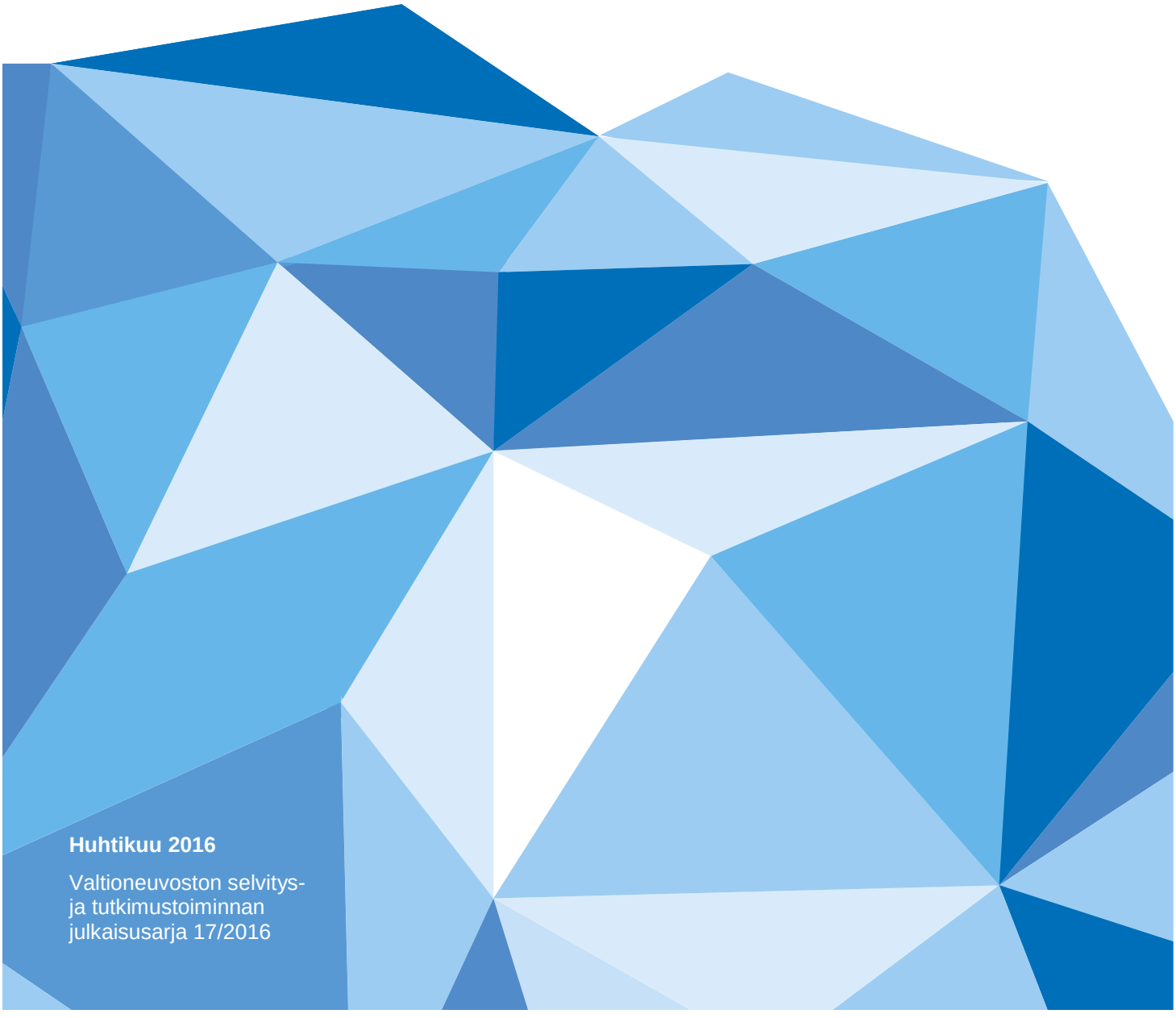
VALTIONEUVOSTON
SELVITYS- JA TUTKIMUSTOIMINTA

Anna Leppänen, Karl Linderborg ja Jarkko Saarimäki

Tietoverkkorikollisuuden tilannekuva



Huhtikuu 2016

Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 17/2016

KUVAILULEHTI

Julkaisija ja julkaisuaika	Valtioneuvoston kanslia, 19.4.2016
Tekijät	Anna Leppänen, Karl Linderborg ja Jarkko Saarimäki
Julkaisun nimi	Tietoverkkorikollisuuden tilannekuva
Julkaisusarjan nimi ja numero	Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 17/2016
Asiasanat	kyberturvallisuus, tietojohtoinen poliisitoiminta, tietoverkkorikollisuus, tilannekuva, poliisi, viranomaisyhteistyö, yritykset
Julkaisuaika	Huhtikuu, 2016 **Sivuja** 37 **Kieli** Suomi

Tiivistelmä

Kyberturvallisuuden yhteisen tilannetietoisuuden parantaminen ja tiedonvaihdon lisääminen viranomaisten, elinkeinoelämän sekä tutkimusyhteisön kesken on useassa kansallisessa strategiassamme esitetty tavoite. Tietoverkkorikollisuuden tilannekuvatyö on yksi osa-alue kyberturvallisuuden yhteistä tilannetietoisuutta ja sen kehittäminen aloitettiin poliisissa Kyberrikostorjuntakeskuksen perustamisen myötä 2015. Tässä selvityksessä kartoitetaan tietoverkkorikollisuuden tilannekuvatyön nykytila ja tavoitteena on luoda pohja tietoverkkorikollisuuden tilannekuvatyön kehittämiselle poliisissa. Lopputuloksena esitetään joukko toimenpide-ehdotuksia, jotka tähtäävät yhteisen tilannetietoisuuden parantamiseen ensisijaisesti nykyisessä lainsäädännöllisessä viitekehyksessä jo olemassa olevin resurssein.

Tietoverkkorikollisuuden tilannekuvatyön organisointi kuuluu poliisin Kyberrikostorjuntakeskukselle ja sen tärkein kehittämistarve on poliisin sisäinen. Suurimman hyödyn saaminen sidosryhmäyhteistyöstä koko poliisiorganisaatiolle edellyttää poliisin oman tilannekuvatyön tavoitteiden, resurssien ja keinojen määrittelyä sekä kehittämisen kytkemistä sisäisiin strategioihin. Tällöin keskustelu tiedonvaihdosta muiden kanssa voidaan viedä riittävän tarkalle tasolle ja rakentaa tilannekuvasta systemaattisempi kokonaisuus. Tietoverkkorikollisuuden tilannekuvan fokukseksi ehdotetaan selvityksen tulosten perusteella rikosten tekotapoja, trendejä ja analyysia rikollisryhmistä. Sidosryhmät odottavat poliisilta sen kaltaista tietoa ja kokevat ilmiöiden taustoittamisen tarpeelliseksi. Lisäksi ne kuuluvat poliisin perustehtävään ja edistävät tietoverkkorikollisuuden kokonaisuuden haltuunottoa poliisissa.

Selvitys toteutettiin ajanjaksolla lokakuu 2015 - helmikuu 2016 Poliisiammattikorkeakoulussa. Muut hankkeen kumppanit olivat Poliisin Kyberrikostorjuntakeskus, Viestintäviraston Kyberturvallisuuskeskus ja Tampereen yliopisto. Selvityksen aineisto koostuu teemahaastatteluista sekä asiantuntijatyöpajan työskentelystä.

Liite 1 Haastatellut organisaatiot
Liite 2 Työpajaan osallistuneet henkilöt ja organisaatiot
Liite 3 Työpajan työryhmät, ennakkotehtävät ja ohjeistus

Tämä julkaisu on toteutettu osana valtioneuvoston vuoden 2015 selvitys- ja tutkimussuunnitelman toimeenpanoa (tietokayttoon.fi).

PRESENTATIONSBLAD

Utgivare & utgivningsdatum	Statsrådets kansli, 19.4.2016		
Författare	Anna Leppänen, Karl Linderborg och Jarkko Saarimäki		
Publikationens namn	Tietoverkkorikollisuuden tilannekuva		
Publikationsseriens namn och nummer	Publikationsserie för statsrådets utrednings- och forskningsverksamhet 17/2016		
Nyckelord	cybersäkerhet, lägesbild, informationsledd polisverksamhet, it-relaterade brottslighet, polis, myndighetssamarbete, företag		
Utgivningsdatum	April, 2016	**Sidantal** 37	**Språk** Finska

Sammandrag

En förbättrad gemensam situationsmedvetenhet inom cybersäkerheten och ökat informationsutbyte mellan myndigheter, näringsliv och forskningssamfund är ett mål som vi har fört fram i flera av våra nationella strategier. Arbetet med lägesbilden av den it-relaterade brottsligheten är ett delområde inom den gemensamma situationsmedvetenheten inom cybersäkerheten. Utvecklingen av arbetet inleddes vid polisen i samband med att Centralen för bekämpning av cyberbrott inrättades 2015. I den här utredningen kartläggs nuläget inom arbetet med lägesbilden av den it-relaterade brottsligheten och syftet är att skapa en grund för utveckling av arbetet med lägesbilden av den it-relaterade brottsligheten vid polisen. Som ett slutresultat presenterar vi ett antal åtgärdsförslag, som siktar på en förbättrad gemensam situationsmedvetenhet framför allt med de befintliga resurserna inom den nuvarande lagstiftningsmässiga referensramen.

Organiserandet av arbetet med lägesbilden av den it-relaterade brottsligheten hör till polisens Central för bekämpning av cyberbrott och det viktigaste behovet av utveckling finns inom polisen. För att hela polisorganisationen ska få ut den största nyttan av samarbetet med intressentgrupperna måste målen, resurserna och metoderna i polisens eget arbete med lägesbilden fastställas och utvecklingen kopplas till de interna strategierna. Då kan diskussionen om ett informationsutbyte med de övriga tas till en tillräckligt noggrann nivå och en mer systematisk helhet skapas av lägesbilden. Som fokus för lägesbilden av den it-relaterade brottsligheten föreslås på basis av utredningsresultaten brottsmetoder, trender och analys av de kriminella grupperna. Intressentgrupperna väntar sig det slags information av polisen och upplever att utredningen av bakgrunden till fenomenen är tillräcklig. Dessutom hör de till polisens grundläggande uppdrag och främjar omhändertagandet av den it-relaterade brottsligheten som helhet vid polisen.

Utredningen gjordes vid Polisyrkeshögskolan under perioden oktober 2015 – februari 2016. De övriga medverkande i projektet var Centralkriminalpolisens Central för bekämpning av cyberbrott, Kommunikationsverkets Cybersäkerhetscentrum och Tammerfors universitet. Utredningens material består av temaintervjuer och arbete inom en expertverkstad

Bilaga 1 Expertutvärderingsprocess och analysmetod (på finska)
Bilaga 2 Beskrivning av statistiska forskningsmetoder (på finska)
Bilaga 3 Förteckning över figurer och tabeller (på finska)

Den här publikation är en del i genomförandet av statsrådets utrednings- och forskningsplan för 2015 (tietokayttoon.fi).

DESCRIPTION

Publisher and release date	Prime Minister's Office, 19.4.2016
Authors	Anna Leppänen, Karl LInderborg and Jarkko Saarimäki
Title of publication	Tietoverkkorikollisuuden tilannekuva
Name of series and number of publication	Publications of the Govenrment´s analysis, assessment and research activities 17/2016
Keywords	cyber security, intelligence-led policing, cybercrime, situational awareness, police, cooperation between authorities, companies
Release date	April, 2016 **Pages** 37 **Language** Finnish

Abstract

Increasing general situation awareness of cyber security and the exchange of information between authorities, businesses and the academia are included in the goals of many of our national strategies. The work for assessing the current status of cybercrime is part of general cyber security situation awareness. The police began to develop this form of work in 2015 when the Cybercrime Center was founded. This study investigates how the current status of cybercrime is assessed, and aims to lay down a foundation upon which the police can develop this work further. The report concludes with a number suggested measures for improving general situation awareness, primarily within the current legislative framework and with existing resources.

The Cybercrime Center of the police is responsible for organizing the work needed to stay up to date with the current situation of cybercrime. This is primarily an internal development need of the police. If the police organization as a whole wishes to benefit from its cooperation with stakeholders as much as possible, the goals, resources and means of the work the police perform to assess the current situation of cybercrime must be defined, and the development of these areas must be linked to internal strategies. If this is accomplished, discussion about information exchange with other parties can be taken to a sufficiently detailed level, enabling a more systematic formation of overall situation awareness. Based on the results of this study, this report proposes that situational awareness of cybercrime should focus on the means by which crimes are committed; crime trends; and an analysis of criminal groups. Stakeholders expect to receive such information from the police, and find it necessary to know the background of different phenomena. Furthermore, these are a part of the police's basic tasks and help the police to have an overall command of cybercrime.

This study was performed between October 2015 and February 2016 at the Police University College. Other project partners include the Police Cybercrime Center, the National Cyber Security Centre of the Finnish Communications Regulatory Authority and the University of Tampere. The material of this study consists of thematic interviews and the results of an expert workshop.

Appendix 1 Expert evaluation process and method of analysis (in Finnish)
Appendix 2 Description of the statistical research methods (in Finnish)
Appendix 3 List of figures and tables (in Finnish)

This publication is part of the implementation of the Government Plan for Analysis, Assessment and Research for 2015 (tietokayttoon.fi).

SISÄLLYS

1. JOHDANTO

Kyberturvallisuuden kehittäminen Suomessa otti harppauksen eteenpäin kansallisen Kyberturvallisuusstrategian (2014) ja sen 74 toimenpidettä sisältävän toimeenpano-ohjelman (2013) julkaisemisen myötä. Yhdessä tehty strategiatyö on tiivistänyt organisaatioiden välisiä suhteita, asettanut tavoitteita sekä luonut uudenlaisia sisäisiä ja yhteistyön toimintamalleja. Hyvänä esimerkkinä on Viestintäviraston Kyberturvallisuuskeskuksen perustaminen ja toiminnan systemaattinen kehittäminen. Yksi Kyberturvallisuusstrategian keskeinen, myös Sipilän hallitusohjelmaan (2015, 36) kirjattu, tavoite on ollut kehittää tilannekuvatyötä.

Poliisiorganisaation näkökulmasta merkittävä kehityshanke on ollut vuoden 2015 aikana toteutettu poliisin kokonaisvaltainen kybersuunnitelma, jossa kyberturvallisuuden parantamista on pohdittu viidessä työryhmässä. Tietoverkkorikollisuuden kokonaisuuden haltuunotto on merkittävä tavoite niin poliisin kansallisen kuin kansainvälisen asiantuntija-aseman vahvistamisessa. Se edellyttää ajantasaista tilannekuvaa monilla eri tasoilla ja on täten kiinteä osa poliisin ennalta estävän toiminnan vahvistamista ja tietojohtoisen poliisitoiminnan kehittämistä. Poliisin Kyberrikostorjuntakeskuksen (poliisin kyberkeskus) perustaminen Keskusrikospoliisiin keväällä 2015 mahdollistaa aiempaa laajemmat edellytykset tietoverkkorikollisuuden tutkintaan, ennaltaehkäisyyn ja tilannekuvatyöhön. Poliisin osalta tietoverkkorikollisuuden tilannekuvatyön kehittämistarve määritellään Kyberturvallisuusstrategian toimeenpano-ohjelman kohdassa 47 (2014, 43). Tilannekuvatyön kehittäminen poliisin sisällä alkoi vuoden 2015 syksyllä ja tämä selvityshanke on osa kehittämistyötä.

Tässä selvityksessä kartoitetaan tietoverkkorikollisuuden tilannekuvatyön nykytila ja tavoitteena on luoda pohja tietoverkkorikollisuuden tilannekuvatyön kehittämiselle poliisissa. Lopputuloksena esitetään joukko mahdollisimman konkreettisia toimenpide-ehdotuksia, jotka tähtäävät yhteisen tilannetietoisuuden parantamiseen ensisijaisesti nykyisessä lainsäädännöllisessä viitekehyksessä jo olemassa olevin resurssein. Lyhyen tähtäimen ratkaisuun on päädytty useasta syystä. Ensinnäkin, tietoverkkorikollisuuden tilannekuvan kehittäminen on vielä alkuvaiheessa, joten tehtävää riittää runsaasti nykyisessä oikeudellisessa viitekehyksessä. Toiseksi, tiedon jakamiseen liittyy joitakin jo vuosia sitten tunnistettuja haasteita, kuten poliisin velvollisuus aloittaa esitutkinta virallisen syytteen alaisissa rikosepäilyissä. Lisäksi tiedustelulainsäädäntöprosessi ja monet muut eri viranomaisten toimivaltuuksien lisäämiseen tähtäävät hankkeet ovat keskeneräisiä, joten niiden mahdollisia vaikutuksia toimintaan on vaikea ennakoida. Lainsäädännölliset muutokset ovat hitaita ja tietoverkkorikollisuus kehittyy ilmiönä niin nopeasti, että pitkän tähtäimen tavoitteiden lisäksi tarvitaan nopeampia ratkaisuja. Keskittyminen yhdessä tekemiseen tässä hetkessä olemassa olevin edellytyksin parantaa nykytilaa ja auttaa hahmottamaan tulevaisuudessa mahdollisia yhteisiä kehitystarpeita.

Selvityksen keskeinen aineisto koostuu kahdesta osasta. Ensimmäisen aineiston muodostavat teemahaastattelut julkisen sektorin ja elinkeinoelämän edustajilta. Haastatteluista saatujen alustavien tulosten perusteella järjestettiin työpaja, johon kutsuttiin viranomaisia sekä elinkeinoelämän ja tutkimuksen edustajia pohtimaan konkreettisia ratkaisuehdotuksia havaittuihin haasteisiin. Lähestymistapa selvityksen toteuttamiseen on yhteiskuntatieteellinen ja tietoverkkorikollisuuden tilannekuvan ylläpitäminen sekä kehittäminen on nähty ensisijaisesti verkostomaisena toimintana. Verkostolähtöistä lähestymistapaa tukevat strategiat sekä tutkimuskirjallisuus, sillä kyberturvallisuuteen liittyviä vastuita on hajautettu useille organisaatioille (ks. tarkemmin Leppänen & Virta 2014). Verkostolähtöisyys näkyy selvityksessä pyrkimyksenä tuottaa toimenpide-ehdotuksia, jotka ovat nousseet yhden organisaation sijaan eri tahojen tarpeista sekä yhteisen pohdinnan lopputuloksena.

Hanke on rahoitettu valtioneuvoston päätöksentekoa tukevan selvitys- ja tutkimustoiminnan määrärahoista (VN TEAS) syksyn 2015 täydentävässä haussa. Toteuttajatahot ovat Poliisiammattikorkeakoulu, Poliisin Kyberrikostorjuntakeskus, Viestintäviraston Kyberturvallisuuskeskus ja Tampereen yliopiston johtamiskorkeakoulu. Hanke toteutettiin ajanjaksolla lokakuu 2015 - helmikuu 2016 ja sen vastuullisena johtajana toimi 31.12.2015 asti Poliisiammattikorkeakoulun erikoistutkija Kari Laitinen. Työn toteutti Poliisiammattikorkeakoulun tutkija Anna Leppänen tutkimusapulainen Annika Tikkasen avustamana. Luvun 4 "Tiedonvaihdon oikeudellinen viitekehys" ovat laatineet Poliisin Kyberrikostorjuntakeskuksen rikostarkastaja Karl Linderborg (luku 4.1) ja Viestintäviraston Kyberturvallisuuskeskuksen johtaja Jarkko Saarimäki (luku 4.2). Tampereen yliopiston johtamiskorkeakoulun professori Sirpa Virta on toiminut hankkeen tieteellisenä ja tutkimusmenetelmällisenä asiantuntijana.

Hankkeen ohjausryhmän toimintaan osallistuivat: Jari Aho (Puolustusvoimat), Pasi Eronen (puolustusministeriö), Tiina Ferm (sisäministeriö), Jarna Hartikainen (Kyberturvallisuuskeskus, Kirsi Karlamaan puolesta), Heikki Haukirauma (työ- ja elinkeinoministeriö), Lauri Holmström (sisäministeriö), Sari Kajantie (Suojelupoliisi), Janne Kanerva (oikeusministeriö), Anna Leppänen (Poliisiammattikorkeakoulu), Jussi Luomajärvi (liikenne- ja viestintäministeriö), Harri Martikainen (ohjausryhmän puheenjohtaja, sisäministeriö), Timo Piiroinen (Keskusrikospoliisi), Antti Savolainen (ulkoministeriö), Hanna-Miina Sihvonen (sisäministeriö) ja Mika Susi (Elinkeinoelämän keskusliitto).

Ohjausryhmä kokoontui 3 kertaa ja osallistujien kokoonpano vaihteli eri kokouksissa. Loppuraportti hyväksyttiin sähköpostimenettelyllä. Kiitokset ohjausryhmälle sekä kaikille selvitystyöhön ja raportin kommentointiin osallistuneille asiantuntijoille.

2. TIETOVERKKORIKOLLISUUDEN TILANNEKUVATYÖN TARVE

Tietojohtoinen poliisitoiminta on johtamismalli, jossa päätöksenteko nojaa rikostiedustelutietoon ja analyysiin. Tiedonkeruun ja analyysin avulla pyritään tunnistamaan esimerkiksi rikosten ennaltaehkäisyn ja keskeyttämisen kannalta strategisesti merkittävät kohteet ja toimenpiteet. (Ratcliffe 2008.) Tietojohtoista poliisitoimintaa on pyritty juurruttamaan 2010-luvulla Suomeen, minkä tuloksena poliisin analyysitoimintaa ja strategista suunnittelua on kehitetty projektilähtöisesti poliisiorganisaation monella tasolla (ks. esim. Pawli et al. 2010a, 2010b; Laitinen & Järvinen 2013; Salmela & Hakaniemi 2015). Oikea ja ajantasainen tilannetietoisuus on edellytys tietojohtoiselle poliisitoiminnalle. Tilannekuvan avulla operatiivisen toiminnan havainnot yhdistetään laajempiin, ilmiötason havaintoihin – sekä toisin päin – ja viestitään tarvittaville tasoille niin organisaation sisällä kuin ulkopuolisille sidosryhmille. Yhteistyö muiden viranomaisten ja elinkeinoelämän kanssa on tärkeää, koska tietoverkkorikollisuus ja kyberuhkat ilmiönä ylittävät rajat paitsi valtioiden myös eri organisaatioiden välillä.

Yhteiskunnan turvallisuusstrategiassa (2010) uhkia käsitellään häiriötilanteina[1]. Suomen kyberturvallisuusstrategia (2013) on jatkumoa Yhteiskunnan turvallisuusstrategialle ja siinä esitetyille tavoitteille kyberuhkien näkökulmasta. Vastuunjako häiriötilanteiden hoitamisessa perustuu eri viranomaisten toimivaltaan. Valtioneuvosto johtaa kyberturvallisuutta poliittisella tasolla strategisten linjausten, resurssien ja toimintaedellytysten kautta. Lähinnä kansliapäälliköistä ja muista ministeriöiden korkea-arvoisista viranhaltijoista muodostuva Turvallisuus-

[1] Häiriötilanne kuvataan Yhteiskunnan turvallisuusstrategiassa (2010, 85–86) seuraavasti: "Uhka tai tapahtuma, joka vaarantaa yhteiskunnan turvallisuutta, toimintakykyä tai väestön elinmahdollisuuksia ja jonka hallinta edellyttää viranomaisten ja muiden toimijoiden tavanomaista laajempaa tai tiiviimpää yhteistoimintaa ja viestintää".

komitea yhteen sovittaa toimintoja sekä seuraa Kyberturvallisuusstrategian kehittämistä ja toimeenpanoa. Toimivaltaiset viranomaiset huolehtivat toimialansa mukaisesta varautumisesta ja häiriötilanteiden hallinnasta. Ministeriöt puolestaan vastaavat oman toimialansa lainsäädäntötyöstä, yhteistyöstä muiden ministeriöiden kanssa sekä johtavat toimialaansa. Erityistehtäviä on määritelty liikenne- ja viestintäministeriölle (sähköiset tieto- ja viestintäjärjestelmät) sekä valtiovarainministeriölle (valtionhallinnon IT-toiminnot, tietoturvallisuus ja yhteisten palvelujärjestelmien turvaaminen). Yrityksiä koskevat vastuut puolestaan määritellään palvelusopimuksissa. (Emt. 19–20.) Edellä kuvatun kokonaisuuden haltuunotto ja ymmärrys edellyttävät monenlaista ja -tasoista tilannekuvaa.

Tilannekuvan tarkoitus on varmistaa viranomaisten riittävä tilannetietoisuus päätöksenteossa ja toiminnassa, erityisesti häiriötilanteissa sekä niihin varautumisessa. Tilannekuvaprosessin lähtökohdaksi on määritelty eri lähteisiin perustuva verkostomainen tiedonhankinta. Tieto tulee järjestää organisaatiotasolla niin, että toimijoilla on mahdollisuus saada itselleen relevantti tieto. Tilannekuva perustuu asiantuntijoiden arvioihin ja sen peruselementit ovat kuvaus vallitsevista olosuhteista, toimintavalmiuksista ja häiriötilanteesta taustoineen sekä arvio tilanteen kehittymisestä. Elementtejä yhdistellään tilannekuvatarpeiden mukaan. Operatiivista tilannekuvaa tarvitaan erityisesti häiriötilanteen aikana ja sen tulee olla mahdollisimman reaaliaikaista. Kuvailevampi, strateginen tilannekuva puolestaan laaditaan määräajoin tai tarkentavaksi analyysiksi ajankohtaisen ilmiön kartoittamiseksi. (Yhteiskunnan turvallisuusstrategia 2010, 57.) Yhteiskunnan turvallisuusstrategia käsittelee tilannekuvaa ensisijaisesti viranomaisnäkökulmasta. Kyberturvallisuudessa kuitenkin korostuu, että myös yrityksillä on käytössään riittävä tilannekuva ja toisaalta yritysten toiminnassa myös syntyy merkittävää tietoa, johon viranomaisilla ei ole näkymää ilman säännöllistä tiedonvaihtoa.

Yksi Viestintäviraston Kyberturvallisuuskeskuksen tärkeimmistä tehtävistä on eri tahojen yhdistetyn tilannekuvan ylläpitäminen ja tuottaminen (Suomen kyberturvallisuusstrategia 2013, 7). Poliisin, kuten muidenkin viranomaisten, rooli kokonaisuudessa on toimia tiiviissä yhteistyössä Kyberturvallisuuskeskuksen kanssa ja koota oman alansa tilannekuvaa osaksi yhdistettyä tilannekuvaa sekä saada tukea työhönsä Kyberturvallisuuskeskuksesta. Kybertilannekuvatietoa tuotetaan teknisen valvonnan ja seurannan lisäksi havaintojen, tiedustelun, muun tiedonhankinnan ja analyysin kautta. (Emt., 23–24.) Tietoverkkorikollisuuden osalta tilannekuvatyöstä vastaa ensisijaisesti Keskusrikospoliisi, jonka näkymä rakentuu ensisijaisesti rikostiedustelun, rikostutkinnan, muun tiedonhankinnan sekä tiedonvaihdon kautta.

Tietoverkkorikokset ja niihin liittyvä tieto muodostavat siis vain yhden osan kybertilannekuvasta. Tietoverkkorikoksen ja kyberrikoksen määritelmät ovat moninaiset ja termien käyttö on usein kontekstiriippuvaista sekä osin päällekkäistä. Tässä raportissa käytetään poliisin hahmottelemaa määritelmää, jonka mukaan "kyberrikoksella tarkoitetaan sellaisten rikosten tekomuotoja, joita esiintyy ainoastaan tietojärjestelmissä, kuten esimerkiksi hakkerointi, hyökkäykset tietojärjestelmiä vastaan, haittaohjelmien avulla tehdyt identiteettivarkaudet ja palvelunestohyökkäykset" (Poliisihallitus 2015, 8). Kyberrikos ja tietoverkkorikos ovat toistensa synonyymeja (emt.). Tietoverkkorikos voi olla tekona yksi häiriötilanteen tyyppi, joskin häiriötilanne käsitteenä viittaa laaja-alaiseen uhkaan tai tapahtumaan. Näin ollen tietoverkkorikollisuuden tilannekuvaa on tarpeellista kehittää sekä tietojohtoisen poliisitoiminnan kontekstissa osana poliisin omaa toimintaa kuin osana valtionhallinnon yhdistettyä häiriötilanteisiin varautumisen kokonaisuutta.

3. AINEISTO JA MENETELMÄT

3.1 Asiantuntijahaastattelut ja analyysi

Tiedonvaihtoa ja tilannekuvatyötä lähestytään selvityksessä kolmen tutkimuskysymyksen kautta:

> *1) Kuinka tietoverkkorikollisuuteen liittyvää tiedonvaihtoa toteutetaan kansallisesti tällä hetkellä?*
>
> *2) Miten eri toimijoiden yhteistä tilannekuvaa ylläpidetään ja millaisia pullonkauloja sekä esteitä siihen liittyy?*
>
> *3) Millaisia asioita tiedonvaihdossa tulee huomioida?*

Ensimmäisen aineiston muodostavat 13 nauhoitettua ja litteroitua asiantuntijahaastattelua. Asiantuntijahaastattelu menetelmänä perustuu ajatukseen, että huolella valitut haastateltavat ovat alansa keskeisiä asiantuntijoita, jotka pystyvät arvioimaan tutkimuskohdetta monipuolisesti (Alastalo & Åkerman 2010, 373–374). Haastateltavista organisaatioista yhdeksän edusti julkista sektoria ja neljä elinkeinoelämää (liite 1: Haastatellut organisaatiot). Kukin haastattelu kesti noin tunnin ja haastateltavia oli mukana tilanteessa yksi tai kaksi. Haastatteluja pohjustettiin tutustumalla poliisin kyberkeskuksen ja Viestintäviraston Kyberturvallisuuskeskuksen tilannekuvatoimintaan jo ennen haastattelurungon laatimista. Sopivia julkisia organisaatioita haastateltavaksi kartoitettiin tutustumalla kansallisen Kyberturvallisuusstrategian toimeenpano-ohjelmaan ja ehdotuksia haastateltavista asiantuntijoista pyydettiin laajasti sidosryhmiltä. Lisäksi tilannekuvatyöstä ja alustavista havainnoista käytiin keskusteluja useiden eri asiantuntijoiden kanssa poliisin sisällä ja muutamien poliisihallinnon ulkopuolisten asiantuntijoiden kanssa. Myös professori Sirpa Virta kommentoi haastattelurunkoa ja tutkimusasetelmaa.

Haastattelut toteutettiin marras-joulukuussa 2015 teemahaastatteluina. Osa kysymyksistä sovitettiin haastattelukohtaisesti ja teemojen järjestys vaihteli haastateltavan luontevan kerronnan mukaan. Haastattelut alkoivat pyynnöllä kertoa omasta työstään, mikä mahdollisti teemojen painottamisen haastateltavan ydinosaamisen perusteella. Esimerkiksi operatiivisia asiantuntijoita ohjattiin ajattelemaan ensisijaisesti oman työnsä näkökulmasta ja strategisen tason viranhaltijoille suunnattiin enemmän kokonaisuuden hallintaan liittyviä kysymyksiä.

Haastatteluaineiston analyysissa käytettiin sisällönanalyysia. Sisällönanalyysissä aineistosta erotetaan tutkimuksen tarkoituksen ja tutkimustehtävän kannalta olennaiset asiat, minkä jälkeen näin kerätty aineisto teemoitetaan, tyypitellään tai luokitellaan. Viimeisenä vaiheena on yhteenvedon tekeminen. (Tuomi & Sarajärvi 2009, 92.) Koska haastattelujen rakenne perustui haastateltavien luontevaan kerrontaan, litteroidut haastattelut luettiin läpi ja selvityksen kannalta keskeisimmät asiat (tilannekuvatyö, poliisin rooli, kehittämiskohteet, tutkimus ja lainsäädäntö) merkittiin värikoodein. Alustavan luokittelun jälkeen analyysia syvennettiin teemoittamalla aineisto kahdeksaan tutkimuskysymyksiä tukevaan pääteemaan (taulukko 1). Kukin teemoista purettiin vielä tarkentaviksi alateemoiksi. Analyysi koottiin yhteenvedoksi, joka esiteltiin poliisin kyberkeskukselle sekä ohjausryhmälle joulukuussa 2016. Myös Tampereen yliopisto ja Viestintäviraston Kyberturvallisuuskeskus saivat alustavat tulokset kommentoitavaksi. Työpajan ohjelma ja työryhmille suunnatut tehtävät koostettiin tulosten ja saatujen kommenttien perusteella. Keskeiset osat yhteenvedosta esitetään myös tämän loppuraportin Tulokset-luvussa loppuraportin julkisuus huomioiden.

Taulukko 1. Aineiston analyysi suhteessa tutkimuskysymyksiin

Tutkimuskysymys	Haastatteluaineiston analyysin pääteemat
1. Kuinka tietoverkkorikollisuuteen liittyvää tiedonvaihtoa toteutetaan kansallisesti tällä hetkellä?	Keskeisten organisaatioiden roolit Poliisin sisäinen tilannekuva
2. Miten eri toimijoiden yhteistä tilannekuvaa ylläpidetään ja millaisia pullonkauloja sekä esteitä siihen liittyy?	Lainsäädäntö Toiveita tiedonjaon ja tilannekuvatyön suhteen poliisille Rikostutkinta
3. Millaisia asioita tiedonvaihdossa tulee huomioida?	Yhteistyössä tärkeää Tilannekuvatyön tavoitteita Tilannekuvatyön kehittämiskohteita

3.2 Työpaja

Organisaatioiden tilannekuvatyötä kehitettiin organisaatioiden sisällä ja välillä jo projektin aikana. Esimerkiksi poliisin kyberkeskus ja Viestintäviraston Kyberturvallisuuskeskus järjestivät 12.1.2016 yhteisen kehittämispäivän. Kehittämispäivästä oli sovittu jo ennen projektin alkua ja se kattoi muitakin teemoja kuin tilannekuvatyön. Se tarjosi kuitenkin erinomaisen tilaisuuden tavoittaa molempien keskusten operatiivinen henkilöstö. Yksi kehittämispäivän työryhmistä keskittyi yhteisen tilannekuvatoiminnon pohtimiseen, joten työryhmän panosta voitiin hyödyntää myös tässä projektissa. Työryhmä koosti lopuksi lyhyet muistiinpanot ehdotuksistaan.

Projektin viimeinen aineistonkeruu tapahtui 13.1.2016 Poliisiammattikorkeakoulussa järjestetyssä työpajassa. Työpajaan osallistui yhteensä 25 henkilöä. Heistä 18 edusti viranomaisia, kolme elinkeinoelämää ja neljä korkeakouluja tai tutkimuslaitoksia (liite 2: Työpajaan osallistuneet henkilöt ja organisaatiot). Työpajaan pyrittiin löytämään osallistujajoukko, jolla olisi hyvä käsitys tilannekuvatyöstä ja tietoverkkorikollisuudesta sekä potentiaalia olla toteuttamassa tai hyödyntämässä tietoverkkorikollisuuden tilannekuvaa tulevaisuudessa. Vaikka elinkeinoelämän ja tutkimuksen edustus voi vaikuttaa vähäiseltä suhteessa viranomaisiin, useammalla osallistujalla oli nykyisen taustaorganisaationsa lisäksi monipuolista työkokemusta eri organisaatioista. Poliisiorganisaation edustus oli puolestaan työpajan aiheen takia selvästi suurin. Poliisin osallistujista lukumääräisesti eniten saapui Keskusrikospoliisista, koska tilannekuvatyön kehittäminen on ensisijaisesti heidän vastuullaan. Lisäksi työpaja päätettiin rajata hankkeen toimeksiannon mukaisesti yhteistyöhön eri viranomaisten ja muiden tahojen kanssa, joten siellä ei käsitelty poliisin sisäisiä kehittämistarpeita.

Asiantuntijoille lähetettiin viikkoa ennen työpajaa haastatteluaineiston perusteella laaditut ennakkotehtävät pohdittavaksi. Ohjeistuksessa kehotettiin pohtimaan mahdollisimman konkreettisia keinoja kehittää tietoverkkorikollisuuden tilannekuvatyötä (liite 3: Työpajan työryhmät, ennakkotehtävät ja ohjeistus). Tavoitteena oli löytää keinoja, jotka voitaisiin tarvittaessa ottaa käyttöön jo vuoden 2016 aikana. Työryhmäjako ja ennakkotehtävät käsittelivät kolmea teemaa:

1) Operatiivinen tiedonvaihto viranomaisten välillä ja lainsäädännön rajat

2) Tiedonvaihto poliisin ja yritysten välillä

3) Tietoverkkorikollisuuden pitkän tähtäimen ilmiötilannekuva

Työpajatyöskentely alkoi aamulla yhteisellä alustuksella, jossa esiteltiin projektin tarkoitusta ja alustavia tuloksia. Poliisin kyberkeskus esittäytyi ja kertoi lisäksi omista tavoitteistaan tietoverkkorikollisuuden tilannekuvatyön kehittämisessä. Sen jälkeen osallistujat jakaantuivat kolmeen ennalta sovittuun pienryhmään keskustelemaan ennakkotehtävien mukaisista teemoista ja heitä pyydettiin kirjaamaan kehitysehdotuksensa ylös sekä esittelemään tuotoksensa iltapäivällä koko työpajalle. Ennakkotehtävien tarkentavista kysymyksistä huolimatta työpajan osallistujia pyydettiin kertomaan työpajassa nimenomaan työryhmän näkemys tärkeistä kehittämiskohteista kuhunkin pääteemaan liittyen. Esitysten jälkeen työryhmien tuotoksista keskusteltiin kaikkien työpajaan osallistuneiden kesken ja keskustelu kirjattiin ylös.

Työpajan keskeiset tulokset koottiin nopeasti ja lähetettiin seuraavana päivänä osallistujille lyhyelle kommentointikierrokselle. Kommenttikierroksen tarkoitus oli varmistaa, että tutkijat olivat ymmärtäneet työryhmien tuotokset oikein ja toisaalta kerätä vielä jälkikäteen mahdollisesti mieleen tulleet ideat. Lisäksi kommentteja saatiin myös oikeusministeriöstä.

4. TIEDONVAIHDON OIKEUDELLINEN VIITEKEHYS

Tässä luvussa avataan viranomaisten väliseen tiedonvaihtoon liittyvää keskeistä lainsäädäntöä. Luvun tarkoitus on eritellä, kuinka eri lait vaikuttavat poliisin ja Viestintäviraston Kyberturvallisuuskeskuksen mahdollisuuksiin jakaa ja vaihtaa tietoa. Kuvaus auttaa ymmärtämään, miten ja miksi tiedonvaihdon oikeudellinen viitekehys toisinaan rajoittaa tiedonvaihtoa organisaatioiden välillä. Toisaalta esimerkiksi ilmiötilannekuvaa pystytään jakamaan riittävällä tasolla poistamalla datasta välitystiedot, jotka voivat paljastaa esimerkiksi epäillyn henkilöllisyyden tai teon kohteeksi joutuneen organisaation. Tilannekuvaan liittyvää yhteistyötä voi siis syventää huomattavan paljon jo nykyisessä oikeudellisessa viitekehyksessä.

4.1 Rikostorjuntatietojen julkisuudesta ja vaitiolovelvollisuudesta - erityisesti tietojen luovuttamisesta viranomaiskäyttöön[2]

Poliisin asiakirjojen osalta salassapitosäännöksiä ja tietojen luovuttamista koskevia säännöksiä on useissa laeissa. Lisäksi poliisilaissa on poliisin henkilöstön osalta säännökset vaitiolovelvollisuudesta ja vaitiolo-oikeudesta. Käsittelen tässä kirjoituksessa salassapitoa ja vaitiolovelvollisuutta ainoastaan esitutkinnassa ja toisaalta tiedustelussa syntyneen sekä muun poliisin tietoon tulleen materiaalin ja muun tiedon osalta. Tarkastelen aihetta ns. yleisöjulkisuuden näkökulmasta, joten asianosaisen asemaa ja tietojen luovuttamista asianosaiselle ei ole käsitelty lainkaan.

Keskeiset säännökset asiasta ovat laissa viranomaistoiminnan julkisuudesta (621/1999), esitutkintalaissa (805/2011), poliisilaissa (872/2011) ja laissa henkilötietojen käsittelystä poliisitoimessa (761/2003). PTR-toiminnon osalta tietojen käsittelystä on omat säännöksensä laissa poliisin, tullin ja rajavartiolaitoksen yhteistoiminnasta (687/2009) sekä PTR-viranomaisen henkilötietojen käsittelyä koskevassa lainsäädännössä[3]. Rahanpesun selvittelykeskuksen hallussa olevien rahanpesun ja terrorismin rahoittamisen estämisessä ja selvit-

[2] Luvun 4.1 on laatinut Karl Linderborg Keskusrikospoliisista.

[3] Laki henkilötietojen käsittelystä poliisitoimessa (621/2003), laki henkilötietojen käsittelystä Tullissa (639/2015) ja laki henkilötietojen käsittelystä rajavartiolaitoksessa (579/2005).

tämisessä tarvittavien tietojen ja asiakirjojen luovuttamisesta muiden viranomaisten käyttöön on lisäksi säännökset laissa rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä (503/2008).

Viranomaisten toiminnan julkisuudesta annetussa laissa (ns. julkisuuslaki, JulkL) säädetään oikeudesta saada tieto viranomaisten julkisista asiakirjoista, viranomaisessa toimivan vaitiolovelvollisuudesta, asiakirjojen salassapidosta ja muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista samoin kuin viranomaisten velvollisuuksista ko. lain tarkoituksen toteuttamiseksi (2 §). Mainitun lain 1 §:n 1 momentin mukaan viranomaisten asiakirjat ovat lähtökohtaisesti julkisia ellei niiden salassapidosta ole laissa erikseen säädetty.

Esitutkintalaissa (ETL) ei ole esitutkinta-asiakirjojen ns. yleisöjulkisuuden osalta omia säännöksiä vaan siinä viitataan julkisuuslakiin (ETL 9:7). Julkisuuslain 24.1 §:ssä määritellään salassa pidettävät viranomaisten asiakirjat. Poliisin esitutkinnan osalta huomionarvoinen on erityisesti saman säännöksen 3 kohta, jossa määrätään esitutkinta-aineiston salassapidosta. Sen mukaan salassa pidettäviä ovat poliisille ja muille esitutkintaviranomaisille ja syyttäjälle sekä tarkastus- ja valvontaviranomaisille tehdyt ilmoitukset rikoksesta, esitutkintaa ja syyteharkintaa varten saadut ja laaditut asiakirjat sekä haastehakemus, haaste ja siihen annettu vastaus rikosasiassa, kunnes asia on ollut esillä tuomioistuimen istunnossa taikka kun syyttäjä on päättänyt jättää syytteen nostamatta tai kun asia on jätetty sikseen, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna rikoksen selvittämistä tai tutkinnan tarkoituksen toteutumista tai ilman painavaa syytä aiheuta asiaan osalliselle vahinkoa tai kärsimystä tai estä tuomioistuinta käyttämästä oikeuttaan määrätä asiakirjojen salassapidosta oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain (370/2007) mukaan.

Kaikki esitutkintaan liittyvät asiakirjat ovat siis lähtökohtaisesti salassa pidettäviä (salassapito-olettama) ellei tutkinnanjohtaja laissa mainituista syistä päätä toisin. Säännös antaa kuitenkin tutkinnanjohtajalle melko paljon harkintavaltaa ottaen huomioon, että lain esityöt ovat näiltä osin varsin suppeat. Tässä yhteydessä on myös hyvä huomioida, että säännös koskee yhtä hyvin tietojen luovuttamista luonnollisille henkilöille kuin niiden luovuttamista viranomaisille.

Säännöksen tarkoituksena on hallituksen esityksen HE 30/1998 vp. perusteluiden mukaan varmistaa esitutkinnan onnistuminen, estää esitutkintatietojen ennenaikaisesta julkiseksi tulosta rikoksesta epäillylle aiheutuvat vahingot sekä turvata tuomioistuimelle mahdollisuus käyttää sille kuuluvaa oikeutta määrätä asiakirjojen salassapidosta oikeudenkäynnin julkisuudesta annetun lain mukaisesti. Salassapidon perusteet liittyvät siis yhtäältä yleiseen etuun ja toisaalta yksityiseen etuun. Toisin kuin saman lain 1 §:ssä on säädetty, säännöksessä tarkoitetut asiakirjat ovat oletusarvoisesti salassa pidettäviä, joskin salassapitovelvoite ei ole ehdoton. Esitutkintaviranomainen voi siten antaa tällaisesta asiakirjasta tiedon, jos on ilmeistä, etteivät esitutkinnan tavoitteet tai tuomioistuimen mahdollisuudet määrätä oikeudenkäynti-asiakirjat salassa pidettäviksi taikka rikoksesta epäillyn edut vaarannu.

Esitutkinnan osalta säännös turvaa ensisijaisesti esitutkinnan tavoitteiden toteutumista. Rikoksen selvittäminen vaarantuisi, mikäli esitutkintaa koskevat asiakirjat tulisivat julkiseksi kovin varhaisessa vaiheessa. Rikoksen selvittäminen voisi vaikeutua mm. siitä syystä, että jo hankittuun tai tulevaisuudessa hankittavaan todisteluun pyrittäisiin vaikuttamaan annetun tiedon johdosta. Toisaalta on suojattava myös rikoksesta epäillyn etua. Keskeistä on etenkin syyttömyysolettama ja siitä johtuvat salassapitovelvoitteet. Ennenaikainen tiedottaminen esitutkinnasta voi aiheuttaa ennen kaikkea rikoksesta epäillyn leimaamisen syylliseksi jo ennen kuin syytteen nostamisesta on ehditty tehdä minkäänlaisia ratkaisuja. Tästä puolestaan voi aiheutua epäillylle säännöksessä tarkoitettua vahinkoa tai kärsimystä.

JulkL 24 §:n 1 momentti sisältää lisäksi lukuisia muita säännöksiä, joiden nojalla viranomaisen hallussa olevat asiakirjat on pidettävä tai voidaan pitää salassa. Salassapidon perusteena on osin julkinen ja osin yksityinen etu. Osa säännösten perusteella salassa pidettävistä asiakirjoista on sellaisia, ettei niistä saa lainkaan antaa tietoja ja osa sellaisia, joista voi antaa tietoja, jos säännöksessä mainitut muut edellytykset täyttyvät. Poliisin ja muun esitutkintaviranomaisen rikoksen ehkäisemistä ja niiden selvittämistä varten ylläpitämät rekisterit ja rikosten ehkäisemistä koskevat selvitykset ovat sellaisia, joita koskee ehdoton salassapitosäännös (JulkL 24.1,4).[4]

Lisäksi poliisin oikeutta antaa tietoja esitutkinnasta rajoittaa esitutkintalain 10 luvun 7 §. Ko. säännös koskee esitutkinnasta tiedottamista. Säännös sisältää samantapaisen vahinkoedellytyslausekkeen kuin edellä mainittu JulKL:n 24 §:n 1 momentin 3 kohta. Esitutkinnasta tiedottaminen on säännöksen mukaan tehtävä niin, ettei ketään aiheettomasti saateta epäilyksenalaiseksi ja että kenellekään ei tarpeettomasti aiheuteta vahinkoa tai haittaa.

Poliisin vaitiolovelvollisuudesta ja vaitiolo-oikeudesta säädetään poliisilain 7 luvussa. Luvun 1 §:n 1 momentin mukaan poliisin henkilöstöön kuuluva virkamies ei saa ilmaista luottamuksellisesti tietoja antaneen taikka valeostajana tai peitehenkilönä toimineen henkilöllisyyttä koskevaa tietoa, jos tiedon ilmaiseminen vaarantaisi luottamuksellisesti tietoja antaneen tai valeostajana tai peitehenkilönä toimineen tai hänen läheistensä turvallisuuden. Vaitiolovelvollisuus on voimassa myös, jos henkilöllisyyttä koskevan tiedon ilmaiseminen vaarantaisi jo käynnissä olevan tai tulevan tiedonhankinnan. Saman säännöksen 2 momentin mukaan muilta osin vaitiolovelvollisuuteen sovelletaan JulkL:n säännöksiä, muun lain säännöksiä ja poliisilain saman luvun muita säännöksiä.[5] Edelleen saman momentin mukaan sama vaitiolovelvollisuus on sillä, joka on työsopimussuhteessa poliisiin tai joka hänelle myönnettyjen poliisivaltuuksien nojalla tai muulla perusteella suorittaa poliisitehtävää.

Huomionarvoinen etenkin tämän kirjoituksen osalta on saman luvun 2 §, jossa säädetään tietojen antamisesta vaitiolovelvollisuuden estämättä. Sen mukaan poliisin henkilöstöön kuuluvan virkamiehen tai muun 1 §:n 2 momentissa tarkoitetun henkilön vaitiolovelvollisuus ei estä tiedon antamista viranomaiselle tai julkista tehtävää hoitavalle yhteisölle, jolla säädetyn tehtävänsä vuoksi on tarve saada tieto muuten salassa pidettävästä seikasta taikka henkilön luotettavuudesta tai sopivuudesta tehtävään.

Poliisin vaitiolovelvollisuuden väistyminen luovutettaessa tietoa toisille viranomaisille on siis sidottu yhtäältä toisen viranomaisen säädettyyn tehtävään ja toisaalta siihen liittyvään tarpeeseen saada tieto ko. salassa pidettävä seikasta. Tämä ei tarkoita sitä, että salassa pidettävää ja vaitiolovelvollisuuden alaista tietoa voisi luovuttaa yksistään näillä perusteilla vaan tiedon luovutusta harkittaessa on otettava huomioon myös muista laeista mahdollisesti johtuvat rajoitteet (esimerkiksi henkilötietoja ja -rekistereitä sekä JulkL:n 24 §:n 1 momentin salassapitoa koskevat säännökset).

Toinen huomionarvoinen poikkeus koskee saman säännöksen 2 momenttia, jonka mukaan säädetty vaitiolovelvollisuus ei estä ilmaisemasta sellaisia tietoja, joiden ilmaisemiseen on yksittäistapauksessa painava syy hengelle tai terveydelle vaarallisen tapahtuman, vapauteen kohdistuvan rikoksen tai huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi taikka valtion turvallisuuden varmistamiseksi. Säännös mahdollistaa salassa pidettävän tiedon luovuttamisen toiselle viranomaiselle tai muulle juridiselle henkilölle taikka luonnollisel-

[4] Ks. HE 30/1998 vp. ja Helminen, Fredman, Kanerva, Tolvanen & Viitanen 2012, 590 - 599.

[5] JulkL:n 23 §:n 1 momentin mukaan viranomaisen palveluksessa oleva samoin kuin luottamustehtävää hoitava ei saa paljastaa asiakirjan salassa pidettävää sisältöä tai tietoa, joka asiakirjaan merkittynä olisi salassa pidettävä, eikä muutakaan viranomaisessa toimiessaan tietoonsa saamaa seikkaa, josta lailla on säädetty vaitiolovelvollisuus.

le henkilölle säännöksen mainitsemissa olosuhteissa, mikäli myös muut lain säännökset tämän sallivat.

Kansainvälisessä tietojenvaihdossa syntyy asiakirjoja, joita koskevat osin omat säännöksensä. Kansainväliseen poliisiyhteistyöhön liittyvät tietojen käsittelyä koskevat säännökset ovat henkilötietojen käsittelyä poliisitoimessa koskevan lain 6 luvussa. Oikeusapumenettelyä koskee puolestaan laki kansainvälisestä oikeusavusta rikosasioissa (4/1994) ja laki keskinäisestä oikeusavusta rikosasioissa Euroopan unionin jäsenvaltioiden välillä tehdyn yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta ja yleissopimuksen soveltamisesta (148/2014). Tässä yhteydessä on syytä huomioida, että oikeusapua antanut valtio voi asettaa erityisehtoja tietojen käyttämiselle mm. niin, että tietoja voidaan käyttää vain esitutkinnassa, syyteharkinnassa ja asiaa koskevassa tuomioistuinmenettelyssä. Näiden tietojen käsittelystä on säännöksiä kansallisen lainsäädännön lisäksi useissa eri kansainvälisissä sopimuksissa, Euroopan Unionin lainsäädännössä ja Neuvoston puitepäätöksissä.

Yhteenvetona voisi todeta, että edellä mainitut säännökset antavat poliisille jokseenkin laajan harkintavallan siitä, mitä tietoja poliisi voi kussakin tilanteessa luovuttaa ainakin muiden viranomaisten käyttöön. Toisaalta tietojen luovuttamista on säännelty hyvinkin tarkasti tiukoin vaitiolo- ja salassapitosäännöksin sekä esimerkiksi henkilötietojen osalta käyttötarkoitussidonnaisuutta koskevin säännöksin.

Tietoja luovuttaessa on edelleen huomioitava, että ETL 2 luvun 2 §:n mukaan esitutkintaa johtaa tutkinnanjohtaja, joka tarkoittaa sitä, että tutkinnanjohtaja tekee esitutkintaa koskevat päätökset joko itsenäisesti tai keskusteltuaan syyttäjän kanssa.

JulkL:n 14 §:n mukaan viranomaisen asiakirjan antamisesta päättää se viranomainen, jonka hallussa asiakirja on. Tiedon antaa henkilöstöön kuuluva, jolle viranomainen on tehtävän määrännyt (2 mom.). Tiedottamisesta vastaa ETL 11 luvun 7 §:n 4 momentin mukaan tutkinnanjohtaja elleivät esimiehet ole muuta määränneet, joten on johdonmukaista, että tutkinnanjohtaja viranomaisessa ratkaisee salassa pidettävyyden, ellei muuta määrätä.

ETL 5:2,2 mukaan syyttäjä päättää esitutkintatoimenpiteestä asian siirryttyä hänelle esitutkinnan päättämisen jälkeen, jolloin myös syyttäjän on eri viranomaisena omalta osaltaan harkittava salassapito syyttäjäviranomaisen hallussa olevan esitutkintapöytäkirjan osalta. Käytännössä syyttäjät ohjaavat pyynnöt JulkL:n 15 §:n perusteella poliisille, joka on laatinut esitutkintapöytäkirjan ja joutuu arvioimaan salassapitokysymykset ennen luovuttamista. Se aineisto, joka tulee oikeudenkäyntiaineistoksi, on tuomioistuimen arvioitava oikeudenkäynnin julkisuudesta annetun lain, julkisuuslain ja erityislakien perusteella.

4.2 Viestintäviraston Kyberturvallisuuskeskuksen tietojenkäsittelyoikeudet[6]

Viestintäviraston oikeudet tietoturvaloukkauksiin liittyvien tietojen käsittelyyn perustuvat Viestintävirastolle tietoyhteiskuntakaaressa (917/2014) säädettyihin tehtäviin. Lain 304 §:n mukaan Viestintäviraston tehtävänä on muun muassa kerätä tietoa verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvista tietoturvaloukkauksista ja niiden uhkista, tiedottaa tietoturva-asioista sekä selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia. Lain 3 §:n mukaan tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden

[6] Luvun 4.2 on laatinut Jarkko Saarimäki Kyberturvallisuuskeskuksesta.

käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä.

Merkittävä osa Viestintävirastolle luovutettavista tietoturvaloukkausten selvittämiseen liittyvistä tiedoista annetaan tietoturvaloukkauksen kohteen toimesta viestinnän osapuolen oikeuksin. Viestintävirastolle on kuitenkin säädetty tietoyhteiskuntakaaren 316 §:ssä myös erityinen tiedonsaantioikeus viestintään liittyvistä tiedoista. Oikeutta käytetään erittäin harvoin. Erityisten tiedonsaantioikeuksiensa perusteella saamien tietojen salassapidosta säädetään tietoyhteiskuntakaaren 318 §:ssä. Muilta osin Viestintäviraston tietoturvaloukkauksiin liittyviin tietoihin sovelletaan pääsääntöisesti julkisuuslakia.

Voimassa oleva sääntely rajoittaa poliisin tiedonsaantioikeuksia Viestintäviraston erityisten tiedonsaantioikeuksiensa perusteella saamista luottamukselliseen viestintään liittyvistä tiedoista. Tiedot ovat sellaisia, joiden saamiseen poliisille on säädetty omat erityiset tiedonsaantioikeudet rajoituksineen. Arvioinnissa on kiinnitetty huomiota myös siihen, että hallituksen esityksessä poliisilaiksi (HE 57/1994 vp) lausutaan 35 §:ää koskevassa perusteluosassa: "Pykälässä määritelty tietojensaantioikeus syrjäyttäisi muualla laissa säädetyt salassapitovelvollisuudet, ellei salassapitovelvollisuutta koskevassa säännöksessä nimenomaan kielletä tietojen luovuttamista poliisille. Kielto voidaan ilmaista myös luettelemalla tietojensaantiin oikeutetut viranomaiset mainitsematta poliisia niiden joukossa".

Viestintäviraston toimintaedellytysten kannalta tietojen luovuttamisen arvioinnissa on keskeistä ennen kaikkea viraston toimintaa kohtaan tunnetun luottamuksen turvaaminen. Jos tietoturvaloukkauksen kohteeksi joutuva taho kieltää Viestintävirastoa ilmoittamasta asiasta poliisille, Viestintäviraston on voitava käsitellä tietoja luottamuksellisesti. Tämä on välttämätöntä, jotta Viestintävirastolle luovutetaan tietoja vapaaehtoisesti myös jatkossa. Poikkeuksen muodostavat kuitenkin rikoslain (39/1889) 15 luvun 10 §:ssä tarkoitetun rikoksen tunnusmerkistön täyttävät tilanteet.

5. TULOKSET

5.1 Tietoverkkorikollisuuden tilannekuvatyön nykytila

Keskusrikospoliisiin sijoitettu poliisin kyberkeskus ja poliisilaitokset vastaavat tietoverkkorikosten tutkinnasta Suomessa. Kyberkeskuksen tehtävä on koota ja välittää tietoverkkorikollisuuden tilannekuvaa valtionhallinnossa. Esimerkiksi Viestintäviraston Kyberturvallisuuskeskuksen laajaan tilannekuvatuotevalikoimaan ei sisälly erillistä rikollisuuden tilannekuvatuotetta, eikä mikään sen nykyisistä toiminnoista ole keskittynyt ensisijaisesti rikollisuuteen, vaan työn näkökulma on pikemminkin poikkeamanhallinta. Tulli ja poliisin kyberkeskus tekevät päivittäistä yhteistyötä keskenään, mutta tullin toimivaltaan kuuluvat rikokset – ja täten tilannekuvatyö – liittyvät enemmän tietoverkoissa tapahtuviin rikoksiin kuin varsinaiseen tietoverkkorikollisuuteen.

Tietoverkkorikollisuuden tilannekuvaa poliisin kyberkeskuksessa kokoaa pääasiassa tiedonhankintatiimi, jonka ensisijainen tehtävä on tukea rikostutkintaa tekemällä tietoverkkorikostiedustelua poliisin kyberkeskuksen tutkinnassa oleviin juttuihin liittyen. Perinteiseen rikollisuuteen kohdistuva internet-tiedustelu (esimerkiksi sosiaalisen median seuranta) suoritetaan tiedusteluosastolla. Tietoverkkorikollisuuden tilannekuvatyön kehittäminen aloitettiin syksyllä 2015. Tyypilliset tiedonkeruun lähteet ovat erilaisia verkkolähteitä. Twitter, monenlaiset online foorumit ja poliisin oma Nettivinkki-palvelu, jonne kansalaiset voivat ilmoittaa rikosepäilyis-

tään, ovat esimerkkejä säännöllisesti seurattavista lähteistä. Sosiaalisen median kautta voi seurata niin tietoturva-alan toimijoiden ja viranomaisten kuin rikollisten toimia. Poliisin kyberkeskus käyttää myös muiden viranomaisten, erityisesti Kyberturvallisuuskeskuksen, toimittamia kyberturvallisuuden raportteja sekä säännöllisiä tilannekuvatuotteita oman tilannetietoisuutensa ylläpitämisessä. Kotimaisten tahojen lisäksi tietoa vastaanotetaan kansainvälisiltä kumppaneilta esimerkiksi raportteina, sähköpostiviesteinä ja tiedustelutietona. Säännöllistä ja järjestelmällistä tilannetietoisuuden lisäämiseen pyrkivää tiedonvaihtokulttuuria kotimaisten poliisilaitosten kanssa ei toistaiseksi ole.

Tietoverkkorikollisuuden tilannekuvaa välitetään tällä hetkellä kotimaisille viranomaisille lähinnä suullisesti viikoittaisissa palavereissa (poliisin kyberkeskus, Kyberturvallisuuskeskus, Suojelupoliisi, Valtioneuvoston tilannekeskus ja Puolustusvoimat) sekä tarpeen mukaan tapahtuvin yhteydenotoin esimerkiksi yhteisten pikaviestintäpalveluiden kautta, sähköpostitse tai puhelimitse. Yhteinen pikaviestintäpalvelu on keskeinen matalan kynnyksen tiedonvälitysväylä niin viranomaisten kesken kuin viranomaisten ja yritysten välillä. Vasta lyhyen aikaa koottu kirjallinen tietoverkkorikollisuuden viikkoraportti sisältää lyhyen kuvauksen Suomeen vaikuttavista ajankohtaisista rikosilmiöistä, esimerkiksi haittaohjelmista, palvelunestohyökkäyksistä ja aktiivisista hakkeriryhmistä. Lisäksi raportissa on kooste valikoiduista poliisilaitosten tutkinnassa olevista tapauksista. Viikkoraportti hakee vielä jakotapaansa ja kohdeyleisöänsä, sillä kysyttäessä haastateltavilta poliisilta saadusta tiedosta, viikkoraportti mainittiin harvoin oma-aloitteisesti. Raportti herätti kuitenkin kiinnostusta useassa viranomaisessa. Viikkoraportti on toistaiseksi melko tuntematon myös poliisin sisällä, sillä edes kaikki poliisin kyberkeskuksen henkilöstöstä eivät tienneet, että tällaista kirjallista raporttia tehdään. Raportin jako poliisilaitoksille, tullille ja rajavartiolaitokselle tapahtuu PTR-kanavaa pitkin, mutta tiedon jakamista kyseisissä organisaatioissa sen pidemmälle ei ole varmistettu. Poliisin kyberkeskuksen ja suojelupoliisin kokoama tietoverkkorikollisuuden vuosikatsaus osoittautui haastatteluissa tutummaksi, joskaan se ei ollut tuttu kaikille. Poliisihallituksen, sisäministeriön poliisiosaston sekä Keskusrikospoliisin johdon suuntaan tieto välittyy pääosin keskustelemalla ja kyselemällä, eikä analysoidun tilannekuvan toimittaminen ole määrämuotoista. Myös erilaiset seminaarit, harjoitukset, tapaamiset, lausunnot sekä yhteistyöryhmät ovat keino välittää ja saada ilmiötason tilannekuvaa.

Poliisin tiedossa oleva, Suomea koskeva tietoverkkorikollisuuden tilannekuvaa tuottava tutkimus on vähäistä eikä kansainvälistä tutkimusta ei seurata säännöllisesti, mikä selittynee osin resurssikysymyksillä ja toisaalta yhteisen kulttuurin puuttumisella. Kyberturvallisuusstrategian toimeenpano-ohjelmassa (2014, 29) Poliisiammattikorkeakoululle on kuitenkin määritetty tehtäväksi lisätä kyberalan tutkimusta ja yhteistyötä yliopistojen kanssa. Sen sijaan minkälaista ja -tasoista kyberalan tutkimusta on tarkoitus lisätä tai minkä tieteenalojen suuntaan olisi tavoiteltavaa verkostoitua, ei ole toistaiseksi määritelty. Otantapohjaista seurantatietoa väestön uhriutumisesta saadaan nykyään vain Eurobarometri-kyselytutkimusten kautta (esim. EC 2012). Kaupan ja teollisuuden alaan kohdistunutta rikollisuutta on kartoitettu kyselytutkimuksella vuonna 2011, jolloin yhtenä teemana oli myös tietoturvallisuus ja tietoverkkorikollisuus, mutta tutkimusta ei ole toistaiseksi toistettu (Salmi et al. 2011).

5.2 Tietoverkkorikollisuuden tilannetietoisuus osana kyberturvallisuuden kokonaistilannekuvaa

Tietoverkkorikollisuuden tilannetietoisuus on yksi osa kybertilannekuvien kokonaisuutta. Onnistuessaan tiedonjako auttaa muita organisaatioita tunnistamaan ja huomioimaan rikosnäkökulman omassa työssään. Samoin poliisi tarvitsee myös muilta organisaatioilta apua oman

tilannekuvatyönsä tueksi. Yhteisen intressin takia on tärkeää, että tietoverkkorikollisuuden tilannekuvatyön kehitys tapahtuu yhteistyössä kybertilannekuvatyön kokonaisuuden kanssa.

Viestintäviraston Kyberturvallisuuskeskus on paitsi toimivaltuuksiensa ja tehtäväkuvansa puolesta myös käytännössä tärkein linkki kyberturvallisuuden kokonaistilannekuvan ylläpitämisessä Suomessa. Näkemystä tukevat sekä viranomaisten että elinkeinoelämän haastattelut. Yhteistyö Kyberturvallisuuskeskuksen kanssa oli tyypillisesti vakiintuneinta ja tiheintä, jopa päivittäistä. Kyberturvallisuuskeskuksen suorat palvelut on luotu ensisijaisesti huoltovarmuuskriittisten yritysten ja valtion tarpeisiin, mutta monet tilannekuvatuotteista, kuten ajankohtaiset varoitukset, tiedotteet ja ohjeistukset ovat julkisia ja palvelevat monenkaltaisia yrityksiä sekä yksityisiä henkilöitä. Kyberturvallisuuskeskus vastaanottaa ilmoituksia tietoturvaloukkauksista lisäksi sellaisilta kotimaisilta ja ulkomaisilta tahoilta, joilla ei ole laissa määrättyä ilmoitusvelvollisuutta. Myös muut julkiset organisaatiot ovat pääsääntöisesti yhteydessä toisiinsa, mutta yhteistyön muoto ja tavoitteet eivät tuntuneet yhtä selkeiltä. Kiinteä yhteistyö Kyberturvallisuuskeskuksen kanssa perustuu heidän asemaansa palvelutuottajana, tiedon kokoajana ja välittäjänä. Tilannekuvatyö on Kyberturvallisuuskeskuksessa harkittu kokonaisuus, jota kehitetään koko ajan eteenpäin. Keskeinen ero muihin operatiivisiin viranomaisiin rikospoliisiin, suojelupoliisiin, puolustusvoimiin ja tulliin nähden on, että kyberturvallisuustyö on muille organisaatioille vain yksi osa-alue muiden joukossa ja perustehtävä on rakentunut fyysisen maailman turvallisuustarpeisiin.

Viranomaisyhteistyön kokonaisuuden kehittäminen tapahtuu tällä hetkellä pääsääntöisesti yhteistyöryhmien ja yhteisten harjoitusten kautta. Kenties tärkeimmät niistä ovat Valtiovarainministeriön vetämä VIRT-yhteistyöryhmä (virtual incident response team) ja Turvallisuuskomitean koordinoimat VALHA-harjoitukset (valtakunnallinen valtionhallinnon valmiusharjoitus). VALHA 15–16 -harjoituksen pääteema on hybridiuhkiin varautuminen ja sen tarkoitus on kehittää valtionhallinnon yhteistoimintakykyä vakavien häiriötilanteiden ja poikkeusolojen hallinnassa (Turvallisuuskomitean tiedote 8.6.2015). Kehittämistyötä tehdään ensisijaisesti valtion ja kriittisen infrastruktuurin näkökulmista.

Yhteistä haastatteluissa oli se, että kaikki julkisen sektorin haastateltavat arvioivat kyberturvallisuuden kokonaistilannekuvan ylläpitämisen edellyttävän eri lähteistä tulevan tiedon yhdistelyä ja poikkihallinnollista analyysia. Haastateltavat tunnistivat, että jo teknisellä tasolla poikkeamahavaintoja syntyy useaan eri paikkaan, eikä yhdelläkään organisaatiolla ole tällä hetkellä kokonaisnäkymää tilanteesta. Poikkeamahavaintojen tueksi tarvitaan muuta tietoa, kuten tietoa muualla tunnistetuista kyberuhkista, orastavista ilmiöistä niin kybertoimintaympäristössä kuin reaalimaailmassa, järjestelmien toiminnasta sekä niiden keskinäisistä suhteista. Jokaisen viranomaisen näkökulma, näkymä ja analyysi koettiin tärkeäksi kokonaiskuvan muodostamisessa. Haastateltavat olivat tietoisia, että eri viranomaisten välisistä yhteisistä rajapinnoista ja tiedonvaihdosta on keskusteltu jo pitkään. Monet mainitsivat, että viranomaisyhteistyö on kehittynyt ja jatkuvasti menossa parempaan suuntaan. Toisaalta osa haastateltavista koki kehityksen turhan hitaana ja samojen tunnistettujen ongelmien odottavan ratkaisua vuodesta toiseen. Tiedonvaihdon merkitys koettiin kriittisenä ja suhtautuminen yhteistyöhön on positiivinen. Yksi tai useampi vastaaja näki, että virkamiesvaihto, "kouluttaminen" lukemaan toisten tilannekuvaraportteja, yhteiset tilannekuvatuotteet ja tiedon vertaaminen ristiin olivat askelia edistää kybertilannekuvatyön kokonaisuutta. Virkamiesvaihdon ajateltiin lisäävän organisaatioiden keskinäistä ymmärrystä. Yksi haastateltu tilannekuvatyön asiantuntija puolestaan totesi raporttien hyödyntämisen jäävän vajavaiseksi, jos tiedon vastaanottajaa ei opasteta lukemaan tuotetta ja niistä ei anneta palautetta. Yhteisten tilannekuvatuotteiden kokoamisen arveltiin tiivistävän yhteistyötä sekä edistävän eri näkökulmien esille tuomista. Yhteistä analyysia pohdittiin toteutettavaksi joko yhdessä kirjoitettujen raporttien avulla (yksi koordinoi ja muut kommentoivat) sekä saman pöydän ääressä keskustelemalla joko tarvitta-

essa tai säännöllisesti. Syvin esitetty yhteistyömalli oli lainsäädäntömuutoksia edellyttävä keskus (ns. fusion center), jonne sekä julkiset organisaatiot että yksityiset yritykset syöttäisivät tietoa analysoitavaksi. Esikäsittelyn perusteella ratkaistaisiin tahot, joille tilanteen hoitaminen kuuluu. Keskitettyyn malliin liittyviä huolia olivat esimerkiksi resurssikysymykset ja se, suodattuuko yksittäisten organisaatioiden näkökulmasta relevanttia tietoa pois esikäsittelyn aikana.

Kyberturvallisuuden tilannekuvaa tuottava tutkimus, tai ainakin sen hyödyntäminen, on Suomessa toistaiseksi satunnaista ja perustuu enemmän yksittäisiin hankkeisiin. Haastatteluissa ei käynyt ilmi, että yhteistyö korkeakoulujen tai tutkimuslaitosten kanssa olisi jatkuvaa ja tuottaisi säännöllistä seurantatietoa tilannetietoisuuden lisäämiseksi. Puolustusvoimien tutkimuslaitoksen ja Maanpuolustuskorkeakoulun tutkimuksella todettiin kuitenkin olevan merkitystä erityisesti Puolustusvoimien tilannekuvatyön kehittämisessä. Potentiaalia yhteistyön syventämiseen on. Esimerkiksi verkkojen turvallisuutta ja monitorointia tutkitaan Aalto yliopistossa, Helsingin yliopistossa, Jyväskylän yliopistossa, Tampereen teknillisessä yliopistossa ja Turun yliopistossa (Lehto & Kähkönen 2015, 36–38). Harjoitusympäristöjä kyberhyökkäyksien toteuttamiseen ja niiltä puolustautumiseen on Jyväskylän ammattikorkeakoulun IT-insituutin kyberturvallisuuden tutkimus-, koulutus- ja kehityskeskuksessa JYVSECTECissä, Tampereen teknillisessä yliopistossa (TUTCyberLabs) ja VTT:lla (Cyber War Room). Jyväskylän yliopiston yksi tutkimusteema on kybertilannekuva ja -tietoisuus. (Emt. 36–38; 20.) VTT:n ja Cyberlab Oy:n Kyberosaaminen Suomessa -tutkimushankkeen alustavia tuloksia valotetaan VTT:n blogissa kertomalla, että vuorovaikutus julkisen hallinnon ja tutkimusmaailman välillä kyberturvallisuudessa ei ole systemaattista. Siksi olisikin syytä harkita, pitäisikö luoda jokin foorumi, joka välittäisi tietoa ja vahvistaisi vuorovaikutusta tutkimus- ja viranomaistoimijoiden välillä. (Pelkonen 2015.)

5.3 Tiedonvaihdon edellytykset, tavoitteet ja toiveet

Kun haastateltavia pyydettiin arvioimaan tiedonvaihdon edellytyksiä, he nostivat esiin kolme selvästi tärkeintä edellytystä. Tiedonvaihdon on hyödytettävä kaikkia osapuolia, tiedonvaihdon onnistumisen on perustuttava luottamukseen ja asetettuja rajoja on noudatettava. Haastateltavat kokivat, että tilannekuvatyön on liityttävä kunkin organisaation perustehtävään ja tiedonvaihto ei saa muodostaa kohtuutonta rasitetta päivittäistoiminnalle. Jos tilannekuvatyö on irrallaan organisaation muusta toiminnasta, sen teho jää heikoksi, sillä tilannekuvatyötä pidettiin ennen kaikkea toiminnan johtamisen ja viestinnän välineenä. Yhteistyön onnistumisen kriteerinä on toiminnasta saatava hyöty ja sitä kautta osallistumisen kannattavuus. Käytännössä se tarkoittaa, että tietoa jaetaan vastavuoroisesti. Tietoa on annettava vaihdossa, yksipuolinen tiedonjako ei pidemmän päälle toimi. Erityisesti elinkeinoelämän edustajat kokivat vastavuoroisuuden erittäin tärkeäksi. Hyötyä arvioitaessa tiedonjakajat toivoivat myös palautetta ja vuoropuhelua siitä, oliko jaettu tieto ollut merkityksellistä vai ei. Palaute auttaa kehittämään toimintaa jatkossa ja se ylläpitää motivaatiota, kun kuulee olleensa avuksi. Organisaatiolle hyödytöntä vapaaehtoista työtä ei yksinkertaisesti kannata tehdä. VIRT-yhteistyö ja Kyberturvallisuuskeskuksen yhteispalaverit yritysten kanssa mainittiin useammassa haastattelussa onnistuneiksi yhteistyömuodoiksi.

Luottamukselliset välit koettiin tärkeäksi tiedonvaihtoa edistäväksi tekijäksi. Haastatteluissa ja keskusteluissa kävi ilmi, että kynnys ottaa yhteyttä tuttuun henkilöön on pienempi kuin vieraaseen ja kasvotusten tapahtuvia tapaamisia pidettiin lähtökohtana luottamuksen lisäämiseksi henkilöiden välillä. Niin viranomaiset kuin elinkeinoelämän edustajat ilmaisivat huolen tiedon hallitsemattomasta leviämisestä. Toisaalta kukaan ei maininnut siitä omakohtaisia negatiivisia kokemuksia tai osoittanut epäluottamusta jotakin nykyistä tiedonvaihtokumppania

kohtaan. Päinvastoin, esimerkiksi poliisia ja Kyberturvallisuuskeskusta, joiden toimintaa tarkasteltiin haastattelujen aikana eniten, pidettiin kumpaakin luotettavana tahona. Samoin kaikki elinkeinoelämän haastatellut kokivat, että liiketoimintaan liittymätöntä tietoa voidaan jakaa myös yritysten välillä luottamuksellisesti, kunhan tiedon jakamisen periaatteista on sovittu etukäteen ja yritykset sitoutuvat noudattamaan niitä.

Asetettujen rajojen noudattamisella haastateltavat viittasivat niin tiedonvaihdon oikeudelliseen viitekehykseen kuin keskinäisten sopimusten, olivatpa ne suullisia tai kirjallisia, noudattamiseen. On tietoa, jota lain mukaan ei voi vaihtaa. Esimerkiksi henkilötiedot on tyypillisesti kyettävä poistamaan jaettavasta tiedosta. Toisaalta jos tiedon käsittelystä ja käyttötarkoituksesta on sovittu tietyllä tavalla, sen rikkominen rikkoo samalla luottamukselliset välit, joten asetettujen rajojen noudattaminen on myös luottamuskysymys.

Poliisin kyberkeskusta pidettiin haastatteluissa pääsääntöisesti tahona, joka olisi sopivin koordinoimaan tietoverkkorikollisuuteen liittyvää tilannekuvatyötä. Perusteluina mainittiin esimerkiksi, että poliisi on ainoa rikostutkintaa tekevä organisaatio ja kyberkeskus suurin tietoverkkorikollisuuteen erikoistunut yksikkö poliisin sisällä. Poliisilla arveltiin myös olevan eniten kokemusta rikoslähtöisestä analyysista. Suuri osa vastaajista koki tiedonvaihdon syventämisen haastavaksi niin kauan kunnes poliisin sisäinen tilannekuvatyö on määritelty. Omien tarpeiden kautta määriteltynä on helpompi etsiä yhteisiä rajapintoja muiden organisaatioiden kanssa ja varmistaa, että yhteistyö perustuu todelliseen tarpeeseen. Lisäksi oman toiminnan kautta määriteltynä pystytään selkeästi esittämään, minkälaista tietoa on mahdollista tarjota muille.

Kun haastateltavilta kysyttiin, minkälaista heitä hyödyttävää tietoa he arvelivat poliisilla olevan, selvästi yleisimmin esiin nousivat rikosten tekotavat ja trendit. Vastaajat perustelivat näkemystään poliisin kansainvälisten kontaktien kautta: Suomi on syrjäinen maa ja pieni kielialue, joten tekotavat näkyvät yleensä jossain muualla ja poliisi saa orastavista uusista tekotavoista tiedon etukäteen. Osa vastaajista myös arveli, että poliisi pystyy rikostilastojen perusteella näkemään, minkä tyyppinen ilmoitettu rikollisuus on yleistynyt pidemmällä aikavälillä. Yleinen mainittu hyöty tekotapojen osalta oli myös oman toiminnan suojaaminen: kun ymmärretään rikoksen mekanismi ja motiivi, pystytään suojautumaan paremmin. Yksi yhteistyön syventämisen ehdotus koski myös tekotapojen analyysin yhteistä kehittämistä. Poliisi voisi salassa pidettävien taktisten menetelmien sallimissa rajoissa auttaa muita tahoja tunnistamaan rikoksia ja niiden motiiveja. Alustavien tulosten esittelytilaisuudessa poliisipuolelta nousi myös ehdotus, että ilmiötason tieto rikollisista ja rikollisryhmistä (esimerkiksi mistä päin maailmaa tietyn tyyppiset tekotavat tulevat ja kuinka keskittynyttä toiminta on) ovat myös osa-alue, josta poliisi pystyy kertomaan taustoja rikosten ennaltaehkäisyn tueksi.

Trendien ja ilmiöiden osalta esiin nostettiin myös tarve jatkuvalle ja säännölliselle tiedonkeruulle. Viranomaistilastot ovat yksi näkökulma tähän, mutta myös kyselytutkimuksilla arveltiin olevan annettavaa tilannekuvaan. Esimerkiksi eri alojen yrityksille suunnattava kyselytutkimus auttaisi piilorikollisuuden määrän ja tyypin hahmottamisessa. Kyselyn toteuttaminen voisi erään ehdotuksen mukaan tapahtua yhteistyössä viranomaisten, elinkeinoelämän ja tutkimusyhteisön kanssa.

Osa vastaajista piti kannatettavana ajatuksena, että tiedonvaihdolle olisi määritelty omien sisäisten tavoitteiden lisäksi yhteisiä päämääriä. Sopivaksi yhdistäväksi päämääräksi arvioitiin kyberuhkien torjuntaa ja ennaltaehkäisyä. Toisaalta eräs haastateltavista totesi hyvin, että toiminnan on saavutettava tietty kypsyys ennen kuin yhteistyötä voidaan syventää eikä pidä laatia tavoitteita, joita ei pystytä täyttämään.

5.4 Työpajassa esitetyt kehittämisehdotukset

Tämä luku perustuu 13.1.2016 järjestetyn työpajan työryhmätyöskentelyn ja loppukeskustelun tuloksiin. Kehittämisehdotukset on kirjattu ranskalaisten viivojen avulla työpajassa esitettyjen huomioiden, ajatusten ja ideoiden tasolla. Työpajassa pohditut kehittämisehdotukset esitetään listana ideatasolla, koska ne on haluttu tuoda avoimesti julki jatkokehittämistä ja keskustelua varten. Ehdotuksia ei arvoteta tässä yhteydessä sen perusteella, tuliko ehdotus työryhmältä, oliko se yksittäisen henkilön näkemys ryhmäkeskustelun aikana tai herättikö se kannatusta osallistujissa. Hankkeen varsinaiset toimenpide-ehdotukset esitetään viimeisessä luvussa.

Yleisiä huomioita

- Poliisin nykyiset oikeudet tietojen saantiin ovat pääosin riittäviä, mutta niitä pitää hyödyntää täysimääräisesti. Rikosperustaisia tiedonhankintavaltuuksia tietoverkkorikosten ennalta estämiseen ja paljastamiseen tarvitaan jatkossa, mutta se ei ole tämän selvityksen ensisijainen kohde.

- Operatiivisen tiedon osalta välitystietojen vaihtaminen on tärkeää, jos tiedon perusteella halutaan lähteä välittömiin toimenpiteisiin. Sen sijaan vaikka ilmiötilannekuva perustuu osaltaan välitystietoihin ja henkilötietoihin, niitä ei ole tarvetta jakaa. Organisaatioiden on pystyttävä järjestämään oma toimintansa niin, että arkaluontoiset asiat voidaan poistaa tarvittaessa tiedonjakoa varten. Tietoa anonymisoitaessa ja jaettaessa on tärkeää kuvata, mitä on anonymisoitu, että osapuolet ymmärtävät mitä on jaettu ja toisaalta mitä tiedosta puuttuu.

- Yritykset tarvitsevat tilannekuvaa toimintansa kehittämisen kannalta: ajantasaista tilannetietoa nopeaa reagoimista edellyttävien suojaustoimenpiteiden suorittamiseksi sekä ilmiötason tietoa tekijäprofiileista, tekojen motiiveista ja luotettavaa tilastotietoa tietoverkkorikollisuudesta.

- Yritykset eivät ilmoita rikoksista poliisille, jos eivät koe saavansa ilmoittamisesta hyötyä. Tähän vaikuttavat sekä pelko sanktioista että julkisuudesta aiheutuva maineriski. Monesti suurten yritysten lakiasiainosasto myös kontrolloi poliisitutkintaan päätyvät asiat. Jos epäiltyä ei kyetä tunnistamaan tai rikosprosessi on hidas, yritys voi kokea, että ilmoittamisesta on enemmän vaivaa kuin hyötyä.

- Ilmiötilannekuvaa tarvitaan kehystämään ja löytämään konteksti yksittäisille tapahtumille. Kehystäminen hyödyttää kaikilla tilannekuvatyön tasoilla ja auttaa ymmärtämään ilmiöitä. Ilmiötilannekuvan ei tule olla teknologiakeskeistä, vaan sen avulla on voitava tuoda asiat myös tekniikkaa ymmärtämättömien ihmisten tietoisuuteen.

- Rikolliset menevät usein siitä, mistä aita on matalin. Uuden teknologian hyödyntäminen rikollisuudessa voi viedä vuosia ja uhkista varoittaminen on epäkiitollista työtä, jos tieto on sellaista, ettei se mene heti aktiiviseen hyödyntämiseen. Lisäksi eri ilmiöiden intressit yhdentyvät, ja välillä on vaikea erottaa, onko esimerkiksi kyse valtiollisesta vai rikollisryhmän toiminnasta.

Konkreettisia lyhyen tähtäimen kehitysehdotuksia

- Viestintäviraston alustan kehittäminen yhteiseksi tiedonvaihtoalustaksi. Alustaa on mahdollista kehittää niin, että myös muut organisaatiot voivat syöttää siihen auto-

maattisesti tietoa. Alusta palvelee sekä operatiivista että ilmiötason tiedonjakamista. Erilaisia tiedonvaihtotapoja voi pilotoida yhteisellä alustalla valitun joukon kesken.

- Virkamiesvaihtojen käynnistäminen. Virkamiesvaihdot ovat hyvä tapa tukea organisaatioiden keskinäistä ymmärrystä. Poliisin esitutkintapakko ei rajoita olennaisesti virkamiesvaihtoa, esimerkiksi poliisi voi suorittaa Viestintäviraston Kyberturvallisuuskeskuksessa monenlaisia tehtäviä, jotka eivät liity suoraan rikollisuuteen. Pohdittava myös voisiko yrityksistä tulla työntekijöitä vaihtoon.

- Yhteistyöasiakirjat viranomaisten välillä. Viranomaiset voivat sopia tiedonvaihdon yleisistä linjauksista, jolloin päätökset jaettavasta tiedosta eivät kuormita kohtuuttomasti yksittäisiä viranhaltijoita.

- Selkeä ohjeistus yrityksille, mitä ja miten toivotaan ilmoitettavan poliisille. Tietoturva-alan yrityksille opastusta, että osaavat neuvoa asiakkaitaan prosessissa. Tietoturva-alan yrityksillä on merkittävä rooli asiakkaan suuntaan. Myös poliisin kyberkeskuksen verkkosivuille voi laatia yrityksille suunnatun tietopaketin ja selvittää, voiko se avata neuvontanumeron yrityksille. Helsingin poliisilaitoksella on hyviä kokemuksia neuvontanumerosta. Neuvonnalla on mahdollista saada henkilökohtainen kontakti ja kannustaa yrityksiä ilmoittamaan rikosepäilystä myös tapauksissa, joissa epäillyn selville saaminen olisi epätodennäköistä. Näin teko ei jää piilorikollisuudeksi ja tulee tilastoiduksi. Ohjeistuksen laatiminen edellyttää myös määritelmistä sopimista: onko tarpeen tehdä rajanveto tietojärjestelmiin kohdistuneiden rikosten ja tietojärjestelmiä käyttäen tehtyjen rikosten välillä?

- Ilmoitusaktiivisuuden lisääminen rikostutkinnan narratiiveja rakentamalla ja viemällä ne yritysten päätöksentekotasolle. Johtoporras näkisi, mitä konkreettista hyötyä rikostutkinnasta on ollut. Esimerkiksi tekijän edesvastuuseen saattamisen lisäksi on voitu löytää toimintatapoja, joilla ennaltaehkäistään rikoksia tulevaisuudessa.

- Yritysten tilannekuvatoiminnasta saaman hyödyn määrittäminen. Esimerkiksi Viestintäviraston Havaro on hyvin markkinoitu palvelu, josta voi ottaa mallia. Tarvitaan hyvä tuote, jotta yritykset saadaan mukaan.

- Rikosten tunnistamisen analyysin kehittäminen yhdessä palveluntarjoajien (esim. suurimmat ISP:t ja käyttöpalvelutuottajat) kanssa. Yhteistyölle laadittava pelisäännöt, korostettava luottamuksellista ilmapiiriä ja tiedonvaihto tehtävä anonymisoidulla tiedolla. Näin liikesalaisuudet eivät vaarannu. Yritykset saisivat suoraa hyötyä ilmiöiden ja trendien tunnistamiseen.

- Eri toimijat voivat seurata samoja teemoja ja verrata tietojaan ristiin. Esimerkiksi poliisi voi alkaa seurata samoja teemoja kuin Viestintäviraston Kyberturvallisuuskeskus. Totuus syntyy eri tahoilla ja tilannekuvat saattavat olla ristiriidassa keskenään, mistä tulee lisäarvoa.

- Viranomaisten, yritysten ja tutkimuksen yhteistyön yhtenä haasteena on tutkimusrahoituksen projektimaisuus. Yhteistä ilmiötason tilannekuvaa voisi luoda esimerkiksi vuosittaisessa seminaarissa, kuten valtakunnallisen turvallisuustutkimuksen seminaarin yhteydessä, mutta se edellyttää jatkuvaa tiedonvaihtoa vuoden aikana – ei niin, että pari viikkoa ennen seminaaria tulee raportti tutustuttavaksi. Norjassa ja Hollannissa viranomaiset sekä akateemiset tekevät konsortiomaisesti töitä koko ajan. Pyydetään norjalainen kollega Suomeen kertomaan heidän mallistaan ja selvitetään

olisiko sovellettavissa Suomeen. Tarvittaessa ilmiötilannekuvaseminaariin voisi osallistua myös ulkomaisia tahoja esim. akuutissa tilanteessa tai jos joku tuntee tarkasteltavan ilmiön hyvin.

- Avointa julkista tiedonjakoa tarvitaan myös rikosten ennalta estämisen ja sen johtamisen sekä tutkimusteemojen ja uusien liikeideoiden löytämisen tueksi. Esimerkiksi loppuyhteenveto-tyyppistä tietoa voi jakaa laajasti, vaikka analyysit jäisivät edelleen vain tekijän tietoon.

- Työpajassa esiintuodut asiat tullaan ottamaan ainakin sisäministeriön työssä huomioon. Lisäksi todettiin, että harjoitukset voisivat muodostaa selkeämmän jatkumon ja toimia samalla seurantana: mitä aikaisemmissa harjoituksissa todetuille asioille on tapahtunut? Päätelmiä puolestaan voisi testata tulevissa harjoituksissa.

Laajempia kehitysehdotuksia

- Nykyinen lainsäädäntö ei salli poliisin perustaa pysyvää analyysirekisteriä tietoverkkorikostutkinnan tueksi. Asia otetaan esiin Euroopan unionin tietosuojalainsäädännön uudistuksen yhteydessä tehtävässä kotimaisessa lainvalmistelussa[7].

- Kyberturvallisuus, kuten moni muukin turvallisuustematiikkaan liittyvä asia, on yhteinen haaste, joka kuuluu useille viranomaisille. Valmisteilla oleva Euroopan unionin tietosuojalainsäädännön uudistus pakottaa arvioimaan myös Suomessa, onko jokaiselle viranomaisella edelleen oma substanssilakinsa vai onko yhteisratkaisu tarpeellinen. Valtioneuvostotasoiseen tiedonvaihtoon liittyvän lainsäädännön voi arvioida poistavan tiedon vaihtamisen esteitä, lisäävän viranomaisten yhteistyötä ja parantavan yhteistä tilannekuvaa. Esimerkiksi Rahanpesun selvittelykeskuksen kaltainen ratkaisu mahdollistaisi ilmoitusten laajamittaisen vastaanoton ja analyysin. Ilmoitukset siirtyisivät mahdolliseen poliisitutkintaan vasta esikäsittelyn jälkeen.

- Ilmoittamismahdollisuuksien parantaminen. Esimerkiksi UK:ssa Action Fraud -keskus[8] vastaanottaa kaikki petosasiat. Samantyyppinen internet-pohjainen ilmoitusalusta voisi sopia myös Suomeen. Se mahdollistaisi ilmoitusten massakäsittelyn, jolloin myös pienet asiat voisi ilmoittaa viranomaisille ja tietojen yhdistely helpottuisi. Jos järjestelmä olisi automaattinen, tietyt tapaukset voisi ohjata suoraan Viestintäviraston Kyberturvallisuuskeskukselle (esim. kalastelusivut) jatkotoimenpiteitä varten. Poliisin osalta edellyttänee esitutkintapakon poistamisen[9]. Nykyisellään poliisin Nettivinkki lähimpänä Action Fraud -keskusta. Nettivinkin kautta on mahdollista vastaanottaa tietoa ilmiöistä, joita ei välttämättä edes haluta rikostutkintaan.

- Luotettavan tietoverkkorikosten tilastointitavan kehittäminen poliisiin. Edellyttää toimenpiteitä sekä kirjaamiskäytäntöjen että tietojärjestelmän osalta.

[7] Laki henkilötietojen käsittelystä poliisitoimessa ei mahdollista tällä hetkellä pysyvän analyysirekisterin käyttöönottoa, mikä vaikeuttaa kyberrikostutkinnan ja -tiedustelun asianmukaista ja tehokasta suorittamista. Tilannetta on paikkailtu perustamalla tilapäisiä analyysirekistereitä (Laki henkilötietojen käsittelystä 6 § 2 mom. 2 kohta), jotka kuitenkin ovat sidoksissa tietyn rikoskokonaisuuden estämiseen, paljastamiseen tai selvittämiseen lain rajoitteista johtuen. Tällä hetkellä saattaa joissakin tapauksissa olla hankalaa esimerkiksi antaa asianmukaista virka- ja oikeusapua ulkomaille, koska poliisi ei pysty hakemaan tietoa keskitetystä tietovarastosta vaan tieto on hajallaan eri tietokannoissa tai se voi olla myös poistettu. (Tarkennus työpajan jälkeen: Karl Linderborg, KRP.)

[8] Action Fraud on kansallinen petosten ja taloudelliseen hyötyyn tähtäävien kyberrikosten ilmoituskeskus. Keskus ohjaa rikosepäilyt poliisitutkintaan sekä analysoitavaksi ja neuvoo uhriksi joutuneita. Keskuksen tarkoitus on vähentää piilorikollisuutta, parantaa tilannekuvaa ja välittää tukea uhriksi joutuneille. (Action Fraud 2015.)

[9] Esitutkintapakosta aiheutuu nykyisin poliisille ainakin kaksi haastetta kyberrikostorjunnan ja tutkinnan osalta. Ensiksi, tutkinnan tuoman julkisuuden vuoksi kaikki yritykset eivät välttämättä saata tapauksia poliisin tietoon, mikä puolestaan vaikeuttaa kokonaistilannekuvan muodostamista. Toiseksi, tietoverkkorikokset ovat tutkinnallisesta näkökulmasta varsin haasteellisia ja työläitä: esimerkiksi maksuvälinepetosjutuissa saattaa olla useita kymmeniä asianomistajia, joiden osalta tulee muun muassa selvittää rikoksella aiheutetut vahingot ja asianomistajien rangaistus- sekä korvausvaatimukset. Tietomurtojutuissa asianomistajien lukumäärä saattaa nousta jopa kymmeniin tuhansiin. Esitutkinnassa tulisi voida luopua yksityisoikeudellisten vaatimusten kattavasta selvittämisestä, koska näiden selvittämisellä on olennaisesti esitutkintaa hidastava vaikutus eikä syyttäjä useinkaan lähde ajamaan asianomistajien vaatimuksia oikeudessa. Syyttäjien rajoitusmahdollisuus toisaalta auttaa tähän. (Tarkennus työpajan jälkeen: Karl Linderborg, KRP.)

- Yritysten kulttuurin muuttaminen tietoverkkorikosten ilmoittamista kohtaan esim. kampanjoiden avulla. Voisiko lentoyhtiöiden low blame -kulttuurista ottaa mallia? Sen sijaan, että etsitään syyllisiä rikoksen kohteeksi joutumiseen, palkittaisiin siitä, että tapaukseen liittyvät tiedot kerrotaan avoimesti. Esimerkiksi varkauden kohteeksi joutumisesta ei häpeillä kertoa.

- Tietoverkkorikollisuuden uhritutkimus olisi erittäin tarpeellinen, kun sen avulla saisi ilmoitettua rikollisuutta laajemman tilannekuvan. Tosin uhritkaan eivät aina tiedä olevansa uhreja.

- Kybervakuutusten yleistyessä voitaneen niihin liittää yrityksille jonkinlaisia velvollisuuksia. Esimerkiksi rikoksesta ilmoittaminen poliisille (vrt. muut vakuutukset). Vakuutusyhtiöiden kiinnostus kasvanee, kun korvaussummat kasvavat.

6. TOIMENPIDE-EHDOTUKSET JA POHDINTA

Hankkeen tavoitteena oli kartoittaa tietoverkkorikollisuuden tilannekuvatyön nykytila ja pohjustaa tietoverkkorikollisuuden tilannekuvatyön kehittämistä poliisissa. Pitkän tähtäimen tavoitteena on luoda prosessi, joka yhdistää viranomaiset, elinkeinoelämän ja tutkimuksen tulokulmat tietoverkkorikollisuuden tilannekuvatyön tueksi. Selvityksen tärkeimpänä lopputuloksena on joukko toimenpide-ehdotuksia, jotka tähtäävät yhteisen tilannetietoisuuden parantamiseen ensisijaisesti nykyisessä lainsäädännöllisessä viitekehyksessä jo olemassa olevin resurssein. Toimenpide-ehdotukset perustuvat haastatteluissa ja työpajassa nousseisiin näkemyksiin tietoverkkorikollisuuden tilannekuvatyöstä sekä sen kehittämisestä. Hankkeen toteuttaja on pyrkinyt rakentamaan kerätyn taustamateriaalin avulla toimivan kokonaisuuden. Työpajassa esitettiin parikymmentä ideaa tietoverkkorikollisuuden tilannekuvatyön parantamiseksi ja monet niistä päätyivät suoraan loppuraportin toimenpide-ehdotuksiksi. Kaikki työpajan kehittämisehdotukset on lueteltu luvussa 5.4 "Työpajassa esitetyt kehittämisehdotukset".

Tietoverkkorikollisuuden tilannekuvatyötä ja tiedonvaihtoa lähestyttiin kolmen tutkimuskysymyksen avulla. Ensimmäinen kysymys: "Kuinka tietoverkkorikollisuuteen liittyvää tiedonvaihtoa toteutetaan kansallisesti tällä hetkellä?" kartoittaa tilannekuvatyön nykytilaa. Haastattelujen ja käytyjen keskustelujen perusteella tietoverkkorikollisuuden näkökulma koetaan tarpeelliseksi osaksi kokonaiskybertilannekuvatyötä, mutta tiedonvaihto ei ole tällä hetkellä systemaattista ja tieto siirtyy enemmän henkilö- kuin organisaatiotasolla. Vakiintuneita tiedonvaihtokanavia ovat esimerkiksi viikoittaiset viranomaisten yhteispalaverit, pikaviestintäpalvelut, viikkoraportit, sähköpostilistat sekä puhelinsoitot. Poliisin kyberkeskus on järjestänyt yhteisiä tapaamisia yritysten kanssa, mutta tietoverkkorikollisuuden osalta tiedonvaihtoa ei ole toistaiseksi suunniteltu kokonaisuutena. Poliisin säännölliset tilannekuvatuotteet, tietoverkkorikollisuuden viikkoraportti ja vuosikatsaus ovat toistaiseksi melko tuntemattomia, vain pieni osa haastatelluista tunnisti ne. Poliisilaitosten ja poliisin kyberkeskuksen välisen säännöllisen tiedonvaihdon aloittaminen parantaisi poliisin kokonaiskuvaa tietoverkkorikollisuudesta sekä auttaisi rikostutkintaosaamisen leviämistä. Yhtä mieltä oltiin siitä, että tiedonvaihto myös eri organisaatioiden välillä on tärkeää ja yhteistyötä pitää syventää. Kahdenvälinen tiedonvaihto Viestintäviraston Kyberturvallisuuskeskuksen kanssa vaikutti olevan pisimmällä kaikkien haastateltujen organisaatioiden osalta, ei pelkästään poliisin.

"Miten eri toimijoiden yhteistä tilannekuvaa ylläpidetään ja millaisia pullonkauloja sekä esteitä näihin liittyen on?" oli toinen tutkimuskysymys. Tietoverkkorikollisuuden osalta tilannekuva-

työn koordinointi kuuluu strategioiden, ohjaavien asiakirjojen ja haastatteluaineiston perusteella poliisin kyberkeskukselle. Koska keskus on perustettu vasta 2015, on luonnollista, että toiminta hakee vielä muotoansa ja tilannekuvatyön kehittäminen on vasta alussa. Täten yksi merkittävä este yhteisen rikostilannekuvan muodostamisessa oli haastattelujen perusteella se, että vaikka tiedonvaihto yksittäisissä tapauksissa sujuu hyvin, tietoverkkorikollisuuden tilannekuvatyöltä on puuttunut tavoitteet ja suunnitelma siitä, miten työtä tehdään. Yhteistyökumppaneille ei ole ollut selvää, millaista tietoa poliisilta on saatavissa ja millaista tietoa se tarvitsee. Tärkeä yhteistyön syventämisen edellytys on kunkin organisaation sisäinen määrittäminen, mihin yhteistyötä tarvitaan, millaiset resurssit on käytettävissä ja millaista tietoa voidaan jakaa. Sen jälkeen on pohjaa viedä keskustelu konkreettisemmalle tasolle.

Kolmas tutkimuskysymys oli "Millaisia asioita tiedonvaihdossa tulee huomioida?" Haastatteluissa korostui kolme tiedonvaihdossa huomioitavaa asiaa: asetettujen rajojen noudattaminen, luottamus ja toiminnasta saatava hyöty. Asetettujen rajojen noudattamisella tarkoitetaan sekä kunkin toimijan oikeudellista viitekehystä että keskinäisten sopimusten, olivatpa ne suullisia tai kirjallisia, noudattamista. Keskinäinen sopiminen viittaa muun muassa yhteistyöhön sitoutumiseen ja siihen, miten saatua tietoa käytetään. Usein esimerkiksi tiedon luovuttava ulkomainen viranomainen on määritellyt tiedon käytön tarkasti. Tai jos yritykset jakavat yhteispalaverissa kokemuksia rikostorjunnasta, on tärkeää, ettei mikään taho käytä tietoja yrityksiä vastaan esimerkiksi saadakseen kilpailuetua. Asetettujen rajojen noudattamisella on suora yhteys luottamukseen: luottamuksen ilmapiiri koettiin ensiarvoisen tärkeäksi tiedonjaossa. Ilman luottamusta tieto jää jakamatta. Kolmas edellytys tiedonjaolle on toiminnasta kaikille osapuolille saatava hyöty. Tiedonvaihto on ennen kaikkea vastavuoroista toimintaa. Vastavuoroisuuden ja saavutetun hyödyn puute heikentävät motivaatiota tiedonvaihtoa kohtaan, ja siksi tiedonvaihdon vaikuttavuutta on tärkeä seurata esimerkiksi palautteen avulla.

6.1 Poliisin sisäiset toimenpide-ehdotukset

Selvityksen perusteella tietoverkkorikollisuuden tilannekuvatyön tärkein kehittämistarve on poliisin sisäinen. Sisäinen tilannekuva ja toimintamalli muodostavat pohjan hyödyn saamiseksi sidosryhmäyhteistyöstä. Tilannekuva on yhteinen asia, jonka tulisi näkyä paitsi poliisin kyberkeskuksen sisällä, myös poliisilaitoksilla, Poliisihallituksessa ja Sisäministeriön poliisiosastolla. Tämä on tärkeää, koska päivittäistoiminnan ohella meneillään on useita keskeisiä lainvalmisteluhankkeita sekä harjoituksia, joihin osallistutaan vaihtelevilla kokoonpanoilla. Tilannekuvatyön tavoitteiden kirjaaminen poliisitoimintaa ohjaaviin asiakirjoihin ja strategioihin (esimerkiksi vuonna 2016 valmistuva ennalta estävän toiminnan suunnitelma) sekä kytkeminen vuotuiseen tulosohjaukseen varmistaisivat, että tilannekuvatyötä viedään eteenpäin ja sen toteuttamista seurataan koko organisaation tasolla. Sisäministeriön hallinnon alan toiminta- ja taloussuunnitelmassa (2016, 14) on jo maininta tilannekuvan kehittämisestä, joten pohja kirjata konkreettisemmat toimenpiteet alempiin ohjaaviin asiakirjoihin on olemassa.

Ylhäältä tapahtuvan ohjauksen lisäksi poliisin sisäistä tiedonvaihtoa edistävät samat tekijät kuin sidosryhmien osalta: luottamus ja hyöty. Toiminta pysyy käynnissä, kun kaikki osapuolet hyötyvät yhteistyöstä ja tiedonvaihto perustuu luottamukseen. Tiedonvaihdosta sovittaessa on tarpeen keskustella myös siitä, millaista tietoa jaetaan ja mihin saatua tietoa käytetään. Hyvä lähtökohta luottamuksen rakentamiselle ja hyödyn löytämiselle on yhdessä tekeminen. Yksi vaihtoehto on, että poliisin kyberkeskus laatii alustavan ehdotuksen tietoverkkorikollisuuden tilannekuvatyön tavoitteista, painopisteistä ja resursseista. Ehdotusta työstetään eteenpäin yhdessä poliisilaitosten ja Suojelupoliisin kanssa sekä sovitaan muutamasta tärkeimmästä ajankohtaisesta toimenpiteestä, joilla tiedonvaihto saadaan käyntiin. Myös yksik-

kökohtaiset resurssit tulisi huomioida työssä ja pohtia, mitkä ovat työnteon näkökulmasta luonnollisia tapoja jakaa ja vastaanottaa tietoa.

Rikosten tekotavat, trendit ja rikollisryhmien analyysi ovat tämän selvityksen perusteella kannattava ja luonnollinen painopiste tietoverkkorikollisuuden tilannekuvatyölle. Sidosryhmät odottavat poliisilta sen kaltaista tietoa ja kokevat sen tarpeelliseksi. Rikosten tekotapojen ja rikollisten/rikollisryhmien analyysi sekä tutkintakäytäntöjen jakaminen hyödyttävät suoraan poliisin rikostutkintaa kaikilla tasoilla. Lisäksi ne kuuluvat poliisin perustehtävään ja edistävät tietoverkkorikollisuuden kokonaisuuden haltuunottoa poliisissa. Trendien, niin ulkomailta mahdollisesti tulevien ilmiöiden ennakointi kuin jälkikäteisseuranta, puolestaan auttavat tunnistamaan rikoksia ja ohjaamaan ennalta estävää toimintaa. Edellä mainitut asiat ovat myös sellaisia, joista poliisi saa kansainvälisiltä kumppaneiltaan runsaasti tietoa, mutta tieto ei päädy systemaattiseen seurantaan. Systemaattisen seurannan järjestäminen on yksi pohdittava haaste: tulisiko uusien ilmiöiden "listaa" ylläpitää siten, että samalla voisi kerätä tietoa niiden mahdollisesta esiintymisestä Suomessa ulkoisten sidosryhmien kautta?

Tietoverkkorikollisuuden tilannekuvatyön määrittely auttaa poliisia myös määrittämään poliisin kyberkeskuksen roolia suhteessa poliisilaitoksiin. Keskeisiä kysymyksiä ovat esimerkiksi kauan aikaa sitten tunnistetut haasteet, kuten mikä on tietoverkkorikoksen ja tietoverkkoja hyväksikäyttäen tehtyjen rikosten suhde[10] sekä kuinka poliisin tilastoista saadaan luotettava tieto tietoverkkorikollisuuden määrästä. Molemmat haasteet liittyvät kiinteästi rikosilmoitusten vastaanottoon ja tunnistamiseen, eikä niihin ole nopeita, täydellisiä ratkaisuja. Arvioidaan, että nykyisellään monet tietoverkkorikoksista jäävät tunnistamatta ilmoitusten vastaanotossa. Yksi melko yksinkertainen keino helpottaa ilmoitusten vastaanottoa, on kuvata esimerkiksi intranetiin keskeiset tietoverkkorikokset ja tietoverkkoja hyväksikäyttäen tehtävät rikokset, millä rikosnimikkeillä niitä tutkitaan ja nimetä yhteyshenkilöt (esimerkiksi laitoskohtaiset), joilta voi kysyä epäselvissä tapauksissa lisätietoja. Samalla sivustolla voisi olla tietoa myös ajankohtaisista huijauskampanjoista ja massarikoksista. Näin ilmoituksen vastaanottaja löytäisi tiedon kootusti yhdestä paikasta, kunhan alusta olisi tehty riittävän tunnetuksi. Yhteyshenkilöiden määrittely puolestaan auttaisi kokonaisuuden hallinnassa ja rajanvedossa tietoverkkorikosten sekä tietoverkkoja hyväksikäyttäen tehtyjen rikosten välillä.

Toimenpide-ehdotukset tiivistetysti

- Määritellään poliisin omat tilannekuvatyön tavoitteet, resurssit, keinot ja toimenpiteiden aikataulu.
- Kytketään tietoverkkorikollisuuden tilannekuvatyön kehittäminen poliisin sisäisiin strategioihin ja tulosohjaukseen.
- Tehdään tietoverkkorikollisuuden tilannekuvasta koko poliisin kyberkeskuksen, poliisilaitosten ja soveltuvissa määrin Suojelupoliisin yhteinen asia. Sama luottamuksen ja hyödyllisyyden periaate kuin sidosryhmäyhteistyössä pätee myös poliisin sisällä.
- Kehittäminen aluksi nykyisillä resursseilla ja pienin, konkreettisin askelin kokeilevaa toimintatapaa noudattaen. Tärkeintä on saada toiminta käyntiin, ettei asia unohdu.

[10] Kyberrikoksella tarkoitetaan samaa kuin tietoverkkorikoksella. Kyberrikoksella tarkoitetaan sellaisten rikosten tekomuotoja, joita esiintyy ainoastaan tietojärjestelmissä, kuten esimerkiksi hakkerointi, hyökkäykset tietojärjestelmiä vastaan, haittaohjelmien avulla tehdyt identiteettivarkaudet ja palvelunesto-hyökkäykset. (Poliisihallitus 2015.)

Tietoverkkoja hyväksikäyttäen tehdyillä rikoksilla tarkoitetaan perinteisiä rikollisuuden tekomuotoja, jotka on tehty tietoverkko- tai tietojärjestelmiä hyväksikäyttäen kuten esimerkiksi; internet petokset, maksuvälinepetokset, lapsen seksuaalista hyväksikäyttöä esittävän materiaalin levittäminen, piratismi ja muut tekijänoikeusrikokset, rahanpesu, kunnianloukkaukset, rasismi jne. (Emt.)

6.2 Poliisin ja yritysten välinen tiedonvaihto

Poliisin ja elinkeinoelämän välinen, säännöllinen tietoverkkorikollisuuden tiedonvaihto on Suomessa vasta alkuvaiheessa. Sen sijaan operatiivisempaa, rikostutkintaan liittyvää yhteistyötä on tehty jo pitkään. Yksittäisten henkilöiden kontaktit yritystoimijoiden kanssa voivat olla tiiviit, mutta siitä on vielä matkaa yleisempään tietoverkkorikollisuuden tilannekuvaan. Organisaatiotasolla yhteistyö vaikuttaa olevan pisimmällä finanssisektorin kanssa. Lisäksi poliisin kyberkeskus on kutsunut säännöllisesti eri tahoja, myös yrityksiä, tutustumaan toimintaansa ja samalla on kartoitettu yhteistyömahdollisuuksia.

Haastatteluissa ja työpajassa nostettiin esiin selkeitä ja hyvin määriteltyjä kehittämisehdotuksia poliisin ja yritysten välillä niin tilannekuvan kuin rikostutkinnan osalta. Rikosten ilmoitusaktiivisuuteen vaikuttaminen koettiin merkittäväksi. Yksi konkreettinen tapa ilmoitusaktiivisuuden parantamiseen nykyisessä oikeudellisessa viitekehyksessä on laatia poliisin kyberkeskuksen verkkosivuille yrityksille suunnattu tietopaketti rikosprosessista ja rikosten ilmoittamisesta sekä avata yrityksille suunnattu neuvontanumero. Neuvonnalla on mahdollista saada henkilökohtainen kontakti ja kannustaa yrityksiä ilmoittamaan rikosepäilystä myös tapauksissa, joissa epäillyn selville saaminen olisi epätodennäköistä. Näin teko ei jää piilorikollisuudeksi ja tulee tilastoiduksi. Tietoturva-alan yrityksillä, esimerkiksi SOC-toimijoilla (security operation center), on kiinteä kontakti asiakasorganisaatioihinsa ja ne ovat ensimmäinen taho, jonka puoleen asiakas kääntyy poikkeamanhallintatilanteessa. Täten asiakkaan tietojärjestelmistä vastaavilla yrityksillä tulisi olla kyky neuvoa asiakasta eteenpäin myös epäillyissä rikosasioissa. Yritysten johtotasoon vaikuttamisella voi puolestaan olla merkitystä sekä ilmoitusaktiivisuudessa että suhtautumisessa ilmiötiedon vaihtamiseen, joten hyvin toimineesta yhteistyöstä kannattaa kertoa esimerkkejä paitsi poliisin omien viestintävälineiden kautta, mutta myös sidosryhmät ja ammattilehdet voivat tarttua aiheeseen. Johtotason kanssa viestittäessä korostuu erityisesti ilmiöiden kehystäminen: ymmärryksen saavuttaminen rikollisuuden taustoista ja vaikutuksista tapahtuu ilman teknisiä yksityiskohtia. Rikoksista puhuminen voi myös osaltaan auttaa hälventämään tietoverkkorikoksen kohteeksi joutumisesta yrityksille aiheutuvaa maineriskiä, jota esimerkiksi omaisuusrikoksiin ei samalla tavalla liity.

Kaikki haastatellut elinkeinoelämän edustajat pitivät poliisiyhteistyön tiivistämistä ilmiötilannekuvan osalta kannatettavana asiana. Hyväksi keinoksi nähtiin yhteisten säännöllisten tapaamisten järjestäminen eri teemojen ympärillä. Tapaamisten toivottiin olevan pienimuotoisia ja luottamuksellisia. Ilmiötilannekuvasta puhuttaessa tiedonvaihdon riittävä taso on anonymisoitu tieto, joten yritysten keskinäinen kilpailuasetelma ei vaarantuisi. Yritykset toivovat yhteistyöltä erityisesti konkreettista hyötyä oman toiminnan suojaamiseksi ja rikosten ennaltaehkäisyn tueksi.

Toimenpide-ehdotukset tiivistetysti

- Rikosten ilmoitusaktiivisuuden lisääminen.
    - Laaditaan yrityksille suunnattu ohjeistus poliisin kyberkeskuksen verkkosivuille siitä, mitä ja miten toivotaan ilmoitettavan poliisille sekä kuinka rikosprosessi etenee. Ohjeistuksen laatiminen edellyttää myös määritelmistä sopimista: onko tarpeen tehdä rajanveto tietojärjestelmiin kohdistuneiden rikosten ja tietojärjestelmiä käyttäen tehtyjen rikosten välillä?
    - Avataan poliisin kyberkeskuksen neuvontanumero yritysten tiedusteluille.

    - Opastetaan tietoturva-alan yrityksiä neuvomaan asiakkaitaan rikosprosessissa.

    - Kohdistetaan viestintää yritysten johtotasolle, että se näkisi, mitä konkreettista hyötyä rikostutkinnasta on ollut. Esimerkiksi on voitu löytää toimintatapoja, joilla ennaltaehkäistään rikoksia tulevaisuudessa.

- Valitaan 1-2 yritystyyppiä (esim. SOC), joiden kanssa aloitetaan säännölliset, yhteistä ilmiötilannekuvaa tukevat tapaamiset. Tapaamisiin valitaan teema, jota alustetaan lyhyesti ja vaihdetaan kokemuksia ajankohtaisista ilmiöistä. Paikalla voi olla samanaikaisesti useita yrityksiä, mutta toiminta pidetään pienimuotoisena, että luottamuksellisuus säilyy. Yhteistyölle laaditaan pelisäännöt, korostetaan luottamuksellista ilmapiiriä ja tiedonvaihto tehdään anonymisoidulla tiedolla. Näin liikesalaisuudet eivät vaarannu ja yritykset saisivat suoraa hyötyä ilmiöiden sekä trendien tunnistamiseen.

    - Yksi tavoite voi olla myös rikosten tunnistamisen ja analyysin kehittäminen.

    - Määritellään, mitä hyötyä tilannekuvayhteistyöstä on yrityksille. Jos poliisilla on tarjota riittävän hyvä, hyvin markkinoitu "tuote", yritykset kokevat tiedonvaihdon hyödylliseksi.

    - Erityisesti yritysvakoilun rajapintaa lähestyttäessä pohdittava, miten Suojelupoliisi voi osallistua ja olla mukana tukemassa yrityksiä.

6.3 Poliisin ja muiden viranomaisten tiedonvaihto

Viranomaisten välistä tiedonvaihdon kokonaisuutta kehitetään Valtiovarainministeriön koordinoimana monella tasolla erilaisten harjoitusten ja yhteistyöpalavereiden kautta. Sen vuoksi on tärkeää, että myös tietoverkkorikollisuuden tilannekuvatyö sovitetaan yhteen kybertilannekuvan kokonaisuuden ja valtionhallinnon poikkeamanhallinnan rakenteiden kanssa. Täten merkittävin kumppani yhteistyön syventämisessä on Viestintäviraston Kyberturvallisuuskeskus, jonka kanssa poliisin kyberkeskus löysi jo hyviä keskinäisiä yhteisen tilannekuvatyön kehittämiskeinoja tammikuun 2016 kehittämispäivässä, jotka tullaan toivottavasti toteuttamaan.

Haastattelujen perusteella esiin nostettuihin haasteisiin löytyi monia konkreettisia kehitysehdotuksia työpajatyöskentelyn aikana. Esimerkiksi useampi taho pohti yhteisen tiedonvaihtoalustan tarvetta viranomaisten välille. Ratkaisuksi ehdotettiin Viestintäviraston jo olemassa olevan alustan kehittämistä siten, että myös muut organisaatiot voisivat syöttää siihen automaattisesti tietoa. Alusta voi palvella sekä operatiivisia että ilmiötason tiedonjakotarpeita ja tiedonjakoa voi pilotoida kehittämistyön aikana pienryhmissä. Haastatteluissa pohdittiin myös virkamiesvaihtojen käynnistämistä organisaatioiden keskinäisen ymmärryksen lisäämiseksi ja miten poliisin esitutkintapakko vaikuttaa mahdolliseen virkamiesvaihtoon. Työpajan aikana tultiin kuitenkin lopputulokseen, että esimerkiksi Kyberturvallisuuskeskuksessa on monenlaisia tehtäviä, jotka eivät liity suoraan rikollisuuteen ja joita pystyy suorittamaan ilman ristiriitaa esitutkintapakosta.

Lisäksi ehdotettiin, että viranomaiset sopivat keskenään tiedonvaihdon yleisistä linjauksista, jolloin vastuu tiedonjaosta on yksittäisen viranhaltijan lisäksi organisaatiotasolla. Näin viranhaltijoiden on helpompi tulkita, millaista tietoa voi tai ei voi jakaa sekä ymmärtää myös lain asettamia rajoituksia toisen organisaation näkökulmasta. Askel kohti yhteistä analyysia puolestaan olisi kokeilu, että viranomaiset ja mahdollisesti myös yritykset alkaisivat seurata sys-

temaattisemmin samoja ajankohtaisia teemoja ja niiden esiintymistä omassa työssään. Tällöin teema-alueiden sisällä tietoa ja siitä tehtyjä päätelmiä voisi verrata keskenään, kun kaikilla on ollut sama tarkastelun ajanjakso ja kohden. Kokeilu toisi käsityksen, miten sama ilmiö näyttäytyy eri viranomaisten näkökulmasta ja minkä verran lisäarvoa vertailulla saavutetaan. Olisi merkittävä havainto huomata, jos eri tahot päätyvät erilaisiin päätelmiin samasta teemasta tai jos vertailun perusteella ei loppujen lopuksi löytynytkään mitään uutta.

Toimenpide-ehdotukset tiivistetysti

- Viestintäviraston alustan kehittäminen yhteiseksi tiedonvaihtoalustaksi.
- Virkamiesvaihtojen käynnistäminen.
- Yhteistyöasiakirjojen laatiminen viranomaisten kesken. Viranomaiset sopivat tiedonvaihdon yleisistä linjauksista, jolloin päätökset jaettavasta tiedosta eivät kuormita kohtuuttomasti yksittäisiä viranhaltijoita.
- Järjestetään kokeilu, jossa eri viranomaiset seuraavat ennalta sovittuja teemoja ja vertaavat tietojaan ristiin.

6.4 Tutkimus ja tiedonvaihto

Tulevaisuuden haaste on yhdistää tiedonvaihtoon ja tietoverkkorikollisuuden tilannekuvatyöhön myös tutkimus. Viranomaisnäkökulmasta tutkimukseen liittyy monia ongelmakohtia, joista yksi keskeisimpiä on yhteistyörakenteiden puuttuminen: kyberturvallisuusalan tutkimus ei muodosta toistaiseksi selkeää verkostoa tai osaamispankkia, johon viranomaisten ja yritysten olisi helppo tukeutua esimerkiksi etsiessään tietynlaista osaamista. Tutkimusta tehdään pääsääntöisesti erillisrahoituksella eripituisina projekteina, monilla tieteenaloilla sekä hajautetusti ympäri Suomen. Tutkimusta on myös erilaista: perus- ja soveltavaa tutkimusta sekä osaamista opinnäytteistä kansainväliseen huippututkimukseen. Lisäksi perinteinen laadunvarmistuskeino, vertaisarviointi, nojaa julkisuuteen ja tulosten julkaisuprosessi voi kestää pitkään.

Yksi keino lisätä vuorovaikutusta olisi järjestää jonkin nykyisen vuosittaisen seminaarin yhteyteen työpaja, jossa analysoidaan yhdessä tietoverkkorikollisuuden ilmiökenttää. Seminaarin taustalla on ajatus, että tiedonvaihto tapahtuisi ympäri vuoden osapuolten välillä. Esimerkiksi Norjan poliisissa on tehty tämän kaltaista yhteistyötä ja malli saattaa olla sovellettavissa Suomeenkin.

Tietoverkkorikollisuuden tutkimusyhteistyötä ja pysyvän mallin löytämistä hidastaa se, että poliisissa ei ole toistaiseksi ratkaistu, kuinka systemaattisesti ja millä resurssein asiaa viedään eteenpäin. Tutkimuksen toteuttaminen ja verkostoituminen edellyttää poliisin omaa säännöllistä tutkimustyötä, jolloin verkostolle on olemassa solmukohta myös poliisissa. Kyberturvallisuusstrategian toimeenpano-ohjelmassa (2014, 29) Poliisiammattikorkeakoululle on asetettu tehtäväksi lisätä kyberalan tutkimusta ja yhteistyötä yliopistojen kanssa, joten luonteva verkoston yhteyspiste poliisin tarvitseman tietoverkkorikollisuuden tilannekuvatutkimuksen osalta olisi Poliisiammattikorkeakoulu. Toinen, helpommin toteutettava rooli on tutkimushankkeiden loppukäyttäjänä toimiminen, jolloin tutkimustulokset saa käyttöön tarvitsematta osallistua varsinaiseen tutkimustyöhön. Kumpikin vaihtoehto vahvistaa yhteistyötä tiedonvaihdon ja tutkimuksen osalta. Sekä työpajassa että haastatteluissa todettiin, että tietoverkkorikollisuuden tilannekuva hyötyisi kansallisen uhritutkimuksen toteuttamisesta.

Toimenpide-ehdotukset tiivistetysti

- Viranomaisten, yritysten ja tutkimuksen yhteisen vuosiseminaarin järjestäminen ilmiötilannekuvan tuottamiseksi. Malli on käytössä esimerkiksi Norjassa. Ensimmäinen askel yhteisen seminaarin järjestämiseen on kuulla lisää kokemuksia Norjan mallista ja kuinka he järjestävät ympärivuotisen tiedonvaihdon tutkimusverkoston kanssa.

- Yhteiset tutkimus- ja kehityshankkeet, joissa poliisi osallistuu tutkimuksen toteuttamiseen tai on loppukäyttäjän roolissa.

6.5 Pohdinta

Tulosten perusteella voi arvioida, että poliisi hyötyy ja saa samalla nostettua profiiliaan yhtenä kyberturvallisuusalan keskeisenä toimijana panostamalla tilannekuvatyöhön. Hyöty on ennen kaikkea tiedon saaminen oman tilannekuvan tueksi, mahdollinen ilmoittamisaktiivisuuden lisääntyminen ja rikosten ennaltaehkäisy. Mitä parempi käsitys esimerkiksi yrityksillä on rikoksista, sen paremmin ne pystyvät suuntaamaan torjuntatoimenpiteet. Mitä laajemman kokonaiskäsityksen eri viranomaiset, esimerkiksi Viestintäviraston Kyberturvallisuuskeskus, saavat kyberturvallisuuden tilasta, sitä paremmin ne pystyvät auttamaan omia sidosryhmiään. Kokonaisuudella on merkittävää vaikutusta siihen, kuinka hyvin Suomi pystyy ylläpitämään valtion johtamisen kannalta tarpeellista tilannekuvaa.

Tilannekuvatyötä kehitettäessä on tärkeä ymmärtää siihen liittyvät erilaiset tarpeet. Päivittäistoiminta, operatiivinen työ, edellyttää nopeaa, tarkkaa, yksityiskohtaista ja konkreettista käsitystä, jonka varassa tehdään päätöksiä arkipäivässä. Tilannekuvaa tarvitsevat ammattilaiset ovat pääsääntöisesti melko kapean alan asiantuntijoita, joilla on syvällinen ymmärrys esimerkiksi tietoverkkorikostutkinnasta tai poikkeamanhallinnasta. Tilannekuvan perusteella tehtävät ratkaisut ovat työsuorituksia, joita toteutetaan useita työpäivän aikana. Toisessa ääripäässä on tilannekuva, jota tarvitsevat johtotason henkilöt, joiden työnkuvaan kyberturvallisuus liittyy vain yhtenä välillisenä asiana muiden joukossa. He eivät ehdi seurata tietoverkkorikollisuuden viimeisimpiä mekanismeja tai ymmärrä teknisiä yksityiskohtia. He tarvitsevat tilannekuvaa yleisellä tasolla ja melko harvoin, kuten silloin, jos jotain poikkeavaa ja kokonaisuuden kannalta merkittävää on tapahtunut tai kun halutaan ennakoida tulevaisuuden uhkia. Ääripäiden väliin mahtuu paljon monenlaista tiedonvaihtoa. Tietoverkkorikollisuuden tilannekuvatyön osalta on tavoiteltavaa, että se pystyy antamaan syötteitä yhteiskunnan kaikille tasoille. Se ei edellytä juurikaan ylimääräistä vaivannäköä, vaan sopivan yhteistyöverkoston löytämistä sekä keskustelua siitä, keille tietoa olisi tarpeen jakaa puolin ja toisin.

Tässä selvityksessä on keskitytty ensisijaisesti tiedonvaihdon ja tilannekuvatyön toteuttamiseen nykyisen oikeudellisen viitekehyksen puitteissa. Tämä siksi, että yhdestä yhteistyön syventämisen pullonkaulasta – asiat todetaan, mutta niille ei tehdä mitään konkreettista – päästäisiin eteenpäin. Tulevaisuudessa kehitystarpeita pohditaan varmasti myös lainsäädännön näkökulmasta. Tunnistettuja oikeudellisia haasteita ovat esimerkiksi poliisin esitutkintapakko virallisen syytteen alaisissa rikoksissa, monimutkainen viranomaisten tiedonvaihtoon liittyvä lainsäädäntö sekä poliisin tarve perustaa pysyvä tietoverkkorikollisuuden analyysirekisteri.

6.6 Selvityksen rajoitukset

Selvityksen toteuttamiseen liittyvä suurin haaste oli se, että tietoverkkorikollisuuden tilannekuvan kehittäminen alkoi poliisin sisäisen tilannekuvatyön sijaan sidosryhmäyhteistyöstä. Tämän vuoksi lähestymistavaksi valittiin jo hankesuunnitelmavaiheessa sidosryhmäyhteistyö ja sidosryhmien näkemykset tietoverkkorikollisuuden tilannekuvatyön tarpeista. Näin sidosryhmien näkemykset voidaan huomioida kehitettäessä poliisin sisäistä tilannekuvatyötä. Loppuraportissa tilanne näkyy kuitenkin siten, että poliisille suunnatut sisäiset toimenpide-ehdotukset eivät ole yhtä konkreettisia kuin muut kehittämisehdotukset. Konkreettiset toimet vaativat vielä paljon määrittelyä ja tarkempien kehittämisehdotusten antaminen (esimerkiksi työnjaosta) kuulematta poliisilaitoksia olisi pikemminkin vienyt pohjaa yhteiseltä tilannekuvatyöltä kuin edistänyt sitä. Tulokset joka tapauksessa osoittavat sisäisen tilannekuvatyön kehittämisen olevan yhteydessä sidosryhmien kanssa tehtävästä tiedonvaihdosta saatavaan hyötyyn ja poliisilta selvästi odotetaan tietoverkkorikollisuuden kokonaisuuden hallintaa.

Selvitystyön toinen haaste aiheutui tiiviistä aikataulusta, joten hankesuunnitelman ulkopuolisille, hankkeen aikana esiin nousseille asioille ei jäänyt joustovaraa. Haaste on tyypillinen lyhyen rahoituksen projekteille, joita varten palkataan yksi tai kaksi henkilöä, joilta edellytetään tietyn teeman erityisosaamista. Selvitys on Poliisiammattikorkeakoulun osalta ohitse loppuraportin myötä ja tulosten huomioiminen käytännöntyössä sekä mahdollinen seurannan järjestäminen jää poliisin koordinoitavaksi. Luonnollinen jatkumo hankkeelle olisi nimenomaan seurannan järjestäminen ja vaikutuksien arviointi. Esimerkiksi poliisilaitosten mukaan tuleminen tilannekuvatyöhön sisältää monia haasteita niin yhdessä tekemisen kulttuurin löytämiseksi kuin käytännöntasolla. Lisäksi tiedonvaihdon vaikuttavuuden arvioiminen, palautteen kerääminen tilannekuvatyön kehittymisestä sekä ennalta estävän toiminnan onnistumisen mittaaminen ovat kaikki resursseja vaativaa työtä, jotka helposti hautautuvat arkirutiinien alle. Toiminnan arvioiminen on kuitenkin sitä tärkeämpää, mitä vähemmän resursseja on käytössä: hyödyttömäksi koettu, mutta rutiiniksi muuttunut toiminta kuormittaa lopulta paitsi organisaatioita myös työntekijöitä henkisesti.

LÄHTEET:

Action Fraud. (2015). Action Fraudin www-sivusto. Saatavilla: http://www.actionfraud.police.uk/. Luettu 5.2.2016.

Alastalo, M. & Åkerman, M. (2010). Asiantuntijahaastattelun analyysi: Faktojen jäljillä. Teoksessa J. Ruusuvuori, P. Nikander ja M. Hyvärinen (toim.) Haastattelun analyysi. Tampere: Vastapaino, 372–392.

EC (2012). Cyber security. Report. Special Eurobarometer 390. Saatavilla: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf. Luettu 17.2.2016.

Hallitusohjelma (2015). Pääministeri Juha Sipilän hallituksen ohjelma 19.5.2015. Hallituksen julkaisusarja 10/2015. Saatavilla: http://tampub.uta.fi/bitstream/handle/10024/97031/978-951-44-9780-3.pdf?sequence=1. Luettu 8.1.2016.

Helminen, K., Fredman, M., Kanerva, J., Tolvanen, M. & Viitanen M. (2012). Esitutkinta ja pakkokeinot. Helsinki: Talentum.

Kyberturvallisuusstrategian toimeenpano-ohjelma. (2014). Helsinki: Turvallisuuskomitea. Saatavilla: http://pardia-fi-bin.directo.fi/@Bin/65ac9bedb18d8af5e1cdc9b11d164736/1456735449/application/pdf/4851679/Kyberturvallisuusstrategian%20toimeenpano-ohjelma.pdf. Luettu 26.1.2016.

Laitinen, K. & Järvinen, J-H. (2013). Poliisin tulevaisuus – tulevaisuuden poliisi. Raportti poliisitoiminnan kehittämishankkeesta – POKEHAsta. Poliisihallituksen julkaisusarja 3/2013. Helsinki: Poliisihallitus.

Lehto, M. & Kähkönen, A. (2015). Kyberturvallisuuden kansallinen osaaminen. Informaatioteknologian tiedekunnan julkaisuja No. 20/2015. Jyväskylän yliopisto.

Leppänen, A. & Virta, S. (2014). Kohti systeemiälykästä kyberturvallisuuden hallintaa - kyberrikollisuus ja sen torjunta. Futura 2/2014, 5–13.

Pawli, J., Antikainen, P., Rissanen, P., Pekkala, E., Appel, M., Pihlava, P., Uotila, P., Onninen, K., Arokoski, R., Salo, S., Pajunen, J. & Kiljunen, M. (2010a). Analyysi johtamisen välineenä. Tietojohtoisen poliisitoiminnan käytäntöjen ja rakenteiden kehittämisprojekti 2009–2010. Väliraportti: nykytilankuvaus ja kehitysnäkymiä poliisilaitoksissa Tampere: Poliisiammattikorkeakoulu.

Pawli, J., Antikainen, P., Rissanen, P., Pekkala, E., Appel, M., Pihlava, P., Uotila, P., Onninen, K., Arokoski, R., Salo, S., Pajunen, J. & Kiljunen, M. (2010b). Tietojohtoisen poliisitoiminnan kehittäminen paikallispoliisissa. Analysoidun tiedon ja päätöksenteon kohtaaminen. Tietojohtoisen poliisitoiminnan käytäntöjen ja rakenteiden kehittämisprojektin loppuraportti. Tampere: Poliisiammattikorkeakoulu.

Pelkonen, A. (2015). VTT:n blogi: Onko Suomi kyberturvallisuusosaamisen edelläkävijä? Saatavilla: http://vttblog.com/2015/12/08/onko-suomi-kyberturvallisuusosaamisen-edellakavija/. Luettu 17.12.2015

Poliisihallitus. (2015). Esitys poliisin kybertoimivaltuuksien muutostarpeista. Työryhmän loppuraportti 21.5.2015.

Ratcliffe, J. (2008). Intelligence-Led Policing. Cullompton: Willan Publishing.

Salmela, M. & Hakaniemi, J. (2015). Tietojohtoisen poliisitoiminnan kehittäminen. Johtamisen työkalupakki -projekti. Poliisin sisäinen raportti.

Salmi, V., Lehti, M. & Keinänen, A. (2011). Kauppa ja teollisuus rikosten kohteena. Oikeuspoliittinen tutkimuslaitos.

Sisäministeriön hallinnonalan toiminta- ja taloussuunnitelma (2016). Sisäministeriön hallinnonalan toiminta- ja taloussuunnitelma 2017–2020 sekä tulossuunnitelma 2016. Sisäministeriön julkaisu 1/2016. Saatavilla: http://www.intermin.fi/download/57433_NettiTTS_2016-2019_TS_2015_julkaisu.pdf?dbfa43bce41cd388. Luettu 26.1.2016.

Suomen kyberturvallisuusstrategia. (2013). Valtioneuvoston periaatepäätös 26.1.2013. Helsinki: Turvallisuuskomitean sihteeristö.

Tuomi, J. & Sarajärvi, A. (2009). Laadullinen tutkimus ja sisällönanalyysi. Jyväskylä: Tammi.

Turvallisuuskomitean tiedote 9.6.2015. Turvallisuuskomitea hyväksyi kokouksessaan VALHA 15-16 -harjoitussuunnitelman. Saatavilla: http://www.turvallisuuskomitea.fi/index.php/fi/ajankohtaista/35-turvallisuuskomitea-hyvaksyi-kokouksessaan-valha15-16-harjoitussuunnitelman. Luettu 17.12.2015.

Yhteiskunnan turvallisuusstrategia. (2010). Valtioneuvoston periaatepäätös 16.12.2010. Helsinki: Puolustusministeriö. Saatavilla: http://www.defmin.fi/files/1696/Yhteiskunnan_turvallisuusstrategia_2010.pdf. Luettu 26.1.2016.

Virallislähteet

Esitutkintalaki 22.7.2011/805.

HE 30/1998 vp. Hallituksen esitys eduskunnalle laiksi viranomaisten toiminnan julkisuudesta ja siihen liittyviksi laeiksi.

HE 57/1994 vp. Hallituksen esitys eduskunnalle poliisilaiksi ja eräiksi siihen liittyviksi laeiksi.

Laki henkilötietojen käsittelystä poliisitoimessa 22.8.2003/621.

Laki henkilötietojen käsittelystä Tullissa 22.5.2015/639.

Laki henkilötietojen käsittelystä rajavartiolaitoksessa 15.7.2005/579.

Laki kansainvälisestä oikeusavusta rikosasioissa 5.1.1994/4.

Laki keskinäisestä oikeusavusta rikosasioissa Euroopan unionin jäsenvaltioiden välillä tehdyn yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta ja yleissopimuksen soveltamisesta 20.2.2004/148.

Laki oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa 30.3.2007/370.

Laki rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä 18.7.2008/503.

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621.

Poliisilaki 22.7.2011/872

Rikoslaki 19.12.1889/39.

Tietoyhteiskuntakaari 7.11.2014/917.

LIITTEET:

Liite 1. Haastatellut organisaatiot

CGI Oy

Elinkeinoelämän keskusliitto

Elisa Oyj

Keskusrikospoliisi

Kyberturvallisuuskeskus*

Poliisihallitus

Puolustusvoimat

Sisäministeriö

SOK-yhtymä

Suojelupoliisi

Tulli

Turvallisuuskomitea

Valtioneuvoston tilannekeskus

Valtionvarainministeriö

* Nauhoittamaton, keskusteleva tutustuminen tilannekuvatyöhön

Liite 2. Työpajaan osallistuneet henkilöt ja organisaatiot

Boberg Henrik, Valtioneuvoston tilannekeskus

El-Bash Amira, Huoltovarmuuskeskus

Eronen Pasi, puolustusministeriö

Ferm Tiina, sisäministeriö

Hartikainen Jarna, Kyberturvallisuuskeskus

Kajantie Sari, Suojelupoliisi

Kurittu Antti, Helsingin poliisilaitos

Laitinen Kari, puolustusministeriö

Lehto Martti, Jyväskylän yliopisto

Leskinen Jari, Keskusrikospoliisi

Liesimaa Tomi, Keskusrikospoliisi

Linderborg Karl, Keskusrikospoliisi

Linna Mika, Finanssialan keskusliitto

Muurman Tero, Keskusrikospoliisi

Piiroinen Timo, Keskusrikospoliisi

Pärssinen Juha, VTT

Risu Jukkapekka, Helsingin poliisilaitos

Räsänen Erkki, Huoltovarmuuskeskus

Saarimäki Jarkko, Kyberturvallisuuskeskus

Salonen Jarno, VTT

Savola Reijo, VTT

Sillanpää Pekka, Nixu

Toiviainen Tero, Poliisiammattikorkeakoulu

Tuomi Mikko, Puolustusvoimat

Vehviläinen Timo, Kesko

Liite 3. Työpajan työryhmät, ennakkotehtävät ja ohjeistus

Työryhmätyöskentely tapahtuu kolmessa työryhmässä, joihin osallistujat on jaettu ennakolta. Kullakin työryhmällä on teema, jonka ympärillä työskentely tapahtuu. Työryhmät koostavat ensisijaisesti konkreettisia, lähitulevaisuuteen suuntautuvia kehitysehdotuksia tietoverkkorikollisuuden tilannekuvatyön kehittämiseksi nykyisen lainsäädännön asettamissa raameissa. Työryhmät kirjaavat ehdotuksensa ylös ja esittävät pohdintansa iltapäivällä koko työpajalle, jolloin koko työpajalla on mahdollista kommentoida aihepiiriä. Työryhmän muistiinpanot lähetetään myös osoitteeseen anna-riitta.leppanen@poliisi.fi

Pohdittavat kysymykset ja väitteet on tarkoitettu alustamaan ja virittämään työryhmän työskentelyä. Ryhmillä on vapaus tunnistaa myös muita keskeisiä kysymyksiä ja pohtia niihin ratkaisuja.

Työryhmät

1) **Operatiivinen tiedonvaihto viranomaisten välillä ja lainsäädännön rajat**

Työryhmän tarkoitus on pohtia tietoverkkorikollisuuden lyhyen tähtäimen, operatiivista toimintaa tukevan, tilannekuvan kehittämistä. Tässä yhteydessä sillä tarkoitetaan ensisijaisesti viranomaisten päivittäistoiminnassa syntyvää ja tarvitsemaa tilannetietoisuutta. Tavoiteltava tilannekuva vastaa kysymykseen: Mitkä ovat ne tietoverkkorikollisuuden tämän hetken uhkat, joiden arvioidaan koskettavan kansalaisia, yrityksiä, viranomaisia tai valtiota? Tilannekuvan tavoite on päivittäistyön ja sen johtamisen helpottaminen.

Pohdittavia kysymyksiä:

- Väite 1: paras keino yhteisen tietoverkkorikollisuuden päivittäistilannetietoisuuden luomiseksi nykyisen lainsäädännön valossa on jakaa tietoa, josta on poistettu tunnistetiedot. Perustele puolesta ja/tai vastaan.
- Väite 2: Olennaista tietoa ei menetetä, jos sovitaan, että jaetaan ensisijaisesti vain tietoa, josta on poistettu tunnistetekijät. Perustele puolesta ja/tai vastaan esimerkein.
- Väite 3: tunnistetietojen poisto datasta on liian suuri vaiva. Perustele puolesta ja/tai vastaan. Miten tiedon anonymisoimista voisi kehittää?
- Väite 4: Viranomaisten väliseen tiedonvaihtoon tarvitaan yhteinen alusta. Perustele puolesta ja/tai vastaan. Millaisia väliaikaisratkaisuja voisi käyttää?
- Mitkä ovat tärkeimmät konkreettiset toimenpiteet, joilla yhteistä tiedonvaihtoa voidaan parantaa lähitulevaisuudessa? Entä pitkällä tähtäimellä?
- Miten päivittäistiedon kokoaminen ja yhdistäminen osaksi laajempaa ilmiötilannekuvaa onnistuisi parhaiten? Ehdotuksia?
- Muuta?

2) **Tiedonvaihto viranomaisten ja yritysten välillä**

Työryhmän tarkoitus on pohtia tietoverkkorikollisuuden tilannekuvatyön kehittämistä yritysten ja viranomaisten yhteisestä näkökulmasta. Tässä yhteydessä sillä tarkoitetaan ensisijaisesti yritysten tarvitsemaa ja toisaalta yrityksissä syntyvää tilannekuvaa tietoverkkorikollisuudesta. Tavoiteltava tilannekuva vastaa kysymykseen: Mitkä ovat ne tietoverkkorikollisuuden tämän hetken tai tulevat uhkat, joiden arvioidaan koskettavan elinkeinotoimintaa? Tilannekuvan tavoite on parantaa yritysten ja viranomaisten valmiutta ennalta ehkäistä tietoverkkorikollisuutta sekä ylläpitää kokonaiskuvaa tietoverkkorikollisuudesta niin päivittäistoiminnassa kuin ilmiötasolla.

Pohdittavia kysymyksiä:

- Millaisia tiedontarpeita tietoverkkorikollisuudesta yrityksillä on poliisille? Haastatteluissa nousi esille, että poliisilta toivotaan tietoa rikosten tekotavoista, trendeistä ja rikollisista. Mitä mieltä olet ja tuleeko mieleen jotain muuta?
- Kuinka suuri merkitys poliisin esitutkintapakolla on yritysten tiedonjakohalukkuuteen? Mitkä ovat parhaat ratkaisut tilanteeseen?
- Tulisiko rikosten tunnistamisen analyysia kehittää yhdessä, että yritykset oppisivat tunnistamaan rikoksia? Olisiko siitä hyötyä? Perustele puolesta ja/tai vastaan.
- Syntyykö yrityksissä ja poliisissa/viranomaisissa tutkimusaineistoja, joista voisi rakentaa systemaattista tilannekuvaa yhteisessä tutkimushankkeessa?
- Kuinka tutkimus voi tukea tietoverkkorikollisuuden tilannekuvan kehittämistä? Millä edellytyksin? Esimerkkejä?
- Mitkä ovat tärkeimmät konkreettiset toimenpiteet, joiden avulla yritysten ja viranomaisten välistä tiedonvaihtoa voisi parantaa? Entä yritysten, viranomaisten ja tutkimuksen?
- Muuta?

3) Tietoverkkorikollisuuden pitkän tähtäimen ilmiötilannekuva

Työryhmän tarkoitus on pohtia tietoverkkorikollisuuden pitkän tähtäimen ilmiötilannekuvan kehittämistä. Tässä yhteydessä sillä tarkoitetaan ensisijaisesti ennakoivaa tilannetietoisuutta. Tavoiteltava tilannekuva vastaa kysymykseen: Mitkä ovat ne tietoverkkorikollisuuden uhkat, joiden arvioidaan koskettavan kansalaisia, yrityksiä, viranomaisia tai valtiota (lähi)tulevaisuudessa? Ilmiötilannekuvan tavoite on kokonaisuuden hallinta ja ennakointi. Ilmiötilannekuvan perusteella voi suunnata tavoitteita ja resursseja sekä tarkentaa millaisiin asioihin päivittäistyössä tulisi kiinnittää huomiota.

Pohdittavia kysymyksiä

- Sopiiko tietoverkkorikollisuuden pitkän tähtäimen ilmiötilannekuvan tavoitteeksi tunnistaa merkittävät uhkat ennakolta torjuntatoimenpiteiden suuntaamiseksi? Perustele puolesta ja/tai vastaan tai esitä vastaehdotus.
- Mikä on tietoverkkorikollisuuden osalta "pitkä tähtäin"? Perustele.
- Mitä tahoja tulisi olla mukana?
- Kuinka tiedonvaihdosta päästään yhteiseen analyysiin? Millä konkreettisin keinoin eri tahojen yhteistä, tulevaisuuteen katsovaa, analyysia ilmiötiedon perusteella voisi tukea?
- Kuinka tutkimus voi tukea tietoverkkorikollisuuden tilannekuvan kehittämistä? Millä edellytyksin? Miten tutkimuksen julkisuus ja viranomaisaineistot olisi yhteen sovitettavissa?
- VTT:n ja Cyberlab Oy:n Kyberosaaminen Suomessa -tutkimushankkeen alustavien tulosten mukaan vuorovaikutus julkisen hallinnon ja tutkimusmaailman välillä kyberturvallisuudessa ei ole systemaattista. Hankkeen johtaja Antti Pelkonen pohti VTT:n blogissa, pitäisikö luoda jokin foorumi, joka välittäisi tietoa ja vahvistaisi vuorovaikutusta tutkimus- ja viranomaistoimijoiden välillä? Miten yhteistyötä voisi lisätä kybertilannetietoisuuden kehittämisessä ja mikä olisi tietoverkkorikollisuuden rooli yhteistyössä?
- Mitkä ovat tärkeimmät konkreettiset toimenpiteet, joilla yhteistä ilmiötiedonvaihtoa ja analyysia voidaan parantaa lähitulevaisuudessa? Entä pitkällä tähtäimellä?
- Muuta?

:

VALTIONEUVOSTON
SELVITYS- JA TUTKIMUSTOIMINTA

tietokayttoon.fi

ISSN 2342-6799 (pdf)
ISBN 978-952-287-251-7 (pdf)