tietojärjestelmän häirintä tai sen yritys
5. Tietomurrot
6. Suojauksen purkujärjestelmä rikos
7. Henkilörekisteririkos
8. Identiteettivarkaus

Salassapitovelvollisuuden rikkominen koskee laeissa tai asetuksissa määriteltyjä salassapitovelvollisuuksia. Viestintäsalaisuuden loukkaamisella taas tarkoitetaan mm. tietoverkossa kulkevan salassa pidettävän tai yksityisyyttä loukkaavan tiedon kaappaamista. Suojauksen purkujärjestelmärikoksella tarkoitetaan mm. suojauksen purkamista tai siihen tarvittavien työkalujen mainostamista, vuokraamista, levittämistä, myyntiä, maahantuontia, asentamista tai huoltoa

sellaisissa tapauksissa, joissa suojatun palvelun tai järjestelmän omistajalle koituu haittaa. (Rikoslaki, 19.12.1889)

Prosessin näkökulmasta katsottuna havaitusta tietomurrosta tai muista poikkeuksista alkaa tutkinta sen jälkeen, kun siitä on tehty rikosilmoitus tai tutkintapyyntö poliisille, sillä kyberrikokset ovat pääasiassa asianomistajarikoksia. (Piiroinen, 2019)

2.1.3 Historiaa

Termiä kyberrikollisuus käytti ensimmäisen kerran Sussman ja Heuston vuonna 1995, mutta kyberrikoksia on tehty jo ennen sitä. Ensimmäiset vakavat kyberrikostapaukset ovat 1980-luvulta ja ensimmäinen kyberrikoksiin liittynyt tuomio annettiin vuonna 1989. (Sabillon ym., 2016)

Kyberrikokset tulivat mukaan lainsäädäntöön ensimmäisen kerran vuonna 1973 Ruotsissa. Vain muutama vuosi tämän jälkeen, vuonna 1977, luotiin USA:ssa nykyaikaisen kyberrikollisuutta koskevan lainsäädännön pohja. (Sabillon ym., 2016)

Kyberrikollisuutta ei voida siis pitää uutena ilmiönä. Teknologian kehitys, internet, digitalisaatio ja teknologiakäyttäjien lukumäärän kasvu ovat vain tuoneet uusia tapoja kyberrikosten toteuttamiseen ja tehnyt siitä helpompaa ja tuottavampaa kuin aikaisemmin.

2.1.4 Nykytilanne

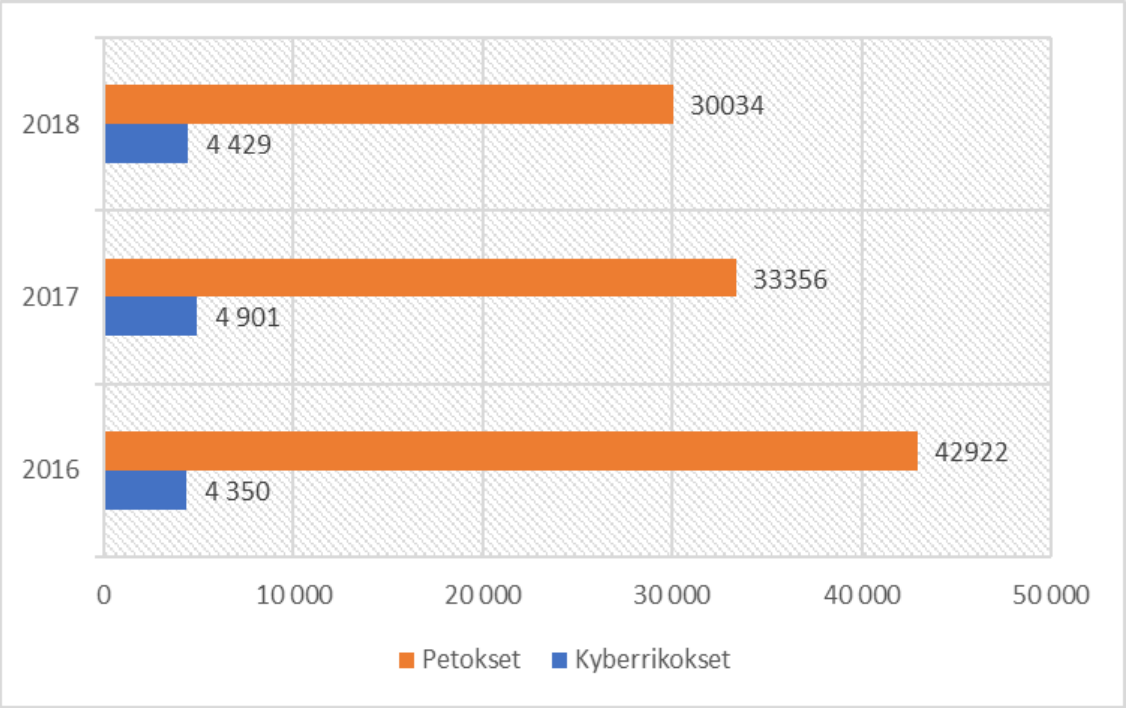
Nykyään kyberrikollisuus voidaan nähdä kannattavampana rikollisten näkökulmasta kuin perinteinen rikollisuus. Tämä näkyykin siinä, että ICT- laitteita ja internettiä hyödyntävien rikosten määrä näytti ylittävän perinteisten rikosten määrän ainakin Isossa Britanniassa jo vuonna 2016 (Europol, 2016) Kuitenkin, jo vuonna 2013 julkaistussa tutkimuksessa on todettu, että todennäköisyys joutua kyberrikosten kohteeksi on suurempi kuin perinteisten rikosten uhriksi joutuminen. (UNODC, 2013)

Viimeisimmän Europolin (2018) IOCTA raportin mukaan tämän hetken kyberrikosten trendejä ovat kiristyshaittaohjelmat, lapsipornografia eri muodoissaan, palvelunestohyökkäykset, skimmauslaitteet, maksukorttien verkkokäyttöhuijaukset (engl. card-not-present fraud), kryptovaluuttaan liittyvät rikokset, käyttäjän manipulointi (engl. social engineering) ja pimeän internetin toiminta. Uutena trendinä raportissa mainitaan ICT laitteiden laskentatehojen kaappaus kryptovaluuttojen louhintaa varten. Raportin kirjoittajat olettavat kryptovaluuttojen louhinnan yleistyvän tulevaisuudessa ja antavan kyberrikollisille tasaisen tulonlähteen, jossa kiinnijäämisen riski on vähäinen. Kaikkein yleisin kyberrikollisuuden muoto on tällä hetkellä kuitenkin kiristyshaittaohjelmat.

Viestintäviraston (2018) julkaisemassa *Tietoturvan vuosi 2017* -raportissa kiristyshaittaohjelmat on nostettu toiseksi merkittävimmäksi uhkaksi organisaatioille. Suomessa tavatut kyberrikokset ovat muutenkin linjassa muualla

maailmassa tavattujen ilmiöiden kanssa. Viestintäviraston raportilla tuodaan esiin käyttäjien manipulointi tietoja kalastelemalla tai käyttäjiä huijaamalla esimerkiksi tilausansoin. Palvelunestohyökkäyksiä oli vuonna 2017 tuhansittain, mutta 74% hyökkäyksistä kesti alle 15 minuuttia ja 97% oli voimakkuudeltaan alle 10 Gbit/s. Raportilla tuodaan myös esiin ns. kohdistetut hyökkäykset, joissa kohteena on tietty organisaatio. Kybervakoilun rinnalle oli tässä tullut hyökkäykset, joiden tarkoituksena on tehdä vahinkoa, kuten esimerkiksi paljon julkisuutta saaneet NotPetya ja Bad Rabbit, jotka näyttävät kiristysohjelmilta, mutta käytännössä niiden käsiin saamia tiedostoja ei pysty palauttamaan. Kohdistettujen hyökkäyksien kohteina olivat raportin mukaan useimmin julkiset tai muuten valtioon kytköksissä olevat organisaatiot ja aikaisempaa enemmän myös huoltovarmuuskriittisiä organisaatioita. (Viestintäviraston, 2018)

Suomessa poliisille ilmoitetut kyberrikokset on jaoteltu poliisin tilastoissa petoksiin ja kyberrikoksiin. Vuoden 2018 ja kahden aikaisemman vuoden kyberrikosilmoitusten määrä esitetään kuviossa 1. (Poliisin tilastotietojärjestelmä, 2018) Kokonaiset taulukot poliisille ilmoitetuista kyberrikoksista löytyvät liitteestä 2.

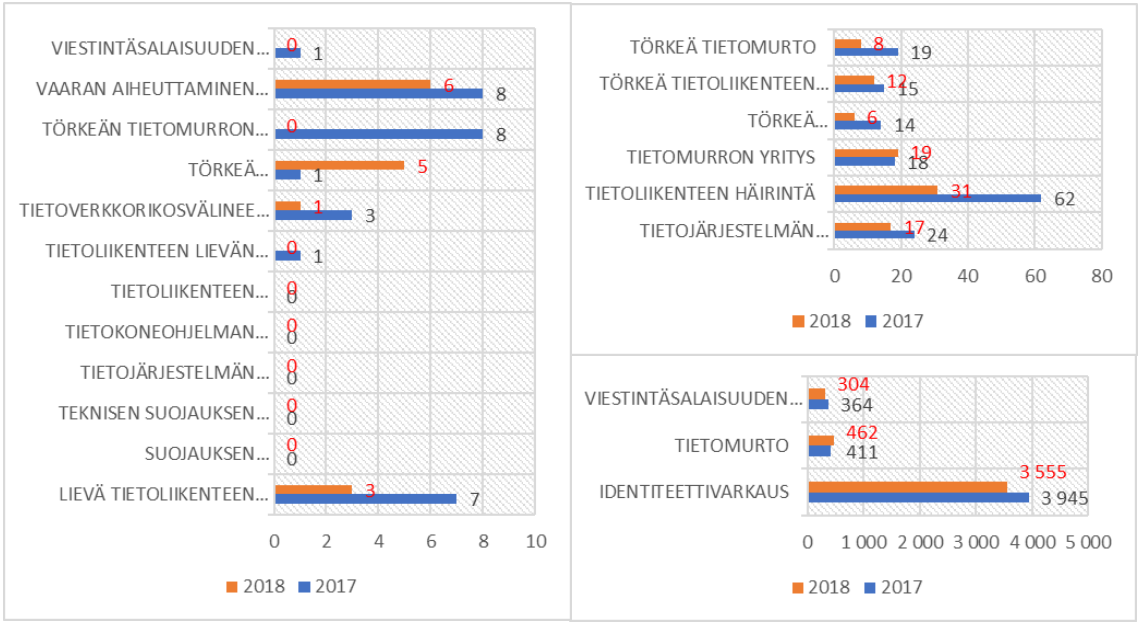


KUVIO 1 Poliisille ilmoitetut kyberrikokset. (Poliisin tilastotietojärjestelmä, 2018, muokattu)

Kyberrikoksiin kuuluvat tässä tilastossa identiteettivarkaudet, tietoliikenteen ja tietojärjestelmän häirinnät, suojauksien purkamiseen tai -kiertämiseen liittyvät rikokset, tietomurrot, tietoverkkorikosvälineiden hallussapito, viestintäsalaisuuteen liittyvät rikokset ja vaaran aiheuttaminen tietojenkäsittelylle (Poliisin tilastotietojärjestelmä, 2018).

Poliisille ilmoitettujen kyberrikosten määrä nousi vuonna 2017 edelliseen vuoteen verrattuna hiukan, mutta vuoden 2018 ilmoitusten määrässä on pientä

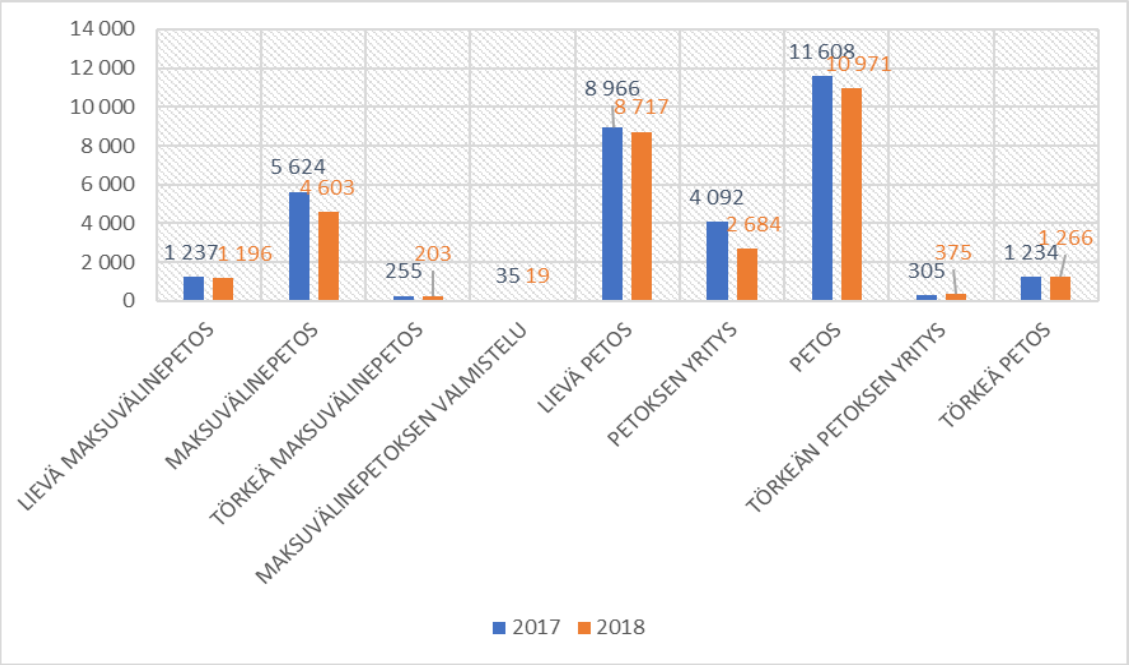
laskua vuodesta 2017. Erot näissä ovat kuitenkin melko pieniä. Selkeästi eniten on ilmoitettu identiteettivarkauksia. Kuviossa 2 on kerätty yhteen kuvaajat, joissa on esitelty tarkemmin vuosina 2017 ja 2018 ilmoitettuja kyberrikoksia. (Poliisin tilastotietojärjestelmä, 2018)



KUVIO 2 Poliisille ilmoitetut kyberrikokset 2017 ja 2018. (Poliisin tilastotietojärjestelmä, 2018, muokattu)

Petoksien listalle kuuluu maksuvälinepetokset, maksuvälinepetoksen valmistelu sekä petokset ja niiden yritykset. Osa näistä rikoksista ei varsinaisesti kuulu kyberrikoksiin. (Piiroinen, 2018)

Maksuvälinepetokset ovat yleisimpiä poliisille ilmoitettuja petosrikoksia. Vuosina 2017 ja 2018 ei ole ollut suurta vaihtelua ilmoitettujen rikosten määrässä. Enemmän eroavaisuutta on vuoteen 2016, jolloin petoksia oli enemmän. Kuviossa 3 on kuvattu vuosina 2017 ja 2018 poliisille ilmoitettuja petoksia. (Poliisin tilastotietojärjestelmä, 2018)



KUVIO 3 Poliisille ilmoitetut petokset 2017 ja 2018. (Poliisin tilastotietojärjestelmä, 2018, muokattu)

Kyberrikoksiin liittyvä tilastointi ei ole ongelmatonta. Yksi ongelma on siinä, että viranomaiset mm. poliisi uskovat, että kyberrikosten sekä kyberrikoksiin kuuluvien petosten määrän olevan sitä suurempi, mitä poliisille ilmoitetut rikokset antavat ymmärtää. (Piiroinen, 2018)

2.2 Kyberturvallisuuden hallinta

Organisaatioiden kyberturvallisuuden hallinta on monimutkainen, jatkuva prosessi, joka koostuu useista erilaisista osista ja vaiheista. Sitä on tutkittu eri näkökulmista useissa tutkimuksissa. Näissä tutkimuksissa on tunnistettu erilaisia ongelmia kyberturvallisuuden hallinnassa ja niissä on esitelty erilaisia malleja näiden ongelmien ratkaisemiseksi. Esimerkiksi Baskerville ja Siponen (2002) sekä Kardya ym. (2004) ovat tutkineet tietoturvapolitiikan luomista sekä sen onnistunutta täytäntöönpanoa. Kyberturvallisuuden hallinnan standardeja ovat tutkineet mm. Siponen ja Willison (2009). He keskittyivät standardien ongelmiin.

Yleisesti määriteltynä kyberturvallisuuden hallinnan tavoitteena on tunnistaa organisaation tietoympäristö, arvioida sen osien kriittisyys, priorisoida kaikkein tärkeimmät toiminnot, tunnistaa siihen kohdistuvat riskit, laatia niiden pohjalta suunnitelmat sekä arvioida ja tarvittaessa päivittää niitä. Näihin päästään erilaisin hallinnollisin, toiminnallisin ja teknisin ohjaimin. (Raggad, 2010)

Tietoturvapolitiikan määrittely ja sen täytäntöönpano ovat sekä Karydan ym. (2004) että Baskervillen ja Siposen (2002) mukaan yleisesti tunnustettu olevan organisaation tietoturvan hallinnan tukipilari, jota hyödynnetään muun kyberturvallisuuden hallinnan suunnittelussa.

Raggad (2010) esittelee kirjassaan GIAC:n (Global Information Assurance Certification) määritelmän tietoturvapolitiikalle. Tämän mukaan tietoturvapolitiikka on kokoelma sääntöjä, joiden tarkoituksena on taata tiedon luottamuksellisuus, saatavuus ja muuttumattomuus. Siinä kuvaillaan toimenpiteet ja määritellään eri henkilöiden vastuut sekä annettaan tarvittava auktoriteetti suunnitelmien toteuttamiselle käytännössä.

Raggad (2010) esittelee kirjassaan myös informaatioturvallisuuden elinkaarimallin (engl. information security life cycle), jossa kuvataan kyberturvallisuuden hallintaa kokonaisuudessaan. Informaatioturvallisuuden elinkaarimallissa kyberturvallisuuden hallinta jaetaan kuuteen vaiheeseen: turvallisuuden suunnitelmaan (engl. security planning), analyysiin, suunnitteluun (security design), täytäntöönpanoon, arviointiin ja jatkuvan turvallisuuden vaiheeseen. Turvallisuuden suunnitelman vaiheessa tunnistetaan organisaatiossa käsiteltävät erilaiset informaatiot sekä laaditaan tietoturvapolitiikka, tietoturvan päämäärät ja sen laajuus. Analyysi -vaiheessa määritellään eri informaatioluokkien turvaamiseen liittyvät vaatimukset. Nämä sisältävät mm. riski-, haavoittuvuus ja olemassa olevien turvatoimien analyysit. Turvallisuuden suunnittelun vaiheessa kehitetään toimia, joilla turvallisuustavoitteet pyritään saavuttamaan. Tämän jälkeen suunnitelma ja toimet päästään ottamaan käyttöön ja niiden vaikutuksia arvioimaan. Jatkuvan suunnittelun vaihe koostuu tarkkailusta, jonka tarkoituksena on pitää huolta siitä, että riskit pysyvät hallinnassa tarpeeksi hyvin. Jos korjattavaa tulee, niin on aloitettava korjaavat toimenpiteet. (Raggad, 2010)

2.2.1 Ongelmat

Kyberturvallisuuden hallinnan tutkimuksissa on tunnistettu useita ongelmallisia kohtia ja osa-alueita kuten kyberulottuvuuden nopeat muutokset, kyberturvallisuustietoisuuden levittäminen ja piittaamattomuus säännöistä. (Lehto ym., 2017; Moodyn ym., 2018; Korpela, 2015)

Lehto ym. (2017) mainitsevat haasteiksi mm. kyberulottuvuuden nopeat muutokset, jossa uusia uhkia syntyy jatkuvasti. Tämä vaikeuttaa mm. riskien arviointia. (Lehto ym., 2017) Riskien arviointi on muutenkin ongelmallista, sillä se perustuu arvioihin uhista, niiden toteutumisen todennäköisyyksistä ja aiheuttamista vahingoista, joita tehdään monimutkaisesta ja vaikeasti selitettävästä ja ennakoitavasta kyberturvallisuusympäristöstä. (Baskerville, 1991).

Kyberturvallisuustietoisuuden levittäminen on tärkeää kyberturvallisuuden kannalta, mutta sen toteuttaminen organisaation henkilökuntaa kouluttamalla on käytännössä hankalaa. Korpela (2015) esittelee epäonnistumisen syiksi mm. vääränlaisen toetutustavan, liian suuret odotukset sekä sen, että kyberturvallisuustietoisuus on ymmärretty kokonaisuudessaan väärin. Epäonnistuneen

koulutuksen seurauksena ja syynä voi esiintyä mm. piittaamattomuutta organisaatioissa laadittuja turvallisuusohjeita kohtaan (Korpela, 2015), mikä vaarantaa organisaation kyberturvallisuuden, sillä varotoimenpiteet toimivat vain, jos sääntöjä noudatetaan ja työkaluja käytetään oikein.

Piittaamattomuus kyberturvallisuussäännöistä on nähty muutenkin ongelmallisena ja siitä on Moodyn ym. (2018) mukaan tutkimuksia, jotka todistavat tottelemattomuuden olevan yleistä. Tätä ongelmaa ratkaisemaan on kehitelty erilaisia malleja, joista Moody ym. (2018) mainitsevat esimerkiksi TRA-teorian (engl. Theory of Reasoned Action), jossa tutkitaan subjektiivisten uskomuksien ja normien vaikutusta käyttäytymiseen sekä PMT-teoria (engl. Protection Motivation Theory), jossa sääntöjen noudattaminen varmistetaan uhkauksilla ja sanktioilla. (Moody ym., 2018)

2.2.2 Standardit ja mallit

Kyberturvallisuuden hallintaan on olemassa standardeja, jotka johdattavat organisaatiot toteuttamaan omia mallejaan, tiettyjä toimenpiteitä ja laatimaan tietynlaisia strategioita sekä dokumentteja. Yksi yleisimmistä standardeista on ISO 27001, joka esittää mallissaan Raggadin kaltaisen syklisen mallin, joka perustuu suunnittele, toteuta, tarkista ja korjaa (engl. Plan-Do-Check-Act) -ajatteluun. Muista standardeista voisi mainita esimerkiksi BS779, joka on vaikuttanut ISO standardeihin sekä maksukorttien tietoturvastandardin PCIDSS. (Susanto, Almunawar ja Tuan, 2011) NIST-mallin (Huergo, 2018) mukainen kyberturvallisuuden hallinta on myös syklinen. Siinä kyberturvallisuuden hallinta jaetaan viiteen jatkuvasti vaihtuvaan vaiheeseen: tunnista, suojele, havainnoi, vastaa ja palaudu. NIST-mallia esitellään tarkemmin myöhemmin. (Huergo, 2018)

Vaikka monet asiantuntijat ja tutkijat pitävät standardeja olennaisen tärkeinä, yleisesti hyväksytyn käytännön mukaisina ja auktoriteetti asemaa kantavina, niin joidenkin asiantuntijoiden mukaan standardien hyödyntäminen kyberturvallisuuden hallinnassa ei ole ongelmatonta. Esimerkiksi Siposen ja Willisonin (2009) kritiikin mukaan standardit eivät mm. huomioi tarpeeksi organisaatioiden yksilöllisiä piirteitä, jotka saavat aikaan kullekin organisaatioille omanlaiset riskit ja sitä kautta omanlaiset suojaustarpeet.

2.2.3 Suomen strategia

Suomen kyberturvallisuuden strategian kokonaisvaltaiset perusteet määriteltiin vuonna 2013 (Turvallisuuskomitea, 2013). Strategiassa määriteltiin valtion sekä yksityisen kyberturvallisuuteen liittyvien organisaatioiden vastuut ja tehtävät, mutta siinä otettiin kantaa myös muiden yksityisten ja julkisten organisaatioiden toimintaan. Tarkemmat tavoitteet ja käytännön toimet määriteltiin toimeenpano-ohjelmissa, joista ensimmäinen hyväksyttiin 2014 ja sitä päivitettiin vuonna 2017 (Turvallisuuskomitea, 2017).

Suomen kyberturvallisuusstrategian visio koostuu kolmesta osasta: Elintärkeät toiminnot on suojattava. Turvallinen kybertoimintaympäristö on taatta-

va niin viranomaisille, kansalaisille kuin yrityksillekin. Suomi tulee olemaan kyberturvallisuuden kärkimaa. (Turvallisuuskomitea, 2013)

Strategian keskeistä sisältöä yksityisen sektorin ja kyberturvallisuuteen suoraan kuulumattomien julkisen sektorin organisaatioiden kannalta oli se, että Suomen kyberturvallisuus perustuu koko yhteiskunnan toimintoihin. Tärkeä osa tässä on kansallinen tilannekuva, jonka ylläpidossa eri organisaatioiden välisellä yhteistyöllä on suuri rooli. (Turvallisuuskomitea, 2013). Muita mainittuja asioita olivat kyberuhkien ja häiriötilanteiden torjunta- ja havainnointi kyvyn sekä kyberosaamisen ja -ymmärryksen parantaminen (Turvallisuuskomitea, 2017). Näiden lisäksi mainittiin kyberturvallisuuden toteuttamiseen tarvittavan lainsäädännön luominen ja kehittäminen (Lehto ym., 2017).

Suomen kyberturvallisuusstrategian tavoitteiden saavuttamista, toteutusta ja ongelmatilanteita on tutkittu ja kartoitettu muutamin tutkimuksin. Lehdon ym. (2017) kyberturvallisuuden nykytilannetta kartoittaneessa tutkimuksessa todettiin, että Suomi on onnistunut tavoitteissaan osittain. Kokonaisuutena kyberturvallisuuden taso on parantunut ja suunnitellut organisaatiot, kuten kyberturvallisuuskeskus on saatu toimintaan. Myös poliisin suorituskyky oli parantunut.

Tutkimuksessa tunnistettiin julkisen organisaatioiden ongelmiksi kybertietoisuuden ja ohjeistuksen toteuttaminen käytännössä sekä resurssien riittämättömyys. Kyberturvallisuuden luonne koko organisaation läpäisevä ja kaikkia organisaation työskentelevien vastuulla olevana asiana, ei ole kaikkialla sisäistetty. Heidän tutkimuksistaan sai myös edelleen sen käsityksen, että osa ei ota asiaa tarpeeksi vakavasti. (Lehto ym., 2017)

Tutkimusten pohjalta yksityisen ja muiden julkisten organisaatioiden kannalta olennaisiksi kehitysehdotuksiksi mainittiin: Tilannekuvan ja siihen liittyvän havainnointikyvyn ja varautumisen laadun parantaminen. Kyberrikoksiin sekä häiriötilanteisiin liittyvän ilmoitusvelvollisuuden ja tiedonjakamisen tehostaminen. Kyberturvallisuuteen liittyvän ymmärryksen syventäminen. (Lehto ym., 2017) Yhdeksi merkittävimmäksi ongelmaksi mainittiin se, että viranomaisten tietoon ei tule kaikki havaitut kyberrikokset tai -loukkaukset (Lehto ym., 2017; Lehto ym., 2018).

2.2.4 Kyberrikollisuuden torjunta Suomessa

Suomen kyberturvallisuusstrategiassa määritellään tavoitteeksi vahva eri julkisten organisaatioiden sekä viranomaisten ja yksityisten sektorin organisaatioiden välinen yhteistyö (Turvallisuuskomitea, 2013). Suomen poliisi toimii jo nyt yhteistyössä mm. Liikenne- ja viestintäministeriössä toimivan Kyberturvallisuuskeskuksen kanssa. (Poliisi, 2018) Silti, Lehdon ym. (2017) tutkimuksessa todetaan, että yhteistyötä voisi edelleenkin tiivistää, varsinkin yksityisen ja julkisen sektorin välillä.

Suomen kyberympäristön hallinta ja erilaiset kyberturvallisuustoimenpiteet on jaettu eri organisaatioiden kesken. Valtioneuvosto johtaa toimintaa. Puolustusministeriön alaisen Turvallisuuskomitean piiriin kuuluu kokonaisturval-

lisuuteen liittyvä ennakointi ja varautuminen. Valtionvarainministeriön vastuulla on hallinnon tietoturvallisuuden kehittäminen sekä yleinen ohjaus. Valtori tuottaa hallinnon ICT-palveluita ja sen TUVE-yksikön vastuulla on erityisvaatimuksien mukaisten palvelujen tuottaminen. Esimerkiksi korkean varautumistasoa vaativille organisaatioille on määritelty erityisvaatimuksia. Viestintäviraston tehtävänä on valvoa annettujen säännösten noudattamista. Huoltovarmuuskeskuksen tehtävänä on huoltovarmuuden ylläpito, kehitys, suunnittelu ja operatiivinen toiminta. Tietosuojavaltuutetun toimiston tehtävänä on valvoa henkilötietojen käsittelyä niin julkisella kuin yksityiselläkin sektorilla. (Lehto ym., 2017)

Suomessa varsinainen kyberrikoksien torjunta on jaettu eri poliisin yksiköille. Suojelupoliisille kuuluu kyberterrorismiin ja vastatiedusteluun liittyvät osa-alueet. (Lehto ym., 2017) Vuonna 2015 perustettu Keskusrikospoliisin kyberrikostorjuntakeskus vastaa mm. tietoverkkorikosten tutkinnasta ja torjunnasta. Lisäksi heidän vastuullaan on tietoverkkorikollisuuden tilannekuvan ylläpito sekä internet- ja verkkotiedustelu. (Poliisi, 2018; Lehto ym., 2017)

Henkilötietoihin liittyvät kyberrikokset ilmoitetaan rikoksesta epäillyn organisaation, eli ns. rekisterinpitäjän, kotimaan tietosuojaviranomaiselle. (EU, 2016) Suomessa tämä tarkoittaa Tietosuojavaltuutetun toimistoa (Talus, Autio, Hänninen ym., 2017). Sen sijaan muista kyberrikoksista voidaan tehdä rikosilmoitus poliisille. Poliisille voi tehdä ilmoituksen internetin kautta, sähköpostitse tai käymällä poliisiasemalla. (Piiroinen, 2018).

2.3 NIST kyberturvallisuuden hallintamallina

Yhdysvaltojen National Institute of Standards and Technology:n eli NIST:n julkaisemassa mallissa kyberturvallisuuden hallinta koostuu kolmesta osasta mallin keskiöstä (engl. framework core), täytäntöönpanon kerroksista ja profiilista

Mallin keskiö jaetaan viiteen keskeiseen aktiviteettiin: tunnista, suojele, havainnoi, vastaa ja palaudu. Nämä aktiviteetit vuorottelevat jatkuvassa syklissä. Mallissa määritellään myös aktiviteetteja ja niiden lopputuloksia tarkemmin. (Huergo, 2018; NIST, 2018)

Tunnista-vaiheessa tarkoituksena on oppia tuntemaan oma organisaatio, jotta juuri omaan organisaation kyberturvallisuuteen liittyviä riskitekijöitä voidaan paremmin arvioida. Tämän vaiheisiin kuuluvat mm. organisaation etujen/arvokkaan tieto-omaisuuden hallinta (engl. asset management), liiketoiminnataympäristön tunnistaminen sekä riskien tunnistaminen ja hallinta. (NIST, 2018)

Suojele-vaiheessa on tarkoitus löytää ja ottaa käyttöön tarvittavat apuvälineet ja prosessit, joilla taataan kriittisten toimintojen jatkuminen. Näihin apuvälineisiin voivat kuulua esim. identiteetin sekä kulku- ja muu lupahallinta, kyberturvallisuuden suojelemiseen tarkoitettujen teknologioiden käyttö sekä kyberturvallisuustietoisuuden parantamiseen tähtäävät koulutukset ja ohjelmat. (NIST, 2018)

Havainnointi-vaiheessa kehitetään ja otetaan käyttöön tapoja, joilla voidaan tunnistaa kyberturvallisuuden poikkeustilanteet (NIST, 2018), kuten kyberrikokset. Havainnointiin kuuluvat kyberturvallisuuteen liittyvien tapahtumien seuranta ja poikkeustilanteiden tunnistamiseen käytetyt prosessit (NIST, 2018).

Vastaa-vaiheessa suunnitellaan ja otetaan käyttöön poikkeustilanteista selviämiseen tarkoitetut prosessit. Tähän prosessivaiheeseen kuuluu poikkeustilanteiden aikaisen viestinnän, analyysin ja vaikutuksia lieventävät, mutta myös toimintaa parantavat toimenpiteet. (NIST, 2018)

Palaudu-vaiheessa keskitytään suunniteltuihin aktiviteetteihin, joiden tavoitteena on palautua tapahtuneesta poikkeustilanteesta ja ylläpitää resilienssiä. Tähän pyrkivät esimerkiksi erilaiset kyberturvallisuuden parantamiseen liittyvät suunnitelmat. Näihin kuuluvat myös palautumiseen liittyvien suunnitelmien laadinta (NIST, 2018), joista esimerkkinä voidaan mainita jatkuvuuden takaavat suunnitelmat.

Palaudu-vaiheen jälkeen päästään taas aloittamaan mahdollisten uusien riskien tunnistaminen ja prosessi jatkuu. Alla olevassa kuviossa 4 on esitetty mallin keskiön aktiviteetit.

KUVIO 4 NIST-kyberturvallisuuden hallintamalli (Huergo, 2018)

NIST- mallin kerrokset kuvaavat, millä laajuudella organisaation kyberturvallisuuden riskienhallinta on toteutettu. Määriteltyjä kerroksia on neljä: osittainen, riskitietoinen, toistava ja mukautuva. Osittaisella kerroksella riskienhallinnan ja riskitietoisuuden kehittäminen on vielä kesken. Riskitietoisella tasolla organisaatio tunnistaa riskien hallinnan tärkeyden, mutta sen käytäntöön viemisessä on vielä kehitettävää. Toistavalla kerroksella riskienhallinta on saatu levitettyä

koko organisaatioon. Mukautuvalla kerroksella riskienhallintaa kehitetään ja nimensä mukaisesti muokataan käytännön kokemuksien perusteella. (NIST, 2018)

NIST-mallin profiili -osaa voidaan käyttää hyödyksi kyberturvallisuuden kehityksessä. Organisaatio voi määrittää nykyisen profiilin ja tavoite profiilin ja selvittää, minkälaisia toimia tarvitaan tavoitteiden saavuttamiseksi. (NIST, 2018)

NIST:n malli on tarkoitettu erityisesti kriittisen infrastruktuurin suojelemiseen, mutta sitä pystyy hyödyntämään ja sitä ovat hyödyntäneet muutkin organisaatiot koosta riippumatta (Huergo, 2018).

NIST- mallin vaiheisiin voidaan löytää monenlaisia työkaluja ja toimintatapoja. Seuraavissa kappaleissa käydään läpi vielä kahta vaihetta hiukan erilaisten työkalujen kautta. Ensimmäisenä käydään läpi tilannetietoisuutta yhtenä mahdollisena tunnistamisen ja havainnoinnin vaiheissa hyödynnettävänä työkaluna. Tilannetietoisuutta käydään myös muiltakin osin läpi. Tämän jälkeen hypätään viidenteen vaiheeseen eli palautumiseen sekä siihen liittyviin suunnitelmiin.

2.4 Tilannetietoisuus

Suomen poliisi toimii yhteistyössä Kyberturvallisuuskeskuksen kanssa vaihtaen tietoja kyberturvallisuuteen liittyen. Poliisit tarvitsevatkin tietoa kyberrikoksista osana valtakunnallisen kyberturvallisuuden tilannekuvan ylläpitoa. (Piiroinen, 2018)

Poliisit eivät ole ainoita, jotka voivat hyödyntää toiminnassaan tilannetietoisuutta. Oman tilannekuvan voi muodostaa myös organisaatio omasta kansallisvaltioita suppeammasta näkökulmasta. Tässä tapauksessa kyberturvallisuuden tilannekuva voidaan nähdä yhtenä päätöksenteon apuvälineenä. (Franke ja Brynielsson, 2014). Tämän voisi lisätä apuvälineeksi esimerkiksi aikaisemmin esittelemämme NIST-mallin tunnistamisen ja havainnoinnin vaiheissa. Seuraavaksi käsitellään tilannetietoisuuden määritelmää ja prosessia niin yleisesti kuin kybertoimintaympäristön näkökulmastakin.

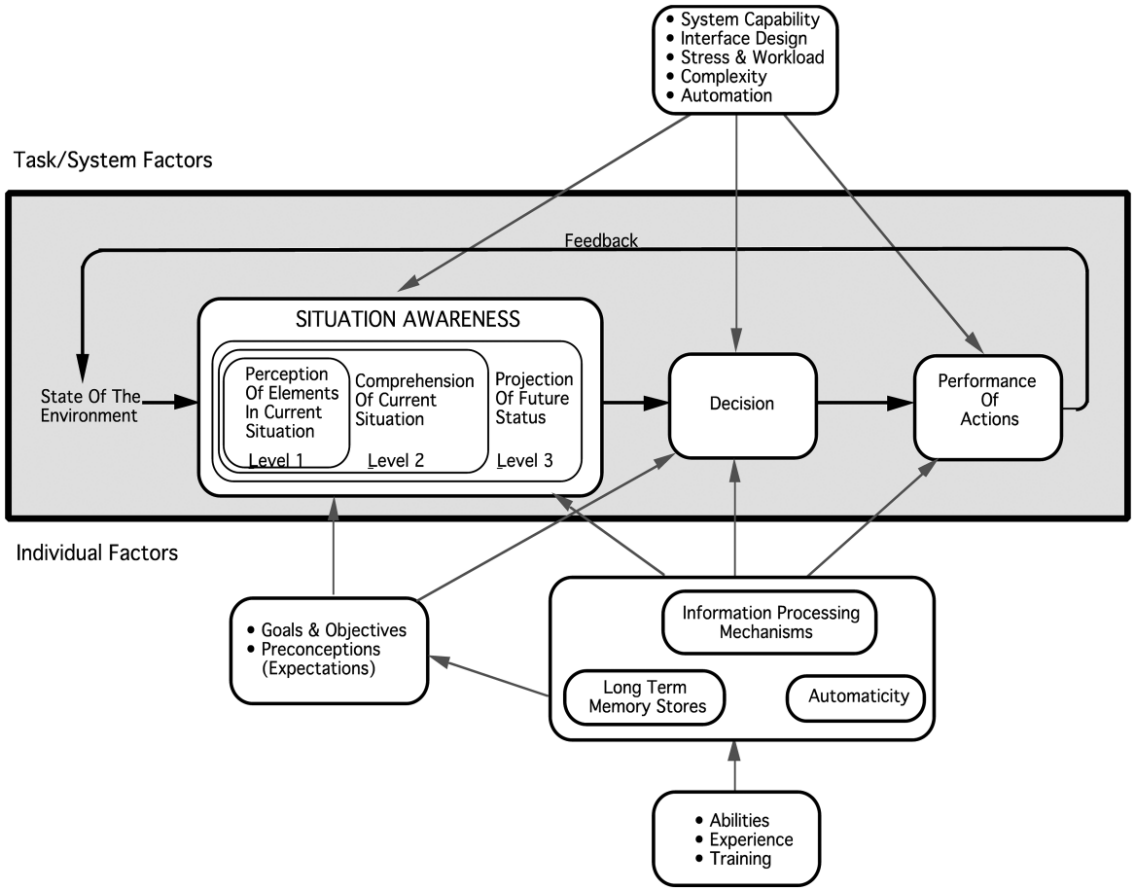
2.4.1 Yleisesti

Tilannetietoisuutta laajasti tutkinut Endsley (1988) määrittää tilannetietoisuuden käsitteen seuraavasti:

> Ympäristössä olevien elementtien havaitsemista ajassa ja paikassa, niiden merkityksen ymmärtämistä sekä ennusteen luomista elementtien tilasta lähitulevaisuudessa. (Ensley, 1988, 792)

Tianfield (2016) esittelee Endsleyn laatiman tilannetietoisuuden mallin artikkelissaan. Mallissa tilannetietoisuus jaetaan kolmeen vaiheeseen: havaitsemiseen (engl. perception), ymmärtämiseen (engl. comprehension) ja ennustamiseen

(engl. projection). Ensimmäisessä vaiheessa havaitaan ja tunnistetaan asiaan kuuluvat attribuutit, tilanne ja dynamiikka. Tarkoituksena on löytää olennaiset osat. Toisessa vaiheessa löydettyihin attribuutteihin, tilanteisiin ja dynamiikkaan perehdytään tarkemmin, jotta saadaan selville, miten nämä vaikuttavat nykytilanteeseen. Kolmannessa vaiheessa tämä nykytilaa koskeva tieto peilataan tulevaisuuteen ja laaditaan ennuste, mitä tulevaisuudessa tulee tapahtumaan. Mallista on myöhemmin päivitetty dynaamisempi versio, joka perustuu tilannetietoisuuden jatkuvaan päivittämiseen. Endsley (2015) myöhemmin kirjoittamassa tekstissä tämä malli on esitetty oheisessa kuviossa 5.



KUVIO 5 Dynaaminen tilannetietoisuuteen perustuvan päätöksenteon malli (Endsley, 2015, 5)

Vaikka Endsleyn malli onkin saanut osakseen kritiikkiä, on se yksi kaikkein viitatuimmista tilannetietoisuuden malleista. Lisäksi Endsleyn mielestä suurin osa kritiikkistä johtuu mallin väärinymmärryksestä, kuten hän on selittänyt uudemmassa tekstissään. (Endsley, 2015)

2.4.2 Kybertilannetietoisuus

Franke ja Brynielsson (2014) määrittävät kybertilannetietoisuuden olevan tilannetietoisuuden alalaji, joka keskittyy kybertoimintaympäristöön ja kyberturvallisuuteen vaikuttaviin tekijöihin.

Kyberturvallisuustilannetietoisuutta voidaankin hallita hyvin samalla tavalla kuin tilannetietoisuutta laajemminkin (Tianfield, 2016). Tianfield (2016), sovelsi tekstissään Endsleyn kolmen vaiheen mallin kybertoimintaympäristöön seuraavasti: Ensimmäisessä vaiheessa selvitetään, millaista tietoa kyberinfrastruktuurista on saatavilla. Nämä voivat olla esimerkiksi palomuurin lokitietoja tai tunkeutumisen havainnointijärjestelmän raportteja. Tähän vaiheeseen kuuluu myös kyseessä olevien verkkojen ja järjestelmien turvallisuuteen liittyvien ilmiöiden tarkkailu. Toisessa vaiheessa havaittujen riskien vaikutukset, tyyppi ja todennäköisyys arvioidaan. Kolmannessa vaiheessa laaditaan edellisten pohjalta ennustuksia tulevaisuudesta ja pyritään varautumaan riskeihin sekä minimoimaan niiden vaikutus.

Kyberulottuvuus on aikaisempaa kiinteämmin kiinni fyysisessä ulottuvuudessa, mikä tarkoittaa, että kyberturvallisuuden tilannekuvaa ei voi erottaa täysin yleisemmästä, fyysiseenkin maailmaan ulottuvasta, tilannekuvasta. Kyberturvallisuuden tilannekuvaa hallittaessa onkin otettava huomioon myös mm. muu tiedustelutieto (Franke ja Brynielsson, 2014).

Tilannetietoisuuden ylläpito ei ole ongelmatonta. Jajodia ym. (2011) mainitsevat artikkelissaan tilannetietoisuuden heikkouksiksi ja ongelmakohdiksi mahdollisen puutteellisen haavoittuvuusanalyysin, epävarmuuden hallinnan, uusiin uhkiin ja tietoverkkoihin mukautumisen vaikeuden sekä epäonnistuneen tilannetietoisuuden päätösprosessin, jossa raaka tieto ei ole jalostunut totuudenmukaiseksi tilannetietoisuudeksi.

2.4.3 Tutkimuksesta

Tilannetietoisuutta on tutkittu laajasti ja monenlaisista näkökulmista, mutta toiset aihealueet ovat laajemmin tutkittuja kuin toiset. (Franke ja Brynielsson, 2014) Franke ja Brynielsson (2014) kävivät kyberturvallisuuden tilannetietoisuuteen liittyviä julkaisuja läpi tutkimuksessaan, jossa kävi ilmi, että tutkituimpia aihealueita olivat teollisuuden hallintajärjestelmät ja tunkeutumisen havaitsemiseen tarkoitettujen järjestelmien algoritmit ja tietofuusiot. Vähemmän tutkittuja alueita taas olivat mm. kyberhyökkäysten tappioiden arviointi sotilaallisissa operaatioissa ja tämän tutkimuksen kannalta olennainen kyberturvallisuuteen liittyvän tilannetietoisuuden jakamiseen liittyvä tutkimus.

Franke ja Brynielsson (2014) tutkivat myös eri valtioiden kansallisia kyberturvallisuusstrategioita tilannetietoisuuteen liittyviä akateemisia julkaisuja koskevaa tutkimustaan varten ja huomasivat, että kyberturvallisuuden tilannetietoisuuden ylläpito oli osana niissä kaikissa. Tavoitteeksi niissä oli määritelty valtiotasoinen kyberturvallisuustilanteen kuvan muodostaminen.

2.4.4 Käytäntö

Kuten monien muidenkin maiden vastaavissa julkaisuissa, myös Suomen kyberturvallisuusstrategian (Turvallisuuskomitea, 2013) yhdeksi tavoitteeksi määriteltiin valtakunnallisen kyberturvallisuuden tilannetietoisuuden luonti ja ylläpito. Suomessa tämä tehtävä annettiin Liikenne- ja viestintäministeriön yhteyteen perustetulle Kyberturvallisuuskeskukselle. Poliisin vastuulle taas on määritelty kyberrikollisuuden tilannekuva, mitä se ylläpitää yhteistyössä Kyberturvallisuuskeskuksen kanssa (Turvallisuuskomitea, 2013).

Strategiassa kybertoimintaympäristön tilannetietoisuuden attribuuteiksi on määritelty esimerkiksi tiedot haavoittuvuuksista, haittaohjelmista, häiriöistä, niiden mahdollisista vaikutuksista sekä arvioita ja ennustuksia tulevaisuudesta (Turvallisuuskomitea, 2013).

Suomen kyberturvallisuusstrategia määrittelee tilannetietoisuuden ylläpidon yhdeksi strategiseksi linjauksekseen. Tietojen vaihto niin julkisten, yksityisten kuin kolmannen sektorin organisaatioiden ja Kyberturvallisuuskeskuksen välillä on tärkeää ajantasaisen tilannekuvan ylläpitämiseksi. Sillä valtio ei saa kerättyä kunnollista kokonaiskuvaa pelkästään omiin toimiin ja havaintoihin luottaen. (Turvallisuuskomitea, 2013) Siksi olisi erittäin tärkeää, että havaituista kyberrikoksista tulisi tieto poliisille ja muille kyberturvallisuudesta vastaaville viranomaisille (Lehto ym. 2017).

2.5 Kyberrikoksista palautuminen

Olennainen osa organisaation kyberturvallisuuden hallinnassa on palautuminen mahdollisista kyberrikostilanteista. Palautuminen on esimerkiksi yksi aikaisemmin esitetyn NIST-mallin aktiviteeteista (NIST, 2018). Palautumista voidaan edistää mm. liiketoiminnan jatkuvuuden takaavilla suunnitelmilla (engl. business continuity planning) (Botha ja Solms,2004).

Akateemisesta kirjallisuudesta ja artikkeleista löytyy monia malleja toiminnan jatkuvuuden suunnitelmien laadintaan ja toteuttamiseen. Botha ja Solms (2004) ovat esitelleet jatkuvuuden takaavien suunnitelmien metodologeja ja he toteavat, että monet mallit muistuttavat rakenteeltaan yleisempiä projektinhallinnan malleja. (Botha ja Solms,2004).

Vaikka valmiita toiminnan jatkuvuuden suunnitelmien malleja onkin olemassa, on otettava huomioon, että liiketoiminnan jatkuvuuden suunnitelmiin ei voi antaa yhtä oikeaa kaavaa. Sopivan ja toimivan suunnitelman sisältö riippuu organisaatiosta ja on yksilöllinen, eli juuri kyseisen organisaation tarpeiden mukaan suunniteltu. (Cerullo ja Cerullo, 2004)

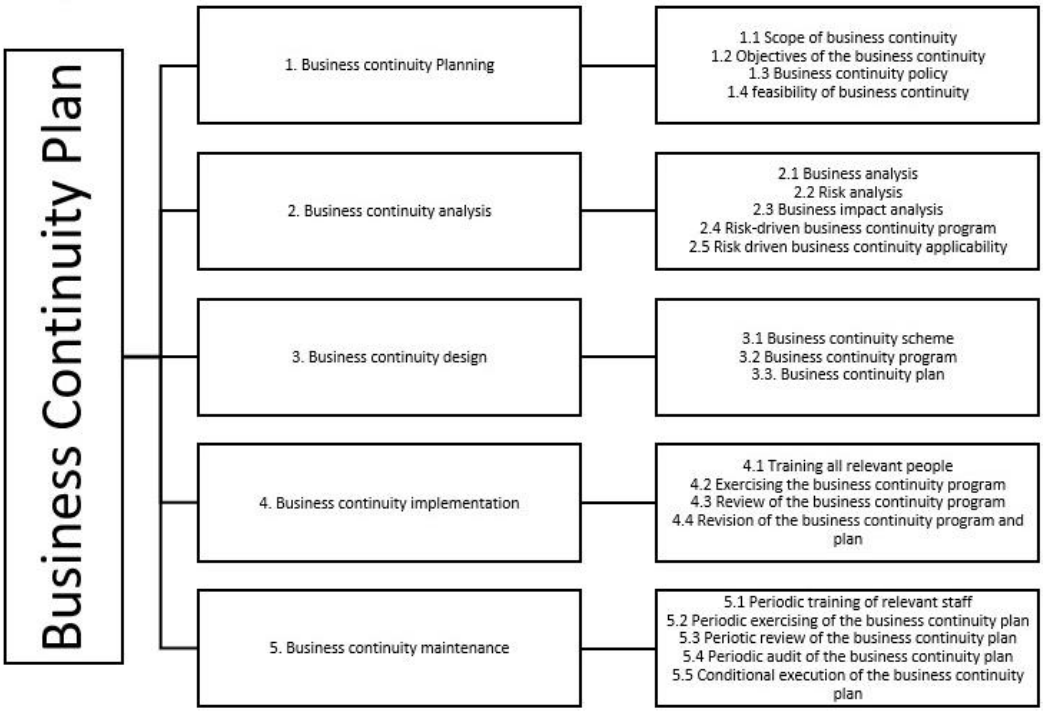
2.5.1 Toiminnan jatkuvuuden takaavat suunnitelmat

Seuraavaksi esitellään tarkemmin Raggadin (2010) ja Cerullon ja Cerullon (2004) esittämät mallit, sillä näitä malleja on esitetty nimenomaan kyberturvallisuuden ja tietojärjestelmien hallinnan kontekstissa. Ensin esitellään malleja ja aihetta yleisesti, sitten keskitytään vaikutusarviointiin ja kriiseistä palautumiseen vielä erikseen.

Toiminnan jatkuvuuden takaavien suunnitelmien tavoitteena on varautua poikkeustilanteisiin niin, että niistä palautuminen olisi mahdollisimman nopeaa ja vahinkoja tulisi mahdollisimman vähän. Kolmantena tavoitteena on, että organisaation henkilökuntaa koulutetaan, jotta he osaavat toteuttaa laadittua suunnitelmaa käytännössä. (Cerullo ja Cerullo, 2004)

Raggad (2010) jakaa organisaatioiden poikkeustilanteiden aiheuttajat neljään ryhmään: ihmisten ja luonnon aiheuttamiin, biologisiin uhkiin sekä teknologian aiheuttamiin. Tässä jaossa kyberrikoksiin liittyvät uhat kuuluvat teknologisiin tai ihmisen aiheuttamiin uhkiin. Cerullo ja Cerullo (2004) mainitsevat näiden lisäksi jaon sisäisiin uhkiin kuten laitteistovikoihin ja ulkoisiin uhkiin kuten haittaohjelmiin.

Raggadin (2010) liiketoiminnan jatkuvuuden suunnitelmien prosessi koostuu viidestä osasta: suunnitelmasta (engl. planning), analyysistä, suunnittelusta (engl. design), toteuttamisesta ja ylläpidosta. Ensimmäisessä vaiheessa määritellään suunnitelman laajuus (engl. scope) ja tavoitteet. Toisessa osassa arvioidaan poikkeustilanteiden vaikutusta organisaation toimintaan ja tehdään riskianalyysiä. Kolmannessa vaiheessa muodostetaan aikaisempien pohjalta jatkuvuuden hallinnan suunnitelmat ja käytännön toimintatavat poikkeustilanteisiin. Neljännessä vaiheessa laaditun suunnitelman toteutus aloitetaan, se arvioidaan ja organisaation henkilökuntaa koulutetaan. Viimeisessä vaiheessa jatkuvuuden takaavia suunnitelmia ylläpidetään niitä arvioiden ja tarvittaessa suunnitelmia muokaten ja kehittäen. (Raggad, 2010) Alla olevassa kuviossa 6 on esitelty kuhunkin vaiheeseen liittyvät toimenpiteet tarkemmin.



KUVIO 6 Jatkuvuuden suunnitelman laatimisen vaiheet (Raggad, 2010, 226, muokattu)

Cerullon ja Cerullon (2004) mallissa on samankaltaisuuksia. He jakavat liiketoiminnan jatkuvuuden mallin kolmeen erilaiseen vaiheeseen: vaikuttavuusarvion ja kriisistä palautumisen suunnitelmien laatimiseen sekä organisaation henkilökunnan koulutuksen suunnittelemiseen ja toteuttamiseen. (Cerullo ja Cerullo, 2004)

2.5.2 Vaikutusarviointi

Liiketoiminnan jatkuvuuden suunnitelmiin kuuluu osana poikkeustilanteiden vaikutusarviointien teko. Tavoitteena on arvioida, millaisia vaikutuksia poikkeustilanteella on organisaation toimintaan.

Cerullo ja Cerullo (2002) määrittävät vaikutusarvioinnin ensimmäiseksi vaiheeksi mallissaan. Sen tavoitteena on tunnistaa organisaation toiminnan kannalta kriittiset toiminnot, tunnistaa niihin liittyvät uhat sekä arvioida niitä.

Raggad (2010) mainitsee vaikutusarvioinnin osaksi mallinsa analyysivaihetta, eli vaihetta kaksi. Muuten se on hyvin samankaltainen Cerullon ja Cerullon esittämän mallin kanssa. Vaikutuksen arviointiin kuuluu toimintaan liittyvän arvokkaan tieto-omaisuuden (engl. assets) tunnistaminen, niihin kohdistuvien riskien tunnistaminen ja riskin toteutumisen todennäköisyyden sekä olemassa olevien suojausmenetelmien arviointi. Hänen mukaansa vaikutusarvioinnin tärkein tavoite on kerätä tarvittavia tietoja jatkuvuuden takaavien suunnitelmien laatimiseen. (Raggad, 2010)

2.5.3 Kriisistä palautuminen

Liiketoiminnan jatkuvuuden takaaviin suunnitelmiin kuuluu useimmissa organisaatioissa myös kriiseistä palautumiseen laaditut suunnitelmat (engl. disaster recovery plan). Termejä kriiseistä palautumisen suunnitelmat ja liiketoiminnan jatkuvuuden takaavia suunnitelmia käytetään joskus kirjallisuudessa sekaisin, synonyymeinä. (Raggad, 2010)

Kriisien palautumisen suunnitelmissa määritellään yksityiskohtaisesti, mitä kriisitilanteiden sattuessa on tehtävä (Raggad, 2010). Cerullo ja Cerullo (2004) lisäävät tähän määritelmän lisäksi poikkeustilanteiden vastuu- ja varahenkilöiden nimeämisen.

Raggad (2010) kertoo kirjassaan kriisien palautumisen suunnitelmien olevan yksi liiketoiminnan jatkuvuuden suunnitelmien prosessin tuotos, jossa määritellään yleensä organisaation ICT–yksikön toimintaa kriisitilanteissa. Muuten sitä ei ole suoraan mainittu osana Raggadin (2010) toiminnan jatkuvuuden suunnittelemisen -mallia.

Cerullon ja Cerullon (2004) esittämässä mallissa kriiseistä palautumisen suunnitelma on toinen tuotos, joka on luotava toiminnan jatkuvuuden suunnitelmia laadittaessa. Muuten se esitetään hyvin samankaltaiseksi kuin Raggadin malli.

2.6 Yhdistelmä

Tässä luvussa on käsitelty tutkimuksen kannalta tärkeitä termejä ja ilmiöitä. Seuraavana on käsitelty vielä, miksi nämä asiat ovat tärkeitä toteutettavan tutkimuksen kannalta. Lisäksi käydään edellä mainittuja asioita läpi tämän tutkimuksen näkökulmasta ennen kuin siirrytään tutkimusmenetelmän teoriaan ja sen jälkeen varsinaiseen tutkimukseen.

Tämän tutkimuksen kohteena on kyberrikokset, joista tehdään rikosilmoitus poliisille. Tämän takia yksi merkittävä kokonaisuus, eli henkilötietoja koskeva kyberrikollisuus, on rajattu tämän ulkopuolella. GDPR:n mukaan henkilötietoja koskevat tietomurrot on ilmoitettava henkilötietoviranomaiselle, joka Suomessa on Tietosuojavaltuutettu (Talus, Autio, Hänninen ym., 2017). Muuten kyberrikollisuuden määritelmää ei ole rajattu.

Kuten aikeisemmin on esitelty, kyberrikollisuuteen liittyen on olemassa tutkimusta, mutta ne ovat osittain kyberrikoksien ilmoittamiseen liittyen vajavaisia. Tutkimuksissa on otettu esille kyberrikosten tietojen jakamisen tärkeys, mutta käytännössä on huomattu, että kaikista tapauksista ei ilmoiteta poliisille (Piiroinen, 2018), vaikka tiivis yhteistyö on määritelty yhdeksi päätavoitteista Suomen kyberturvallisuusstrategiassa (Turvallisuuskomitea, 2013).

Kyberrikoksen uhriksi voi joutua, vaikka olisi varautunut kuinka hyvin. Siksi on tärkeää, että organisaatio on varautunut poikkeustilanteiden varalle mm. laatimalla suunnitelmat, joiden avulla taataan toiminnan jatkuvuuden ja

kriisistä palautuminen mahdollisimman nopeasti ja vähin vahingoin. Tutkimuksen tarkoituksena on selvittää salassapito rajoitusten sallimissa rajoissa, miten ja millaisia suunnitelmia organisaatiot ovat laatineet kyberhyökkäysten torjumiseksi.

Kyberrikostilanteessakin päätöksiä tekee organisaation johto. Tutkimuksen yksi selvityskohteista on löytää henkilöt, jotka tekevät päätöksiä poikkeustilanteissa. Siksi tutkimuksessa on esitetty kyberturvallisuuden hallintaan sekä siihen liittyviä ongelmia pääpiirteittäin. Enemmän kuitenkin keskityttiin Suomen kyberturvallisuuden strategiaan ja sen antamiin ohjeisiin ja vaatimuksiin niin julkisille kuin yksityisillekin organisaatioille.

Kybertoimintaympäristössä ja kyberturvallisuudessa tieto on olennaisen tärkeää (Lehto ym., 2017). Suomen kyberturvallisuuden tilannekuvan tärkeää materiaalia on organisaatioiden antamat tiedot mm. kohtaamistaan kyberrikoksista. Tämän takia on käsitelty myös kyberturvallisuuden tilannekuvan suunnittelua ja hallintaa.

3 MENETELMÄT

Seuraavaksi esitellään tässä tutkimuksessa käytetyt menetelmät. Menetelmiä käsitellään aiheeseen liittyvää teorian ja tutkimuksen kautta. Lisäksi esitellään tarkemmin menetelmiin liittyviä työkaluja sekä metodeja, joita käytetään tässä tutkimuksessa hyväksi.

3.1 Laadullinen tutkimus

Laadullinen tai pehmeä tutkimus on tutkimussuuntaus, joka keskittyy matemaattisten ja tilastollisten menetelmien sijaan aineiston keräämiseen ja aineistosta usein muiden menetelmien avulla tehtyihin päätelmiin. (Laaksovirta, 1984)

Laadullinen tutkimus voi olla rakenteeltaan vapaampi määrälliseen tutkimukseen verrattuna esimerkiksi sillä tavalla, että laadullisessa tutkimuksessa ei välttämättä ole alkuhypoteesia. (Saaranen-Kauppinen ja Puusniekka 2006 ; Maxwell 2008) Lisäksi laadullista tutkimusta voidaan muokata tutkimuksen edetessä ja siihen joissain tapauksissa rohkaistaankin. (Maxwell, 2008)

Tarkka rajanveto laadullisen ja määrällisen tutkimussuuntauksen välillä on kuitenkin vaikeaa, sillä erot eivät ole niin suuret kuin kuvitellaan. Laadullisessakin tutkimuksessa voidaan käyttää määrällisestä tutkimuksesta tuttuja menetelmiä esimerkiksi laadullisen aineiston yksinkertaistamiseksi. Laadullista ja määrällistä tutkimusmenetelmää voidaan käyttää myös sekaisin. (Laaksovirta, 1984)

Laadullista tutkimusta voidaan toteuttaa ja tietoa voidaan kerätä monin eri tavoin (Saaranen-Kauppinen ja Puusniekka 2006). Esimerkiksi tapaus- ja toimintatutkimusta sekä etnografiaa käytetään laadullisissa tutkimuksissa (Darke, Shanks ja Broadbent, 1998) Tiedonkeruu voidaan suorittaa esimerkiksi haastatteluin, havainnoinnein tai olemassa olevaa dokumentaatiota kuten kirjeitä tutkimalla (Saaranen-Kauppinen ja Puusniekka 2006).

Seuraavaksi esitellään tarkemmin tapaustutkimusta, joka on Darken, Shanksin ja Broadbentin (1998) mukaan laajimmin käytetty tutkimusmenetelmä tietojärjestelmiin liittyvissä tutkimuksissa. Tapaustutkimusta käsitellään ensin yleisesti. Sitten keskitymme tapaustutkimuksen toteuttamiseen käytännössä sekä esittelemme tapaustutkimuksessa käytettyjä tiedonkeruumenetelmiä. Tämän jälkeen perehdytään vielä tarkemmin haastatteluun, joka on yksi laadullisen tutkimuksen käytetyimmistä tiedonkeruunmenetelmistä (Myers ja Newman, 2007). Viimeisenä käydään läpi vielä erilaisia tiedonanalyysimenetelmiä.

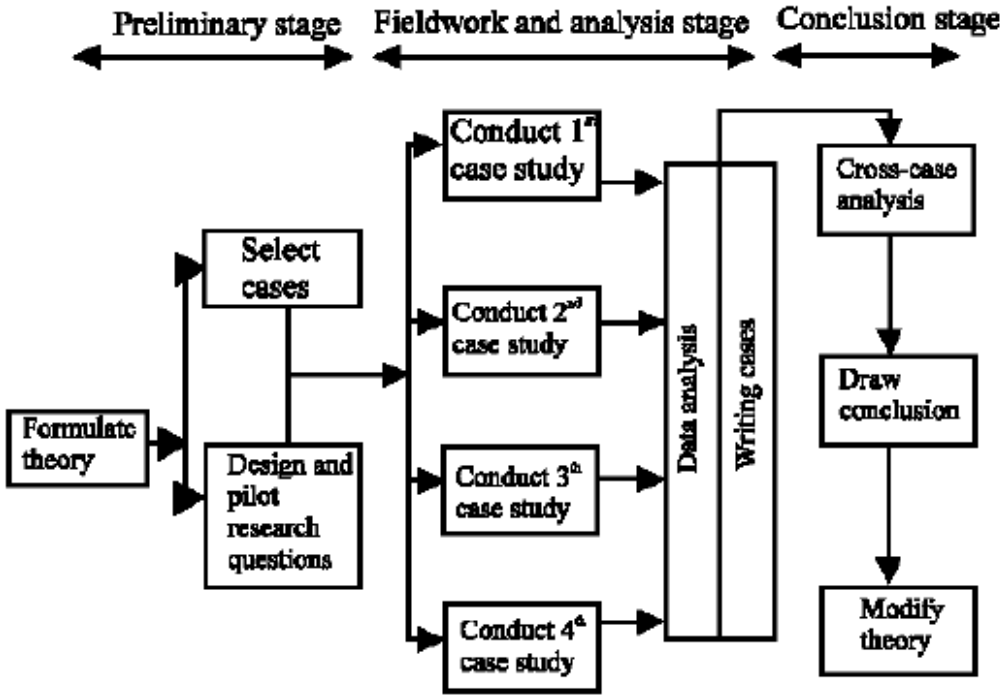
3.2 Tapaustutkimus

Tapaustutkimuksessa tutkitaan nimensä mukaisesti joko yhtä tai useampaa ennalta määriteltyä tapausta. Yhden tapauksen muodostaa usein jokin ilmiö tai tapahtumakulku, jota on tarkoitus tutkia mahdollisimman tarkasti.(Laine, Bamberg ja Jokinen, 2015) Tapaustutkimusta voidaan käyttää kuvailemaan tutkittavaa ilmiötä, uuden teorian luomiseen sekä uuden teorian testaamiseen (Darke, Shanks ja Broadbent, 1998).

Tapaustutkimus sopii tutkimusmenetelmäksi sellaisiin tilanteisiin, joissa ilmiötä halutaan tutkia luonnollisessa ympäristössään, päämääränä on tutkia käytännön ilmiöitä (Benbasat, Goldstein ja Mead, 1987) tai sosiaalisia tilanteita (Darke, Shanks ja Broadbent, 1998), silloin kun tutkittavasta asiasta ei ole välttämättä olemassa paljon aikaisempia tutkimuksia sekä silloin, kun halutaan keskittyä johonkin tapahtumaan liittyviin henkilöihin tai kontekstiin (Benbasat, Goldstein ja Mead, 1987). Se sopii hyvin myös monimutkaisten kokonaisuuksien tutkimiseen ja vastaamaan miten ja miksi kysymyksiin (Laine, Bamberg ja Jokinen, 2015).

3.2.1 Kulku

Noor (2008) kuvaa tapaustutkimuksen lähtevän liikkeelle tutkimukseen liittyvän kirjallisuuden ja aikaisempien tutkimusten laaja-alaisesta analysoinnista. Näiden pohjalta muodostetaan tutkimuksen viitekehys. Viitekehyksen muodostamisen jälkeen valitaan tutkimuksen tapaukset ja suunnitellaan tiedonhankintamenetelmät. Sen jälkeen aloitetaan tutkimusmateriaalin keräys ja analyysi. Tapaustutkimukselle on tyypillistä, että tutkimusmateriaalin analyysiä aloitetaan jo materiaalin keräämisen aikana. (Noor, 2008) Alla olevassa kuviossa 7 on tapaustutkimuksen kulkua esittävä kaavio Noorin (2008) mukaan.



KUVIO 7 Tapaustutkimuksen kulku (Noor, 2008, 1603)

3.2.2 Vahvuudet ja heikkoudet

Tapaustutkimukseen liittyen on olemassa paljon tieteellistä materiaalia, joka käsittelee asiaa useiden eri tieteenalojen tutkimusmenetelmänä. Näissä tutkimuksissa on tunnistettu tapaustutkimukselle sekä vahvuuksia että heikkouksia.

Tapaustutkimuksen vahvuuksiksi voidaan lukea, että se antaa mahdollisuuden tutkia asioita tai ilmiöitä, joita olisi vaikea tutkia muilla menetelmillä. Tällaisesta voi olla esimerkkinä tutkimus, jonka tavoitteena on selvittää, miten jokin tietty prosessi toimii organisaatiossa (Noor, 2008) Tapaustutkimuksen vahvuuksiksi voidaan lukea myös, että se mahdollistaa tapauksen syvällinen tutkiminen useammasta näkökulmasta (Noor, 2008) ja luonnollisessa tilassaan (Benbasat, Goldstein ja Mead, 1987).

Tapaustutkimuksen heikkouksiksi on akateemisessa kirjallisuudessa listattu tieteellisen täsmällisyyden (engl. rigour) ja luotettavuuden puute sekä tutkimuksen toistettavuuteen ja tulosten yleistämiseen liittyvät vaikeudet (Noor, 2008). Tieteellisen täsmällisyyden ja luotettavuuden kyseenalaistamisen syynä on, että tapaustutkimus perustuu suurelta osin tutkijan tekemiin tulkintoihin aineistosta (Benbasat, Goldstein ja Mead, 1987). Yleistämiseen liittyvät ongelmat perustellaan sillä, että tapaustutkimuksien otannat ovat usein pieniä (Flyvbjerg, 2006).

Näihin ongelmiin on kuitenkin esitetty myös ratkaisuja. Noor (2008) toteaa, että tapaustutkimuksessa saatavien tulosten yleistämistä voidaan edistää tutkimalla useampaa tapausta yhden sijaan. Flyvbjerg (2006) taas on pyrkinyt

perustelemaan myös yhteen tapaukseen keskittyvien tutkimusten yleistämisen hyötyjä. Darke, Shanks ja Broadbent (1998) suosittelevat tiedonanalyysistrategian ja -menetelmien valitsemista ja niiden esittelemistä tieteellisen täsmällisyyden ja luotettavuuden lisäämiseksi.

3.2.3 Tiedonkeruumenetelmät

Tapaustutkimuksissa voidaan kerätä aineistoa usealla tavalla ja näitä voidaan tarvittaessa tai halutessa yhdistellä eri tavalla (Saaranen-Kauppinen ja Puusniekka, 2006). Tietoja voidaan myös kerätä tutkimuksen kuluessa lisää ja saatuja tietoja on tarkoitus analysoida jo tiedonkeruun aikana (Maxwell, 2008).

Benbasat, Goldstein ja Mead (1987) listaavat tekstissään viisi tapaustutkimuksen tietolähdettä ja tietojenkeruu menetelmää: olemassa oleva dokumentaatio, arkistot, fyysiset tietolähteet, haastattelu ja tarkkailu. Dokumentaatiolla voidaan tarkoittaa mm. suunnitelmia tai uutisartikkeleita. Arkistoista voisi mainita esimerkkinä erilaiset raportit. Fyysisinä tietolähteinä voidaan käyttää laitteiden sisältämää tai esimerkiksi työkaluista päätteltävää tietoa. Näistä tietojenkeruumenetelmistä haastattelua on käyty vielä tarkemmin läpi seuraavaksi.

3.2.4 Haastattelu

Haastattelut ovat monien laadullisten tutkimusten suosituimpia ja käytetyimpiä aineistonkeruumenetelmiä, joita käytetään kaikenlaisissa laadullisissa tutkimuksissa. Laadullisten tutkimusten lisäksi haastattelua voidaan käyttää esimerkiksi toiminta- ja etnografisissa tutkimuksissa. (Myers ja Newman, 2007)

Myers ja Newman (2007) esittelevät tekstissään kolme haastattelutyyppiä strukturoidun, puolistrukturoidun ja ryhmähaastattelun. Strukturoidussa haastattelussa ei ole tilaa improvisoinnille haastattelutilanteessa vaan kaikki esitettävät kysymykset on laadittu etukäteen. Puolistrukturoidussa tai osittain avoimessa haastattelussa on ennalta laadittuja kysymyksiä, mutta siinä jätetään mahdollisuus keksiä uusia kysymyksiä keskustelun aikana. Strukturoituun haastatteluun verrattuna puolistrukturoitu haastattelu antaa enemmän vapauksia. Ryhmähaastattelulla viitataan haastattelun suunnittelun sijaan haastateltavien määrään, mikä ryhmähaastattelussa on useampi kuin yksi henkilö kerrallaan joko strukturoidusti tai puolistrukturoidusti.

Haastattelujen suunnitteleminen ja toteuttaminen eivät kuitenkaan ole ongelmattomia. Myers ja Newman (2007) kritisoivat tekstissään, että haastatteluiden ongelmakohtiin ei kiinnitetä tutkimuksissa tarpeeksi huomiota. He listaavat haastatteluiden ongelmallisiksi kohdiksi haastattelu tilanteiden keinotekoisuuden, luottamuksellisen suhteen luomisen vaikeuden, ajan puutteen aiheuttamat ongelmat laatuun, tutkijan asema haastateltaviin nähden, haastateltavien valinnan suppeus, vastausten tai kysymysten väärät tulkinnat. Näiden lisäksi haastattelut voivat epäonnistua muista syistä.

Haastattelutilanteen keinotekoisuus ja luottamuksellisen suhteen puuttuminen haastattelijan ja haastateltavan välillä voivat tehdä haastatteluista epämukavia haastateltavalle, mikä taas voi vaikuttaa siihen millaisia vastauksia hän antaa. Haastateltava voi esimerkiksi tuntea painetta vastata niin kuin hänen odotetaan vastaavan sen sijaan että hän vastaisi totuudenmukaisesti. Näin vastaukset vääristyvät (Maxwell, 2008). Haastattelijan asema haastateltavaan nähden voi myös olla ongelmallinen, jos haastattelija on tullut organisaatioon haastateltavaa organisaation hierarkiassa alempana olevan henkilön kautta. Tällöin haastateltava ei välttämättä suhtaudu haastattelijaan tarpeeksi vakavasti. Haastattelukysymysten ymmärtäminen ja tulkinta voivat myös aiheuttaa ongelmia, sillä eri ihmiset voivat ymmärtää sanat eri tavalla. (Myers ja Newman, 2007)

Myers ja Newman (2007) vertaavat tekstissään haastattelutilannetta näytelmään. Tämä perustuu heidän esittelemään Goffmanin dramaturgiseen malliin. Niin kuin näytelmässä myös haastattelussa voidaan tunnistaa näyttelijät, yleisö, käsikirjoitus, lava, sisääntulo ja poistuminen sekä muita näytelmistä tuttuja elementtejä. Haastateltava ja haastattelija voidaan nähdä sekä näyttelijöinä että yleisönä. Käsikirjoituksena toimii ennalta valmistellut haastattelukysymykset. Kuten näytelmän laatua Myers ja Newman näkevät näiden seikkojen vaikuttavan myös haastatteluiden laatuun.

Tämän perusteella Myers ja Newman (207) antavat seitsemän ohjetta kvalitatiivisten haastattelujen onnistumiseen:

1. Muista ottaa huomioon haastattelijan vaikutus tilanteeseen.
2. Pyri välttämään kaikkea, mikä voi saada haastateltavan tuntemaan olonsa epämukavaksi.
3. Pyri haastattelemaan eritasoisia ihmisiä organisaation sisältä.
4. Muista, että jokainen osapuoli tulkitsee asioita hiukan omalla tavallaan.
5. Peilaa haastateltavaa kommenteissa tai seuraavissa kysymyksissä mm. käyttämällä samoista asioista samoja sanoja.
6. Suosi avoimia tai osittain avoimia, eli puolistrukturoituja, haastatteluja, jolloin saat haastattelusta avoimemman. Lisäksi se mahdollistaa improvisoinnin tilanteen mukaan.
7. Haastattelun luottamuksellisuudesta ja avoimuudesta on myös muistettava sopia.

3.2.5 Tiedonanalyysimenetelmät

Laadullisissa tutkimuksissa voidaan käyttää hyvin erilaisia tiedonanalyysimenetelmiä. Mitään selkeitä kaavoja ei kuitenkaan ole vaan erilaisia menetelmiä yhdistellään tapauksen mukaan. Tavoitteena on tutkia ainestoa systemaattisesti. (Saaranen-Kauppinen ja Puusniekka 2006)

Laadulliseen tutkimukseen ja sitä kautta myös tapaustutkimukseen sopivia analyysimenetelmiä on käsitelty ja kategorioitu eri tavoilla eri teksteissä. Darke, Shanks ja Broadbent (1998) käsittelevät ja lajittelevat analyysikeinoja positivistisen ja relativistisen filosofisen todellisuuskuvan mukaan jaoteltuna.

He esittelevät myös Milesin ja Hubermanin analyysimallin, joka koostuu neljästä vaiheesta tietojen valitsemisesta, yksinkertaistamisesta, abstraktoinnista ja muodonmuutoksesta. Maxwell (2008) taas jakaa laadullisen tutkimuksen analyysikeinot kolmeen kategorisoiviin strategioihin, yhdistäviin strategioihin sekä muistiinpanoihin ja kuvantamiseen (engl. memos and displays).

Postivistisen filosofian mukaan todellisuus on olemassa itsenäisesti, kun taas relativistisen filosofian mukaan todellisuus on subjektiivinen ja perustuu ihmisen arvojen ja uskomusten kautta tehtyihin tulkintoihin. Positivistisen tutkimusotteen omaavissa tapaustutkimuksissa aineistosta pyritään löytämään säännöllisyyksiä ja kaavoja. Relativistisessa tutkimusotteessa taas esitellään toisten ihmisten tulkinnoista tehtyjä tulkintoja ja keskitytään kontekstiin. (Darke, Shanks ja Broadbent, 1998)

Maxwellin (2008) esittämiin kategorisoiviin strategioihin kuuluvat mm. koodaus ja temaattinen analyysi. Yhdistäviin strategioihin kuuluvat taas mm. narratiiviset analyysit. Näitä erilaisia analyysityylejä tulisi yhdistellä tutkimusaineiston analyysejä tehdessä (Maxwell, 2008).

Laadullisessa tutkimuksessa koodauksella on tarkoituksena selventää tutkimusaineistoa tekemällä siihen merkintöjä. Merkintöjä voidaan tehdä esimerkiksi värein tai numeroin. (Saaranen-Kauppinen ja Puusniekka 2006) Koodattua aineistoa on helpompaa analysoida eteenpäin mm. kategorioita luomalla. Kategorioita voidaan käyttää hyödyksi esimerkiksi tutkimustulosten vertailussa (Maxwell, 2008). Tapaustutkimuksessa voidaan aineiston analyysi aloittaa tiivistämällä jokaisen tapauksen tärkeimmät asiat ja jatkaa sitten siitä eteenpäin (Saaranen-Kauppinen ja Puusniekka 2006)

Alkutoimenpiteiden jälkeen aineistosta voidaan esimerkiksi etsiä teemoja, kaavoja tai säännöllisyyksiä sekä luoda kategorioita tai tyyppejä. Teemoitetusta aineistosta kerätään tunnistettuun teemaan liittyviä asioita yhteen. (Saaranen-Kauppinen ja Puusniekka 2006) Tämä muistuttaa Maxwellin (2008) sekä Darken Shanksin ja Broadbentin (1998) kuvaamaa kategorisointia, jossa yhdistellään koodauksella hajotettua tietoa kategorioiden sisään. Tämän jälkeen voidaan vertailla kategorioiden sisällä olevia tietoja keskenään. Vertailua voidaan tehdä myös eri kategorioiden välillä (Maxwell, 2008).

Tiedon analyysin jälkeen tulokset voidaan esitellä ja aloittaa johtopäätösten sekä esimerkiksi teorioiden luominen, kuten aikaisemmin esitellyn Noorin tapaustutkimuksen kulun kaaviossa (ks. kuvio 7) kuvattiin.

4 TUTKIMUSASETELMA

Tässä luvussa esitetään toteutettavan tutkimuksen asetelma. Mikä on lähtöongelma, miksi asiaa halutaan tutkia, mikä on tutkimuskohde, miten ja miksi sitä on rajattu sekä millä työkaluilla tätä ongelmaa selvitetään. Viimeisenä tässä luvussa kerrotaan tarkempia yksityiskohtia tutkimuksen toteutuksesta.

4.1 Tutkimusongelma

Tutkimuksen tavoitteena oli selvittää, miksi poliisille ei ilmoiteta kaikista organisaatioissa havaituista kyberrikoksista. Seuraavaksi esitellään tutkimusongelman motivaattoreita, käydään läpi tutkimusongelmaan tehtyjä rajauksia perustellen ne ja lopulta määritellään tutkimusongelma kysymyksen muotoon ja esitellään siitä johdetut ala-kysymykset, jotka auttavat tutkimuksen toteutuksessa.

4.1.1 Motiivi

Tutkimuksen inspiroijana toimi KRP:n kyberrikostorjuntakeskuksen päällikkö Timo Piiroinen, joka kertoi kiinnostuksestaan asiaa kohtaan. Käytännössä poliisi on huomannut, että kaikista tapauksista ei ilmoiteta poliisille (Piiroinen, 2018). Negatiivista julkisuutta on pidetty yhtenä syynä rikosilmoituksien ja ylipäätänsä havaittujen kyberhyökkäysten ilmoittamatta jättämiseen. (Pelkonen ym. 2016; Piiroinen, 2018). Piiroisella (2018) on kuitenkin sellainen käsitys, että tämä ei olisi ainoa syy. Hän on kiinnostunut kuulemaan ja tutkimaan millainen prosessi kyberrikoksien ilmoittaminen on organisaatioissa ja kuka tekee päätöksen ilmoittamisesta ja miksi joitain ilmoituksia jätetään tekemättä. (Piiroinen, 2018)

Kyberrikoksista ilmoittaminen viranomaisille on määritelty tärkeäksi Suomen kyberturvallisuusstrategian asettaman kansallisen kybertuvallisuuden tilannekuvan kannalta (Turvallisuuskomitea, 2013). Silti, monissa strategian toteuttamista käsittelevissä tutkimuksissa havaituista tapauksista ilmoittamatta

jättäminen on mainittu yhdeksi olennaisimmista kehityskohteista. (Lehto ym., 2017; Lehto ym., 2018; Pelkonen ym., 2016) Kyberrikoksia koskevat ilmoitukset ovat tärkeä lähde kyberrikollisuuden tilannekuvan ylläpitämiseksi. Kun poliisilla on hyvä tilannekuva, he pystyvät paremmin tiedottamaan ja varoittamaan uhista. Yksittäisellä ilmoituksella ei välttämättä saada rikollista kiinni, mutta kun samasta kampanjasta tulee ilmoituksia useammasta paikasta, saadaan monipuolisempaa tietoa, mikä voi johtaa rikoksen ratkaisemiseen. (Piiroinen, 2019)

Tutkimusongelman selvittämiseen on siis poliisin edustajan kiinnostus, mutta sen lisäksi kysymykseen vastaamalla voidaan myös tarttua asiaa, joka on tutkijoiden mukaan yksi Suomen kyberturvallisuuden tärkeimmistä kehityskohteista. (Piiroinen, 2018 ; Lehto ym., 2017; Lehto ym., 2018; Pelkonen ym., 2016)

4.1.2 Rajaukset

Tutkimusongelmaa rajattiin Pro Gradu -tutkimukseen sopivaksi määrittämällä tutkimuksen kohteeksi julkiset organisaatiot. Julkisista organisaatioista tutkimusta rajattiin vielä isompiin kaupunkeihin Suomessa, jotta olisi mahdollista saada aikaan mahdollisimman laaja otos samankaltaisia organisaatioita. Tämä takaa sen, että tutkimustuloksista voidaan paremmin tehdä yleistyksiä kuten mm. Noor (2008) ja Darke ym. (1998) artikkeleissaan mainitsevat. Kaupungit ovat tämän lisäksi kiinnostava kohde sen takia, että niiden vastuulla on monien kansalaisille tärkeiden palveluiden tuottaminen ja ylläpito. Monia näistä palveluista on myös siirretty tai on tarkoitus siirtää internettiin, mikä lisää entisestään kyberrikollisten kiinnostusta kaupunkeja kohtaan. (Piiroinen, 2018)

Tutkimus toteutettiin KRP:n Timo Piiroisen ehdotusten pohjalta, siksi tutkimusongelman ulkopuolelle rajattiin kaikki henkilötietoja koskevat kyberrikokset. GDPR :n voimaan astuttua on huomioitava, että henkilötietoihin kohdistuvat kyberrikokset ilmoitetaan poliisin sijaan Suomen tietosuojasta vastaavalle viranomaiselle, joka Suomessa on Tietosuojavaltuutetun toimisto (Piiroinen, 2018).

4.1.3 Määrittely

Aikaisemmin esiteltyjen rajausten jälkeen tutkimusongelma voidaan tiivistää päätutkimuskysymykseen :

> **Miksi kaupungit eivät ilmoita kaikista havaitsemistaan kyberrikoksista poliisille?**

Tätä kysymystä lähdettiin selvittämään haastatteluin, joita tehtiin kaupunkien tietohallinnosta tai kyberturvallisuudesta vastaaville henkilöille tai heidän alaisilleen. Tutkimusongelmasta jodettiin seuraavat neljä ala-kysymystä, joiden

pohjalta haastattelukysymykset laadittiin. Haastattelukysymykset esitetään tarkemmin seuraavassa luvussa.

1. Miksi kyberrikoksista ilmoitetaan tai jätetään ilmoittamatta ?
2. Onko kaupungeilla olemassa olevaa suunnitelmaa kyberrikosten varalle ?
3. Onko kaupunkien työntekijöillä tarpeeksi tietoa kyberrikoksista?
4. Mitä poliisi voisi tehdä ilmoittamiskynnyksen madaltamiseksi ?

Kysymyksellä numero yksi tähdättiin ensisijaisesti tutkimuksen pääongelman vastaamiseen. Ainakin sillä oli tarkoitus selvittää, mitä mieltä haastateltavat asiantuntijat ja päättäjät olivat asiasta. Loput kysymykset voidaan nähdä ennen kaikkea antavan tukevaa materiaalia ensimmäiseen kysymykseen.

Kysymyksellä numero kaksi oli tarkoitus selvittää, kuinka hyvin kaupungit ovat varautuneet kyberrikoksiin ja muihin poikkeustilanteisiin. Näin pystyttiin tekemään karkeaa arviota organisaatioiden kyberrikoksiin varautumisesta ja mahdollisesti tehdä arvioita johtuisiko kyberrikoksien ilmoittamattomuus puutteista organisaation varautumisessa. Kaikki kaupungit eivät olleet halukkaita antamaan tarkkoja tietoja prosessista, mutta karkean tason kuva saatiin.

Kysymyksellä numero kolme oli tarkoitus saada jonkinlaista kuvaa siitä, onko kaupungin työntekijöillä tarpeeksi osaamista, jotta he voivat tunnistaa kyberrikokset ja osaavat toimia poikkeustilanteessa suunnitelman mukaan. Näin pystyi tekemään jonkinlaista arviota johtuisiko kyberrikoksien ilmoittamatta jättäminen siitä, että kaupunkien työntekijöillä ei ole tarpeeksi kokemusta ja osaamista. Päättäjät eivät pysty ilmoittamaan asiasta, jos he eivät saa tietoa tapahtumista.

Kysymyksellä numero neljä haettiin vastauksia toiseen poliisia kiinnostavaan kysymykseen. Timo Piiroisen (2018) mukaan poliisit ovat kehittämässä mm. kyberrikoksiin liittyviä ilmoittamispalveluita ns. kuluttajaystävällisemmiksi, jotta ilmoittamattomien kyberrikosten määrä saataisiin pienenemään. Neljännellä kysymyksellä annettiin haastateltaville mahdollisuus tuoda esiin mielipiteitään ja ehdotuksiaan asian tiimoilta.

4.2 Toteutettava tapaustutkimus

Tutkimusmetodologiaksi valittiin tapaustutkimus, koska tarkoituksena oli tutkia kyberrikostapauksien ilmoittamiseen liittyvää sosiaalista tilannetta ja prosessia. Mitä tehdään, kun kyberrikos havaitaan? Kuka tekee ja mitä ? Kuka päättää toimista? Kuinka kyberrikoksiin on varauduttu? Muun muassa Ben-basat ym. (1987) sekä Darke ym. (1998) ovat määrittäneen tapaustutkimuksen olevan sopiva tämän tyyppisiin tutkimuksiin, kuten luvussa 3. esitettiin.

Tutkimuksessa päädyttiin suorittamaan usean tapauksen tutkimus yhden tapauksen tapaustutkimuksen sijaan. Tämä tukee tutkimusongelmaa, jossa on tavoitteena tutkia tiettyä tilannetta ja pyrkiä saamaan aikaan yleinen kuva, jota

voidaan tietyin rajoituksin soveltaa muihin organisaatioihin. Noor (2018) ja Darke ym. (1998) ovat tapaustutkimusta käsittelevissä kirjoituksissaan ottaneet esille, että usean tapauksen tapaustutkimuksella saadaan paremmin yleistettäviä tuloksia.

Tutkimuksessa oli mukana yhdeksän kaupunkia. Yhden kaupungin kyberrikostapausten käsittely prosessi muodostaa tutkimuksessa yhden tapauksen. Yksi tutkimuksen kohteena oleva kaupunki muodostaa luonnollisen yksikön tutkimuksen mielenkiinnon kohteena olevassa tilanteessa.

Tutkimus toteutettiin Noorin (2008) esittämän tapaustutkimuksen mallia mukaillen, joka jakaa tapaustutkimuksen kolmeen osaan tutkimuksen valmistelun, kenttätyön ja analyysin sekä johtopäätöksen vaiheisiin. Tämä malli esitettiin aikaisemmin kuviossa 7.

Tutkimus aloitettiin tutkimusongelman ja sen ala-kysymyksien määrittelyllä ja tausta-aineiston haulla. Noorin (2008) mallista aloitus poikkeaa sillä, että varsinaista hypoteesia ei laadittu.

Seuraavaksi suunniteltiin haastattelukysymykset, haastattelun toteutustavat ja valittiin tapaukset. Haastattelukysymykset ja haastatteluiden toteutus esitellään tarkemmin seuraavassa luvussa.

Tapauksien valinnassa etsittiin Suomen isoimmista kaupungeista ihmisiä mukaan tutkimukseen. Tapauksia kerättiin ympäri Suomea, jotta mukaan saataisiin mahdollisimman laaja otos. Mukaan saatiin yhdeksän eri kaupunkia.

Seuraavaksi oli kenttätyön eli haastatteluiden teon ja analyysin aika. Haastatteluja tehdessä kerättiin ylös alustavia ideoita ja huomioita, joita pystyi käyttämään hyödyksi seuraavassa haastattelussa. Haastattelut ja muu materiaali litteroitiin ja tiivistettiin tapauskertomuksiksi. Kun kaikki haastattelut oli tehty, litteroinnit ja tiivistelmät viimeisteltiin.

Johtopäätöksien vaihe alkoi tiivistettyjen tapauksien koodauksesta, jotta toisiinsa liittyvät asiat löytyisivät helposti ja tapauksia pääsisi näin paremmin vertailemaan keskenään, mikä oli seuraavaksi vuorossa osana johtopäätöksien tekoa. Vertailun ja tyypittelyn jälkeen päästiin vetämään johtopäätökset yhteen ja keräämään ehdotuksia ja ideoita tutkimusongelmaan vastaamiseksi. Vaikka suoraa teoriaa ei muodostettukaan, laadittiin tutkimuksen pohjalta ehdotuslista toimenpiteistä, joilla tutkimusongelmaa voisi mahdollisesti ratkaista. Aineiston analyysissä ja johtopäätöksien teossa käytetyistä menetelmistä on kerrottu vielä tarkemmin seuraavassa luvussa.

4.3 Tutkimuksen toteutus

4.3.1 Haastattelu

Tutkimuksessa tarvittavat tiedot kerättiin pääasiassa puolistrukturoiduin haastatteluin. Tarkoituksena oli jättää tilaa tarkentaville kysymyksille sekä mahdollistaa vapaa keskustelun aiheeseen liittyen. Haastatteluja täydennettiin

erilaisin kirjallisin lähtein, jos haastateltavat olivat halukkaita niitä antamaan tutkimuksen käyttöön.

Haastattelukysymyksien luonnissa käytettiin apuna tutkimusongelman määritellyn yhteydessä luotuja neljää ala-kysymystä. Näin varmistetiin, että haastattelukysymykset vastasivat tutkimusongelmaan. Neljä alakysymystä olivat :

1. Miksi kyberrikoksista ilmoitetaan tai jätetään ilmoittamatta ?
2. Onko kaupungeilla olemassa olevaa suunnitelmaa kyberrikosten varalle ?
3. Onko kaupunkien työntekijöillä tarpeeksi tietoa kyberrikoksista?
4. Mitä poliisi voisi tehdä ilmoittamiskynnyksen madaltamiseksi ?

Näiden pohjalta laadittiin 12 haastattelukysymystä, jotka toimivat puolistrukturoidun haastattelun peruskysymyksinä ja kysyttiin kaikilta haastateltavilta. Nämä kaksitoista haastattelukysymystä olivat :

1. Kuka tekee päätöksen kyberrikoksista ilmoittamisesta?
2. Kuka tekee ilmoituksen kyberrikoksista ja millä tavalla?
3. Millä perusteella havaittuja kyberrikoksia arvioidaan?
4. Onko organisaatiolla suunniteltu prosessi ja toimintatavat kyberrikosten varalle?
5. Onko vastuuhenkilöistä päätetty?
6. Onko laadittu toiminnan jatkuvuuden takaavia suunnitelmia?
7. Onko laadittu kriiseistä palautumisen suunnitelmia?
8. Tietävätkö organisaation työntekijät kenelle ilmoittaa havaitsemastaan kyberrikoksesta?
9. Ovatko organisaatiossa työskentelevät tietoisia, mitkä ovat kyberrikoksia?
10. Onko henkilökuntaa koulutettu kyberrikoksiin liittyen?
11. Millä tavalla olisit yhteydessä poliisiin mieluiten?
12. Voisiko poliisi auttaa teitä jollain lailla enemmän kyberrikoksiin liittyen?

Kaikille haastateltaville lähetetiin nämä kysymykset etukäteen sähköpostitse. Kysymysten läpikäymisen helpottamiseksi haastattelukysymykset jaettiin tutkimusongelman ala-kysymysten mukaisesti nimettyjen otsikoiden alle. Liitteessä 1 on listattu haastattelukysymykset sellaisessa muodossa kuin ne lähetettiin haastateltaville.

Tutkimuksessa haastateltiin kunkin yhdeksän kaupungin kyberturvallisuuden parissa työskentelevää henkilöä. Haastateltavat toimivat kaupunkiensa tietohallinnon tai muun kyberturvallisuuden vastaavina tai heidän alaisuudessaan. Haastateltaviksi valikoitui sellainen ihminen, jolla oli kussakin kaupungissa heidän omasta mielestään eniten tietämystä asiasta.

Haastattelut toteutettiin sähköposti-, puhelinhaastatteluina tai niiden yhdistelmällä riippuen siitä, mikä haastateltavan usein kiireiseen aikatauluun

sopi parhaiten. Kaikille kuitenkin lähetettiin haastattelun peruskysymykset sähköpostitse. Näiden peruskysymysten lisäksi haastateltavilta kysyttiin täydentäviä kysymyksiä, jotka perustuivat heidän antamiin vastauksiin. Kysymysten lisäksi haastatteluissa oli mukana vapaampaa keskustelua aiheeseen liittyen. Puhelinhaastattelu -osuudet nauhoitettiin.

Haastatteluiden toteutuksessa pyrittiin ottamaan huomioon Myersin ja Newmanin (2007) esittämät haastatteluiden heikkoudet, jotka on esitelty luvussa 3.2.4. Haastattelut toteutettiin haastateltavien haluamaan aikaan ja haluamalla ravalla, jotta he tuntisivat olonsa mahdollisimman mukavaksi. Luottamuksellisuus otettiin esiin jo ensimmäisessä sähköpostissa ja tarpeen vaatiessa käytiin läpi vielä haastattelutilanteessa. Puolistrukturoitu haastattelu -menetelmä valittiin myös rentoutta ja improvisointia silmällä pitäen. Haastatteluissa käytiin läpi mm. määritelmiä, jotta väärinymmärrysten määrä puolin ja toisin pystyttiin minimoimaan. Haastattelijana pyrin ottamaan huomioon oman tekemiseni ja sanomiseni vaikutukset joka tilanteessa ja kirjoitin haastattelun aikana syntyneitä ajatuksia itselleni ylös.

Kaikkea ei kuitenkaan saatu pro gradun laajuuteen sopivaan tutkimuksen toteuttamisen puitteissa toteutettua. Näitä heikkouksia on käyty läpi tarkemmin luvussa 6. Haastatteluissa oli kuitenkin hyvä ilmapiiri ja haastateltavat olivat itsekriittisiä ja vaikuttivat avoimilta.

4.3.2 Aineiston analyysi

Kerätyn aineiston käsittely aloitettiin puhelinhaastattelujen litteroinnilla, jotta kaikki haastattelumateriaali saatiin kirjalliseen muotoon ja valmiiksi analyyseja varten. Haastatteluiden analyysissä käytettiin hyväksi tapauksien tiivistämistä ja koodausta. Tämän jälkeen aineistosta etsittiin yhteneväisyyksiä, säännöllisyyksiä ja teemoja vertailemalla tapauksia keskenään.

Analyysit aloitettiin tiivistämällä jokainen tapaus, eli jokaista kaupunkia koskeva materiaali, helpommin käsiteltäviksi kokonaisuuksiksi. Tiivistäminen tehtiin kirjalliseen muotoon. Tämän jälkeen tiivistetyt haastattelut koodattiin seuraavien aiheiden mukaan :

- Suora ilmoittamatta jättämisen syy
- Kaupunkien sisäisen ilmoittamisen prosessi
- Kaupunkien varautumiseen liittyvät suunnitelmat
- Kaupunkien ulkoistuksen tilanne
- Henkilökunnan osaaminen
- Kehitysehdotus poliisille
- Mieluisin yhteydenpitotapa

Koodatuista tiivistelmistä etsittiin tämän jälkeen säännöllisyyksiä, toistuvuutta ja kaavoja, jotta jonkinlaisia johtopäätöksiä pystyttiin tekemään. Vastauksista saatiin näin yhdistettyä tiettyjä teemoja ja ilmiöitä, joista saatiin vastauksia tutkimuskysymykseen ja sen ala-kysymyksiin. Haastatteluista kerättiin myös haastateltujen antamia kehitysehdotuksia poliisille yhteistyön parantamiseksi.

Lopuksi kaikista materiaaleista laadittiin vielä erillinen lista poliisille tavoista, joilla voisi olla mahdollista lisätä kyberrikoksista tehtyjen ilmoituksien määrää.

5 TULOKSET

Tässä kappaleessa esitetään tutkimuksen tulokset. Ensiksi käydään läpi haastatteluiden eli tapauksien tulokset tiivistettyinä läpi. Seuraavaksi kerätään yhteen haastatteluiden perusteella kerätyt syyt siihen, miksi kaikista tapauksista ei tehdä rikosilmoitusta.

5.1 Haastattelut tiivistettynä

Haastattelujen vastaukset on jaettu aikaisemmin esitettyjen tutkimuksen neljän ala-kysymyksen mukaan neljään osaan kyberrikoksista ilmoittamiseen, kyberrikoksiin varautumiseen, henkilöstön osaamiseen ja kehitysehdotuksiin liittyviin kysymyksiin. Neljä aikaisemmin määriteltyä alakysymykset olivat:

1. Miksi kyberrikoksista ilmoitetaan tai jätetään ilmoittamatta?
2. Onko kaupungeilla olemassa olevaa suunnitelmaa kyberrikosten varalle?
3. Onko kaupunkien työntekijöillä tarpeeksi tietoa kyberrikoksista?
4. Mitä poliisi voisi tehdä ilmoittamiskynnyksen madaltamiseksi?

Haastatteluista valmistettiin tiivistelmät, jotka sen jälkeen koodattiin. Vastaukset esitetään tiivistetysti myös taulukko muodossa, jossa yhdessä taulukossa käsitellään yhteen alakysymykseen liittyvät vastaukset tapauksittain eli kaupungeittain.

Kyberrikoksista ilmoittamiseen liittyvien kysymysten vastauksia lukiessa voi huomata, että vastuu päätöksistä kuului pääasiassa tietohallinnon, tietoturvallisuuden tai turvallisuus osaston päälliköille tai tietosuojavaltuutetulle. Kaupunki A:lla toimii erillinen kriisiryhmä, joka koostuu tietohallinnon, tietoliikenteen ja viestinnän osastoilta valituista henkilöistä sekä tietosuojavastaavasta ja sen toimialan edustajasta, jota havaittu tapahtuma koskee. Kaupunki E:llä taas lopullinen päätösvastuu on kaupungin lakimiehellä.

Haastatteluiden mukaan varsinaisen ilmoituksen poliisille tekee usein sama taho, joka päättää ilmoittamisen tekemisestä. Poikkeuksena on Kaupunki I, jossa tietoturvapäällikkö tai tietosuojavastaava antaa vastuun ilmoituksen tekemisestä kaupungin lakimiesosastolle. Toinen poikkeus on Kaupunki F, jossa tietohallintojohtaja antaa vastuun ilmoituksen tekemisestä tietoturvapäällikölle.

Kyberrikoksien vakavuuden arviointitavat erosivat haastatelluilla kaupungeilla, vaikka yhteneväisyyksiäkin löytyi. Vaikuttavuus- ja taloudellinen arviointi olivat yleisimpiä mainittuja tapoja. Kaupungilla H arviointi toteutetaan määritellyn arviointiprosessin mukaan. Kaupungit E ja I taas luottavat asiantuntija-arvioihin.

Tiedot kaikkien haastatteluun osallistuneiden kaupunkien kyberrikoksien ilmoittamiseen liittyvistä käytänteistä ja vastuuhenkilöistä löytyvät tiivistetysti taulukosta 1.

TAULUKKO 1 Kyberrikoksista ilmoittaminen

Kaupunki	**Kuka päättää?**	**Kuka tekee ilmoituksen ja miten?**	**Miten kyberrikoksia arvioidaan?**
Kaupunki A	Kriisiryhmä. Kuuluu mm. tietohallinto ja tietosuojavastaava	Kriisiryhmä päättää. Verkossa	Laajuus Ketä koskettaa?
Kaupunki B	Tietosuojavastaava tai tietohallintojohtaja	Tietosuojavastaava, tietohallintojohtaja tai muu esimies Verkossa tai suoraan	Taloudelliset ja toiminnalliset vaikutukset
Kaupunki C	Tietoturvavastaava tai palveluntuottajan edustaja	Tietoturvavastaava tai palveluntuottajan edustaja Suoraan tai verkossa	Vaikuttavuusarviointi, riskianalyysi, kriittisyys
Kaupunki D	Tietohallintojohtaja	Tietohallintoyksikkö	ICT-tuottajan kyberturvallisuustilannekuvan ja tietohallinnon digiturvallisuuden tilannekuvan mukaan
Kaupunki E	Kaupungin lakimies	Kaupungin lakimies Tapauskohtaisesti	Laadullinen arvio, asiantuntija-arvio
Kaupunki F	Tietohallintojohtaja	Tietoturvapäällikkö	Vaikuttavuusarviointi Taloudelliset seikat
Kaupunki G	Tietoturvapäällikkö, tietosuojavastaava tai tietohallinto	Tietoruvapäällikkö, tietosuojavastaava tai tietohallinto, kirjallisesti	Vaikuttavuusarviointi, taloudellinen arviointi, asiakkaiden yksityisyys
Kaupunki H	Tietoturvapäällikkö	Tietoturvapäällikkö Verkossa	Arviointi tiimin suorittaman arviointiprosessin mukaan.
Kaupunki I	Tietoturvapäällikkö ja tietosuojavastaava	Kaupungin lakimiesyksikkö	Tietoturvapäällikön ja tietosuojavastaavan tekemä arvio.

Kyberrikoksiin varautumisen aste oli kaupungeissa haastatteluiden mukaan melko samankaltainen. Kaikissa haastatelluissa kaupungeissa oli määritelty vastuuhenkilöt poikkeustilanteiden varalle, vastuuhenkilöille oli nimetty varahenkilöt ja kaikkien kaupunkien suunnitelmiin kuului tarvittaessa rikosilmoitusten tekeminen poliisille. Lähes kaikissa kaupungeissa oli kaikki kysytyt suunnitelmat ainakin osittain tehtyinä tai niiden laadintaa oli tarkoitus aloittaa lähiaikoina. Esimerkiksi Kaupunki A:n ja Kaupunki C:n edustajat mainitsivat osan dokumentaatiosta olevan vielä keskeneräisiä. Kaupunki A:n edustaja kertoi myös, että heillä on tarkoitus saada loput mainituista suunnitelmista pian laadittua.

> Ei vielä [toiminnan jatkuvuuden ja kriiseistä palautumisen suunnitelmia], mutta on tiedostettu, että se tulee tehdä lähiaikoina. (Kaupunki A)

Kaupunki C oli poikkeus siinä, että heiltä puuttui kriiseistä palautumisen suunnitelmat. Kaupunki F oli toinen, jonka mukaan kriiseistä palautumisen suunnitelmien laadinta vaati sen verran päivittämistä, että sitä ei voida sanoa juurikaan olevan.

> ”Ei oikeestaan, vois sanoa sen, että vaikka meillä on tohon [kriiseistä palautumisen suunnitelmiin] jo tehty aika paljon, mutta ympäristön laajuuden vuoksi niin se on sitä jatkuvaa, että sitä pitää, niin kun jatkuvasti kehittää ja tehdä niitä harjoituksia.” (Kaupunki F)

Muidenkin haastateltujen kaupunkien edustajat tunnistivat tarpeen suunnitelmien jatkuvalle päivittämiselle. Kaupunki E oli tehnyt päivityksiä omiin malleihinsa viimeksi vuoden 2018 loppupuolella. Silti suunnitelmien päivittäminen tarpeeksi usein koettiin joidenkin kaupunkien edustajien mielestä haasteeksi. Esimerkiksi Kaupunki C:n edustaja kuvasi asiaa seuraavasti:

> ”Mutta tää on jännä tää valmius asia, mikä on tullut monessa muussakin esille, että pitää olla melkein harjoitus- tai joku muu vastaava, joka ottaa esille sen, että näitä oikeasti päivitetään, muuten se sykli on harvempi kuin joka vuosi, milloin näitä käydään läpi.” (Kaupunki C)

Kaupunkien E ja F:n edustajat toivat myös esiin suunnitelmien toteuttamisen harjoitukset. He kertoivat harjoittelevansa suunnitelmien toteuttamista säännöllisesti. Kaupunki F:n edustaja kertoi, että heillä otetaan kerrallaan tietty joukko harjoitteluun mukaan.

Jatkuvuuden ja kriiseistä palautumisen suunnitelmia on tehty myös muuhun kaupunkien toimintaan liittyen, sillä siitä on olemassa aikaisempaa lainsäädäntöä. Nämä asiat toivat mm. Kaupunki C:n, B:n ja A:n edustajat haastatteluissaan.

> ”--valmisharjoituksiahan on säännöllisin väliajoin, tässä joitakin vuosia takaperin yhtenä aiheena oli kyberuhka.” (Kaupunki C)

”Meillähän on viranomaisten välillä yhteistyötä näiden jatkuvuussuunnitelmien osalta jo lakisääteisestikin, että [ei] sitten välttämättä tällaisen tietoturvaa liittyen. --” (Kaupunki B)

Pelastuslaitoksella tosin on suunnitelmat olemassa, sillä ne kuuluvat osaksi valtakunnallista pelastussuunnitelman toimintaa. (Kaupunki A)

Haastateltujen kaupunkien antamat vastaukset kyberrikoksiin varautumiseen liittyviin suunnitelmiin ja vastuuhenkilöihin liittyen on luettavissa tiivistetysti taulukosta 2.

TAULUKKO 2 Kyberrikoksiin varautuminen

Kaupunki	**Vastuuhenkilöt**	**Suunnitelmat kyberrikostilanteiden varalle**	**Toiminnan jatkuvuuden suunnitelmat**	**Kriisistä palautumisen suunnitelmat**
Kaupunki A	Kyllä	Dokumentaatio kesken	Ei vielä. Tehdään lähiaikoina	Ei vielä. Tehdään lähiaikoina
Kaupunki B	Kyllä	Kyllä, osa riskienhallintaa	Kyllä	Kyllä
Kaupunki C	Kyllä	Dokumentaatio ja ohjeistukset kesken	Kyllä	Ei
Kaupunki D	Kyllä	Kyllä	Kyllä	Kyllä
Kaupunki E	Kyllä	Kyllä	Kyllä	Kyllä
Kaupunki F	Kyllä	Kyllä, osa tietovuoto prosessia	Kyllä	Ei oikeastaan Vaatii kehittämistä.
Kaupunki G	Kyllä	Kyllä	Kyllä	Kyllä
Kaupunki H	Kyllä	Kyllä	Kyllä	Kyllä
Kaupunki I	Kyllä	Kyllä	Kyllä	Kyllä

Henkilöstön osaamiseen liittyvissä kysymyksissä vastaukset olivat pääpiirteissään samankaltaisia. Nämä vastaukset löytyvät tiivistetysti taulukossa 3.

Kaikissa haastatelluissa kaupungeissa ainakin osa henkilöstöstä on saanut tietoturvallisuuteen ja tietosuojaan liittyvää koulutusta ja heillä pitäisi olla tiedossa kenelle pitää ilmoittaa havainnoista.

”Joo, meillä on prosessikuvaukset ja henkilöstöä on koulutettu. Intrassa on ohjeita siitä, miten toimitaan näissä tilanteissa ja esimies porukka on koulutettu infotyyppisesti asiaan. Kyllä tätä sanaa on levitetty varsin hyvin.” (Kaupunki B)

Jokainen on velvollinen käymään koulutuksen, yleensä kun tulee taloon. Tietohallinto järjestää koulutusta noin 2-4 vuoden välein. (Kaupunki D)

Kaupungit D, E ja G, toivat esille, että heillä tietoturvaan ja tietosuojaan liittyvää koulutusta järjestetään säännöllisesti. Näistä poiketen Kaupungit C ja H taas kertoivat, että heillä henkilöstön osaaminen tarvitsisi päivittämistä.

Koulutuksen määrästä huolimatta lähes kaikki haastatellut, olivat sitä mieltä, että kyberturvallisuuden tietoisuuden taso vaihteli kaupungin henkilöstön sisällä. Tähän nähtiin yhdeksi syyksi kaupunkien henkilökunnan heterogeenisuus. Kaupungeilla työskentelee paljon hyvin erilaisia ihmisiä hyvin erilaisissa työtehtävissä, jolloin koulutuksen saaminen koko henkilökunnan kattavaksi on vaikeaa. Kuten Kaupunki I:n edustaja kertoi.

> ”--koulutuksien osalta meillä on siis tarjolla henkilöstölle tietoturvaan, tietosuojaan ja yleensä turvallisuuteen liittyviä verkkokursseja sekä tilaisuuksia/koulutuksia. Valitettavasti millään näillä keinoilla emme tavoita koko henkilöstöä eli aina löytyy niitä henkilöitä, jotka eivät tiedä miten esim. tietoturvarikkomuksista pitäisi ilmoittaa eteenpäin.” (Kaupunki I)

Kaikki haastateltavat tunnistivat joitain ongelmia, joiden syynä on henkilöstön tietoisuuteen liittyvät puutteet ja tarpeen toimenpiteille asian parantamiseksi. Ongelmat näkyvät esim. siinä, että kaikista tapahtumista ei välttämättä tule ilmoitusta päättäville tahoille asti, koska jokin luokitellaan vaarattomammaksi kuin se on. Kaupunki D:n edustajan mukaan taas kaikki työntekijät eivät vielä ymmärrä, että kyberuhkien torjuminen ei ole pelkästään alan ammattilaisten asia, vaan vastuu kuuluu kaikille.

> ”Jotenkin työntekijät kokevat sen kuuluvan ammattilaisille, vaikka se kuuluu jokaiselle tasolle. Sitä tässä yritetään jalkauttaa organisaatiossa eteenpäin.” (Kaupunki D)

Useimmissa haastatelluissa kaupungeissa henkilöstö on koulutettu ottamaan tietoturvaan ja tietosuojaan eli mahdollisiin kyberrikoksiin liittyvistä havainnoista yhteyttä IT-lähitukeen, esimieheen tai tietohallintoon. Tältä toiselta tasolta tiedot välittyvät sitten eteenpäin kunkin kaupungin päättävälle taholle. Kaupunkien C ja E edustajat ottivat esiin ongelman, että kaikista vakavammista havaituista ongelmista ei tule tietoa rikosilmoituksesta päättäville henkilöille asti.

> ”--ei osasta niistä tulee ilmoituksia. Osassa painetaan vaan deleteä ja oletetaan, että tämä on normaalia, vaikka kyseessä olisi oikeasti ollutkin isompikin uhka.” (Kaupunki C)

> ”--jos henkilö huomaa sen ja ilmoittaa mikrotuelle tämmöistä alkaa tuleen, niin se helposti jää siihen, että [lähituki] poistaa ne viestit ja se oli siinä se case. -- sit todetaan vaan että nyt on päässyt jostain suodattimesta läpi ja kiristetään suodatinta ja tavallaan sitten helposti jää sinne lähituen tasolle.” (Kaupunki E)

Osa jää ilmoittamatta jo työntekijän tasolle ja osa sitten seuraavalle tasolle. Tulleiden ilmoitusten suodattamisesta ja niihin liittyvistä ongelmista huolimatta Kaupunki E:n edustaja oli sitä mieltä, että tietylle ilmoitusten

niputtamiselle ja esikäsittelylle on tarvetta, sillä tapahtuma määrä voisi kasvaa liian suureksi.

> ”Semmoista ei tosiaan pysty oleen et kaikki asiat ylöspäin raportoitais -- et sitä pitäisi pystyä sitten ilmiötasolle niputtamaan ja sit tavallaan löytää sieltä ne missä on oikeasti kyse jostain vakavammasta kuin pelkästään vaikka spämmistä tai sitten niin kuin tämmöisestä kohdentamattomasta mallista.” (Kaupunki E)

Haastatellut kaupunkien edustajat arvioivat henkilökuntansa kyvyn tunnistaa tietosuoja ja tietoturva poikkeamia olevan kuitenkin ainakin melko hyvä kaikista aikaisemmin manituista ongelmista huolimatta.

Käsitteistä tietoturvan ja tietosuoja uskottiin olevan tuttuja, mutta kyberrikos-termin uskottiin kuitenkin olevan vieraampi. Kaupunki I:n edustaja kertoi, että heillä ei käytetä kyber-sanaa yhden verkkokurssin nimeä lukuun ottamatta sen monitulkintaisuuden takia. Tämä monitulkintaisuus tuli esille muutenkin haastatteluissa. Kyberrikoksen käsite aiheutti joissain haastatelluissakin hämmennystä ja kysymysten väärin ymmärtämistä, mikä viittaa siihen, että sen käyttöä ei näytä omaksuneen kaikki ammattilaisetkaan.

TAULUKKO 3 Henkilöstön osaaminen

Kaupunki	**Kenelle ilmoitetaan havainnoista?**	**Tunnetaanko kyberrikokset?**	**Onko henkilökuntaa koulutettu?**
Kaupunki A	Kyllä, tietohallintoon	Osittain	Osittain
Kaupunki B	Kyllä, esimiehelle, myös muille	Kyberrikosta ei Tietoturva ja tietosuojarikkomukset kyllä	Kyllä
Kaupunki C	Osittain	Osittain Vaatii päivittämistä.	Osittain Vaatii päivittämistä
Kaupunki D	Kyllä	Tietoturva, kyllä Kyber-asiat osittain	Kyllä, säännöllistä velvollisuus
Kaupunki E	Kyllä, lähitukeen	Kyllä, osittain	Kyllä, säännöllistä
Kaupunki F	Kyllä, esimiehelle tai suoraan tietohallintojohtajalle tai tietoturvapäällikölle	Osittain	Osittain, panostettu
Kaupunki G	Kyllä, helpdesk	Kyberrikos termi vieras Tietoturva asioista osittain	Osittain, säännöllistä
Kaupunki H	Kyllä	Pääasiassa kyllä	Osittain
Kaupunki I	Kyllä helpdesk, esimies, tietosuojavastaava tai tietohallintojohtaja	Kyber-termi vieraampi Tietoturva, tietosuoja tutumpia	Osittain

Kehitysehdotuksiin liittyvissä kysymyksissä tuli esiin muutamia toistuvia, mutta myös joitain yksittäisiä ehdotuksia. Vain yhdellä haastatelluista ei ollut kehitysehdotuksia ollenkaan ja monilla taas oli niitä useita. Poliisille ilmoittamiseen ja kehitysehdotuksiin liittyvät vastaukset näkyvät tiivistetysti taulukossa 4.

Useimmin toistunut kehitysehdotus koski **poliisin vasteaikaa**, eli aikaa mikä kuluu ilmoituksen tekemisestä siihen, että poliisista otetaan yhteyttä. Tämän otti esille neljä haastatelluista. Pitkät yhteydenottoajat ja niiden yhteydessä usein näkyvät tutkimukseen tehdyt rajaukset aiheuttivat haastateltujen mielestä ongelmia ja vaikuttivat muutamien mukaan myös halukkuuteen olla yhteydessä poliisiin.

> ”-- jos vaste poliisin suunnasta on huono, on turhauttavaa tehdä ilmoituksia, jotka vievät työaikaa ja resursseja, jos on tiedossa, että poliisi ilmoittaa vuoden päästä, että ei ota tapausta tutkintaan --” (Kaupunki G)

> ”-- joskus poliisi kysyy jotain tietoja vasta, kun tapahtumasta on kulunut jo pitkä aika esim. useampi kuukausi, jona aikana tapahtumaan liittyvät lokit tai varsikin kameratallenteet on jo usein poistettu.” (Kaupunki I)

> ”-- kun ne joutuu niitä [rajauksia] tekemään niin kyllä se vähän niin kun vähentää sitä motivaatiota, et kannattaako sitä [ilmoitusta] tehdä, jos sitten poliisin resurssit ei riitä tutkimaan sitä massajuttua.” (Kaupunki E)

Vasteajan lisäksi kehitysehdotukset keskittyivät poliisin ja kaupunkien väliseen yhteistyön ja viranomaisyhteistyön parantamiseen ja keinoihin, joilla poliisi voisi osallistua yleisen kybertietoisuuden parantamiseen.

Yhteistyön kehittämiseen liittyviä parannusehdotuksia olivat kommunikaation lisääminen, jälkitiedottamisen parantaminen ja esiselvitykseen liittyvän käsikirjan luominen. Poliisin **jälkitiedottamisen puute** koettiin ongelmaksi ja jopa poliisin kanssa asioinnin motivaatioita vähentäväksi tekijäksi samalla tavalla kuin aikaisemmin mainitut pitkät vasteajat ja tutkinnan rajaaminen.

> ”Täällä paikan päällä niitä on tosi harvoin kuultu jälkeenpäin niistä [ilmoitetuista tapauksista], mitään niin ehkä tämmöinen, niin kuin jälkitiedottaminen sitten yhteyshenkilölle voisi olla hyvä.” (Kaupunki B)

> ”Kaikesta ei itseasiassa oo mulle aina tullut tietoo. Et katsoin tossa noita ilmoituksia, mitä me ollaan tehty, niin [osaan ei ole] ikinä kontaktoitu meitä sen ilmoituksen jälkeen -- ” (Kaupunki G)

Tarve esiselvitystä käsittelevän kirjan aikaansaamisesta tuli esille Kaupunki E:n haastattelussa. Hänen ajatuksenansa oli, että tähän käsikirjaan listattaisiin toimenpiteitä, mitä kaupungin tai organisaation tarvitsisi itse tehdä ennen poliisin tutkintaa. Siinä kerrottaisiin mm. mitä tietoa tarvitsisi kerätä ja missä

muodossa tiedon pitäisi olla. Näin kaupungit osaisivat toimia oikein ja tarvittavaa tietoa ei katoaisi tai todistusaineiston koskemattomuus kärsisi.

Haastatteluissa ehdotettiin myös **kommunikaation lisäämistä** yleisesti. Esimerkiksi Kaupunkien A, D ja E edustajat toivoivat poliisin kertovan enemmän omista toiveistaan, tavoitteistaan ja avaavan asiaa **poliisin näkökulmasta**.

Kaupunki G ehdotti yhteistyön parantamista eri poliisilaitosten ja muiden poliisin osastojen tietopyyntöihin liittyvien **toimintatapojen yhtenäistämisellä**. Hänen kokemustensa perusteella eri laitoksilla on nykyään erilaisia toimintatapoja, mikä hankaloittaa poliisin kanssa asioimista.

Vaikka poliisin toimintaa kritisoitiin monellakin tavalla, oli osa haastateltavista tyytyväinen poliisiin. Kaupunki F:n edustaja ei keksinyt mitään parannettavaa poliisin toiminnassa. Kaupunkien B, E, H ja I edustajat totesivat myös, että vaikka ongelmiakin on, niin pääasiassa yhteystyö toimii hyvin varsinkin paikallispoliisin kanssa.

Kyberturvallisuuden tilannetietoisuuden parantamiseen liittyviä ehdotuksia olivat case-kuvaukset, koulutustilaisuuksien järjestäminen, kansallisen apua ja neuvoja tarjoavan puhelinpalvelun luominen ja kybertoimintaympäristön tilannekuvan kehittäminen ja laajempi jakaminen.

Kaksi kaupunkia ottivat esiin oikean elämän **case-kuvaukset,** joiden kautta kaupunkien edustajat pääsisivät tutustumaan oikean elämän tapauksiin. Mielenkiintoa olisi erityisesti case–kuvauksien antamiin opetuksiin ja vastauksiin kysymyksiin: miksi näin tapahtui, miten toimittiin ja miten sen olisi voitu estää. Kaupunki C:n edustaja uskoi näiden kasvattavan tietoisuutta ja antavan parempaa kuvaa, mitä kybermaailmassa tapahtuu. Kaupunki E:n edustaja otti esiin samoja asioita ja lisäsi vielä, että olisi kaikille tahoille hyödyllistä jakaa poliisin tietämystä.

> ”Tykkäisin, jos tulisi näitä niin kun caseja niin niistä olis niin kun sinällään hävitetty, mihin se kohdentui tai muuta, mutta tulisi caseja, jotka on todella tapahtunut, koska ne on niitä parhaita, mitkä sitten herättää.” (Kaupunki C)

> ”Poliisillahan on ihan valtava se hyvä kuva siitä, että miten tekijä toimii tuolla bitti-maailmassa, mut ei meillä muilla vielä, saatikaan sitten julkishallinnon ulkopuolisilla organisaatioilla, ei voi olla sitä tietoa, et miten tämmöinen tekijä [hakkeri yms.] toimis.” (Kaupunki E)

Kaupunki C ehdotti, että nämä case-kuvaukset voisivat olla saatavilla kirjallisena, mutta kaupunki E:n edustaja taas ehdotti, että niiden ympärille voisi rakentaa esimerkiksi KRP:n pitämiä koulutustilaisuuksia.

Kaupunkien A ja D edustajat toivoivat poliisin järjestävän kyberturvallisuuteen liittyviä **koulutustilaisuuksia** myös **yleisemmästä näkökulmasta**. Aiheina voisi olla esimerkiksi, miten kyberhyökkäykset näkyvät poliisille niin paikallisesti kuin valtakunnallisestikin tai miltä kyberturvallisuuden tilannekuva näyttää tällä hetkellä.

Kaupunki C:n edustaja ehdotti kansallisen **auttavan puhelimen** perustamista, jonka kautta julkisensektorin organisaatioilla ja yrityksillä olisi

mahdollista saada yhteys sellaiseen poliisiin, joka kohtaa kyberrikoksia jokapäiväisessä työssään, tuntisi hyvin sen hetken uhat ja osaisi antaa joitain yleisiä neuvoja. Hän uskoi, että tällä tavalla voisi paikata esimerkiksi paikallispoliisilla mahdollisesti ilmenevää kyberrikoksiin liittyvän osaamisen henkilöitymisestä aiheutuvia ongelmia.

Kybertoimintaympäristön tilannekuvan aikaisempaa laajempi jakaminen tuli esille poliisin koulutustilaisuuksiin ja seminaareihin liittyvässä kohdassa, mutta Kaupunki E:n edustaja toi esille ajatuksen siitä, että kybertoimintaympäristön tilannekuvaa kehitettäisiin kokonaisuudessaan. Hänen mielestään voisi olla hyvä idea, jos kybertoimintaympäristöstä annettaisiin tietoa **ilmiötasolla** kampanjatason sijaan. Arvioiden tekeminen voisi olla silloin helpompaa.

> ”-- jos esimerkkinä laittaa vaikka laittaa suojelupoliisin terrorismiuhkatason niin, että jos se on nyt tällä hetkellä kohonnut niin, mitä meidän kybertoimintaympäristö sanoo. Minkä tyyppinen uhkamaisema meillä sielä on, niin siitä ei ole saatavissa sellaista pureksittua niin kuin selkeetä arviota, että missä me mennään niin kun yhteiskunnan tasolla.” (Kaupunki E)

Kaupunki E:n edustaja toi haastattelussa esille myös laajempia ehdotuksia. Hän heitti ilmaan ehdotuksen, että voisiko poliisi kerätä kyberrikoksiin liittyvää tietoa ja tilannekuvaa jonkin **muun ilmoitustyypin** kautta kuin rikosilmoituksen, missä ei olisi esitutkinnan velvollisuutta.

> ”-- jos sulla on case, jossa voidaan suoraan jo sanoa, että tää on kiinalainen hakkeri, jota ei ikinä saada kiinni. Niin onko se tutkintapyynnön tekeminen siitä kiinalaisesta hakkerista, jota on nolla prosentin mahdollisuudet saada se kiinni ja rikosoikeudelliseen vastuuseen, niin onko se [rikosilmoitus] oikee tapa tuottaa tilannekuvaa--” (Kaupunki E)

Toinen hänen ehdotuksensa koski valtion strategia-tasoa. Hänen mielestään, olisi hyvä, että Suomella olisi julkisen sektorin organisaatioille määritelty varautumisen minimi taso. Päätös siitä minkälaisiin tapauksiin varaudutaan vaikuttaa kuitenkin suuresti kustannuksiin.

Kehitysehdotusten lisäksi haastatteluissa kysyttiin mieluisinta asiointikanavaa poliisin kanssa. Vaikka monet mainitsivatkin mieluisimman yhteydenottovan riippuvan mm. tapauksen vakavuudesta viiden kaupungin edustajat ilmoittivat suosituimmaksi ilmoittamistavaksi internetin kautta joko lomakkeella tai sähköpostitse. Sähköposti mainittiin mieluiseksi tavaksi neljän kaupungin haastatteluissa. Kaksi kaupunkia taas ilmoittivat mieluisimmaksi tavaksi myös suoran yhteydenoton poliisille esimerkiksi soittamalla. Suoran yhteydenoton vahvuutena nähtiin vastauksen saamisen nopeus ja mahdollisuuden pyytää apua ja neuvoja heti.

> ”Kyllä on pakko tunnustaa, että todella pienimuotoisissa voisi täyttää sen lomakkeen, mutta tosi nopeasti mulla on se puhelin kädessä. Koska siis tilanne on sen verran, ehkä jotenkin uusi itsellekin, että jos jotain voisi siinä nopeesti tehdä tai vaikut-

taa, niin sen haluaisi kuulla siinä vaiheessa eikä kolmantena päivänä ensimmäisestä yhteenotosta." (Kaupunki C)

Muista poiketen Kaupunki A esitti toiveen siitä, että kaupunkien ei tarvitsisi ottaa yhteyttä kuin yhteen tahoon Viestintävirastoon tai Tietosuojavaltuutetulle, mistä tieto menisi myös poliisille ilman erillistä ilmoitusta.

TAULUKKO 4 Kehitysehdotukset

Kaupunki	**Miten mieluiten ilmoittaa?**	**Mitä kehitysehdotuksia?**
Kaupunki A	Ilmoituksen ulkoistus Tietosuojavaltuutetun toimistolle tai viestintä virastolle. Sähköpostilla Yhdellä ilmoituksella kaikkialle.	Poliisi keräämän tilannekuvan jakaminen. Poliisi omien toiveiden esittäminen. Viranomaisyhteistyön kehittäminen.
Kaupunki B	Tapauskohtaista Verkossa tai sähköpostitse	Poliisin tekemä jälkitiedottaminen ja vasteajat.
Kaupunki C	Puhelimitse	Kansallinen puhelinnumero, josta vastaisi kyberrikokset tunteva poliisi ja josta saisi apua. Case- kuvauksien keruu, anonymisointi ja jakaminen.
Kaupunki D	Puhelimitse tai sähköpostitse	Poliisin järjestämät koulutustilaisuudet.
Kaupunki E	Suoraan tai tapauskohtaisesti	Kansallisen minimitason määritys. Viranomaisyhteistyön kehittäminen Poliisin vasteajan lyhentäminen. Esiselvitys-käsikirjan luominen. Case-kuvauksien esittäminen koulutuksissa. Kybertoimintaympäristön uhan aste
Kaupunki F	Verkossa tai suojattu sähköposti	Ei ole
Kaupunki G	Verkossa	Viranomaisyhteistyön parantaminen. Poliisien toimintatapojen yhtenäistäminen. Vasteajan lyhentäminen.
Kaupunki H	Verkossa	Asiointi on sujunut hyvin, vaikka hitautta on havaittu.
Kaupunki I	Verkossa	Vasteajan lyhentäminen. Ilmoittamislomake voisi olla yksinkertaisempi

5.2 Miksi kyberrikoksista ei ilmoiteta?

Haastatteluista saaduista vastauksista pystyy löytämään kaksi isoa syytä, miksi ilmoituksia ei tehdä. Yksi on se, että **kaupunkien johto ja ilmoitusten tekemisestä päättävät ihmiset eivät saa tietää kaikista havaituista tapauksista**. Toinen on **poliisille tehtävään rikosilmoitukseen liittyvät ongelmat**. Seuraavaksi tarkastellaan näitä syitä tarkemmin.

5.2.1 Tiedonkulku

Haastatteluissa löytyi muutama syy siihen, että kaupunkien johto ei kuule kaikista havaituista kyberrikostapauksista. Osa syistä johtuu siitä, että useammassa haastatellussa kaupungissa on ilmoittamisen sisäisessä prosessissa yksi tai useampi väliporras. Työntekijät eivät siis useinkaan ole suoraan yhteydessä ilmoittamisen tekemisestä päättävään johtoon. Näille välitasoille on tarvetta sillä useissa haastatelluissa kaupungeissa ei haluta työntekijöiden olevan suoraan yhteydessä johtoon, vaikka taas toisissa kaupungeissa sitä ei pidetty ongelmallisena.

> ”Semmoista ei tosiaan pysty oleen et kaikki asiat ylöspäin raportoitais niin kuin ihan tämmöisen manuaalisen mallin mukaan, et mehän hukuttas täällä ja johto varsinkin siten hukkuis siihen.” (Kaupunki E)

> Toimimme yhden luukun (kahden luukun) periaatteella, eli henkilöstö ilmoittaa aina tapauksesta helpdeskiin. Poikkeuksena tästä ovat esimerkiksi epäilyt henkilötietojen väärinkäytöksistä tai siihen liittyvistä poikkeamista. (Kaupunki G)

Yksi syy ilmoittamatta jättämiseen näyttää olevan näiden välitasojen osaamisessa. **Vakavia tapauksia ei aina tunnisteta vakavaksi** vaan tiedot hävitetään vähemmän vakavien kanssa. Esimerkiksi kohdennetummat sähköpostilla tulleet tietojenkalastelukampanjat poistetaan kohdentamattomien kalastelukampanjoiden mukana.

> ”--vahinkojen rajaamiseen ja ehkä tämmöiseen niin kun sit todetaan vaan että nyt on päässyt jostain suodattimesta läpi ja kiristetään suodatinta ja tavallaan sitten helposti jää sinne lähituen tasolle näin isossa organisaatiossa.” (Kaupunki E)

Kaupunki E:n edustaja tunnisti ongelmaksi myös yleisen **teknisen kyberturvallisuuden osaamisen puutteet** ja teknisen osaamisen saamisen vaikeudet. Teknisen kyberturvallisuuden osaajille tarjotaan korkeammat palkat yksityisellä puolella ja kaupunkien on vaikea kilpailla heistä.

5.2.2 Ilmoituksen tekemisen ongelmat

Erilaiset ilmoituksen tekemiseen liittyvät ongelmat muodostivat haastatelluista merkittävimmät syyt sille, että motivaatio ilmoittaa poliisille havaittuja kyberrikoksia laskee. Haastatteluista pystyi nostamaan esille kolme ongelmaksi koettua asiaa, jotka on listattu alla.

1. Poliisille ilmoittamisesta koetaan olevan enemmän haittaa kuin hyötyä
2. Pitkät vasteajat
3. Poliisia ja heidän vähäisiä resurssejaan ei haluta tuhlata turhien tapausten tutkimiseen.

Ilmoittamisen tekemisen haitoiksi nousivat haastatteluissa ilmoitusten valmisteluun ja sisäiseen tutkintaan kuluva aika, johon ei koeta saavan poliisilta tarpeeksi suurta vastinetta. Poliisi saattaa esimerkiksi rajata tapauksen tutkimusta tai päättää olla tutkimatta asiaa kokonaan, jolloin esimerkiksi Kaupunki G:n edustajan mukaan, tuntuu siltä, että he ovat kaupungilla tehneet turhaa työtä.

Poliisin pitkiksi koetut vasteajat tehtyihin ilmoituksiin olivat usean haastattelun mielestä ongelmallisia. Ongelmia aiheutui erityisesti siitä, että, jos poliisi palaa ilmoitettavaan asiaan vasta pitkän ajan kuluttua, on tarvittavaa todistusmateriaalia kuten kamerakuvaa, lokeja yms. saattanut jo hävitä, sillä niitä tallennetaan usein vain tietyn ajan. Kaupunki G:n edustaja toi esiin, että osaan heidän ilmoituksistaan ei ole koskaan tullut vastinetta. Vasteajat mainitsevat myös sellaisten kaupunkien edustajat, jotka muuten sanoivat olevan tyytyväisiä poliisin toimintaan.

Vasteajoista ja julkisesta keskustelusta on voinut tehdä päätelmiä poliisin resursseista. Useampi haastatelluista kertoi, että pienet tai vain vähäistä vahinkoa aiheuttavat tapaukset jätetään ilmoittamatta, jotta ne eivät kuormittaisi turhaan niin kaupunkeja itseään kuin poliisiakaan.

> Ihan yksittäisistä pienistä ei ilmoiteta. Eli kaikki dokumentoidaan ja jos havaitaan että se on osa isompaa niin asia arvioidaan ja tämän jälkeen ilmoitetaan viranomaisille (Kaupunki A)

> Varsinaisesti poliisille ilmoitettavia kyberrikoksia tapahtuu todella vähän. (Kaupunki H)

> ”--ei me sitten tehdä, kun sellaisissa merkittävissä tapauksissa asioista ilmoituksia, että kun käytännössä me ei saada itse juuri mitään--” (Kaupunki G)

Haastattelujen mukaan myös sellaisia tapauksia saatetaan jättää ilmoittamatta, missä olemassa olevista tiedoista voidaan nähdä, että tekijää ei tulla koskaan saamaan rikosoikeudelliseen vastuuseen.

Kaupunki E ja Kaupunki C ottivat esiin myös kysymyksen negatiivisen julkisuuden pelon aiheuttaman ilmoittamatta jättämisen, mutta he kumpikin olivat sitä mieltä, että tämä oli enemmän yksityisen sektorin organisaatioiden

kuin kaupunkien ja muiden julkisen sektorin organisaatioiden ongelma. Muut kaupungit eivät maininneet sitä ollenkaan.

6 ANALYYSI JA JOHTOPÄÄTÖKSET

Tässä luvussa esitetään tutkimuksen tuloksista tehtyjä analyysejä ja johtopäätöksiä. Ensiksi tehdään analyysia jo aikaisemmista osista tuttujen neljän otsikon näkökulmasta. Nämä neljä otsikkoa ovat kyberrikoksista ilmoittaminen, kyberrikoksiin varautuminen, henkilöstön osaaminen ja kehitysehdotukset poliisille. Neljännen otsikon alla esitellään vielä haastatteluista löydetyt syyt ilmoittamatta jättämiselle ja analysoidaan niitä. Viidennen otsikon alla esitetään aikaisempien analyysien perusteella lista ehdotuksista, joilla poliisi voisi mahdollisesti vaikuttaa havaituista kyberrikoksista tehtävien ilmoitusten määrään. Näiden jälkeen esitellään omissa osissaan tutkimuksen hyödyt sekä tunnistetaan ja analysoidaan heikkoja kohtia.

6.1 Kyberrikoksista ilmoittaminen

Tehtyjen haastatteluiden mukaan kaupungeissa kyberrikoksien ilmoittamisesta poliisille päättävät ja varsinaisen ilmoitukset tekevät sellaiset ihmiset, joilla on osaamista ja ymmärrystä kyberrikoksista. Lakimiesten kautta toimivissa kaupungeissakin tietoturvasta ja tietohallinnosta tietävät antavat lakimiehelle tietoja ja oman suosituksensa päätöksentekoa varten, kuten voidaan seuraavassa sitaatissa nähdä.

> Mikäli tapaus on sellainen, että kyseeseen voisi tulla ilmoitus poliisille, niin olemme yhteydessä kaupungin lakimiesyksikköön, joka sitten tekee varsinaisen ilmoituksen poliisille käyttäen meiltä saamiaan tarkempia tietoja tapauksesta. (Kaupunki I)

Kaikilla haastatelluilla kaupungeilla oli määritelty tai he osasivat kertoa, millaisin kriteerein kyberrikoksien vakavuutta arvioidaan. Missään ei siis päättäville tasoille tietoon tulleista havaituista kyberrikoksista jätetty vaikutuksia arvioimatta.

Näiden perusteella voidaan tehdä sellainen johtopäätös, että kyberrikoksien ilmoittamatta jättäminen ei voida näiden haastatteluiden

perusteella nähdä johtuvan rikosilmoituksesta päättävien tai sen käytännössä tekevien ammattitaidon puutteesta tai siitä, että havaittuja kyberrikoksien vakavuutta ei arvioitaisi.

6.2 Kyberrikoksiin varautuminen

Haastateltujen kaupunkien varautumisen taso kyberrikostilanteisiin oli hyvällä tasolla, vaikka haasteitakin tuli esille mm. suunnitelmien päivittämisen ja testauksen osalta.

Haastatellut tunnistivat olemassa olevien suunnitelmien päivittämisen tarpeet ja osa toi esille myös jatkuvan päivittämisen prosessin luomisen tarpeellisuuden nopeasti muuttuvan kybertoimintaympäristön takia.

Edellä mainituista voidaan päätellä, että vaikka osalla haastatelluista kaupungeista on kyberrikoksiin varautumisessa ongelmia, pääasiassa kaupunkien johdossa oli suunniteltu, miten kyberrikos ja muissa poikkeustilanteissa pitäisi toimia. Omat puutteet ja ongelmat tunnistettiin ja niiden kehittäminen tuntui olevan esillä. Kyberrikoksiin varautumisesta ei saada ainakaan näiden haastattelujen perusteella merkittävää selitystä kyberrikoksien ilmoittamatta jättämiselle.

6.3 Henkilöstön osaaminen

Haastattelujen perusteella kaupungit ovat panostaneet henkilökunnan osaamisen kehittämiseen, mutta silti kyberrikoksien kannalta osaamisessa on puutteita, sillä kaupunkien monimuotoinen ja suuri henkilöstömäärä vaikeuttavat kyberturvallisuustietoisuuden koulutusta ja opitun jalkauttamista käytäntöön.

Osaamisen puutteiden takia kaupunkien kyberrikosilmoituksista päättävät ihmiset eivät välttämättä saa tietoja kaikista vakavammista tapauksista, sillä henkilökunta tai ilmoituksia käsittelevä toinen taso eivät aina osaa erottaa massatapahtumaa kohdistetummasta ja vakavammasta tapauksesta. Osa näistä voi tulla sitten ihan vahingossa esiin, kuten Kaupunki E:n edustaja alla kuvaa.

> ”Meilläkin johdolle on sitten tullut tällaisii toimitusjohtaja huijauksia viimeisen viikon sisällä aika paljon. Se oli ihan sattumaa et me saatiin tietää, että tämmöisiä on nyt liikkeellä ja ihan taitavasti tehtyjä vielä, et oli kaivettu silleen oikeet henkilöt ja sitten oli vielä osattu osoittaa semmoiselle, jolla on hankintavaltuuksia.” (Kaupunki E)

Jos kaupunkien johtohenkilöt eivät saa tietoja havaituista tapahtumista, ei niistä myöskään tehdä rikosilmoitusta poliisille. Henkilöstön osaamisen puutteet

voidaankin tunnistaa näiden haastattelujen perusteella yhdeksi kyberrikoksien ilmoittamisen vähyyttä selittäväksi tekijäksi.

Näitä samoja henkilöstön kouluttamisen vaikeuksia on tuonut esiin mm. Korpela (2015) henkilökunnan kyberturvallisuuden tilannetietoisuuden kouluttamista käsittelevässä tekstissään.

6.4 Kehitysehdotukset poliisille

Haastatteluissa tuli esiin monenlaisia kehitysehdotuksia tavoista, joilla poliisi voisi helpottaa kyberrikoksista tehtävien ilmoituksien tekemistä tai muuten auttaa kaupunkeja kyberrikoksiin liittyvissä asioissa.

Esiin tulleiden kehitysehdotusten taustalla oli usein kohdattuja ongelmia ja näiden ongelmien kuvauksista ja haastateltavien antamista perusteluista voidaan tunnistaa syitä sille, miksi osasta havaituista kyberrikoksista ei tehdä ilmoitusta poliisille. Alla on Kaupunki G:n edustajan kuvaus yhdestä syystä.

> ”--se hyöty mitä me saadaan [kyberrikoksista ilmoittamisesta] tai meille se ei niin kun näy millään tasolla ja ei me sitten tehdä kun sellaisissa merkittävissä tapauksissa asioista ilmoituksia--” (Kaupunki G)

Kehitysehdotuksista sai myös sellaisen vaikutelman, että kaupungeissa työskenteleville ei ole selvillä, miten poliisissa nähdään kyberrikokset tai edes kyberturvallisuus yleisesti. Kaupungeilla tuntuisi kuitenkin olevan kiinnostusta ymmärtää poliisia paremmin, mitä kuvaa esimerkiksi kehitysehdotukset koskien poliisin järjestämiä koulutustilaisuuksia asian tiimoilta. Lisäksi tätä tuotiin suoraan esiin esimerkiksi Kaupunki A:n ja D:n toimesta.

> Poliisin olisi hyvä käydä kertomassa kaupungille (tietohallinnolle, esimiehille, viestinnälle jne.), miten kyberhyökkäykset näkyvät poliisin suuntaan paikallisesti ja valtakunnallisesti. -- Olisi myös hyvä tietää, olisiko poliisilla millaista toivetta asian suhteen? (Kaupunki A)

> Kyllä ilman muuta, esim. seminaarit, joissa poliisi tuo omalta näkökulmalta kyberrikollisuusteemaa tarkemmin julkishallinnolle esille. (Kaupunki D)

Havainnoista voidaan löytää yhteneväisyyksiä Lehdon ym. (2017) ja muiden tutkimukseen, jossa tuotiin esiin samanlaisia kehitysehdotuksia kuten tiedonjakamisen tehostaminen ja kybertietoisuuden syventäminen.

Kehitysehdotuksissa ilmi tulleista ongelmista ja niiden ratkaisuista pystytäänkin tunnistamaan muutamia merkittäviäkin syitä siihen, miksi kaupungit eivät ilmoita kaikista havaitsemistaan kyberrikoksista poliisille.

6.5 Toimenpide-ehdotukset

Edellisistä kappaleista mukaillen voidaan vetää yhteen lista mahdollisista toimenpiteistä, joilla poliisilla haastatteluiden perusteella olisi mahdollisuutta kasvattaa havaituista kyberrikoksista tehtävien rikosilmoitusten määrää. Lista ei ole minkäänlaisessa tärkeysjärjestyksessä.

- Järjestää koulutustilaisuuksia ja seminaareja, joissa
    - Käydään läpi syitä, miksi poliisi haluaa tietoa kyberrikoksista.
    - Esitellään toteutuneita tapauksia case- kuvauksin.
    - Esitellään kyberrikosympäristön nykytilaa.
    - Parannetaan yleistä kyberturvallisuuden tietämystä.
- Kaupunkien itse tehtävää esiselvitystä koskevan ohjeistuksen luominen.
- Tapahtuneiden case-kuvausten julkaisu kirjallisena.
- Kansallisen neuvontapuhelimen luominen.
- Tehdä ilmoittamisesta mahdollisimman helppoa ja tarjota sekä
    - sähköinen ilmoittamistapa että
    - suora yhteydenotto puhelimitse.
- Pyrkimys vasteajan parantamiseen.
    - Nopeampi reagointi ilmoittamiseen.
    - Kaupunkien ja poliisin välisen kommunikaation lisääminen.
    - Jälkitiedottamisesta huolehtiminen.
- Poliisin ja kaupunkien välisen käytännön yhteistyön parantaminen.
    - Poliisin toimintatapojen yhtenäistäminen.
    - Muun avun tarjoaminen.
    - Sovitaan kaupunkien ja poliisin kesken tietyistä toimintatavoista aikaisempaa tarkemmin.

On selvää, että kaksi viimeisintä ehdotusta, eivät ole kokonaan poliisin käsissä. Esimerkiksi omille resursseilleen poliisi ei voi tehdä oikein mitään. Nämä kaksi ovatkin mukana tässä enemmän pidemmän tähtäimen tavoitteena, joita voisi olla hyödyllistä viedä eteenpäin.

Muita ehdotuksia voi olla helpompi toteuttaa. Tiedon välittämisellä voidaan parantaa kaupunkien ymmärrystä, miksi ilmoittaminen olisi tärkeää ja mitä hyötyjä siitä voisi olla kaupungeillekin, vaikka jotakin heidän ilmoittamaa tapausta ei lähdettäisikään tutkimaan. Näitä ja muita listassa mainittuja seikkoja voidaan käydä läpi erilaisissa koulutustilaisuuksissa ja seminaareissa. Näitä tilaisuuksia voidaan vielä tukea esimerkiksi case- kuvauksia julkaisemalla.

Kaupunkien esiselvitystä koskevan ohjeistuksen luomisella, voisi ohjeistaa kaupunkia ottamaan tutkinnassa todennäköisesti tarvittavaa tietoa talteen ennen kuin loki- tai muut tiedostot häviävät tavanomaisen kierron mukana, vaikka poliisi ei pääsisikään tutkimaan asiaa heti. Lisäksi valmiiksi kerätyllä aineistolla voisi mahdollisesti nopeuttaa ja helpottaa poliisin tutkintaa.

Kaupungilla on kyberturvallisuuden ammattilaisia, mutta haastatteluista tuli esiin pyyntöjä siitä, että poliisi voisi auttaa yleisen kyberturvallisuuden tietämyksen kasvattamisessa, tehdä tiedosta helpommin saatavaa ja tuoda esiin asiaa poliisin omasta näkökulmasta. Kyberturvallisuustietämystä pystyttäisiin parantamaan, sillä että poliisi jakaisi aikaisempaa enemmän tietämystään alalta. Nykyään kaupungeilla tehdään toimenpiteitä omien tietämystensä mukaan. Esimerkiksi kaupunki E arvioi tilannetta seuraavasti:

> ”---tän [kyberrikoksien ilmoittamisen] teeman kommunikointi eri viranomaisilla ja yhteisöille voisi olla paikallaan, että ei ainakaan sellaista omaehtoista niin kun rajoittamista [mitä ilmoitetaan ja mitä ei] tehtäis organisaatiossa, ellei poliisi sitä toivo.” (Kaupunki E)

6.6 Hyödyt

Tutkimuksen ensisijainen hyöty on siinä, että sitä voidaan käyttää pohjana jatkotutkimuksille ja toimenpiteiden suunnittelussa, sillä aiheesta ei ole olemassa aikaisempaa tutkimusta ja asia on kuitenkin tunnustettu tärkeäksi mm. poliisin (Piiroinen, 2018) ja muutaman haastatellun kaupungin edustajan mielestä.

Tuloksissa pystyttiin selvittämään havaittujen kyberrikoksien ilmoittamisen prosessin vastuuhenkilöitä, löytämään erilaisia syistä ilmoittamatta jättämiseen ja sulkemaan alustavasti joitain mahdollisia syitä pois. Lisäksi pystyttiin laatimaan ehdotettujen toimenpiteiden lista.

6.7 Heikkoudet

Tehdystä tutkimuksesta voidaan tunnistaa erinäisiä heikkouksia niin tutkimus-, tietojenkeruu kuin analyysimenetelmissäkin. Tätä tutkimusta suunniteltaessa on kuitenkin pyritty nämä heikkoudet ottamaan huomioon gradu työn laajuuden antamissa rajoissa.

Tapaustutkimuksella on tutkimusmenetelmänä tunnetut heikkoutensa, mistä tämäkään tutkimus ei ole täysin vapaa. Näitä heikkouksia on pyritty ottamaan huomioon valitsemalla useamman tapauksen tapaustutkimus ja pyrkimällä siihen, että tutkimuksessa mukana olevat kaupungit ovat samankaltaisia. Samankaltaisuudella tarkoitetaan tässä tapauksessa sitä, että kaupungit ovat kooltaan isompia ja muodostavat isoja organisaatioita.

Haastatteluiden suunnittelussa pyrittiin ottamaan huomioon Myersin ja Newmanin (2007) tekstissään esittämät heikkoudet, mutta joitain asioita ei saatu sovitettua Pro gradu -tutkimuksen laajuuden puitteisiin. Heikkouksiksi voidaan luokitella se, että kustakin kaupungista valittiin vai yksi haastateltava ja sekin oli usein johtavassa asemassa oleva henkilö, joka pystyi antamaan vain

oman arvionsa esimerkiksi henkilöstön osaamisesta. Ketään haastateltavaa haastattelija ei ollut tavannut aikaisemmin, vaikka ajoista sopiminen tarkoittikin jotakin yhteydenpitoa ennen varsinaista haastattelua.

Haastatteluja tehdessä oli kuitenkin havaittavissa hyvä ja avoin ilmapiiri. Haastateltavat olivat itsekriittisiä ja kävivät läpi sekä vahvuuksiaan että heikkouksiaan haastattelijan mielestä avoimesti.

Haastatteluja ja materiaaleja analysoinnin heikkoutena voidaan nähdä, se että ne perustuvat suurelta osin tutkimuksen toteuttajan tekemiin tulkintoihin. Aineistoa on kuitenkin pyritty käsittelemään monesta näkökulmasta ja tuloksia esittämään monella tavalla. Analysointimenetelmät on myös esitetty tässä raportissa mahdollisimman tarkasti, jotta lukija saa mahdollisimman hyvän kuvan siitä, miten aineistoa on käsitelty.

7 YHTEENVETO

Kyberrikokset ovat yksi isoimmista ongelmista organisaatioissa nykyään ja nämä ongelmat koskettavat myös yksityishenkilöitä. Organisaatiot voivat ehkäistä kyberrikoksia erilaisin kyberturvallisuuden hallinnan menetelmin, kuten aikaisemmin tässä raportissa esitellyn NIST-kyberturvallisuuden hallintamallin avulla. Kuitenkin, vaikka kyberturvallisuuteen olisi varautunut kuinka hyvin, silti jatkuvasti joku rikollinen onnistuu aikeissaan.

Suomessa kyberrikollisuuden torjunnasta vastaa poliisin eri laitokset, mutta yhteistyö eri viranomaisten välillä on tärkeää. Viranomaistahojen välisen yhteistyön lisäksi tarvitaan myös tiivistä yhteistyötä muiden julkisten sekä yksityisen sektorin organisaatioiden kanssa. (Lehto ym., 2017)

Tutkimus lähti KRP:n Timo Piiroisen ehdotuksesta. Hän oli kiinnostunut organisaatioiden kyberrikoksien ilmoittamisen prosessista. Rikollisten saattaminen rikosoikeudelliseen vastuuseen on poliisin tehtävä, mutta he hyödyntävät kyberrikosilmoituksista saamaansa tietoa myös kyberrikoksien tilannekuvan ylläpidossa. Sen avulla poliisit pystyvät tarvittaessa antamaan varoituksia tai tiedottaa kansalaisia ja organisaatioita uhista (Piiroinen, 2019). Tähän kaikkeen tarvitaan tietoa, mutta poliisilla on sellainen käsitys, että kaikista tapauksista ei tehdä ilmoituksia (Piiroinen, 2018). Tämä ongelma tiivistettiin yhteen tutkimuskysymykseen, josta lähdettiin liikkeelle: Miksi kaikista kyberrikoksista ei ilmoiteta poliisille?

Tutkimus toteutettiin tapaustutkimuksena ja aineisto kerättiin haastatteluin. Tutkimukseen osallistui yhdeksän Suomen suuremman kaupungin tietohallinnon, tietoturvallisuuden tai turvallisuus osaston johtohenkilöä tai heidän alaisiaan.

Haastatteluista pystyttiin löytämään kaksi isoa syytä, miksi kyberrikoksista jätetään ilmoittamatta. Ensimmäinen oli se, että kyberrikoksen ilmoittamisesta koettiin aiheuttavan enemmän haittaa kuin hyötyä. Negatiivista julkisuutta ei kuitenkaan nähty kaupungeissa haittana. Toinen oli se, että kaupunkien johto ja ihmiset, jotka ovat vastuussa ilmoittamisesta eivät saa kuulla kaupunkien henkilöstöltä kaikista havaituista tapauksista.

Haastatteluissa kysyttiin myös, miten poliisi voisi auttaa kaupunkeja kyberrikoksiin liittyen. Haastatteluissa tulikin monenlaisia ehdotuksia, jotka koskivat pääasiassa poliisin vasteajan parantamista, poliisin ja kaupunkien välisen yhteistyön parantamista ja poliisin aikaisempaa vahvempaa osallistumista yleisen kybertietoisuuden parantamiseen. Tulokset olivat linjassa muiden kyberturvallisuuden kehittämiseen liittyviin tutkimuksiin.

Tämä tutkimus toimii hyvänä pohjana asiassa, jota ei ole vielä juurikaan tutkittu, vaikka gradun laajuuden rajoissa ei kaiken kattavaa haastattelututkimusta voitukaan toteuttaa. Tutkimuksen avulla löydettiin syitä ilmoittamatta jättämiselle ja laadittiin lista mahdollisista toimenpide-ehdotuksista, joilla poliisilla voisi olla mahdollisuus vaikuttaa kaupunkien kyberrikoksien ilmoittamisen motiivia nostavasti ja lisätä näin kyberrikoksista tehtävien ilmoitusten määrää.

LÄHTEET

Baskerville, R. (1991). *Risk analysis: an interpretive feasibility tool in justifying information systems security*. European Journal of Information Systems, 1(2), 121-130.

Baskerville, R., & Siponen, M. (2002). *An information security meta-policy for emergent organizations*. Logistics Information Management, 15(5/6), 337-346.

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). *The case research strategy in studies of information systems*. MIS quarterly, 369-386.

Botha, J., & Von Solms, R. (2004). *A cyclic approach to business continuity planning*. Information Management & Computer Security, 12(4), 328-337.

Cerullo, V. & Cerullo, M. (2004). *Business Continuinty Planning: Comprehensive Approach*. www.ISM-Journal.com, Summer, 70–78.

Darke, P., Shanks, G., & Broadbent, M. (1998). *Successfully completing case study research: combining rigor, relevance and pragmatism*. Information Systems Journal, 8(4), 273-289.

Endsley, M. R. (1988). *Situation awareness global assessment technique (SAGAT)*. Proceedings of the National Aerospace and Electronics Conference. (s. 789-795). New York: IEEE Computer Society.

EU. (2016). Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. *Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)*. Saatavilla: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI

EU komissio. (2007). *Tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi*. Euroopan komission tiedonanto 22.5.2007. KOM/2007/267/lopull.2007. Haettu 13.3.2019 osoitteesta: https://eur-lex.europa.eu/legal-content/FI/TXT/DOC/?uri=CELEX:52007DC0267&from=FI

Europol. (2016). *2016 Internet Organized Crime Threat Assessment (IOCTA)*. Hague: Europol's European Cybercrime Centre (EC3). Haettu 22.10.2018 osoitteesta https://www.europol.europa.eu/iocta/2016/resources/iocta-2016.pdf

Europol. (2018). *2018 Internet Organized Crime Threat Assessment (IOCTA)*. Hague: Europol's European Cybercrime Centre (EC3). Haettu 22.10.2018 osoitteesta https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf

Euroopan neuvosto. (2001). *Convention on Cybercrime*. ETS No. 185, 23.11.2001. Haettu 1.4.2019 osoitteesta: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

Euroopan neuvosto. (2007). *Tietoverkkorikollisuutta koskeva yleissopimus*. L60/2007.2007. Haettu 13.3.2019 osoitteesta: https://www.finlex.fi/fi/sopimukset/sopsteksti/2007/20070060/20070060_2

Flyvbjerg, B. (2006). *Five misunderstandings about case-study research*. Qualitative inquiry, 12(2), 219-245. Haettu 12.2.2019 osoitteesta: http://journals.sagepub.com/doi/pdf/10.1177/1077800405284363?casa_token=ewoXh8QL9w4AAAAA:VarqFyp8-8SzWlHWHKCmFrdra5tGz--C-zmq4ICwI4NrpyD0vRRCFjXQ_28XA17BmRDzrmzG6EZk

Franke, U., & Brynielsson, J. (2014). *Cyber situational awareness - a systematic review of the literature*. Computers & Security, 46, 18-31.

Herranen, T. (2018). *Kevyttä keskustelua vai tiivistä tietojen vaihtoa?: tietoverkkorikollisuuden tilannetietoisuuden jakaminen luottamusverkostossa*. (Pro Gradu -tutkielma, Jyväskylän yliopisto). Haettu osoitteesta: https://jyx.jyu.fi/bitstream/handle/123456789/58590/1/URN%3ANBN%3Afi%3Ajyu-201806153242.pdf

Huergo, J. (2018). *NIST Releases Version 1.1 of its Popular Cybersecurity Framework*. NIST. 16.4.2018. Haettu 13.3.2019 osoitteesta: https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework

Jajodia, S., Noel, S., Kalapa, P., Albanese, M., & Williams, J. (2011). *Cauldron mission-centric cyber situational awareness with defense in depth.* MILCOM November 2011. (pp. 1339-1344).

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). *Information systems security policies: a contextual perspective.* Computers & Security, 24(3), 246-260.

Keyser, M. (2017). *The Council of Europe Convention on Cybercrime*. In Computer Crime (pp. 131-170). Routledge.

Korpela, K. (2015). *Improving cyber security awareness and training programs with data analytics*. Information Security Journal: A Global Perspective, 24(1-3), 72-77.

Laaksovirta, T. H. (1984). *Kvalitatiivisista menetelmistä ja niiden käytöstä*. Informaatiotutkimus, 18-20

Laine, M., Bamberg, J., & Jokinen, P. (2015). *Tapaustutkimuksen taito*. 3. painos. Helsinki: Gaudeamus. ISBN: 978-952-495-697-0

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T. & Salminen, M., (2017). *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi*. Haettu 11.12.2018 osoitteesta http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160233/Suomen_kyberturvallisuuden_nykytila,__tavoitetila_ja.pdf?sequence=1

Lehto, M., Limnéll, J., Kokkomäki, T., Pöyhönen, J., & Salminen, M. (2018). *Kyberturvallisuuden strateginen johtaminen Suomessa*. Haettu: 11.12.2018 osoitteesta: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160717/28-2018-Kyberturvallisuuden%20strateginen%20johtaminen.pdf?sequence=1&isAllowed=y

Maxwell, J. A. (2008). *Designing a qualitative study*. The SAGE handbook of applied social research methods, 2, 214-253.

Moody, G. D., Siponen, M., & Pahnila, S. (2018). *Toward a Unified Model of Information Security Policy Compliance*. MIS Quarterly, 42(1).

Myers, M. D., & Newman, M. (2007). *The Qualitative interview in IS research: Examining the craft.* Information and organization, 17(1), 2-26.

Nevalainen, S. (2018). *Keskeiset kyberrikokset Suomen oikeusjärjestelmässä.* Pro Gradu -tutkielma, Itä-Suomen yliopisto.

NIST (2018). *Framework for Improving Critical Infrastructure in Cybersecurity*. NIST. 16.4.2018. Haettu 13.3.2019 osoitteesta: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Noor, K. B. M. (2008). *Case study: A strategic research methodology*. American journal of applied sciences, 5(11), 1602-1604. Haettu 13.12.2018 osoitteesta: https://www.researchgate.net/profile/Khairul_Baharein_Mohd_Noor/publication/26517241_Case_Study_A_Strategic_Research_Methodology/links/5462bd800cf2c0c6aec1b83e/Case-Study-A-Strategic-Research-Methodology.pdf

Pelkonen, A., Ahlqvist, T., Leinonen, A., Nieminen, M., Savola, R., Salonen, J., & Remes, J. (2016). *Kyberosaaminen Suomessa – Nykytila ja tiekartta tulevaisuuteen.* Valtioneuvoston kanslia, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 9/2016, ISSN Web: 2342-6799

Piiroinen, Timo. (2018). Keskusrikospoliisin rikosylikomissario, sähköpostihaastattelu 13.12.2018, haastattelija: Sari Valkama

Piiroinen, Timo. (2019). Keskusrikospoliisin rikosylikomissario, sähköpostihaastattelu 18.3.2019, haastattelija: Sari Valkama

Poliisi. (2018). *Kyberrikollisuus.* Haettu 8.11.2018 osoitteesta https://www.poliisi.fi/rikokset/kyberrikollisuus

Poliisin tilastotietojärjestelmä. (2018).

Raggad, B.G. (2010). *Information security management: Concepts and practice.* CRC Press. ISBN: 978-1-4200-7854-1

Rikoslaki 19.12.1889/39. Haettu 25.10.2018 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Saaranen-Kauppinen, Anita & Puusniekka, Anna. (2006). *KvaliMOTV – Menetelmäopetuksen tietovaranto*. Tampere: Yhteiskuntatieteellinen tietoarkisto Haettu 6.11.2018 osoitteesta: http://www.fsd.uta.fi/menetelmaopetus/

Sabillon, R., Cavaller, V., Cano, J. & Serra-Ruiz, J. (2016). *Cybercriminals, cyberattacks and cybercrime.* International Conference on Cybercrime and Computer Forensic. Vancouver, BC: IEEE Computer Society.

Siponen, M., & Willison, R. (2009). *Information security management standards: Problems and solutions.* Information & Management, 46(5), 267-270.

Susanto12, H., Almunawar, M. N., & Tuan, Y. C. (2011). *Information security management system standards: A comparative study of the big five.* International Journal of Electrical Computer Sciences IJECSIJENS, 11(5), 23-29. Haettu 31.10.2018 osoitteesta: http://www.academia.edu/download/30294093/113505-6969-ijecs-ijens.pdf

Talus, Autio, Hänninen, Pihamaa ja Kantonen. (2017). *Miten valmistautua EU:n tietosuoja-asetukseen?* Oikeusministeriö. ISBN: 978-952-259-558-4. Saatavilla: http://urn.fi/URN:ISBN:978-952-259-558-4

Tianfield, H. (2016). *Cyber security situational awareness*. Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE

Smart Data (SmartData), 2016 December IEEE International Conference on (pp. 782-787). IEEE

Turvallisuuskomitea. (2013). *Suomen kyberturvallisuustsrategia ja taustamuistio*. Haettu 6.11.2018 osoitteesta: https://turvallisuuskomitea.fi/wp-content/uploads/2018/05/Suomen-kyberturvallisuusstrategia-ja-taustamuistio.pdf

Turvallisuuskomitea. (2017). *Suomen kybertruvallisuustrategian toimeenpano-ohjelma 2017-2020*. Haettu 6.11.2018 osoitteesta: https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf

UNODC. (2013). *Comprehensive Study on Cybercrime*. Vienna: United Nations Office on Drugs and Crime. Haettu 31.03.2107 osoitteesta. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Viestintävirasto. (2018). *Tietoturvan vuosi 2017*. Viestintäviraston julkaisu 001/2018 J, Haettu 23.10.2018 osoitteesta https://viestintavirasto.fi/attachments/cert/tietoturvakatsaukset/Tietoturvan-vuosi-2017.pdf

LIITE 1 HAASTATTELUKYSYMYKSET

Jokaiselle haastateltavalta kysyttiin seuraavat kysymykset:

Kyberrikoksista ilmoittaminen
- Kuka tekee päätöksen kyberrikoksista ilmoittamisesta?
- Kuka tekee ilmoituksen kyberrikoksista ja millä tavalla?
- Millä perusteella havaittuja kyberrikoksia arvioidaan?

Kyberrikoksiin varautuminen
- Onko organisaatiolla suunniteltu prosessi ja toimintatavat kyberrikosten varalle?
- Onko vastuuhenkilöistä päätetty?
- Onko laadittu toiminnan jatkuvuuden takaavia suunnitelmia?
- Onko laadittu kriiseistä palautumisen suunnitelmia?

Henkilöstön osaaminen
- Tietävätkö organisaation työntekijät kenelle ilmoittaa havaitsemastaan kyberrikoksesta?
- Ovatko organisaatiossa työskentelevät tietoisia, mitkä ovat kyberrikoksia?
- Onko henkilökuntaa koulutettu kyberrikoksiin liittyen?

Kehitysehdotuksia poliisille
- Millä tavalla olisit yhteydessä poliisiin mieluiten?
- Voisiko poliisi auttaa teitä jollain lailla enemmän kyberrikoksiin liittyen?

LIITE 2 POLIISILLE ILMOITETUT KYBERRIKOKSET

Taulukossa löytyy ilmoitetut rikokset vuosilta 2016 ja 2017 sekä vuoden 2018 rikokset joulukuun 11. päivään asti.

Petokset

Ilmoitettu Kpl	2016	2017	2018
LIEVÄ MAKSUVÄLINEPETOS	2 980	1 237	1 196
MAKSUVÄLINEPETOS	12 576	5 624	4 603
TÖRKEÄ MAKSUVÄLINEPETOS	169	255	203
MAKSUVÄLINEPETOKSEN VALMISTELU	27	35	19
LIEVÄ PETOS	9 678	8 966	8 717
PETOKSEN YRITYS	3 576	4 092	2 684
PETOS	12 411	11 608	10 971
TÖRKEÄN PETOKSEN YRITYS	221	305	375
TÖRKEÄ PETOS	1 284	1 234	1 266
Summa	**42 922**	**33 356**	**30 034**

Lähde: Poliisin tilastotietojärjestelmä

Kyberrikokset

Ilmoitettu Kpl	2016	2017	2018
IDENTITEETTIVARKAUS	3 354	3 945	3 555
LIEVÄ TIETOLIIKENTEEN HÄIRINTÄ	9	7	3
SUOJAUKSEN PURKUJÄRJESTELMÄRIKOS	0	0	0
TEKNISEN SUOJAUKSEN KIERTÄMINEN	0	0	0
TIETOJÄRJESTELMÄN HÄIRINNÄN YRITYS	0	0	0
TIETOJÄRJESTELMÄN HÄIRINTÄ	38	24	17
TIETOKONEOHJELMAN SUOJAUKSEN POISTOVÄLINEEN LUVATON LEVITTÄMINEN	0	0	0
TIETOLIIKENTEEN HÄIRINNÄN YRITYS	0	0	0
TIETOLIIKENTEEN HÄIRINTÄ	67	62	31
TIETOLIIKENTEEN LIEVÄN HÄIRINNÄN YRITYS	0	1	0
TIETOMURRON YRITYS	13	18	19
TIETOMURTO	409	411	462
TIETOVERKKORIKOSVÄLINEEN HALLUSSAPITO	3	3	1
TÖRKEÄ TIETOJÄRJESTELMÄN HÄIRINTÄ	16	14	6
TÖRKEÄ TIETOLIIKENTEEN HÄIRINTÄ	9	15	12
TÖRKEÄ TIETOMURTO	8	19	8
TÖRKEÄ VIESTINTÄSALAISUUDEN LOUKKAUS	3	1	5
TÖRKEÄN TIETOMURRON YRITYS	0	8	0
VAARAN AIHEUTTAMINEN TIETOJENKÄSITTELYLLE	4	8	6
VIESTINTÄSALAISUUDEN LOUKKAUKSEN YRITYS	3	1	0
VIESTINTÄSALAISUUDEN LOUKKAUS	414	364	304
Summa	**4 350**	**4 901**	**4 429**

Lähde: Poliisin tilastotietojärjestelmä