T A M P E R E E N Y L I O P I S T O

Kyberrikostorjunta tietojohtoisessa poliisitoiminnassa

Paikallispoliisi torjumassa globaalia järjestäytynyttä rikollisuutta?

Hallintotiede, turvallisuushallinto
Pro gradu -tutkielma
Helmikuu 2016
Ohjaajat: Sirpa Virta ja Anna Leppänen

Pentti Kangasniemi

Tiivistelmä

Tampereen yliopisto	Johtamiskorkeakoulu, Turvallisuushallinto
Tekijä:	PENTTI KANGASNIEMI
Tutkielman nimi:	Kyberrikostorjunta tietojohtoisessa poliisitoiminnassa. Paikallispoliisi torjumassa globaalia järjestäytynyttä rikollisuutta?
Pro gradu -tutkielma:	105 sivua
Aika:	Helmikuu 2016
Avainsanat:	kyberrikostorjunta, järjestäytynyt rikollisuus, tietojohtoinen poliisitoiminta, tiedustelu, tiedonhankinta, rikostorjunta, poliisi

---

Tietoverkot ovat tulleet osaksi ihmisten elämää ja ovat osa ympärillä olevaa avaruutta. Rikollisuus ja eritoten sen järjestäytyneisyys ei ole jättänyt hyödyntämättä tilaisuuttaan päästä ujuttautumaan monin muodoin yhteiskuntaan ja aiheuttamaan suurta vahinkoa. Kansakunnat ja niiden ydintoiminnot ovat rakentuneet entistä enemmän tietoteknisen infrastruktuurin ympärille, jonka johdosta kannamme taskussamme koko kybermaailmaa puhelimiemme kautta. Kyberrikollisuus ja sen torjunta ovat tällä hetkellä ajankohtainen aihe. Tutkimus kertoo nykytilan siitä, miten poliisin suorittamaa tiedonhankintaa kybertoimintaympäristössä vakavan ja järjestäytyneen rikollisuuden torjunnassa on ohjattu. Näkökulmana on ollut tietojohtoinen poliisitoiminta, jota poliisiyksiköissä toteutetaan ohjausasiakirjojen välityksellä.

Tutkimus on hallintotieteellinen tutkimus, jonka teoreettinen ydin muodostuu sen tarkastelusta, miten Euroopan unionin ja kansalliset strategia-asiakirjat ohjaavat tietoverkoissa tapahtuvan vakavan ja järjestäytyneen rikollisuuden torjuntaa rikostiedustelun ja tietojohtoisen poliisitoiminnan lähtökohdista paikallispoliisissa. Kyseessä on kuvaileva kvalitatiivinen sisällönanalyysillä tehty tutkimus, jossa asiakirja-aineistoa on tarkasteltu tietojohtoisen poliisitoiminnan teoreettisessa viitekehyksessä. Tutkimuskysymykset ovat: Mitä asiakirjamateriaalia on laadittu ohjaamaan paikallispoliisin kyberympäristössä tapahtuvaa tiedustelutoimintaa ja tiedonhankintaa paikallispoliisin toiminnan järjestämiseksi sekä miten vakavan ja järjestäytyneen rikollisuuden kybertiedustelutoiminta tulisi paikallispoliisin näkökulmasta järjestää ottaen huomioon tietojohtoisen poliisitoiminnan vaatimukset?

Tutkimuksen johtopäätöksenä voidaan todeta, että tutkimuksen kohteena olevaa kybermaailmasta tehtävää tiedonhankintaa ja toiminnan järjestämistä ohjaavaa asiakirjamateriaalia ei ole. Poliisilta puuttuu oma kyberstrategia, joka sisältäisi keskeiset toimintalinjat ja keinot kyberturvallisuuden kehittämiseksi ja sisäisen turvallisuuden toteuttamiseksi. Lainsäädäntö ei kaikilta osin ole ajantasainen ja anna poliisille toimivaltuuksia nykyisessä toimintaympäristössä sen haasteiden ratkaisemiseksi. Jatkossa tulisi tarkastella sitä, vastaavatko nykyiset poliisin organisaatiorakenteet ja erityisesti poliisin rikostutkinnan järjestelyt kyberrikostorjunnan nykypäivän ja tulevaisuuden haasteita ja vaatimuksia.

Sisällysluettelo

1 JOHDANTO

Tietoverkot ovat olleet hyödyntämässä ihmisten elämää kymmenien vuosien ajan. Ensimmäiset tietokoneverkot syntyivät 1950-luvulla, kun useita päätteitä alettiin yhdistää yhteen keskustietokoneeseen. Myöhemmin myös suurtietokoneita alettiin yhdistää toisiinsa. Internet alkoi muodostua 1960-luvun alussa. Pohjana oli idän ja lännen välinen kilpavarustelu ja erityisesti avaruusraketti Sputnikin laukaisu vuonna 1957, jonka seurauksena Yhdysvaltojen puolustusministeriö perusti ARPA-hankkeen (Advanced Research Projects Agency) edistämään tutkimusta. Ensimmäinen suunnitelma verkolle, jota kutsuttiin ARPANETiksi, julkaistiin vuonna 1967 ja se oli käytössä armeijan lisäksi lähinnä yliopistoilla ja tutkimuslaitoksissa. Armeijan oma tietoverkko irrottautui ARPANET:sta vuonna 1983 omaksi MILNET-verkokseen, jonka johdosta jäljelle jäänyt verkko alkoi laajentua myös Yhdysvaltain ulkopuolelle. 1980- ja 90-lukujen vaihteessa ARPANET muuttui Internetiksi. (Willa ja Uusitupa 2007, 155–156)

Samaan aikaan suomalainen yhteiskunta on muuttunut kovalla vauhdilla ja siirtynyt kiinteäksi osaksi globalisoitunutta maailmaa. Maailmanlaajuisesti noin kolme miljardia ihmistä käyttää internetiä (Poliisin kybertyöryhmän loppuraportti 2015, 4). Internetistä ja tietoverkoista on tullut keskeinen osa elämää, tietoverkot hallitsevat suurelta osin arkea ja suurin osa tekemistämme asioista päivittäin liittyvät tietoverkkoihin. Tietoverkoissa on jo tällä hetkellä suunnaton määrä erilaista informaatiota, jonka määrä kasvaa koko ajan. Tietoverkoista on tullut ihmiskunnalle uusi elämänalue, jonne myös monialainen rikollisuus on siirtynyt. Lähes kaikilla rikollisuuden alueilla rikokset ovat siirtyneet lähes kokonaan tai ainakin osittain tietoverkkoihin hyödyttämään rikollisten tarkoitusperiä.

Digitaalisen toimintaympäristön voidaan sanoa olevan ihmisten luoma digitaalinen rinnakkaistodellisuus, joka maailmanlaajuisesti yhdistää informaatioteknologian, automatisoitujen ohjausjärjestelmien, internetin ja sosiaalisen median kautta toisiinsa ihmisiä ja laitteita valtioiden rajojen yli. Digitaa-

lisuudella tarkoitetaan loputonta joukkoa sovelluksia, mediaa, pelejä ja virtuaalitodellisuuksia, jotka kehittyneissä maissa läpäisee modernin elämäntavan kokonaisuudessaan. (Poliisin kybertyöryhmän loppuraportti 2015, 4)

Kyberrikollisuus on jatkuvasti kasvava rikollisuuden ala ja rikolliset ovat siirtymässä entistä enemmän toimimaan tietoverkkoihin, joissa rikolliseen toimintaan ei pystytä tällä hetkellä kohdistamaan torjuntatoimia siinä määrin kuin yhteiskunnan turvallisuuden tarve on. Syinä tämänhetkiseen torjunnan tasoon voidaan pitää muun muassa riittämätöntä toimintaan kohdistettua resursointia, lainsäädäntöä, toimintakentän ja toimijoiden hajanaisuutta ja sen johdosta riittämätöntä torjuntatoiminnan johtamista ja koordinointia.

Järjestäytynyt ja vakava rajat ylittävä rikollisuus on yleisesti ottaen edelleen suuri uhka Euroopan Unionin (EU) sisäiselle turvallisuudelle. Se aiheuttaa vakavaa vahinkoa uhreille ja koko yhteiskunnalle. Vuonna 2013 Europol arvioi, että EU:ssa toimii noin 3 600 järjestäytynyttä rikollisryhmää. Järjestäytyneiden riskiryhmien soluttautuminen lailliseen talouteen on EU:n keskeinen turvallisuusuhka. (EU:n Sisäisen turvallisuuden strategian täytäntöönpano vuosilta 2010–2014, 13)

Suomalainen poliisi yhtenä turvallisuusorganisaationa on totuttelemassa toimimaan tietoverkoissa ja erityisesti tietoverkoissa tapahtuvan rikollisuuden torjuntaan ja ennalta estämiseen. *Tässä opinnäytetyössä tarkastelen tietoverkoissa tapahtuvan erityisesti vakavan ja järjestäytyneen rikollisuuden torjuntaa tietojohtoisen poliisitoiminnan lähtökohdista sekä rikostiedustelun ja paikallispoliisin näkökulmasta*.

2 TUTKIMUSONGELMA JA TAVOITE

2.1 Tutkimuksen tausta ja rajaaminen

Kybermaailma ja – avaruus (tietoverkot) ovat nousseet yhdeksi keskeiseksi omaksi ”elämänmuodokseen”, joka on siirtänyt yhteiskuntia uuteen maailmaan[1], jossa ulottuvuudet ovat lähes rajattomia mahdollistaen kansalaisille asioita, joissa vain mielikuvitus on rajoitteena. Kyberympäristö on haaste poliisin rikostorjunnalle, joka on laissa säädetty yhdeksi poliisin tehtäväksi[2]. Tietoverkkorikollisuuden torjunta poikkeaa merkittävästi tavanomaisesta poliisitoiminnasta. Se edellyttää asiantuntijuutta ja erityisosaamista uusilla sektoreilla, joissa poliisi on vain yksi toimijoista. Tietoverkot eivät toimi alueellisesti tai paikallisesti, vaan kyse on kyberavaruudesta, jossa toimiminen edellyttää erityisiä toimintamalleja, toimintojen organisointia ja rakenteita. Vaaditaan muun muassa yhtenäistä ja loogista lainsäädäntöä, uusia keinoja ja toimintatapoja sekä uudenlaista laajaa ajattelumallia poliisin tehokkaasta rikostorjunnasta.

2.2 Tutkimuskysymykset

Tutkimukseni kohteeksi valitsin kyberympäristössä tapahtuvan vakavan ja järjestäytyneen rikollisuuden torjunnan rikostiedustelun ja tietojohtoisen poliisitoiminnan lähtökohdista paikallispoliisissa. Nämä tutkimuskysymykset liittyvät työhöni ja aihealueena kyberrikollisuus yleisesti ja sen torjunta on

[1] Muun muassa viimeisten kymmenen vuoden aikana verkkokaupan asiakkaiden määrä on suunnilleen kolminkertaistunut. Vuonna 2004 runsas miljoona 16–74-vuotiasta oli ainakin joskus ja lähes 600 000 viimeisen kolmen kuukauden aikana ostanut jotain Internetin kautta. Vuonna 2013 vastaavat luvut olivat 2,9 miljoonaa ja 1,9 miljoonaa. Vuonna 2013 verkkokaupan kokonaisarvo oli 7,0 miljardia euroa, josta palveluiden osuus oli 3,7 miljardia euroa ja tavaraostojen osuus lähes 2,9 miljardia euroa. (Tilastokeskuksen verkkosivut 2015: http://www.stat.fi)

[2] 1 luvun 1 § (Poliisin tehtävät): Poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen. Poliisi toimii turvallisuuden ylläpitämiseksi yhteistyössä muiden viranomaisten sekä yhteisöjen ja asukkaiden kanssa ja huolehtii tehtäviinsä kuuluvasta kansainvälisestä yhteistyöstä.
Poliisi suorittaa lisäksi lupahallintoon liittyvät ja muut sille laissa erikseen säädetyt tehtävät sekä antaa jokaiselle tehtäväpiiriinsä kuuluvaa apua. Jos on perusteltua syytä olettaa henkilön kadonneen tai joutuneen onnettomuuden uhriksi, poliisin on ryhdyttävä tarpeellisiin toimenpiteisiin henkilön löytämiseksi.
Rikosten esitutkinnasta säädetään esitutkintalaissa (805/2011) ja rikosten esitutkinnassa käytettävistä pakkokeinoista pakkokeinolaissa (806/2011).” (Poliisilaki 872/2011)

uusi, kiinnostava tutkimuskohde, jota poliisihallinnossa ei ole paljoa tähän mennessä tutkittu.

Tutkimuksessa pyrin selvittämään:

1. Mitä asiakirjamateriaalia on laadittu ohjaamaan paikallispoliisin kyberympäristössä tapahtuvaa tiedustelutoimintaa ja tiedonhankintaa paikallispoliisin toiminnan järjestämiseksi?

   Tutkimuksessa tarkastellaan sekä EU-tasolla että kansallisesti laadittuja asiakirjoja, joista ilmenee vakavan ja järjestäytyneen rikollisuuden torjunnan hallinnollinen ohjaus tietojohtoisen poliisitoiminnan näkökulmasta tällä hetkellä. Tarkastelussa keskitytään löytämään vastauksia siihen, ohjaavatko asiakirjat paikallispoliisin toiminnan järjestämistä ja sitä, miten sen tulisi linkittyä muihin yksiköihin ja toimijoihin sekä millaisilla resursseilla toiminta tulisi järjestää?

2. Miten vakavan ja järjestäytyneen rikollisuuden kybertiedustelutoiminta tulisi paikallispoliisin näkökulmasta järjestää ottaen huomioon tietojohtoisen poliisitoiminnan vaatimukset?

Tutkimuksen toisessa teemassa tarkastelen sitä, miten tutkimuksen kohteena oleva toiminta tulisi paikallispoliisiin rakentaa siten, että se täyttäisi tietojohtoisen poliisitoiminnan kriteerit ja toimisi tehokkaasti ja tuloksekkaasti. Tarkastelussa pohjana käytän Itä-Uudenmaan poliisilaitoksen toimintaympäristöä, organisaatio- ja tehtävärakenteita, jotta tarkastelussa säilyy reaalimaailman liityntä.

Tutkimuskysymyksen toinen osio on sisällytetty tutkimuksen pohdintaosaan, koska tutkimuksessa ei ole käytettävissä valmista ohjaavaa asiakirjaaineistoa.

2.3 Tutkimusasetelma ja menetelmät

Kyseessä on kuvaileva kvalitatiivinen sisällönanalyysillä tehty tutkimus, jossa asiakirja-aineistoa on tarkasteltu tietojohtoisen poliisitoiminnan teoreettisessa viitekehyksessä. Tutkimuksessa kuvailevan tutkimuksen käyttö on perustelua, koska aihealueesta ei ole juuri aiempaa tutkimusta, jolloin ennakkotietoja ei ole käytettävissä (Metsämuuronen 2003, 24). Tutkimuksen metodologiaksi on valittu kvalitatiivinen tutkimus, koska tutkimuksen kohteena ovat asiakirjat, joita on tarkasteltu yksityiskohtaisesti niiden sisältämistä hallinnon ohjaukseen soveltuvasta lähtökohdasta (Metsämuuronen 2003, 167). Kyseessä on myös tutkimus, joka on luonteeltaan kokonaisvaltaista tiedonhankintaa, koska tutkimusta varten on pyritty hankkimaan kaikki saatavilla olevat keskeiset asiakirjat, joissa tutkimusaihetta on käsitelty (Hirsjärvi & Remes & Sajavaara 2007, 160). Sisällönanalyysin avulla on mahdollista tarkastella kvalitatiivisin keinoin kerättyä tutkimusmateriaalia ja sillä on saatu edellä mainituin kriteerein kerätty aineisto järjestetyksi johtopäätöksien tekoa varten (Grönfors 1985, 94).

Tutkimuksen viitakehyksenä olevaa tietojohtoista poliisitoiminta-mallia toteutetaan jo monissa eri poliisihallinnon toiminnoissa, joten sitä on testattu jo käytännössä. Koska tietojohtoinen poliisitoiminta – malli on keskeinen poliisihallinnon tapa toimia ja järjestää toimintonsa, on perusteltua tarkastella myös kyberympäristössä tapahtuvaa vakavan ja järjestäytyneen rikollisuuden torjuntaa rikostiedustelun ja tietojohtoisen poliisitoiminnan lähtökohdista paikallispoliisin näkökulmasta.

Tutkimusaineiston kerääminen on tehty kriittisesti ja siinä on otettu huomioon aineiston soveltuvuus ja luotettavuus (Metsämuuronen 2003, 192). Lisäksi tutkimuksen kohde, menetelmät ja toteuttaminen on pyritty kuvaamaan tarkasti, jotta tutkimuksen luotettavuutta ja pätevyyttä pystytään arvioimaan sekä laajalla aineistonotannalla että asiakirjojen taulukoinnilla, josta valintaperusteet asiakirjojen lähdeaineistoiksi hyväksymiseksi käy selville, pyritään vielä vahvistamaan tutkimuksen pätevyyttä (Hirsjärvi & Remes & Sajavaara 2007, 226–227). Tutkimusaineisto on kerätty tarkastelemalla

aluksi tutkimusaihetta, sen käytettävyyttä sekä sopivuutta teoreettisessa viitekehyksessä asetettuihin tutkimuskysymyksiin, jonka jälkeen aineisto on koostettu yhteen ja saadun materiaalin perusteella pohdinnan avulla on päädytty johtopäätöksiin (Metsämuuronen 2003, 198).

Asiakirjat on valittu tutkimusaineistoksi sen perusteella, onko niissä käsitelty tutkittavana olevaa asiaa tai kyber-/ tietoverkkorikollisuutta ylipäätään. Tutkimusaineisto on hankittu ja koostuu Internetin avoimista lähteistä hankituista asiakirjoista, kirjallisessa muodossa olleesta materiaalista sisältäen hallinnon sisällä tuotettuja ohjausasiakirjoja sekä erilaisten työryhmien käsittelemää aineistoa. Lisäksi aineistossa on käytetty hallinnossa tuotettua tai käsiteltyä materiaalia, jossa tutkittavana olevaa asiaa on käsitelty teoreettiseen viitekehykseen soveltuvalla tavalla. Tutkimusaineiston valinta ja järjestäminen on ollut mahdollista tehdä sisällönanalyysin avulla, koska sisällönanalyysia voidaan kohdistaa hyvin monenlaisiin teksteihin. Lisäksi sisällönanalyysiin on päädytty, koska muulla järkevällä aineiston keruutavalla tutkimusaineistoa olisi ollut lähes mahdoton saada kerättyä. Sisällönanalyysi tuottaa raaka-aineet teoreettiseen pohdintaan, mutta itse pohdinta tapahtuu tutkijan järjellisen ajattelun keinoin. Sisällönanalyysillä ja siihen yhdistetyllä kontekstianalyysillä parhaimmillaankin voidaan tuottaa vain kuvailevaa tietoa, jolloin tutkijalle jää tehtäväksi sisällöstä tehtävät päätelmät ja johtopäätökset (Grönfors 1985, 94).

3 TEOREETTINEN VIITEKEHYS

Tutkimus on hallintotieteellinen tutkimus, jonka teoreettinen ydin muodostuu sen tarkastelusta, miten Euroopan unionin ja kansalliset strategia-asiakirjat ohjaavat tietoverkoissa tapahtuvan vakavan ja järjestäytyneen rikollisuuden torjuntaa rikostiedustelun ja tietojohtoisen poliisitoiminnan lähtökohdista paikallispoliisissa. Tutkimuksella pyrin selvittämään, millaisia ja minkä tason strategisia asiakirjoja on laadittu sekä sitä, miten ne ovat vaikuttaneet poliisin operatiiviseen toimintaan paikallispoliisin toimintaympäristössä.

Opinnäytetyön tutkimusaineistona on käytetty poliisitoimintaa ohjaavia sekä Euroopan Unionin ja Komission laatimia että kansallisesti laadittuja asiakirjoja. Tutkimuksen aineistoksi valituista asiakirjoista on laadittu taulukko (sivu 30). Valitut asiakirjat sisältävät aihealueeseen liittyviä keskeisiä strategisia linjauksia tai muulla tavalla ohjaavat tietoverkoissa tapahtuvaa vakavan ja järjestäytyneen rikollisuuden torjuntaa tai vaikuttavat sen toteuttamisen.

Tässä luvussa käyn läpi tutkimuksessa käytettyjä keskeisiä käsitemääritelmiä sekä kuvaan lyhyesti tutkimuksen aihealueeseen liittyviä aiempia tutkimuksia. Keskeiset käsitteet liittyvät kyberrikollisuuteen, vakavaan ja järjestäytyneeseen rikollisuuteen ja sen torjuntaan. Olen lähemmin tarkastellut tietojohtoisen poliisitoiminnan, kyberrikollisuuden, järjestäytyneen rikollisuuden, rikostorjunnan, rikosten ennalta estämisen, ja tiedustelun määritelmiä. Joidenkin määritelmien osalta tietopohjana on käytetty kansainvälistä aineistoa, koska suomalaista kirjallisuutta kaikista määritelmistä ei ole saatavilla. Keskeisenä määriteltävänä käsitteenä on tietojohtoinen poliisitoiminta, joka toimii yhtenä tutkimuksen ydinteemana ja tarkastelukulmana.

Omassa luvussaan tarkastelen kyberrikollisuutta määritelmien pohjalta lisäksi yhdenlaisena ilmiönä. Tarkoituksena on kuvata laajemmin kyberrikollisuuden mukaan tuomia haasteita, joihin poliisin olisi kyettävä vastaamaan

muuttuneessa toimintaympäristössä. Ilmiön kuvauksen tutkimus itsessään ei sisälly tämän tutkimuksen tutkimusasetelmaan.

3.1 Keskeiset käsitteet

3.1.1 Tietojohtoinen poliisitoiminta

Suomalainen tietojohtoinen poliisitoiminta alkoi kehittyä 2000-luvun alkupuolella ja varsinaisesti sitä on alettu kehittää muun muassa erilaisin poliisin ylijohdon käynnistämien projektien avulla vuosina 2009[3] ja 2011[4]. Tietojohtoinen poliisitoiminta on ymmärretty tiedusteluperusteisena, tieto-ohjattuna tai tietojohdettuna poliisitoiminnan johtamismallina, jonka taustalla on ajatus siitä, että kaiken poliisitoiminnan tulisi perustua luotettavaan ja analysoituun tietoon sekä sen käytettävyyteen toiminnan suuntaamiseksi. Tieto on poliisin toiminnan suunnittelun, kohdentamisen ja seurannan työkalu. Tietojohtoinen poliisitoiminta tuottaa tietoa alueen ilmiöistä, ongelmista ja muista toiminnan maalikohteista. (Lähipoliisitoiminnan strategia 2010, 10)

Tietojohtoisuus edellyttää tilannekuvaa, josta saadaan toiminnan suuntaamiseksi tietoa kolmessa ajallisessa tilannekuvaulottuvuudessa. Ennakoivaan tilannekuvaan kerätään toimintaympäristön heikkoja signaaleja ja tiedustelutietoa, jonka analysoinnin perusteella voidaan ennakoida ja ennakolta ehkäistä orastavia ilmiöitä. On line – tilannekuvatieto antaa valmiudet nopeaan reagointiin ja varhaiseen puuttumiseen sekä akuuteissa, odotettavissa olevissa tilanteissa että ennakoimattomissa, yllättävissä tilanteissa. Eilisen tilannekuva (tilastot) sisältää jo tapahtuneet rikokset, häiriöt ja ongelmat, jotka edellyttävät järjestyksen tai turvallisuuden palauttavaa tai muuta ongelmia korjaavaa toimintaa tietyllä aikajänteellä. (Lähipoliisitoiminnan strategia 2010, 10).

[3] Poliisin ylijohto asetti kehittämisprojektin, jonka tavoitteena oli luoda suosituksia ja malleja, jotka ohjaavat poliisilaitosten johtamiskäytäntöjä ja rakenteita. Projektiin osallistui viisi poliisilaitosta ja yksi valtakunnallinen yksikkö.

[4] Poliisihallitus asetti tietojohtoisen poliisitoiminnan systemaattista kehittämistä ja arviointia varten ”Operatiivisen tietojohtoisen poliisitoiminnan kehittämisryhmän”, jonka tehtävänä oli laatia ehdotus tietojohtoisen poliisitoiminnan kattavasta käyttöönotosta poliisiyksiköissä ja poliisin analyysitoiminnan, tutkimus- ja kehittämistoiminnan sekä analyysikoulutuksen järjestämisestä yhtenäisenä kokonaisuutena. (Hakaniemi 2012, 10)

Tietojohtoista poliisitoimintaa on määritelty kansainvälisesti monin eri tavoin ja eri tarkastelukumista. Tiedusteluun pohjautuva poliisitoiminta on eräänlainen liiketoimintamalli sekä informaation käsittelyyn organisoitu toiminto, jonka avulla poliisiyksiköt paremmin ymmärtävät heidän rikollisuuttaan, osaavat mitoittaa resurssejaan ja tehdä oikeanlaisia ja oikea-aikaisia päätöksiä valitessaan toimintataktikoitaan rikollisuuden ehkäisyyn (Ratcliffe & Guidetti 2008, 3). Suomalaisen tietojohtoisen poliisitoiminnan taustalla on muun muassa Intelligence-led policing johtamisjärjestelmä, joka perustuu englantilaiseen National Intelligence Model (NIM) malliin, jonka tavoitteena on parantaa yleisön turvallisuutta ja vähentää rikollisuutta rikostiedustelutiedon avulla. National Intelligence Model (NIM) – malli otettiin käyttöön vuonna 2004 Englannin ja Walesin poliisissa. Suomennettuna intelligence-led policing -käsite tarkoittaa muun muassa tieto-ohjattua tai informaatio-ohjattua poliisitoimintaa ja se on strategisen johtamisen malli, jonka tarkoitus on varmistaa analysoidun tiedon saanti johtamisen ja päätöksenteon tueksi (Virta 2005, 85–86). Kansainvälisen yhteistyön myötä tieto-ohjattua poliisitoiminnan mallia (European Criminal Intelligence Model) on kehitetty Europolin rakenteisiin sopivaksi (Hakaniemi 2012).

Yhtenä tietojohtoisen poliisitoiminnan tarkastelumallina käytetään Yhdysvalloista peräisin olevaa Compstat -mallia, joka tähtää poliisitoiminnan kehittämiseen ja mitattavuuden parantamiseen. Siinä keskeisenä ajatuksena on koota, analysoida ja kartoittaa dataa sekä muuta oleellista tietoa, joka tukee johtamista valittujen tavoitteiden saavuttamiseksi. Compstat -tulosjohtamismalli perustuu pitkälle tilastojen tuottamaan aineistoon, jolloin malli ei ole niin proaktiivinen kuin tietojohtoinen malli yleisesti käsitteenä ymmärretään.

Compstat – tulosjohtamismalli on suorituskyvyn hallintajärjestelmä, jota käytetään vähentämään rikollisuutta ja sen avulla on tarkoitus saavuttaa muut poliisilaitokselle asetetut tavoitteet. Compstat -malli korostaa tiedon jakamista, vastuullisuutta, tuloksentekokykyä ja sen tarkoitus parantaa tehokkuutta. Malliin sisältyy neljä yleisesti tunnustettua ydinkomponenttia: täsmällinen ja ajankohtainen tietämys tilanteesta, toimintaedellytysten suun-

taaminen reagoiden nopeasti ongelmiin, tehokkaat toimintataktiikat ja säälimätön toiminnan seuranta. (The Police Executive Research Forum 2013, 2)

Lähipoliisitoiminta ja ongelmasuuntautunut poliisitoiminta on yksi tapa tarkastella tietojohtoista poliisitoimintamallia. Lähipoliisitoiminta on osa poliisin perustehtävää ja sillä tarkoitetaan poliisin perustehtävän hoitamista kansalaisläheisesti, laadukkaasti ja tehokkaasti. Suomessa lähipoliisitoiminta ymmärretään yleisen järjestyksen ja turvallisuuden ylläpitämiseen sekä rikostorjuntaan liittyvänä ajattelu- ja toimintatapana, kuten myös toimenkuvaan mahdollisesti sisältyvänä asiantuntijatyönä. Paikallisen ennalta estävän työn keskeinen yhteistyömalli on paikallinen turvallisuusyhteistyö ja sen suunnittelu. Tietojohtoisen poliisitoiminnan elementtien kehittäminen edesauttaa ennalta estävän toiminnan, lähipoliisitoiminnan ja turvallisuusyhteistyön onnistumista ja vaikuttavuutta. (Lähipoliisitoiminnan strategia 2007, 13; Lähipoliisitoiminnan strategia 2010, 7-8)

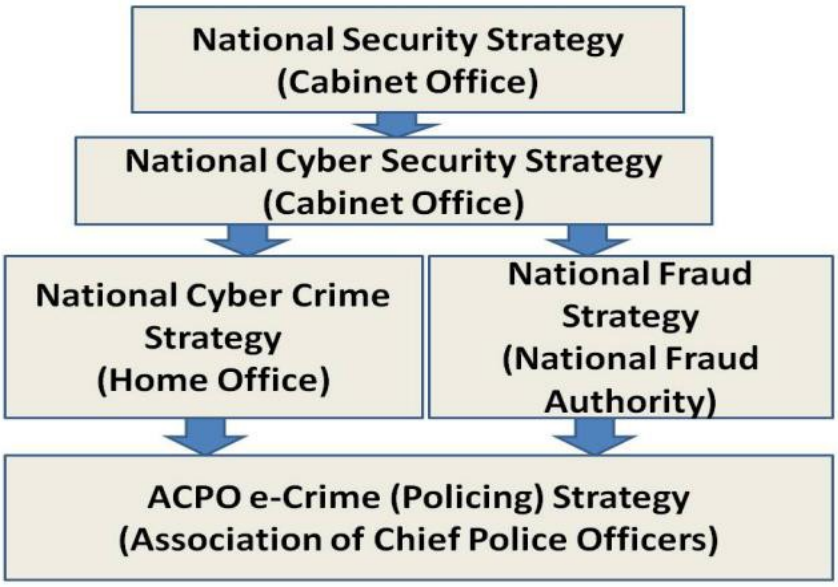
Ongelmasuuntautunutta poliisitoimintaa voidaan tarkastella muun muassa kuvaamalla malli, jossa paikallisen turvallisuusstrategian muodostus ja toimeenpano jaetaan seitsemään osaan: ympäristöanalyysi, priorisointi, tapahtuma-analyysi, turvallisuusongelman mallintaminen, keinovalikoiman etsiminen ja valinta, strategian toimeenpano sekä toiminnan arviointi (Kiehelä & Mälkiä 1999, 129.). Ongelmasuuntautunut poliisitoiminta keskittyy muuttamaan niitä olosuhteita, jotka aiheuttavat jatkuvia ongelmia. Ongelmiin ja niiden taustasyihin on perehdyttävä syvällisesti ja analyysin avulla kehitettävä ratkaisumalleja, joilla epäedullisia olosuhteita saadaan muutettua ja ongelmat poistettua tai niiden määrä vähennettyä. Tietojohtoisen poliisitoiminnan keskiössä on keskittyminen yksittäisten tapausten sijasta laajemmin ilmiöihin sekä toisena ulottuvuutena tietojohtoisen poliisitoiminnan tekijäkeskeisyyteen keskittyvä luonne (Ratcliffe 2008, 86–88). Ongelmasuuntautuneen poliisitoiminnan tavoitteena on löytää kokonaisvaltaisia keinoja ongelmien poistamiseksi. Ongelmasuuntautunut poliisitoiminta-ajattelumalli on auttanut avaamaan laajalti tietojohtoisen poliisitoiminta-mallin ymmär-

tämistä, koska sen avulla käsitetään rikosanalyysin merkitys operatiivisten strategioiden suunnittelulle ja ongelman ratkaisulle (Ratcliffe 2008, 30).

Tietojohtoinen poliisitoiminta toimii tämän tutkimuksen kantavana teoriana. Se voidaan kiteyttää seuraavasti: Tietojohtoinen poliisitoiminta on strategialähtöisesti kerätyn luotettavan ja analysoidun tiedon hyödyntämistä päätöksenteossa, joka ohjaa oikea-aikaista, oikein suunnattua ja resursoitua toimintaa.

3.1.2 Kyberrikollisuus

Kyberrikollisuus on noussut uudeksi käsitteeksi viime vuosien aikana eikä sillä ole selkeää suomalaista määrittelyä. Kyberrikollisuudeksi ymmärretään monesti kaikki tietoverkoissa tapahtuva tavanomainen rikollisuus (esimerkiksi petokset), rikokset, joiden tekemisessä hyödynnetään tietoverkkoja tai rikoksia, jotka kohdistuvat varsinaisesti tietoverkkoihin tai siellä toimiviin tahoihin ja joka on varsinaista tietoverkkorikollisuutta rikosten tunnusmerkistöjen perusteella. David S. Wall on kirjoituksessaan Policing cybercrimes: Situating the Public Police in Networks of Security within Cyberspace (2008/2011) kuvannut poliisin tietoverkkorikollisuuden ja muun poliisitoiminnan strategioiden synkronointia Isossa Britanniassa oheisella kuvalla (sivu 15). Kyberrikollisuuden käsitteen (cybercrime) syntyyn ja sen tulkintaan on vaikuttanut mahdollisesti teknologian verkostoituminen tieteiselokuviin ja kirjoihin, joissa rikoksia on alettu kuvata kyberrikoskäsitteellä virtuaaliympäristössä tapahtuvia rikoksia ja näin käsite on saanut eräänlaisen myyttisen statuksen Internetin leviämisen myötä 1990-luvulla (Wall 2008, 46–48).



KUVIO 1: The UK Cyber security structure / Wall policing cybercrimes 2008, 13

Kyber-etuliitteen käyttö on lisääntynyt 2000-luvulta lähtien (Leppänen & Kankaanranta 2013, 55). Leppänen ja Kankaanranta ovat tutkineet kyber-sanan käyttöä ja tulleet siihen lopputulokseen, että kyber-etuliite liitetään nykyisin tyypillisesti uhkaan, rikollisuuteen tai sodankäyntiin. Kyber-sana etuliitteenä ilmentää tietoverkoissa tapahtuvaa niin uhkaa, häiriöitä kuin laitteisiin liittyviä toimintavarmuus- ja tietoverkkoihin liittyviä käyttöhäiriöitä (Leppänen & Kankaanranta 2013, 55). Kyberturvallisuus on noussut yhdeksi keskeiseksi käsitteeksi, johon myös kyberrikollisuus liittyy. Kyberturvallisuus määritellään kansallisessa kyberturvallisuusstrategiassa tavoitetilaksi, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan (Suomen kyberturvallisuusstrategia 2013, 13). Kyberturvallisuuden käsitettä on täsmennetty kolmen ulottuvuuden kautta: 1) Kyberturvallisuuden tavoitetilassa kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriötä sähköisen tiedon (informaation) käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle, 2) luottamus kybertoimintaympäristössä muodostuu toimijoiden tarkoituksenmukaisesta ja riittävästä tietoturvallisuusmenettelystä ja 3) yhteiskunnan elintärkeät toiminnot ja kriittinen infrastruktuuri on suojattu (Suomen kyberturvallisuusstrategia 2013, 13).

Kyberrikoskäsitteen määrittelyyn vaikuttaa osaltaan kyberrikosten taustalla olevat motiivit, jotka vaihtelevat harrastelijoiden kokeiluista ammattimai-

seen toimintaan ja valtiollisiin motiiveihin (Leppänen & Virta 2014, 8). Kyberrikollisuutta voidaan jaotella tekijöiden mukaan a) tunkeutujiin, jotka muun muassa vakoilevat verkossa, syyllistyvät vandalismiin tai terrorismiin, b) syyllistyvät varkauksiin, c) syyllistyvät törkeyksiin tai säädyttömyyteen esimerkiksi levittämällä säädytöntä materiaalia tietoverkossa tai d) väkivaltaisesti käyttäytyvät, jotka ryhmäytyvät ja kirjoittavat vihapuheita tai uhkauksia kohdistaen niitä esimerkiksi vähemmistöihin (Wall 1998, 203).

Kyberrikollisuus kriminologiassa määritellään tyypillisesti tietotekniikan merkityksen näkökulmasta, jolloin kaikesta tietokoneen sisältävästä rikollisuudesta tulee osittain kyberrikollisuutta. Toisen määritelmän mukaan kyberrikokset voidaan jakaa kolmeen kategoriaan: tietokone rikoksen kohteena, tietokone rikoksen tekovälineenä ja tietokone rikoksen oheisvälineenä, joka ei välttämättä täytä varsinaista kyberrikollisuuden määritelmää. (Leppänen & Virta 2014, 8)

Kyberrikollisuutta voidaan tarkastella myös aikaperspektiivillä, joka on sidottu yhteiskunnan ja teknologian kehitykseen. Alkuvaiheessa tietokoneet toimivat lähinnä rikosten teon oheisvälineinä eikä niitä käytetty varsinaisesti rikoksen toteuttamisessa. Seuraavassa vaiheessa rikoksia tehtiin tietoverkoissa, jolloin kyse oli jo tietokoneen käyttämisestä varsinaisen rikoksen toteuttamiseen. Tietokone ja tietoverkko olivat edellytyksiä rikoksen toteuttamisessa. Tällä hetkellä rikokset toteutetaan hajanaisesti, globaalisti ja niiden toteuttaminen onnistuu vain tietoverkoissa. Rikolliset teot automatisoidaan siten, että esimerkiksi tietokoneet kaappaavat toisia tietokoneita asettamalla niihin haittaohjelmia, jotka jatkavat haittaohjelman levittämistä[5]. Haittaohjelmien avulla pystytään suorittamaan esimerkiksi palvelunestohyökkäyksiä[6] ja haittaamaa tällä tavalla palvelujen tuottajien toimintaa,

[5] Botnet-verkot: Botnet-hyökkäyksessä hyökkääjän ohjauspalvelimelta komennetaan tavallisten Internet-käyttäjien tietokoneet osallistumaan hyökkäykseen. Hyökkäykseen voi osallistua tuhansia ellei jopa miljoonia murrettuja tietokoneita niiden käyttäjien siitä tietämättä. Botnet-verkkoa voidaan käyttää erilaisiin tarkoituksiin, muun muassa erilaisiin roskapostikampanjoihin tai kohdistaen DDoS hyökkäyksiä muihin verkkoihin ja järjestelmiin. Myös mobiililaite voi olla osa botnet-verkkoa. (Viestintäviraston Internet-sivut 2015 ja Europol IOCTA 2014, 25)

[6] Palvelunestohyökkäyksessä tyypillisesti luodaan keinotekoisesti ruuhkaa palveluun. Palvelunestohyökkäystä voi verrata siihen, että hyökkääjä muodostaa ”kätyreistään” asiakas-

(muun muassa pankit ja kaupunkien palvelut) jotta rikos saadaan toteutettua. Rikokset tehdään suunnitelmallisesti taloudellisen hyödyn tavoittelemiseksi ja taustalla vaikuttaa ja toimintaa ohjaa monesti järjestäytyneen rikollisuuden toimijat. (Leppänen & Kankaanranta 2013, 57)

3.1.3 Järjestäytynyt rikollisuus

Järjestäytyneen rikollisuuden on todettu olevan uhka Euroopan taloudelle ja yhteiskuntajärjestelmälle. Euroopassa arvioidaan olevan noin 3600 järjestäytynyttä rikollisryhmää, joista yli puolet vaikuttaa huumausaineiden salakuljetuksessa ja ihmiskaupassa (SOCTA 2013, 33). Järjestäytynyt rikollisuus on monimuotoista (ihmisten, aseiden ja huumeiden salakuljetus, talousrikollisuus, korruptio rahanpesu ja niin edelleen) ja viime vuosien aikana se on laajentanut toimialaansa muun muassa tietoverkko- ja ympäristörikollisuuteen. Muun muassa asunto- ja liikemurrot, autovarkaudet, huumekauppa ja luottokorttipetokset ovat usein osa laajempaa rikollista toimintaa, jonka lonkerot ulottuvat yli maantieteellisten rajojen ja myös verkkoympäristöön. Rikolliset hyödyntävät yhä enemmän Internetiä sekä vähäisten rikosten että laaja-alaisten hyökkäysten tekemisessä. EU:n ulkorajojen yli salakuljetetaan niin ihmisiä kuin tavaroita ja rikollisverkostot hankkivat valtavia tuloja kierrättämällä julkisia varoja rahoittamaan toimintaansa. Kansainvälisen valuuttarahaston (IMF) arvion mukaan pelkästään talousrikoksista saatava hyöty vastaa jopa viittä prosenttia maailman kansantulosta[7]. (EU:n komission muistio 2010, 1)

Tarkkoja laskelmia järjestäytyneen rikollisuuden aiheuttamista haitoista[8] tai sen aiheuttamasta rikosvahingon määrästä ei ole saatavilla, koska näkemyk-

palvelutiskille pitkän jonon, hyökkääjän kätyrit ottavat useita vuoronumeroita ja menevät vuorollaan palvelutiskille tuppisuuna kuluttamaan aikaa. Oikeita asiakkaita on vaikeaa, ellei mahdotonta erottaa valeasiakkaista. (Viestintäviraston Internet-sivut 2015)

[7] Maailman teollisuusmaiden bruttokansantulo vuonna 2010 oli noin 36 000 miljardia (Suomen pankki 2010: Maailmantalouden muutoksesta ja Euroopan talouden haasteista)

[8] Vuonna 2012 pelkästään huumeet aiheuttivat julkiselle sektorille noin 253–323 miljoonan euron haittakustannukset. Huumehaittakustannukset muodostuvat pääosin haittojen hoitamisesta ja korjaamisesta. Huumehaittakustannusten rakenne painottuu sosiaalihuollon sekä yleisen järjestyksen ja turvallisuuden ylläpidon kustannuksiin. (Terveyden ja hyvinvoinnin laitos 2014, 25) Huumetilanne Suomessa 2014

set järjestäytyneen rikollisuuden määristä ja uhkakuvista vaihtelevat merkittävässä määrin. Lainvalvontaviranomaisten katsauksissa määrät ovat huomattavan suuria, moninkertaisia verrattuna siihen, kuinka paljon vuosien mittaan on kertynyt tuomioita, joissa olisi sovellettu jotain järjestäytyneitä rikollisryhmiä koskevista erityissäännöksistä. Monet syyt ovat olleet osaltaan vaikuttamassa siihen, että ilmiön laajuudesta on ollut vaikea saada yksiselitteistä kuvaa. Järjestäytynyt rikollisuus yhteiskuntaan liittyvänä ilmiönä voidaan ymmärtää hyvin monella tavalla. Esimerkiksi oikeus- ja lainvalvontaviranomaisten käytössä ovat erilaiset määritelmät niin EU:ssa kuin Suomessakin. (Palo 2010, 49)

Järjestäytyneen rikollisuuden ilmentyminen Kyberympäristössä muuttaa myös käsitystä perinteisestä järjestäytyneen rikollisuuden määrittelystä. Järjestäytynyt rikollisuus lähestyy aiempaa enemmän ja konkreettisemmin kansalaisten arkipäivää ja sekoittuu lailliseen yhteiskuntajärjestelmään. Järjestäytynyt rikollisuus näyttäytyy kybermaailmassa nettipetoksina, tietojenkalasteluna, identiteettivarkauksina ja muina arkirikollisuutta muistuttavana rikollisuuden osa-alueina. Järjestäytyneen rikollisuuden siirtyessä kyberympäristöön rikollisryhmien hierarkinen rakenne voi myös muuttua joustavammaksi ja sirpaloituneemmaksi sekä jopa laajentua maailmanlaajuiseksi johtuen kybermaailman mahdollisuuksista. Tulevaisuudessa kyberympäristöön saattaa syntyä verkkorikollisuuden kartelleja, jotka eivät toimi samalla tavoin kuin reaalimaailman järjestäytyneen rikollisuuden luomat kartellit. (Brenner 2002, 25, 36–46)

EU:n neuvoston[9] mukaan järjestäytyneeseen rikollisuuteen liittyy useamman kuin kahden henkilön pitkäaikaista yhteistyötä, järjestäytyneeseen ri-

[9] Järjestäytyneen rikollisuuden määritelmät eri oikeuslähteissä poikkeavat hieman toisistaan. EU:n neuvoston päätöksen 6204/2/97 ENFOPOL 35 REV 2 mukaisessa niin sanotussa ENFOPOL-määritelmässä järjestäytynyt rikollisuus on määritelty 11 kriteerin avulla, ja näistä kriteereistä kuuden on täytyttävä, jotta rikollisryhmä täyttää järjestäytyneisyyden kriteerit. Järjestäytyneen rikollisuuden EU-kriteerit ovat: useamman kuin kahden henkilön yhteistyö, ryhmän jäsenillä on omat määrätyt tehtävät, ryhmä toimii pitkän tai rajoittamattoman ajan, ryhmä käyttää sisäistä kuria, ryhmää epäillään törkeistä rikoksista, ryhmä toimii kansainvälisellä tasolla, ryhmä käyttää väkivaltaa tai muita uhkailukeinoja, ryhmä käyttää peiteyhtiöitä, ryhmä harjoittaa rahanpesua, ryhmä pyrkii vaikuttamaan poliitikkoihin, julkiseen hallintoon, tiedotusvälineisiin, oikeusviranomaisiin tai talouselämän edusta-

kollisryhmään kuuluvia henkilöitä epäillään vakavista rikoksista, ja sen toimintaa leimaavat muun muassa väkivallan käyttö ja rahanpesu. Ryhmät voivat olla hierarkkisia tai verkostomaisia ja niiden tarkoitus on tuottaa jäsenilleen voittoa tai valtaa rikollisen, mutta myös lailliselta näyttävän toiminnan kautta. Ryhmien toiminta voi olla paikallista, kansallista tai rajat ylittävää. (Valtioneuvoston periaatepäätös järjestäytyneen rikollisuuden torjunnan strategiasta 2013, 4)

3.1.4 Rikostorjunta

Poliisilain 1 pykälän (872/2011) mukaan poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen. Poliisi toimii turvallisuuden ylläpitämiseksi yhteistyössä muiden viranomaisten sekä yhteisöjen ja asukkaiden kanssa ja huolehtii tehtäviinsä kuuluvasta kansainvälisestä yhteistyöstä. Rikosten esitutkinnasta säädetään esitutkintalaissa ja rikosten esitutkinnassa käytettävistä pakkokeinoista pakkokeinolaissa.

Rikoksen ennalta estämisellä tarkoitetaan niitä toimia, joilla puututaan rikokseen jo ennen sen tekemistä. Rikoksen paljastamisessa on kysymys poliisin toimenpiteistä, joilla pyritään paljastamaan jo tehdyn tai vielä tekeillä tai suunnitteilla olevaan rikokseen liittyviä seikkoja esitutkinnan aloittamisen perustaksi. Rikoksen selvittämisellä tarkoitetaan toimenpiteitä, joihin ryhdytään sen jälkeen, kun esitutkintakynnys on ylittynyt. Esitutkintaviranomaisen on toimitettava esitutkinta, kun sille tehdyn ilmoituksen perusteella on syytä epäillä, että rikos on tehty. (Poliisilaki 22.7.2011/872 ja esitutkintalaki 22.7.2011/805)

jiin, ryhmän toiminnassa taloudellisen hyödyn ja/tai vallan tavoittelu on määräävänä tekijänä. Rikoslain 17 luvun 1a §:n 4 momentin mukaan järjestäytyneellä rikollisryhmällä tarkoitetaan vähintään kolmen henkilön muodostamaa tietyn ajan koossa pysyvää rakenteeltaan jäsentynyttä yhteenliittymää, joka toimii yhteistuumin tehdäkseen 1 momentissa tarkoitettuja rikoksia. (Valtioneuvoston periaatepäätös järjestäytyneen rikollisuuden torjunnan strategiasta 2013, 4)

Rikoksen esitutkinnassa poliisi selvittää onko tapahtunut rikos, sen tekoolosuhteet ja keitä asia koskee. Esitutkinnassa selvitetään myös rikoksella aiheutettu vahinko, saavutettu hyöty ja mitä vaatimuksia asianomistajalla eli rikoksen uhrilla on. Tutkinnanjohtaja päättää esitutkinnan aloittamisesta, tutkinnan laajuudesta sekä tutkinnan lopettamisesta. Rikostorjunta käsitteellisesti painottuu ajallisesti aikaan ennen kuin rikos toteutuu. Käsitteellisesti rikostorjunta sisältää rikosten ennalta estämisen, paljastamisen, selvittämisen ja syyteharkintaan saattamisen. Rikoksen paljastamisessa on kysymys poliisin toimenpiteistä, joilla pyritään paljastamaan jo tehdyn tai vielä tekeillä tai suunnitteilla olevan rikoksen välittömästi relevantteja seikkoja (erityisesti tekijä, tekoaika ja -paikka ja rikostunnusmerkistöön kuuluvat elementit) esitutkinnan aloittamisen perustaksi (HE 224/2010[10]). (Helminen, Kuusimäki, Rantaeskola 2012, 60–61)

Poliisin tehtävämäärittelyssä[11] tärkeän osatekijän muodostavat odotettavissa oleviin tai tehdyiksi epäiltyihin rikoksiin liittyvät toimenpiteet. Toimenpiteet ovat tyypiltään kahdenlaisia: yhtäältä odotettavissa olevien rikosten estäminen ennalta (rikospreventio) ja toisaalta jo tapahtuneiden tai tapahtuneiksi epäiltyjen rikosten selvittäminen. Jälkimmäisessä tapauksessa tarkoitusperänä on selvitetyn rikoksen saattaminen syyteharkintaan tai muiden rikosoikeuden piiriin kuuluvien toimenpiteiden mahdollistaminen. Poliisilain 1 luvun pykälän 1 momentissa mainitaan rikostorjunnan kohdalla myös rikoksen paljastaminen. Rikoksen paljastamisella tarkoitetaan esitutkinnan aloittamisen edellytysten selvittämistä tapauksessa, jossa rikoksen tekemisestä on vain heikko, "voidaan olettaa" -tasoinen epäily. Käsite mainitaan erityisesti salaisten tiedonhankintakeinojen käyttämistä koskevissa säännöksissä (ks. PolL 5:1,3 ja 5:2). Tässä yhteydessä on syytä korostaa, että jaottelu ennalta estäviin ja rikoksen selvittämistä tarkoittaviin toimenpiteisiin on erittäin tärkeä poliisin toimivaltuuksien kannalta. (Helminen, Kuusimäki, Rantaeskola 2012, 60–61)

[10] Poliisilaki
[11] Poliisilaki 1 luvun 1 § (872/2011)

3.1.5 Rikosten ennalta estäminen

Poliisin ennalta estävän toiminnan tavoitteena on yhteiskunnan turvallisuuden parantaminen ja rikosten torjunta. Poliisi estää rikoksia, järjestyshäiriöitä, onnettomuuksia ja ratkaisee ongelmia yhteistyössä ihmisten, muiden viranomaisten ja keskeisten kumppaneiden kanssa. Poliisi näkyy, neuvoo, valistaa ja tiedottaa sekä valvoo, puuttuu ja reagoi. Ennalta estävän toiminnan tulokset näkyvät yhteiskunnan turvallisuuden ja ihmisten turvallisuuden tunteen parantumisena. Poliisin ennalta estävä toiminta on poliisin kaikkeen toimintaan poikkileikkaavasti sisältyvä toimintatapa, jota tehdään poliisiorganisaation kaikilla tasoilla alueellinen ja ihmisten yhdenvertaisuus huomioiden. Ennalta estävän toiminnan kokonaisuus muodostuu ennalta estävästi suoritetusta jokapäiväisestä poliisin toiminnasta ja erityistoiminnasta, jossa poliisi toteuttaa toimenpiteitä ensisijaisena tavoitteenaan ennalta estävä turvallisuuden parantaminen. (Poliisin ennalta estävän toiminnan strategia 2014, 2)

Poliisin ennalta estävä toiminta on kokonaisvaltaisesti ja tietojohtoisesti suunniteltua, järjestettyä, johdettua ja toteutettua tavoitteellista toimintaa turvallisuuden parantamiseksi ja rikosten torjumiseksi poliisiorganisaation kaikilla tasoilla. Ennalta estävä toiminnan perusta on tietojohtoisuus, jossa hyödynnetään poliisin eri toiminnoissa aktiivisesti hankittua, saatua ja analysoitua tietoa ennalta estävyyden saavuttamiseksi. Tietojohtoisuus edellyttää tilannekuvaa, joka sisältää eilisen tietoa (tilastot), ajantasaista tietoa ja ennakoivaa tietoa. (Poliisin ennalta estävän toiminnan strategia 2014, 3)

3.1.6 Tiedustelu

Tiedustelu-käsitettä voidaan määritellä monin eri tavoin. Yksi tiedustelusanan englanninkielinen vastine on lainvalvontaviranomaisten usein käyttämä termi ”Intelligence”. Sanakirjassa sana on käännetty muun muassa tarkoittamaan älyä, älykkyyttä, tiedustelua, tiedustelutietoa ja älyllisyyttä (Sanakirja.org). Sanana Intelligence linkittyy joka tapauksessa jollakin tavoin

tiedon käsitteeseen[12]. Intelligence määritellään informaatioksi, joka joko on merkityksellistä tai mahdollisesti merkityksellistä käynnissä olevalle tutkimukselle tai käynnistettävälle tutkimukselle (Brown 2007, 336 – 340).

Poliisitoiminnassa tieto on poliisin toiminnan suunnittelun, kohdentamisen ja seurannan työkalu sekä sen tulee olla kaiken toiminnan perusta (Lähipoliisitoiminnan strategia 2010, 10). Tietojohtoisen poliisitoiminnan[13] määrittelyn myötä Intelligence-käsitteestä on tullut käytännöllinen ja kokonaisvaltainen määritelmä siitä, mitä sillä tarkoitetaan ja joka soveltuisi sekä turvallisuuspalvelujen että lainvalvonta viranomaisten käyttöön (Brown 2007, 336 – 340).

Tiedustelu voidaan jakaa myös seitsemään tiedustelun pääkohtaan: geospatiaalisiin tiedustelutietoihin (GEOINT)[14], henkilötiedusteluun (HUMINT)[15], signaalitiedusteluun (SIGINT)[16], pieniin signaaleihin kohdistuvaan tiedusteluun (MASINT)[17], avoimiin lähteisiin kohdistuvaan tiedusteluun (OSINT)[18],

[12] Tieto on käsitteenä varsin laaja. Sitä voidaan kuitenkin jäsennellä eri tavoin. Yksi tietojohtamiseen liitetty jäsentelytapa on käyttää kolmea eri käsitettä kuvaamaan tiedon eri tasoja. Nämä tasoja kuvaavat käsitteet ovat data, informaatio ja tietämys. Niiden lisäksi akateemisessa kirjallisuudessa on myös niin sanottua korkeampaa tietoa jaoteltu älykkyyteen, ymmärrykseen, viisauteen ja totuuteen. (Tietojohtaminen 2013, 17–18)

[13] Intelligence-led-policing-käsitettä on Suomessa määritelty tietojohtoiseksi poliisitoiminnaksi. Käsite tietojohtoinen poliisitoiminta eli intelligence - led policing kytkeytyy poliisitoiminnan johtamiseen ja ohjaukseen. Määritelmä on osa käsitteistöä, jolla kuvataan modernia poliisitoimintaa, mitä toiminnan tulisi olla tai mihin suuntaan sitä tulisi kehittää. Tietojohtoisessa poliisitoiminnassa rikoksiin liittyvä tiedustelutieto määritellään analysoiduksi informaatioksi, jossa yhdistyy tieto rikosanalyyseista, rikoksen tekomalleista sekä tiedustelutieto rikollisten käyttäytymisestä. Hyvä tiedustelutieto juontaa juurensa sekä rikoksentekijöitä koskevaan tietoon että rikostapahtumiin. (Hakaniemi 2012)

[14] Maantieteellisiä tiedustelutietoja (muun muassa paikannustiedot, satelliittipaikannus) (Komission ehdotus Euroopan parlamentin ja neuvoston päätökseksi avaruusvalvonnan ja -seurannan tukiohjelman perustamisesta 2013)

[15] Henkilötiedustelu eli HUMINT (Human Intelligence) on tiedustelulaji, jossa tiedustelun kohteena ja tiedustelijana on ihminen (Grabar 2012, 1)

[16] Signaalitiedustelu (Signals intelligence) on tiedustelutieto, joka on saatu viestinnässä käytetyistä signaaleista, (sähköisistä tai instrumentointilaitteiden signaaleista) (Yhdysvaltain puolustusministeriö: Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms 12.7.2007)

[17] MASINT (Measurement and Signatures Intelligence) on signaalin erityisominaisuuksiin perustuva teknisen tiedustelun alalaji. Se mahdollistaa jopa laiteyksilöiden tunnistamisen signaalin pienistä yksilöllisistä eroista. Tiedustelua voidaan käyttää esimerkiksi auttaa tunnistamaan kemiallisia aseita tai paikantamaan tuntemattomia asejärjestelmiä (FBI:n verkkosivut: Intelligence Collection Disciplines (INTs) 2015)

valokuvien ja kuvantamisen avulla tapahtuvaan tiedusteluun (IMINT)[19] ja vastavakoiluun (CI)[20]. (Chesbro 2010, 56)

Yleiskäsitteenä tiedustelu on avoimista, suljetuista, ulkoisista ja sisäisistä tietolähteistä systemaattisesti kerätyn tiedon keräämistä, tallentamista ja käsittelyä. Tieto (data) muuttuu tiedustelutiedoksi (informaatio), kun se on käsitelty ja sille on annettu merkitys (analysointi). Tiedustelu on kohdennettua, systemaattista tiedonhankintaa ja edellyttää suorittavalta viranomaiselta lakitasoista toimivaltasäännöstöä. Tiedustelun käynnistävä tapahtuma tai tieto, ei vielä itsessään sisällä perusteltua epäilyä tapahtuvasta tai tapahtuneesta rikoksesta, vaan sisältää sellaisia seikkoja, joista asiaa huolellisesti arvioiva henkilö voi perustellusti päätellä johtavan vaaran tilaan tai rikokseen. (Poliisin kybertoimivaltuudet 2015, 9)

Poliisin operatiivisessa toiminnassa tietoverkkotiedustelulla[21] tarkoitetaan verkon sisällön ja verkon käytön turvallisuuden valvontaa ja tiedonhankintaa internetistä. Tietoverkkotiedustelun tavoitteena on paljastaa tietoverkoissa esille tulevia erilaisia ilmiöitä ja tapahtumia, joilla voidaan arvioida olevan merkitystä poliisitoiminnallisesti, joko ennalta estävässä tai rikostorjunnallisessa merkityksessä. Yleisterminä tietoverkkotiedustelu kattaa alla olevat käsitteet; valvonta, tekninen valvonta, tiedustelu ja rikostiedustelu, niiltä osin kuin toiminta tapahtuu tietoverkoissa tai -järjestelmissä. (Poliisin kybertoimivaltuudet 2015, 9)

---

[18] Avoimiin lähteisiin kohdistuva tiedustelu (Open-Source Intelligence) tarkoittaa yleisesti saatavilla oleviin, julkisiin lähteisiin kohdistuvaa tiedustelu (media, hallitusten ja yhteisöjen raportit, tutkimukset ja niin edelleen) (FBI:n verkkosivut: Intelligence Collection Disciplines (INTs) 2015)

[19] Yksi varhaisimmista valokuvien avulla toteutetusta tiedustelusta (Imagery Intelligence) tehtiin I ja II maailman sodan aikana, jolloin sotilaat keräsivät ilmapallojen avulla tietoja ympäristöstään sekä kuvaamalla vihollisen lentokoneita. Nykyaikana vastaavaa tiedustelua tehdään satelliittien avulla. (FBI:n verkkosivut: Intelligence Collection Disciplines (INTs) 2015)

[20] Vastavakoilulla tarkoitetaan tiedusteluorganisaatioiden yrityksiä ehkäistä muiden valtioiden tiedusteluorganisaatioiden tiedonhankintaa eli vakoilua. Vastavakoilutoimintaan kuuluu myös väärän tiedon eli disinformaation levittäminen. Vastavakoilun keskiössä on kyberympäristössä tehtävät havainnot uhkista, jotka uhkaavat julkisen ja yksityisen sektorin tietojärjestelmiä sekä estää niiden toteutuminen. (FBI Counterintelligence National Strategy 2011)

[21] Suomessa ei ole varsinaista tietoverkkotiedusteluun liittyvää lainsäädäntöä(Suomalaisen tiedustelulainsäädännön suuntaviivoja 2015, 14)

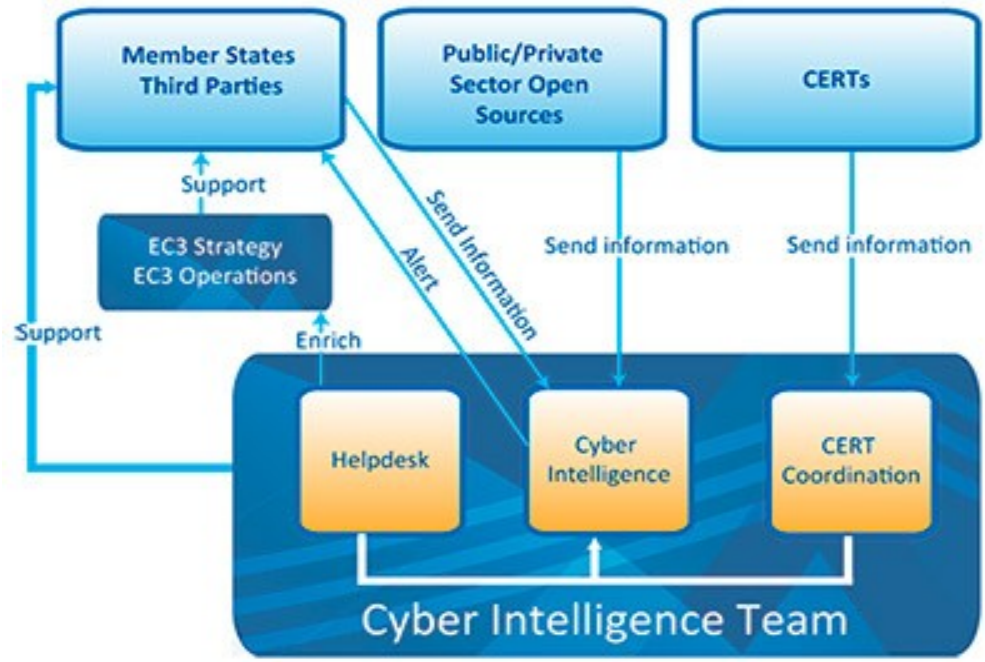
Poliisin toimivaltuussäännösten perusteella tietoverkkotiedustelussa on toisaalta kyse niin sanotusta säätelemättömästä yleisvalvonnasta ja toisaalta Poliisilain (872/2011) 5 luvussa tai Pakkokeinolain (806/2011) 10 luvun säädetyistä tiedonhankintakeinoista, joka on kohdennettua toimintaa rikoksen estämiseksi tai selvittämiseksi. Tietoverkkotiedustelun tavoitteena on paljastaa julkisissa tietoverkoissa esille tulevia erilaisia ilmiöitä ja tapahtumia, joilla voidaan arvioida olevan merkitystä poliisitoiminnallisesti joko ennaltaehkäisevässä tai rikostutkinnallisessa merkityksessä. Pääasiassa valvontaa tehdään joko yksittäisten toimeksiantojen perusteella tai vaihtoehtoisesti tarkistetaan ulkopuolisten vihjeiden perusteella yksittäisten Internetsivustojen sisältöjä tai muuta niiden sisältämää merkittävää tietoa. (Tietotekniikkatutkinnan järjestäminen poliisissa 2008, 10–11)

Suomessa Suojelupoliisin tehtävänä on poliisin hallinnosta annetun lain 10 §:n mukaan torjua sellaisia hankkeita ja rikoksia, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta sekä suorittaa tällaisten rikosten tutkintaa. Sen tulee myös ylläpitää ja kehittää yleistä valmiutta valtakunnan turvallisuutta vaarantavan toiminnan estämiseksi. Suojelupoliisin tehtävänä on kerätä tietoa Suomen ulkoista turvallisuutta koskevan toimintaympäristön kehittymisestä ja kansallista turvallisuutta vaarantavista ilmiöistä ja täten omalta osaltaan tukea Suomen ulko- ja turvallisuuspoliittista päätöksentekoa. Tehtävää toteutetaan niin reaalimaailmassa kuin tietoverkoissa. (Poliisin kybertoimivaltuudet 2015, 12)

Poliisitoiminnassa yleisen järjestyksen ja turvallisuuden ylläpitämiseen on katsottu kuuluvan kaiken sellaisen toiminnan, jonka tarkoituksena on luoda ja ylläpitää turvallista ja viihtyisää elin- ja toimintaympäristöä yhteiskunnan jäsenille, torjua ja estää ennakolta oikeudenloukkauksia ja häiriöitä sekä poistaa tapahtuneet häiriöt ja selvittää tapahtuneet oikeudenloukkaukset. Poliisin suorittama valvonta on poliisin ennalta estävän toiminnan ydinosa. Poliisin suorittamalla yleisvalvonnalla tarkoitetaan ennalta määräämättömään ihmisryhmään kohdistuvaa valvontaa. Valvonta voi tapahtua aistinvaraisesti tai sen suorittamiseksi voidaan käyttää myös teknisiä laitteita. Poliisin tehtäväkenttään kuuluu myös tietoverkoissa suoritettava yleisvalvonta, jota sää-

televää toimivaltuusnormia ei tällä hetkellä ole voimassa. (Poliisin kybertoimivaltuudet 2015, 15–16)

Euroopan kyberrikollisuuden torjunnan keskus (EC3) aloitti toimintansa tammikuussa 2013. Sen tehtävänä on keskittyä torjumaan kyberrikollisuuden järjestäytyneitä ryhmiä, jotka saavat suuria rikoshyötyjä laittomalla toiminnallaan, vakavaa haittaa aiheuttaviin tietoverkoissa tehtäviin rikoksiin (esimerkiksi laajojen lasten seksuaalinen hyväksikäyttö -rinkien paljastaminen) sekä kriittiseen infrastruktuuriin ja tietojärjestelmiin kohdistuvia uhkia EU:n alueella. Lisäksi Europolin yhteydessä toimii Kyberrikollisuuden tiedusteluryhmittymä[22], joka keskittyy tiedon keräämiseen julkista, yksityisistä ja avoimista lähteistä yhdistäen ne lainvalvontaviranomaisilta[23] saataviin tietoihin (kuva sivulla 26). (Europolin verkkosivut 2015)



KUVIO 2: CIT (Cyber Intelligence Team) (Europolin verkkosivut, EC3, 2015)

[22] Cyber Intelligence Team (CIT)

[23] Muun muassa Suomen kansallinen toimija Kyberturvallisuuskeskus CERT (Computer Emergency Response Team), jonka tehtävänä on selvittää verkkopalveluihin, viestintäpalveluihin ja lisäarvopalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia, kerätä tietoa tällaisista tapahtumista ja tiedottaa tietoturva-asioista yleensä. (Viestintäviraston verkkosivut)

3.2 Aihealueen aikaisemmat tutkimukset

Koska tietoverkkorikollisuuden tutkinta ja torjunta on vielä melko uusi poliisitoiminnan osa-alue, ei alan kansallista tutkimusta vielä ole paljoa saatavissa suoraan tutkittavana olevaan aiheeseen liittyen. Kansainvälistä tutkimusta liittyen kyberrikollisuuteen on paljon ja varsinaisesti rikostorjunta- tai tiedustelulähtöisesti tehdyt tutkimukset ovat lähinnä alan asiantuntijalehdissä julkaistuja artikkeleita, joita tässä en käsittele sen tarkemmin. Suomessa tehtyjä väitöskirjoja tai Pro Gradu-tutkimuksia, jotka käsittelevät tietoverkkorikollisuutta on tehty vain muutamia.

Antti Pihlajamäki vuonna 2004 on väitöskirjassaan: ”Tietojenkäsittelyrauhan rikosoikeudellinen suoja-datarikoksia koskeva sääntely Suomen rikoslaissa”, käsitellyt Suomen datarikoksia koskevaa sääntelyä. Datarikoksella on tarkoitettu rangaistavaa tekoa, jonka kohteena tai rikosvälineenä on tietojärjestelmässä oleva data. Väitöskirja on ensimmäinen suomalainen tietotekniikkarikoksia koskeva laaja oikeustieteellinen tutkimus. Tutkimuksessa on päädytty siihen, että suomalainen lainsäädäntö on tietotekniikkarikollisuuden näkökulmasta välttävällä tasolla ja tietotekniikkarikoksia koskevaa kriminalisointia on jatkossa kehitettävä, jotta se muodostaisi yhtenäisen ja loogisen kokonaisuuden koko ajan muuttuvassa haasteellisessa ja voimakkaasti muuttuvassa tietoverkkoympäristössä.

Timo Kilpeläinen on vuonna 2011 Pro Gradussaan: ”Virtuaalinen poliisitoiminta - toreilta tietoverkkoihin”, tarkastellut virtuaalista poliisitoimintaa. Tutkimuksessa on selvitetty, mitä poliisissa on tehty kansalaisläheisyyden lisäämiseksi tietoverkoissa eli miten poliisi eri muodoissaan on toiminut sillä hetkellä virtuaalisessa ympäristössä. Tutkimuksessa on todettu, että poliisin näkyvä toiminta sosiaalisessa mediassa voidaan selkeästi jakaa useampaan eri toiminnalliseen kokonaisuuteen: Uusien viestintäkanavien hyödyntäminen osana poliisin viestintästrategiaa, ennalta estävä toiminta neuvoin, ohjein ja kehotuksin, varhainen puuttuminen ensisijaisesti nuorten ongelmiin ja yhteistyö sosiaalisessa mediassa toimivien sidosryhmien kanssa sekä

tutkintaan liittyvät toimenpiteet. Toisena havaintona on todettu virtuaalisen poliisitoiminnan olevan suurimmalta osin ennalta estävää työtä. Virtuaalisen toiminnan painopisteenä on normaalitilanteissa jakaa kansalaisille tietoa neuvoin, ohjein ja kehotuksin. Virtuaalisessa poliisitoiminnassa on kyseessä lähipoliisitoiminnan uusi ilmenemismuoto.

”Tietotekniikkatutkinnan olympiadi poliisihallinnossa 2006–2009”, Ulla Köckritz on vuonna 2011 Pro Gradussaan tarkastellut tietotekniikkatutkinnan valtakunnallista järjestämistä poliisin hallinto-rakennemuutoksen yhteydessä tavoitteena kuvata muutoksen johtamisen vaiheita johtamisnäkökulmasta tarkastelemalla tietotekniikkarikosten tutkintajärjestelyjä. Tutkimuksessa todettiin, että johtaminen on muutoksenteon väline ja muutosta voidaan tietoisesti hallita vain johtamisella. Muutos on mahdollista saattaa johdetuksi päätökseen, mutta johtamisella voi vaikuttaa vain johtamisen alaisuudessa oleviin asioihin. Toisena johtopäätöksenä tutkimuksessa on todettu tietoteknisen kielen olleen vakiintumatonta, käsitteistön sekavaa ja teknologisen kehittymisen vauhdin olevan kiihtyvää. Tutkimuksessa on todettu, että vaikeiden käsitteiden ja monimutkaisten teknisten sanojen käytön avulla oli mahdollista luoda asian etenemistä auttavia mielikuvia. Terminologian käytöllä ja termien selittämisellä oli tarkoitus myös lisätä tietoa sekä ymmärrystä ja kuvailla tietotekniikkatutkinnan luonnetta erityisosaamista vaativana toimintona.

Thor Kottelin on vuonna 2013 Pro Gradussaan: ”Pakkokeinot tietomurtorikosten esitutkinnassa”, on tarkastellut lainopillisesta näkökulmasta, miten pakkokeinolaissa säädetyt pakkokeinot soveltuvat käytettäviksi tietomurtojen esitutkinnassa ja millaisia muutoksia 1.1.2014 voimaan tullut uusi pakkokeinolainsäädäntö on aiheuttanut. Lisäksi on tarkasteltu empiirisesti, kuinka pakkokeinoja on vuosina 2009–2012 käytetty tietomurtorikosten esitutkinnassa. Tutkimuksessa on todettu, että haittaohjelmien automaattisesta levitystavasta johtuen tietomurtorikoksia tehdään erittäin paljon. Poliisin tietoon kuitenkin tulee vain joitakin satoja tietomurtorikoksia vuodessa, ja pakkokeinoja käytetään vuosittain noin 20:ssa tietomurtorikosta koskevassa esitutkinnassa ja tietomurtorikosten tutkinnassa keskeisiä pakkokeinoja ovat

kotietsintä ja takavarikko, jotka mahdollistavat todisteiden etsimisen tietoteknisistä laitteista, sekä televalvonta, jolla rikoksentekijä voidaan löytää hänen tietoverkossa jättämiensä jälkien perusteella. Tutkimuksessa on käyty läpi vanhaa ja uutta lainsäädäntöä esimerkkien avulla eikä varsinaista johtopäätös- tai lopetusosiota ole.

Maanpuolustuskorkeakoulussa vuonna 2013 tehdyssä Pro Gradussaan: ”Yhteiskunnan toiminta uusia uhkia vastaan” Mika Isometsä on tutkinut, miten suomalainen yhteiskunta toimii uusia uhkia vastaan. Aiheen valintaan on vaikuttanut kansallisen kyberturvallisuusstrategian valmistuminen saman vuonna. Tutkimuksen rajauksena on käytetty uhkana ainoastaan kyberuhkaa, mitä vastaan yhteiskunnan toimia tutkittiin. Tutkimuksesta käy ilmi, että mikään keskus ei yksin kykene toimimaan, vaan se vaatii vahvasti yhteistyötä yksityisen ja julkisen sektorin välillä. Tutkimuksesta käy ilmi, että valtiohallinto on panostanut kyberturvallisuuden kehittämiseen jo lainsäädännön alalla. Lainsäädännössä on kyberuhkat ja niiden haittavaikutukset jo huomioitu. Laissa määritellään poikkeusolot ja niihin rinnastettavat hyökkäykset. Tutkimuksessa kyberhyökkäyksen on todettu juuri sellaisen hyökkäyksen, joka täyttää poikkeusolojen tunnusmerkit, jolloin kyetään ottamaan voimakkaampia lakeja viranomaisten käyttöön, jotta ne voivat puolustautua kybertoimintaympäristössä.

Mervi Mattila on tehnyt vuonna 2013 Pro Gradun: ”Tietoverkkorikollisuus haasteena torjuntayhteistyölle” Oulun yliopiston luonnontieteellisen tiedekunnan tietojenkäsittelytieteiden laitoksella tietojenkäsittelytieteestä, jonka käyttö on rajoitettu.

Mika Toppinen on tehnyt Maanpuolustuskorkeakoulussa vuonna 2014 Pro Gradun: ”Tietoverkkovaikuttamisen toimeenpano”, joka on turvaluokiteltu.

Suomessa on tehty myös muutamia väitöskirjoja ja opinnäytetöitä, joissa tietotekniikka on yhdistetty muuhun aiheeseen eri tieteenaloilla sen ollessa vain yksi osa tai väline tutkimusta eikä tietotekniikka ole ollut näiden tutki-

musten varsinaisessa keskiössä. Näitä opinnäytetöitä ei ole listattu tähän tutkimukseen.

4 KYBERTURVALLISUUDEN KIRJAVA STRATEGIAKENTTÄ

Tutkimuksen lähteinä on käytetty saatavissa olleita kansainvälistä, lähinnä EU-tason asiakirjoja, jossa kyberrikollisuutta käsitellään, vaikka kyseisessä asiakirjassa ei ole ollutkaan kysymys tutkimusaiheena olevasta asiasta. Tutkimusaineiston keräämisessä on otettu huomioon kaikki valtion hallinnossa tuotetut asiakirjat, joilla on katsottu olevan merkitystä tutkimuslähteenä, koska tutkimusongelmaan on saatavissa tällä tavalla suoraan vastauksia ((Hirsjärvi & Remes & Sajavaara 2007, 181). Tutkimuslähteiksi on otettu asiakirjoja, jotka käsittelevät kyberrikollisuutta ja sen tutkintaa tai torjuntaa. Varsinaista tutkimusaihetta laajemmalla lähdeotannalla on pyritty luomaan kuvaus kyberrikollisuudesta ja sen torjunnan ohjausasiakirjoista tutkimusaihealueen nykytilan selvittämiseksi, koska tutkimuksessa on ollut tarkoitus ymmärtää ja kartoittaa tutkittavana olevaa asiaa mahdollisemman laajalti (Hirsjärvi & Remes & Sajavaara 2007, 176–177).

Tutkimuksen lähdeaineistoksi valituista asiakirjoista olen tehnyt taulukon. Läheskään kaikkea Euroopan Unionin tai muiden kansainvälisten turvallisuusorganisaatioiden tuottamaa asiakirja-aineistoa ei ole otettu tähän tutkimukseen, vaikka ne ovat osa sitä kehystä, joka vaikuttaa suomalaiseen kyberrikostorjuntaan. Edellä mainittua aineistoa on määrällisesti paljon ja sillä on lähinnä välillistä vaikutusta tutkittavana olevaan asiaan. Kansallisesti laaditut keskeisimmät asiakirjat on pyritty ottamaan mukaan tutkimusaineistoon. Taulukon sisältö-sarakkeessa asiakirja on kuvattu olennaisilta osiltaan sekä arvioitu sen merkittävyys tutkimuksen kannalta. Varsinaiset tutkimustulokset on kuvattu sivulla 67.

ASIAKIRJA	SISÄLTÖ
Euroopan neuvoston vuonna 2001 tekemä tietoverkkorikollisuutta koskevassa yleissopimus.(ETS 185, 23.11.2001.)	Asiakirja kehottaa jäsenmaita parantamaan tietoisuuttaan tietoverkkorikollisuudesta sekä kehittämään tietoverkkorikoksiin liittyvää lainsäädäntöään. Lisäksi asiakirjassa kehotetaan luomaan yhteistyösuhteita yksityisen sektorin kanssa sekä tehostamaan kansainvälistä yhteis-

	työtä. Asiakirja on keskeinen Suomen poliisin tietoverkkorikostorjuntaa ohjaava asiakirja.
Tampereen ohjelma - Euroopan Unionin oikeus- ja sisäasioiden yhteistyön kehittämistä koskeva strategia-asiakirja vuosille 2000–2004.	Tampereen ohjelma oli ensimmäinen Euroopan Unionin hyväksymä viiden vuoden ohjelma, joka koski Euroopan Unionin oikeus- ja sisäasioiden yhteistyön kehittämistä. Asiakirjassa mainitaan poliisi- ja oikeusviranomaisten yhteistyön tiivistämistarve erityisesti järjestäytyneen rikollisuuden, huumausaine- ja ihmiskauppatutkinnassa sekä työssä terrorismia vastaan. Sekä terrorismin että järjestäytyneen rikollisuuden torjunnan mainitaan liittyvän kiinteästi tietoverkkorikollisuuteen ja sen torjuntaan. Tampereen ohjelman voidaan katsoa olevan myös kyberrikostorjuntaan liittyviä ensimmäisiä strategiatason ohjausasiakirjoja.
Euroopan Unionin oikeus- ja sisäasioiden yhteistyön kehittämistä koskeva strategia-asiakirja vuosille 2005 – 2009 (ns. Haagin ohjelma).	Ohjelmassa Euroopan komissio painotti terrorismin ehkäisyä ja tiedonvaihdon merkitystä sekä pyrki keskittymään värväykseen ja rahoitukseen liittyviin näkökohtiin, terrorismin ehkäisyyn, riskianalyysiin, riskialttiiden infrastruktuurien suojeluun ja seurausten hallintaan. Lisäksi ohjelmassa mainitaan strategisen lähestymistavan kehittäminen järjestäytyneen rikollisuuden torjuntaan sekä Eurooppalaisen rikostiedustelumallin kehittäminen. Kyseinen asiakirja ei suoranaisesti käsittele kyberrikollisuutta tai sen tutkintaa ja torjuntaa, mutta sillä voidaan katsoa olevan ohjaavaa merkitystä laajemmassa mittakaavassa.
Euroopan Unionin oikeus- ja sisäasioiden yhteistyön kehittämistä koskeva strategia-asiakirja vuosille 2010 – 2014 (ns. Tukholman ohjelma).	Ohjelmassa tietoverkkorikollisuus on nostettu erilliseksi painopistealueeksi. Ohjelman mukaan Unionin olisi edistettävä toimintapolitiikkaa ja lainsäädäntöä, jolla varmistetaan verkkojen turvallisuuden erittäin korkea taso ja mahdollistetaan entistä nopeampi reagoiminen verkkohäirintään ja verkkohyökkäyksiin.

	Tukholman ohjelmassa kehotetaan jäsenvaltioita perustamaan kansallisia alustoja, joita käytetään tietoverkkorikollisuuden torjumiseen sekä yhteistyöhön Euroopan unionin ulkopuolisten maiden kanssa. Lisäksi kehotetaan ryhtymään toimenpiteisiin julkisen ja yksityisen sektorin kumppanuuksien vahvistamiseksi tai tehostamiseksi. Ohjelmassa kehotetaan jäsenvaltioita selventämään kyberavaruuteen sovellettavia toimivaltasääntöjä. Asiakirja on keskeinen Suomen poliisin tietoverkkorikostorjuntaa ohjaava asiakirja.
Euroopan neuvoston raportti: Tackling digital crime through the establishment of a Cybercrime Centre - The way forward (14243/12, Brussels, 26 September 2012).	Asiakirjassa määritellään Euroopan kyberkeskuksen (EC3) pääasiasialliset tehtävät, joiden osalta Suomi jäsenmaana saa tietoa ja koulutusta tietoverkkorikollisuudesta. Euroopan kyberkeskuksen luomien yhteistyökanavien avulla myös suomalainen poliisi voi päästä mukaan EU:n ulkopuolisen maan kanssa perustettuun tutkintaryhmään. Asiakirja osaltaan ohjaa Suomen poliisin tietoverkkorikostorjuntaa.
Hallitusohjelma vuosille 1999–2003 (Lipposen hallitus)	Hallitusohjelmassa nostetaan tietoverkkojen turvallisuuskysymykset ensimmäistä kertaa yhdeksi Suomen hallituksen strategisista tavoitteista. Hallitusohjelman tavoitteena on selvittää, miten tietoliikenteen ja tietoverkkojen turvallisuus ja suojaustekniset kysymykset tulisi hallinnollisesti järjestää. Kyseinen asiakirja ei suoranaisesti käsittele kyberrikollisuutta tai sen tutkintaa ja torjuntaa, mutta se nosti tietoverkot strategiseen keskusteluun.
Hallitusohjelma vuosille 2003–2007 (Vanhasen hallitus sekä Jäätteenmä-	Hallituksen ohjelmassa edellytetään laajan, hallinnonalojen rajat ylittävän sisäisen turvallisuuden ohjelman laatimista erityisesti huumausai-

en hallitus 17.4. – 24.7.2003)	ne-, väkivalta- ja uusintarikollisuuden vähentämiseksi. Jäätteenmäen hallitusohjelmassa korostetaan kansalaisten ja yritysten luottamuksen lisäämistä tietoyhteiskunnan palveluihin tietoturvaa ja viestinnän yksityisyyden suojaa parantamalla. Lainsäädännön uudistaminen koskien viestinnän luottamuksellisuuden varmistamiseksi sekä työelämän tietosuojan parantamiseksi on otettu ohjelmatavoitteeksi (Tietoyhteiskuntakaari). Ohjelmaan on kirjattu lainsäädäntötarve liittyen tietoturvauhkiin ja tietotekniikkarikollisuuden torjuntaan. Ohjelmassa huomioidaan uudenlaiset riskit ja uhat, jotka liittyisivät kansalliseen varautumiseen ja maanpuolustukseen. Strategiatason asiakirjassa on mainittu tietoverkkorikostorjunnan lainsäädännön muutostarve.
Hallitusohjelmat vuosille 2007–2011 (Vanhasen hallitus sekä Kiviniemen hallitus 2010 – 2011)	Hallitusohjelmassa mainitaan tietoverkkoja koskien pyrkimys edistää kansalaisten ja yritysten luottamusta arjen tietoyhteiskunnan palveluihin. Lisäksi painopisteenä on yrityssalaisuuksien suojan kehittäminen. Kyseinen asiakirja ei suoranaisesti käsittele kyberrikollisuutta tai sen tutkintaa ja torjuntaa.
Hallitusohjelma vuosille 2011–2014 (Kataisen hallitus)	Hallitusohjelmassa tuodaan esiin keskinäisriippuvaisuudessa elävän maailman uudet turvallisuushaasteet, kuten muun muassa kansainvälinen rikollisuus, joukkotuhoaseiden leviäminen, terrorismi ja tietoverkkoihin kohdistuvat hyökkäykset. Näiden katsotaan vaativan laajan turvallisuuskäsityksen mukaista johdonmukaista varautumista. Hallitusohjelman yksi keskeinen kirjaus on kansallisen tietoverkkoturvallisuutta koskevan kyberstrategian laatiminen. Samoin keskeisiä kirjauksia on tietoverkkorikollisuuden ja järjes-

	täytyneen rikollisuuden liittyminen yhteen sekä niiden torjunta. Asiakirja on keskeinen Suomen poliisin tietoverkkorikostorjuntaa poliittisella tasolla ohjaava asiakirja.
Hallitusohjelma vuosille 2015–2018 (Sipilän hallitus)	Hallitusohjelman keskeisin kyberrikostorjuntaa koskeva kirjaus on tietoverkkorikollisuuden torjuntaan tarvittavien resurssien, toimintatapojen sekä lainsäädännön tarpeista. Samoin strategisia mainintoja ovat viranomaisten, oppilaitosten ja yritysten yhteisen osaamisen kehittämisen tehostaminen, yhteisen tilannekuvan luominen tietoverkkojen ja tietoliikenteen turvallisuudesta sekä luotettavan ja turvallisen tietojen vaihdon varmistaminen eri toimijoiden välillä. Asiakirja on selkeästi kyberrikostorjuntaa eteenpäin vievä, jonka pohjalta esitetään tehtäväksi konkreettisia toimenpiteitä.
Sisäisen turvallisuuden ohjelma (II) - Turvallinen elämä jokaiselle vuodelta 2008	Vasta toisessa Sisäisen turvallisuuden ohjelmassa tietoverkkorikollisuus kirjattiin yhdeksi keskeiseksi sisäisen turvallisuuden haasteeksi. Tietoverkkorikosten torjuntatavoitteiksi on kirjattu lainsäädännön ajantasaisuuden selvittäminen niin rikosepäilyjen kuin niiden tutkinnan osalta. Tavoitteeksi on kirjattu poliisin resurssien parantaminen tietoverkkorikostutkinnassa ja –torjunnassa. Tietoverkkorikollisuuden torjuntaan liittyvän koulutuksen lisääminen on yksi kirjattu haaste. Ohjelmassa on mainittu myös tietoverkkorikollisuuden olevan osa piilorikollisuutta. Asiakirja on keskeinen kansallinen ohjausasiakirja, jossa laajasti käsitellään tietoverkkorikollisuutta.
Sisäisen turvallisuuden ohjelma (III) – Turvalli-	Viimeisimmässä Sisäisen turvallisuuden ohjelmassa tietoverkkorikollisuuteen liittyvistä haas-

sempi huominen vuodelta 2012	teista ei ole samalla tavalla kirjauksia kuin edellisessä ohjelmassa. Ohjelmassa mainitaan yritysten tietopääomaan liittyvä rikollisuus, joka nähdään haasteena yritystoiminnalle sekä tunnistetaan huoltovarmuuskriittisten, mutta myös niiden alihankkijoihin kohdistuvien tietoturvauhkien merkitys yhteiskunnalle. Internetissä tapahtuvat, lapsiin ja nuoriin kohdistuvat seksuaalirikokset ja niihin puuttuminen ovat toinen tietoverkkorikollisuuteen kirjattu maininta. Nettipoliisityö sekä lainsäädännön muutostarpeet mainitaan tietoverkkorikollisuuden haasteina. Asiakirja ei ole merkittävä varsinaisen kyberrikostorjunnan kannalta.
Yhteiskunnan turvallisuusstrategia 2010	Strategian yhdeksi uhkamalliksi on kirjattu tietoliikenteen ja tietojärjestelmien vakavat häiriöt, kyberuhkat. Sähköisten palveluiden ja viestinnän toimivuutta voivat uhata luonnonilmiöiden, inhimillisen toiminnan tai tekniikan pettämisen aiheuttamat onnettomuudet, järjestelmiin kohdistuvat tahalliset sähköiset ja fyysiset hyökkäykset (esimerkiksi palvelunestohyökkäykset[24]), sekä tietoverkkojen haavoittuvuuksia hyväkseen käyttävät järjestäytynyt rikollisuus ja terrorismi. Strategiassa mainitaan sisäisestä turvallisuudesta vastaavien viranomaisten toimintakyvyn turvaaminen yhteistyössä järjestöjen ja yritysten kanssa. Tiedustelun, analyysitoiminnan ja viranomaisyhteistyön, erityisesti EU- ja kansainvälinen yhteistyön kehittäminen, rajat ylittävien rikosten ennalta ehkäisy, paljastaminen ja selvittäminen sekä operatiiviseen toimintaan liit-

[24] Palvelunestohyökkäys (Denial of Service, DoS) tarkoittaa verkkohyökkäystä, jossa pyritään estämään verkkosivuston tarkoitettu käyttö. Tavallisimmin tämä toteutetaan kohdistamalla verkkosivustolle niin paljon liikennettä, että tämä ei käytännössä kykene palvelemaan asiakkaitaan.

	tyvää tiedonvaihto EU:n ja Suomen kannalta keskeisten maiden kanssa on mainittu strategian tavoitteiksi. Asiakirja on yleisluonteinen eikä varsinaisesti käsittele kyberuhkaa tai – rikoksia ja niiden torjuntaa edellä mainittua tarkemmin.
Suomen kyberturvallisuusstrategia 2013	Kansallinen kyberturvallisuusstrategia on varsinaisesti ensimmäinen strategiatason asiakirja, joka koskettaa myös poliisihallintoa kyberturvallisuuden alalta siinä olevien yksityiskohtaisemmin poliisitoimintaa ohjaavien toimintalinjojen johdosta. Poliisin osalta yksi keskeinen toimintalinja on kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi luotava viranomaisten ja muiden toimijoiden välinen tehokas yhteistoimintamalli, jonka tavoitteena on jaettu tilannetietoisuus ja tehokas uhkien torjunta. Kokonaisvaltaisen kyberturvallisuuden tilannetietoisuuden ja tilanneymmärryksen parantaminen yhteiskunnan elintärkeiden toimintojen turvaamiseen osallistuvien keskeisten toimijoiden välillä on poliisitoiminnan kannalta toinen keskeinen toimintalinjaus. Asiakirjassa poliisin osalta huolehditaan siitä, että poliisilla tulee olla tehokkaat edellytykset ennalta ehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia. Strategia mainitsee erikseen poliisin olevan kybertoimintaympäristöön kohdistuvien ja sitä hyödyntävien rikosten keskeinen torjuja. Kansainvälisen toiminnan osalta poliisi velvoitetaan omalla toimialallaan harjoittamaan yhteistyötä erityisesti kyberturvallisuudessa kehittyneiden valtioiden ja organisaatioiden kanssa. Keskeinen kirjaus poliisitoiminnan kannalta on

	linjaus kansallisesta lainsäädännöstä, jolla varmistetaan tehokkaan kyberturvallisuuden toteuttamisen edellytykset eli tiedustelulainsäädännön kehittäminen. Yhtenä poliisitoimintaan vaikuttavana linjauksena strategiassa määritellään viranomaisille ja elinkeinoelämän toimijoille kyberturvallisuutta koskevat tehtävät ja palvelumallit sekä yhteiset perusteet kyberturvallisuuden vaatimusten hallinnalle. Huolimatta siitä, että asiakirja on yksi keskeinen strategiatason asiakirja, siinä ei mainita, kuinka poliisitoiminta osaltaan huolehtii strategiassa viranomaisille annetuista vastuista ja tehtävistä, mitä rikosten ennalta estäminen ja paljastaminen kybermaailmassa tarkoittavat.
Valtioneuvoston periaatepäätös järjestäytyneen rikollisuuden torjunnan strategiasta 2013	Päätösasiakirja on poikkihallinnollinen ohjausasiakirja, jossa velvoitetaan eri ministeriöitä ryhtymään päätöksessä mainittuihin toimenpiteisiin järjestäytyneen rikollisuuden torjunnan tehostamiseksi. Yhdeksi toimenpiteeksi on kirjattu panostaminen tietoverkkoja hyödyntävän rikollisuuden torjuntaan osana järjestäytyneen rikollisuuden torjuntaa. Asiakirja on strateginen ohjausasiakirja jolla on erityinen vaikutus poliisin järjestäytyneen rikollisuuden torjuntaan ja sen yhtenä osa-alueena olevaan kyberrikostorjuntaan.
Kyberturvallisuusstrategian toimeenpano-ohjelma, 2014	Kyberturvallisuuden toimeenpano-ohjelma sisältää laajan, eri hallinnon aloja koskevan osaltaan yksityiskohtiin menevän yhteenvedon kyberturvallisuusstrategian jalkauttamiseksi. Poliisin osalta toimeenpano-ohjelmassa mainitaan rikostorjunnan kyberosaamisen kehittäminen, esitutkintaviranomaisen toimivaltuuksien selvittäminen kyberrikostorjunnassa, tietoverkkorikososaamisen liittäminen poliisin 24/7 yhteyspisteeseen ja kansainvälisten palveluiden turvaaminen, kyberrikostilannekuvan ja – tie-

	donhankinnan kehittäminen sekä kyberrikostutkinnan järjestäminen ja resursointi. Asiakirja on selkeästi poliisitoimintaa strategiatason asiakirja.
Vuonna 2015 voimaan tullut lainsäädäntökokonaisuus - Tietoyhteiskuntakaari	Jäätteenmäen hallitusohjelmaan tehtyjen kirjausten johdosta vuonna 2015 astui voimaan Tietoyhteiskuntakaari – niminen lainsäädäntö, jonne on koottu keskeiset sähköistä viestintää koskevat säädökset. Asiakirjassa käsitellään muun muassa poliisin ja teleyritysten välistä työn ja vastuiden jakoa, jotka osaltaan antavat poliisitoiminnalle toimivallan raamit, vaikka ei varsinainen strategia-asiakirja olekaan.
Suomalaisen tiedustelulainsäädännön suuntaviivoja 2015	Asiakirja käsittelee tiedustelua tietoliikennetiedustelun näkökulmasta, jossa on kyse teknisestä pääsystä kaikkeen tietoliikenteeseen. Asiakirjassa ei tarkastella tavanomaisena pidettävää verkkorikollisuuden torjuntaa, vaan kansalliseen turvallisuuteen kohdistuvien vakavien uhkien havaitsemista ja tunnistamista sekä niiden torjuntaa. Tähän liittyvää lainsäädäntöä asiakirjassa kehotetaan laatimaan. Mietintö ei suoranaisesti käsittele kyberrikostorjuntaa poliisin näkökulmasta poislukien Suojelupoliisi, koska siinä ei ole otettu huomioon lainsäädäntöä, joka määrittelisi selkeämmin kohdennetun tietoverkoissa tapahtuvan tiedonhankinnan, joka poliisitoiminnan kannalta olisi olennaista ja vaikuttaisi erityisesti paikallispoliisin työhön.
Tietotekniikkatutkinnan järjestäminen poliisissa 2008	Raportti käsittelee laajasti ja useasta eri näkökulmasta poliisin tietotekniikkatutkinnan järjestämistä Keskusrikospoliisissa ja paikallispoliisissa. Raportissa ei käsitellä tietoverkkorikollisuuden (kyberrikos) torjuntaa tiedustelulähtöisesti, vaikka muuten raportti esittää konkreettisia ehdotuksia toimintojen järjestämiseksi.
Järjestäytyneen rikollisuuden ja terrorismin	Raporttiin on kuvattu yksityiskohtaiset toimenpide-ehdotukset tietoverkkorikollisuuden ja

torjunta, Sisäisen turvallisuuden ohjelman valmisteluun osallistuneen asiantuntijaryhmän loppuraportti, 2008	Internetin käyttöön liittyvien riskien ja uhkien torjumiseksi. Lainsäädäntömuutokset, tietoverkkorikostorjunnan toimintaedellytysten turvaaminen ja osaamisen kehittäminen sekä kansalaisten ilmoitusaktiivisuuden lisääminen ovat raportin keskeisiä esityksiä tietoverkkorikostorjunnan kehittämiseksi. Raportti on selkeästi kyberrikostorjuntaa ohjaava hallinnon asiakirja.
Poliisihallituksen määräys vakavien tietoverkkorikosten ja verkon kautta tapahtuvien rikosten tehokkaasta ennalta estämisestä, paljastamisesta ja tutkintaan sekä vakaviin verkkorikosuhkiin liittyvästä nopean reagointikyvyn varmistamisesta, 2013.	Salassa pidettävää asiakirjaa ei tässä tutkimuksessa käsitellä. Raportti on käytännön työtä ohjaava asiakirja.
Poliisin kybertoimivaltuudet 2015	Raportti sisältää 14 poliisin kiireellisintä käytännön ongelmaa liittyen kybertoimivaltuuksien muutostarpeisiin. Raportti sisältää muun muassa kybertoimintaympäristöön liittyvien käsitteiden määrittelyn (muun muassa tietotekninen valvonta tietoverkoissa, tietoverkkotiedustelu ja turvallisuustiedustelu), joita ei aiemmin tämän tason asiakirjoissa ole tehty. Raportti on osaltaan toimintaa ohjaava asiakirja.
Poliisin strategia 2015	Poliisin strategisten päämäärien saavuttamiseksi asiakirjassa mainitaan yhtenä toimenpiteenä suunnata resurssien suuntaaminen tietoverkkorikostorjuntaan sekä kyberosaamisen kehittämiseen. Strategisina tavoitteina mainitaan kyberrikollisuuden torjunnan osaamisen kasvattaminen, resurssien kohdistaminen kyberrikostorjunnan lisäksi omien toimintojen suojaamiseen kyberuhilta sekä tarve selvittää tietoverkoissa tapahtuvan tiedonhankinnan toimivaltuuksien kehittämistarpeet.

	Asiakirja on poliisihallinnon ohjausasiakirja, jossa kyberrikollisuuden torjunta on nostettu omaksi osa-alueekseen.
Muita asiakirjoja	Poliisi on laatinut hallinnon sisäisiä ja osin salassa pidettäviä asiakirjoja, joita ei tässä tutkimuksessa käsitellä. Asiakirjat ohjaavat pääosin käytännön työtä ja sen järjestämistä.

4.1 Eurooppalaiset keskeiset tietoverkkorikollisuuden torjuntaa ohjaavat asiakirjat

Euroopan neuvoston vuonna 2001 tekemä tietoverkkorikollisuutta koskevassa yleissopimus on keskeinen Suomen poliisin tietoverkkorikostorjuntaa ohjaava asiakirja, jonka Suomen eduskunta hyväksyi vuonna 2007[25]. Sopimuksessa kehotettiin muun muassa allekirjoittajavaltioita nostamaan tietoisuuttaan asianomaisesta rikollisuudesta sekä huomioimaan yhteiskunnan suojeleminen tietoverkkorikollisuudelta muun muassa asiaan liittyvän lainsäädännön ja tehokkaamman kansainvälisen yhteistyön avulla. Sopimuksessa kehotettiin huomioimaan yhteistyö myös kansallisesti yksityisen sektorin toimijoiden kanssa. Sopimus ohjeistaa valtioita kriminalisoimaan muun muassa tietojärjestelmiin kohdistuvat rikokset, tietokoneavusteiset petokset sekä lapsipornografiaan ja tekijänoikeuksiin liittyvät tietojärjestelmien avulla tehtävät rikokset. Sopimus ohjeistaa säätämään myös rikostutkintaa edistäviä tekijöitä, kuten tiedonsaantioikeuksia. **(**Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus 2001)

Toisena eurooppalaisena ohjauskirjana voidaan mainita Euroopan neuvoston asiakirja (14243/12), jossa määritellään Euroopan kyberkeskuksen (EC3) pääasiasialliset tehtävät. Tehtäviin kuuluu muun muassa pitää yllä eurooppalaista tilannekuvaa tietoverkkorikollisuudesta, tukea jäsenmaiden tietoverkkorikostutkintaa sekä kehittää toimintoja. Kyberkeskuksen tehtävänä on toimia yhteistyössä EU:n ulkopuolisten maiden kanssa ja yhteistyön voidaan katsoa hyödyttävän mahdollisesti vakavan rikollisuuden torjuntaa

[25] Laki Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta, 539/2007

myös paikallispoliisin näkökulmasta. Tämän johdosta suomalaisen poliisin on mahdollista päästä mukaan kansainvälisiin tutkintaryhmiin, joissa toimii myös EU:n ulkopuolisia valtioita. Asiakirjan voidaan katsoa välillisesti ilman suoranaista ohjaavaa vaikutusta liittyvän myös tiedustelulähtöiseen rikostorjuntaan tietojohtoiseen poliisitoiminnan näkökulmasta, koska Euroopan kyberturvallisuuskeskus toimii koordinoivana yhteistyöpisteenä pitäen yllä tietoverkkorikollisuuden tilannekuvaa, joka on hyödynnettävissä myös paikallistasolla.

Tampereen ohjelma

Viisitoista vuotta sitten laadittu strategia-asiakirja, niin sanottu Tampereen ohjelma[26] (1999), oli ensimmäinen Euroopan Unionin hyväksymä viiden vuoden ohjelma, joka koski Euroopan Unionin oikeus- ja sisäasioiden yhteistyön kehittämistä (Justice and Home Affaris JHA). Tampereen kokouksen päätelmien pohjalta lähdettiin kehittämään muun muassa yhteistä eurooppalaista turvapaikkajärjestelmää, poliisi- ja oikeusviranomaisten yhteistyötä ja rikostorjuntaa. Päätelmissä korostui myös rikostorjunnan yhteiseurooppalainen näkökulma. Poliisi- ja oikeusviranomaisten yhteistyötä lähdettiin tiivistämään erityisesti huumausaine- ja ihmiskauppatutkinnassa sekä työssä terrorismia vastaan. Myös yhteistyö vakavan järjestäytyneen rikollisuuden torjunnassa, lähti kehittymään päätelmien pohjalta. Sekä terrorismin että järjestäytyneen rikollisuuden torjunta liittyvät kiinteästi tietoverkkorikollisuuteen ja sen torjuntaan. (Sisäministeriö 2014)

Haagin ohjelma

Haagin monivuotisessa ohjelmassa[27] luetellaan unionin 10 painopistettä, joiden avulla pyritään vahvistamaan vapauden, turvallisuuden ja oikeuden aluetta viiden seuraavan vuoden aikana. Yhtenä painopisteenä ohjelmassa mainitaan **terrorismin tehokas torjunta**. Ohjelman mukaan se vaatii katta-

[26] Euroopan Unionin oikeus- ja sisäasioiden yhteistyön kehittämistä koskeva strategia-asiakirja vuosille 2000–2004.
[27] Euroopan Unionin oikeus- ja sisäasioiden yhteistyön kehittämistä koskeva strategia-asiakirja vuosille 2005 – 2009.

vaa lähestymistapaa, jonka on oltava yhtenäinen ja johdonmukainen. Ohjelmassa Euroopan komissio painotti terrorismin ehkäisyä ja tiedonvaihdon merkitystä sekä pyrki keskittymään värväykseen ja rahoitukseen liittyviin näkökohtiin, terrorismin ehkäisyyn, riskianalyysiin, riskialttiiden infrastruktuurien suojeluun ja seurausten hallintaan. Ohjelmaan on myös kirjattu jäsenmaiden yhteistyö kolmansien maiden kanssa välttämättömänä asiana. (Tiivistelmät EU:n lainsäädännöstä - Internet-sivusto)

Toisena painopistekohtana ohjelmassa on mainittu **Strategisen lähestymistavan kehittäminen järjestäytyneen rikollisuuden torjuntaan**. Ohjelmassa on mainittu tavoitteeksi jäsenvaltioiden lainvalvontaviranomaisten, kuten poliisin ja tullin yhteistyön tehostaminen, jota tehokas järjestäytyneen rikollisuuden torjunta edellyttää. Ohjelmaan on liitetty maininta myös **Eurooppalaisen rikostiedustelumallin** kehittämisestä, joka on yksi painopisteistä.

Tukholman ohjelma

Ohjelmassa mainitaan, että asiat, joita aikaisempiin ohjelmiin on kirjattu, ovat edistyneet. Tukholman ohjelma[28] on laaja ja yhtenä kehittämisalueena mainitaan tarve sisäisen turvallisuuden strategialle, jolla parannetaan turvallisuutta unionissa ja suojellaan sillä tavoin Euroopan kansalaisten henkeä ja turvallisuutta sekä puututaan järjestäytyneeseen rikollisuuteen, terrorismiin ja muihin uhkiin. Strategialla pyrittäisiin vahvistamaan lainvalvonnan, rajaturvallisuuden, pelastuspalvelun ja katastrofien hallinnan sekä rikosoikeuden alalla tehtävää yhteistyötä.

Ohjelmassa mainitaan oikeudellisen yhteistyön tehostamistarve, samoin kuin esitetään verkostojen luonti eri maiden ylimpien virkamiesten välille. Rikosten tutkintaan liittyen ohjelmassa esitetään, että eri maissa tulisi soveltaa yhteisiä syyteperusteita ja yhteisiä enimmäisseuraamusten vähimmäistasoja, kun kyse on erityisen vakavasta rikollisuudesta, jolla voi tällaisten rikosten luonteen tai vaikutusten taikka niiden erityisen yhteisen torjumis-

[28] Tukholman ohjelma – Avoin ja turvallinen Eurooppa kansalaisia ja heidän suojeluaan varten Euroopan Unionin oikeus- ja sisäasioiden yhteistyön kehittämistä koskeva strategia-asiakirja vuosille 2010 – 2014.

tarpeen johdosta olla rajat ylittäviä vaikutuksia. Etusijalle olisi asetettava terrorismi, ihmiskauppa, laiton huumausainekauppa, naisten ja lasten seksuaalinen hyväksikäyttö ja lapsiporno sekä tietokonerikollisuus. Järjestäytyneen sekä rajat ylittävän rikollisuuden torjuntaa on painotettu ja ohjelmassa on esitetty järjestäytyneen rikollisuuden torjunta osana sisäisen turvallisuuden strategiaa.

Tietoverkkorikollisuus on nostettu erilliseksi painopistealueeksi[29]. Ohjelman mukaan Unionin olisi edistettävä toimintapolitiikkaa ja lainsäädäntöä, jolla varmistetaan verkkojen turvallisuuden erittäin korkea taso ja mahdollistetaan entistä nopeampi reagoiminen verkkohäirintään ja verkkohyökkäyksiin. Ohjelmassa viitataan Euroopan neuvoston vuoden 2001 tietoverkkorikollisuutta koskeva yleissopimukseen, jota olisi käytettävä tietoverkkorikollisuuden maailmanlaajuisen torjumisen oikeudellisena viitekehyksenä.

Tukholman ohjelmassa Eurooppa-neuvosto kehottaa lisäksi jäsenvaltioita antamaan täyden tukensa kansallisille alustoille, joita käytetään tietoverkkorikollisuuden torjumiseen sekä yhteistyölle Euroopan unionin ulkopuolisten maiden kanssa. Lisäksi kehotetaan ryhtymään toimenpiteisiin julkisen ja yksityisen sektorin kumppanuuksien vahvistamiseksi tai tehostamiseksi sekä Europolia tehostamaan tietoverkkorikollisuuden strategista analysointia. Ohjelmassa kehotetaan myös kyberavaruuteen sovellettavien toimivaltasääntöjen selventämistä.

4.2 Kansalliset tietoverkkorikollisuuden ohjaavat asiakirjat

Hallitusohjelmat vuosille 1999–2014

Lipposen toinen hallitus vuosien 1999–2003 ohjelmassa nosti tietoverkkojen turvallisuuskysymykset ensimmäistä kertaa yhdeksi Suomen hallituksen strategisista tavoitteista, jonka jälkeen tietoverkkoihin liittyvät asiat ovat kasvattaneet merkitystään myös hallitusohjelmissa. Lipposen hallitusohjelmaan kirjattiin tavoitteeksi selvittää, miten tietoliikenteen ja tietoverkkojen turvallisuus ja suojaustekniset kysymykset tulisi hallinnollisesti järjestää.

[29] Tukholman ohjelma: kohta 4.4.4; sivu 47

Julkisten palveluiden käytön helppous ja kustannustehokkuus tieto- ja viestintätekniikan avulla ottaen huomioon tietoturvallisuusnäkökohdat sekä kansalaisille jaettava sähköinen henkilökortti olivat ohjelman lisäkirjauksia. (Leppänen & Kankaanranta, 60, 62)

Vanhanen I 2003–2007:

Vanhasen hallituksen ohjelmassa vuosille 2004–2007 käynnistettiin sisäisen turvallisuuden ohjelman valmistelu. Hallitusohjelmassa hallituspuolueet määrittelevät keskeisimmät tavoitteensa tulevalle hallituskaudelle. Hallitusohjelma on monipuoluejärjestelmässä keskeinen asiakirja, jossa yhteen sovitetaan puolueiden näkökannat ja sitoudutaan yhteiseen työskentelyyn. Ohjelma käsittää suurten linjojen, kuten työllisyyden ja tasa-arvon, lisäksi myös yksityiskohtaisempia tavoitteita. Vuosien 2004–2007 Hallituksen ohjelmassa edellytettiin laajan, hallinnonalojen rajat ylittävän sisäisen turvallisuuden ohjelman laatimista erityisesti huumausaine-, väkivalta- ja uusintarikollisuuden vähentämiseksi. Sisäisen turvallisuuden ohjelman laatimiseen osallistui yhdeksän ministeriötä ja lukuisa määrä muita asiantuntijoita. (Arjen turvaa. Sisäisen turvallisuuden ohjelma 2004–2007, 2-3)

Jäätteenmäki 2003

Jäätteenmäen hallitusohjelmassa 2003 vuonna korostettiin kansalaisten ja yritysten luottamusta tietoyhteiskunnan palveluihin tietoturvaa ja viestinnän yksityisyyden suojaa parantamalla. Lainsäädännön uudistaminen koskien viestinnän luottamuksellisuuden varmistamiseksi sekä työelämän tietosuojan parantamiseksi oli otettu ohjelmatavoitteeksi. Myös tietoturvauhat ja tietotekniikkarikollisuuden torjuntaan liittyvän lainsäädännön uudistamistarve oli kirjattu ohjelmaan. Ohjelmassa oli huomioitu uudenlaiset riskit ja uhat, jotka liittyisivät kansalliseen varautumiseen ja maanpuolustukseen. Painopistealueiksi oli kirjattu muun muassa huoltovarmuus, väestönsuojelu, tietojärjestelmien suojaaminen ja viestinnän valmiudet. Hallitusohjelmaan oli otettu mukaan lisäksi Tietoyhteiskuntaohjelman toteuttaminen, johon

liittyvä laaja lainsäädäntöuudistus: Tietoyhteiskuntakaari[30] astui pääosin voimaan vuonna 2015. (Leppänen & Kankaanranta, 62)

Vanhasen hallitusohjelmassa oli pitkälti samat painotukset kuin olivat olleet Jäätteenmäen hallitusohjelmassa. Vanhasen ensimmäisen hallituksen ohjelma kiinnitti huomiota tietoturvaan ja viestinnän yksityisyyden suojaa parantamiseen. Tietoyhteiskunnan tarjoamien palveluiden tulisi nauttia kansalaisten ja yritysten luottamusta. Olennaisena osana asian kehittämisessä oli lainsäädännön muuttaminen erityisesti työelämän tietosuojan osalta. Tietoturvauhkiin ja tietotekniikkarikollisuuteen varautuminen oli myös mukana hallitusohjelmassa samoin kuin viranomaisverkon rakentaminen. (Leppänen & Kankaanranta, 61)

Vanhanen II 2007–2010 sekä Kiviniemi 2010–2011:

Seuraavalla hallituskaudella vuonna 2010 Vanhanen erosi pääministerin tehtävästään ja pääministeriksi vaihtui Kiviniemi. Tämän kauden hallitus kirjasi tietoverkkoja koskien pyrkimyksen edistää kansalaisten ja yritysten luottamusta arjen tietoyhteiskunnan palveluihin. Ohjelmakirjauksen mukaan tavoite oli varmistaa yritysten toimintaedellytykset kaikissa oloissa kriittisen infrastruktuurin toimintavarmuus. Lisäksi painopisteenä oli yrityssalaisuuksien suojan kehittäminen. Varsinaisena uutena asiana hallitusohjelmassa kiinnitettiin erityistä huomiota lasten ja nuorten asemaan tietoyhteiskunnan kansalaisina ja tavoitteenaan oli luoda kaikille turvallinen digitaalinen ympäristö. (Leppänen & Kankaanranta, 61)

[30] Liikenne- ja viestintäministeriön valmistelemaan tietoyhteiskuntakaareen on koottu keskeiset sähköistä viestintää koskevat säädökset. Tietoyhteiskuntakaari sisältää 352 pykälää. Nyt voimassa olevista säädöksistä on poistettu päällekkäisyydet ja sääntelyä on selkeytetty. Tietoyhteiskuntakaarta on valmisteltuja vuorovaikutteisesti sidosryhmien kanssa. (Liikenne- ja viestintäministeriön verkkosivut)

Katainen 2011–2014:

Kataisen hallitusohjelmaan oli aiempiin hallitusohjelmiin verrattuna tuotu uusia asioita. Kataisen hallitusohjelmassa tuotiin esiin keskinäisriippuvaisuudessa elävän maailman uudet turvallisuushaasteet, kuten ilmastonmuutos, hallitsemattomat muuttoliikkeet, köyhyys ja eriarvoisuus, epidemiat, kansainvälinen rikollisuus, joukkotuhoaseiden leviäminen, terrorismi ja tietoverkkoihin kohdistuvat hyökkäykset. Näiden katsottiin vaativan laajan turvallisuuskäsityksen mukaista johdonmukaista varautumista. (Leppänen & Kankaanranta, 61)

Entisestään korostettiin tietoverkkojen toimintavarmuutta, jonka todettiin olevan välttämätöntä modernin tietoyhteiskunnan toiminnalle. Hallitusohjelman yksi keskeinen kirjaus oli kansallisen tietoverkkoturvallisuutta koskevan kyberstrategian laatiminen. Hallitusohjelmaan kirjattiin myös selkeä tavoite, jonka mukaan Suomi on yksi johtavista maista kyberturvallisuuden kehittämisessä. (Leppänen & Kankaanranta, 61)

Tietoverkkorikollisuuden ja järjestäytyneen rikollisuuden liittyminen yhteen sekä niiden torjunta olivat keskeisiä kirjauksia. Identiteettivarkauksien torjunta oli yhtenä merkittävänä kirjauksena. Lainsäädäntöön ei ollut siihen mennessä otettu mukaan kyseistä rikollisuuden alaa. Lisäksi kansalaisten oikeusturvan yhdenvertainen toteutuminen digitaalisessa ympäristössä oli kirjattu hallitusohjelmaan. Poliisitoiminnan rahankäyttöön liittyvä, merkittävä kirjaus oli jakamisen oikaiseminen viranomaisten ja teleoperaattorien välillä. Tähän mennessä poliisi käytännössä pitkälti oli vastannut teletunnistetietojen tallentamiskustannuksista. (Leppänen & Kankaanranta, 61)

Sipilä 2015–2018:

Sipilän hallitusohjelmaan on kirjattu muun muassa sisäisen turvallisuuden palvelutason parantaminen digitalisaation sekä uusien teknologioiden avulla sekä poliisin operatiivisen toimintakyvyn turvaaminen. Keskeisin kyberrikostorjuntaa koskeva kirjaus on tietoverkkorikollisuuden torjuntaan tarvitta-

vien resurssien, toimintatapojen sekä lainsäädännön tarpeista. Samoin strategisia mainintoja ovat viranomaisten, oppilaitosten ja yritysten yhteisen osaamisen kehittämisen tehostaminen, yhteisen tilannekuvan luominen tietoverkkojen ja tietoliikenteen turvallisuudesta sekä luotettavan ja turvallisen tietojen vaihdon varmistaminen eri toimijoiden välillä. (Hallituksen julkaisusarja 10/2015)

Sisäisen turvallisuuden ohjelmat[31] vuosille 2004–2015

Ensimmäinen Sisäisen turvallisuuden ohjelma annettiin vuonna 2004. Ohjelmassa tunnistettiin ja kuvattiin tietoverkkorikollisuuden silloinen tila, ja tietoyhteiskunnan haavoittuvuus nostettiinkin yhdeksi keskeisistä tulevaisuuden haasteista. Kuitenkaan tietoverkkorikollisuuden torjunta tai muut kyberturvallisuus eivät nousseet kirjauksiksi ohjelmaan.

Toisessa Sisäisen turvallisuuden ohjelmassa vuonna 2008 tietoverkkorikollisuus oli kirjattu yhdeksi keskeiseksi sisäisen turvallisuuden haasteeksi. Tietoverkkorikosten torjuntatavoitteiksi oli lainsäädännön ajantasaisuuden selvittäminen niin rikosepäilyjen kuin niiden tutkinnan osalta. Tavoitteeksi oli myös kirjattu poliisin resurssien parantaminen tietoverkkorikostutkinnassa ja – torjunnassa. Tietoverkkorikollisuuden torjuntaan liittyvän koulutuksen lisääminen oli yksi haaste. Yksi olennainen ohjelman kirjaus oli tietoverkkorikollisuuden olevan osa piilorikollisuutta.

Viimeisimmässä vuonna 2012 laaditussa Sisäisen turvallisuuden ohjelmassa tietoverkkorikollisuuteen liittyvistä haasteista ei ole samalla tavalla kirjauksia kuin edellisessä ohjelmassa. Yritysten tietopääomaan liittyvä rikollisuus on nähty haasteena yritystoiminnalle ja ohjelmassa tunnistetaan huoltovarmuuskriittisten, mutta myös niiden alihankkijoihin kohdistuvien tietoturvauhkien merkitys yhteiskunnalle. Toiseksi haasteeksi on kirjattu Internetissä tapahtuvat, lapsiin ja nuoriin kohdistuvat seksuaalirikokset, joihin puut-

[31] Valtioneuvosto on vuodesta 2004 alkaen antanut kolme periaatepäätöstä Sisäisestä turvallisuudesta neljän vuoden välein. Nämä Sisäisen turvallisuuden ohjelmat laaditaan ja toteutetaan poikkihallinnollisesti sisäasianministeriön johtamana.

tumista parannettaisiin lasten sekä heidän vanhempiensa tietoisuuden kasvattamista näistä rikosmuodoista. Nettipoliisityö sekä lainsäädännön muutostarpeet on mainittu haasteina, mutta sitä vastoin ohjelmassa ei ole kirjattu tietoverkkorikollisuuden olevan osa rajat ylittävää, järjestäytynyttä rikollisuutta. (Leppänen & Kankaanranta, 64)

Yhteiskunnan turvallisuusstrategia

Valtioneuvosto antoi 16.12.2010 periaatepäätöksen yhteiskunnan turvallisuusstrategiaksi[32]. Vuosina 2003 ja 2006 laadituissa valtioneuvoston periaatepäätöksissä yhteiskunnan elintärkeiden toimintojen turvaamisesta määriteltiin elintärkeät toiminnot ja eri hallinnonalojen vastuut niiden turvaamiseksi. Periaatepäätös on kokonaisvaltainen ja poikkihallinnollinen, joka ottaa huomioon lähivuosien arvioitua turvallisuusympäristön kehitystä ja suomalaisen yhteiskunnan muutosta. Periaatepäätös on laadittu kaikissa tilanteissa turvattavien yhteiskunnan elintärkeiden toimintojen näkökulmasta ja siinä kuvataan elintärkeitä toimintoja vaarantavat uhkamallit. (Yhteiskunnan turvallisuusstrategia, 1-2)

Strategian yhdeksi uhkamalliksi on kirjattu tietoliikenteen ja tietojärjestelmien vakavat häiriöt, kyberuhkat. Sähköisten palveluiden ja viestinnän toimivuutta voivat uhata luonnonilmiöiden, inhimillisen toiminnan tai tekniikan pettämisen aiheuttamat onnettomuudet, järjestelmiin kohdistuvat tahalliset sähköiset ja fyysiset hyökkäykset (esimerkiksi palvelunestohyökkäykset[33]), sekä tietoverkkojen haavoittuvuuksia hyväkseen käyttävät järjestäytynyt rikollisuus ja terrorismi. (Yhteiskunnan turvallisuusstrategia, 66)

Strategiassa mainitaan sisäisestä turvallisuudesta vastaavien viranomaisten toimintakyvyn turvaaminen yhteistyössä järjestöjen ja yritysten kanssa. Tiedustelun, analyysitoiminnan ja viranomaisyhteistyön, erityisesti EU- ja kan-

[32] Yhteiskunnan turvallisuusstrategia, Valtioneuvoston periaatepäätös 2010

33 Palvelunestohyökkäys (Denial of Service, DoS) tarkoittaa verkkohyökkäystä, jossa pyritään estämään verkkosivuston tarkoitettu käyttö. Tavallisimmin tämä toteutetaan kohdistamalla verkkosivustolle niin paljon liikennettä, että tämä ei käytännössä kykene palvelemaan asiakkaitaan.

sainvälinen yhteistyön kehittäminen, rajat ylittävien rikosten ennalta ehkäisy, paljastaminen ja selvittäminen sekä operatiiviseen toimintaan liittyvää tiedonvaihto EU:n ja Suomen kannalta keskeisten maiden kanssa on mainittu strategian tavoitteiksi. . (Yhteiskunnan turvallisuusstrategia, 27–29)

Kansallinen kyberturvallisuusstrategia ja taustamuistio

Suomen ensimmäinen kyberturvallisuusstrategia sekä taustamuistio julkaistiin vuonna 2013 Turvallisuuskomitean[34] sihteeristön tuottamana Puolustusministeriön hallinnonalalta. Turvallisuuskomitea perustettiin kokonaisturvallisuuden alalla toimivaksi, varautumisen pysyväksi yhteistoimintaelimeksi, jonka tehtävistä säädetään erikseen ja siihen kuuluu kansliapäälliköitä sekä muita korkeita virkamiehiä. Kyberturvallisuusstrategia julkaistiin osana Yhteiskunnan turvallisuusstrategiaa[35]. Strategiassa kyberturvallisuutta ei ole tarkoitettu oikeudelliseksi käsitteeksi, joka perustaisi uusia toimivaltuuksia viranomaisille tai muille toimielimille. Siinä ei ehdoteta muutoksia varautumisjärjestelyjen perusteisiin eikä eri viranomaisten toimivaltamäärittelyihin. Strategiassa kuvataan kyberturvallisuuden visio, toimintamalli ja strategiset linjaukset. Strategisten linjausten toimeenpanolla vahvistetaan suomalaisen turvallisuusyhteistyön vahvuudeksi koettua julkisen ja yksityisen sektorin välistä yhteistoimintaa. Tämän yhteistyön avulla voidaan parhaiten palvella koko yhteiskuntaa ja tukea sen elintärkeitä toimintoja tuottavia toimijoita. Päämääränä on huolehtia eri toimintojen häiriöttömästä ja turvallisesta jatkumisesta arjessa ja häiriötilanteissa. (Kansallinen kyberturvallisuusstrategia, 1-2, 6)

Kansallinen kyberturvallisuusstrategia on varsinaisesti ensimmäinen strategiatason asiakirja, joka koskettaa myös poliisihallintoa kyberturvallisuuden alalta siinä olevien yksityiskohtaisemmin poliisitoimintaa ohjaavien toimin-

[34] Valtioneuvosto 2013c, 11; Valtioneuvosto 2013b

[35] Yhteiskunnan turvallisuusstrategia, Valtioneuvoston periaatepäätös 16.12.2010. Yhteiskunnan turvallisuudesta huolehtiminen on valtiovallan keskeisimpiä tehtäviä. Periaatepäätös on laadittu kaikissa tilanteissa turvattavien yhteiskunnan elintärkeiden toimintojen näkökulmasta. Elintärkeitä toimintoja ovat valtion johtaminen, kansainvälinen toiminta, Suomen puolustuskyky, sisäinen turvallisuus, talouden ja infrastruktuurin toimivuus, väestön toimeentuloturva ja toimintakyky sekä henkinen kriisinkestävyys.

talinjojen johdosta. Poliisitoiminnan osalta myös Yhteiskunnan turvallisuusstrategiassa on nostettu esiin poliisin ja muiden lainvalvonta- ja tutkintaviranomaisten toimintakyvyn sekä perustuslain mukaisen oikeusvaltion toiminnan turvaamisen edellytykset. Yleisen järjestyksen ja turvallisuuden ylläpitämisellä suojataan osaltaan yhteiskunnan keskeinen infrastruktuuri, ennalta estetään ja torjutaan terrorismi sekä järjestäytynyt ja muu vakava rikollisuus sekä vakavat häiriöt. Sattuneiden vakavien onnettomuuksien ja muiden poikkeuksellisten tapahtumien itsenäisellä ja riippumattomalla turvallisuustutkinnalla tuetaan vastaavien tapahtumien mahdollisimman tehokasta ennaltaehkäisyä. Sisäisen turvallisuuden ylläpitämisessä korostuu toimivaltaisten viranomaisten operatiivinen toiminta, johon lainsäädäntö antaa hyvät edellytykset. Tiivis yhteistyö muiden viranomaisten ja muiden toimijoiden kesken kaikilla hallinnon tasoilla tukee tätä työtä. (Yhteiskunnan turvallisuusstrategia, 27)

Kansallisessa kyberstrategiassa on määritelty **Suomen kyberturvallisuusvisio** (kaavio sivulla 51): 1) Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan, 2) Kansalaisilla, viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti sekä 3) Vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa. (Kansallinen kyberturvallisuusstrategia, 3)

KUVIO 2: Suomen kyberturvallisuuden visio (kaavio)

Kyberturvallisuusstrategia koostuu kymmenestä strategisesta linjauksesta. Poliisin osalta yksi keskeinen toimintalinja on kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi luotava viranomaisten ja muiden toimijoiden välinen tehokas yhteistoimintamalli, jonka tavoitteena on jaettu tilannetietoisuus ja tehokas uhkien torjunta. Viranomaisten ja yksityisen sektorin toimijoiden on omien harjoitustensa avulla kehittävä valmiuttaan toimia elintärkeiden toimintojen häiriötilanteita varten. Toimijat parantavat kansainvälisissä harjoituksissa parhaiden käytänteiden ja saatujen oppien hyödyntämistä tehostamalla tiedonvaihtoa ja koordinaatiota. Harjoitustoiminnan tavoitteena on parantaa osallistujien mahdollisuuksia havaita oman toimintansa ja järjestelmiensä haavoittuvuuksia, kehittää suorituskykyjään ja kouluttaa henkilöstöään. Tehokas kyberuhkien torjuminen edellyttää tiedonvaihtoa viranomaisten ja elinkeinoelämän kesken, jonka edistämiseksi kehitetään sääntelyä ja yhteistyötä. (Kansallinen kyberturvallisuusstrategia, 7)

Kokonaisvaltaisen kyberturvallisuuden tilannetietoisuuden ja tilanneymmärryksen parantaminen yhteiskunnan elintärkeiden toimintojen turvaamiseen osallistuvien keskeisten toimijoiden välillä on poliisitoiminnan kannalta toinen keskeinen toimintalinjaus. Linjauksella tavoitellaan eri toimijoiden tilannetietoisuuden parantamista tarjoamalla niille ajantasaista, koottua ja analysoitua tietoa haavoittuvuuksista, häiriöistä ja niiden vaikutuksista. Tämä sisältää myös kybertoimintaympäristöstä aiheutuvien uhkien arviot ja ennusteet. Näiden kyberuhkien ennakointi edellyttää poliittisen, sotilaallisen, sosiaalisen, kulttuurisen, teknisen ja teknologisen sekä taloudellisen tilanteen arviointia. Linjauksessa edellytetään perustettavan käytännön toimijaksi Viestintävirastoon Kyberturvallisuuskeskus yhdistetyn kyberturvallisuuden tilannekuvan tuottamiseksi ja ylläpitämiseksi. Tilannekuvan pohjalta eri toimijoiden tulee arvioida häiriön vaikutuksia oman tahonsa toimintaan. Tilannekuva välitetään Valtioneuvoston tilannekeskukseen, jolla tulee olla käytettävissään luotettava, kattava ja ajantasainen kokonaistilannearvio kyberturvallisuudesta. Tällä tavoin Valtionjohdolla on käytettävissään kokonaistilannearvio sekä arvio muun toimintaympäristön kehityksestä päätöksenteon pohjaksi. (Kansallinen kyberturvallisuusstrategia, 7)

Poliisin osalta strategiassa huolehditaan siitä, että poliisilla tulee olla tehokkaat edellytykset ennalta ehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia. Poliisi on rikosten esitutkintaviranomaisena kybertoimintaympäristöön kohdistuvien ja sitä hyödyntävien rikosten keskeinen toimija. Poliisin on koottava analysoitu ja korkealaatuinen tilannekuva yhteistyössä Kyberturvallisuuskeskuksen kanssa kyberrikollisuudesta ja jaettava se osaksi edellä mainittua yhdistettyä tilannekuvaa. Se edellyttää, että poliisilla tulee olla riittävät toimivaltuudet, resurssit sekä osaava ja motivoitunut henkilöstö, joka hoitaa kybertoimintaympäristöön kohdistuvien ja sitä hyödyntävien rikosten ennaltaehkäisemisen, taktisen esitutkinnan sekä digitaalisen todistusaineiston käsittelyn ja analysoinnin. Kansainvälinen operatiivinen yhteistyö ja tiedonvaihto EU:n ja muiden maiden lainvalvontaviranomaisten ja vastaavien toimijoiden (muun muassa Europol) on keskeinen kehitettävä painopistealue. (Kansallinen kyberturvallisuusstrategia, 8)

Kyberturvallisuuden globaalisuus tulee esille linjauksessa, jossa edellytetään vahvistettavan kansallista kyberturvallisuutta osallistumalla aktiivisesti ja tehokkaasti kyberturvallisuuden kannalta keskeisten kansainvälisten organisaatioiden ja yhteistyöfoorumeiden toimintaan. Kansainvälisen yhteistoiminnan tavoitteena on vaihtaa tietoja ja kokemuksia sekä oppia parhaista käytännöistä, jotta kansallisen kyberturvallisuuden tasoa voidaan kohottaa, joka on ehdoton edellytys tehokkaalle, järjestelmälliselle ja koordinoidulle kansainväliselle yhteistyölle. Poliisi osaltaan velvoitetaan omalla toimialallaan harjoittamaan yhteistyötä erityisesti niiden valtioiden ja organisaatioiden kanssa, jotka ovat maailmanlaajuisesti edelläkävijöitä kyberturvallisuuteen liittyvissä asiakokonaisuuksissa. Keinoina ovat muun muassa aktiivinen yhteistyö tutkimus- ja kehittämis- sekä erilaisten sopimusten valmistelutyössä, organisaatioiden työryhmätyöskentelyssä sekä kansainvälinen harjoitustoiminta. (Kansallinen kyberturvallisuusstrategia, 9)

Poliisitoiminnan kannalta mielenkiintoinen ja erityisesti tietoverkkotiedusteluun liittyen on linjaus kansallisesta lainsäädännöstä, jolla varmistetaan tehokkaan kyberturvallisuuden toteuttamisen edellytykset. Tavoitteena on kartoittaa kybertoimintaympäristöön ja -turvallisuuteen vaikuttava ja liittyvä lainsäädäntö sekä sen kehittämistarpeet hallinnonalojen ja elinkeinoelämän yhteistyönä. Sen pohjalta tehdään kehittämisehdotukset, joilla edistetään kyberturvallisuusstrategian mukaisten tavoitteiden toteutumista tarkoituksenaan se, että lainsäädäntö antaisi mahdollisuuden sekä riittävät keinot ja toimivaltuudet eri alojen toimivaltaisille viranomaisille sekä muille toimijoille toteuttaa yhteiskunnan elintärkeiden toimintojen ja erityisesti valtion turvallisuuden suojaamista kyberuhkia vastaan.

Tarkastelun kohteeksi tavoitteena on ottaa ne esteet ja rajoitteet sekä tiedon käsittelyä koskevat velvoitteet, jotka haittaavat kyberuhkien tehokkaaksi torjumiseksi tarvittavan tiedon saamista, luovuttamista ja vaihtamista eri viranomaisten ja muiden toimijoiden välillä. Tarkastelussa arvioitaisiin lisäksi sitä, tulisiko vastuuviranomaisille luoda nykyistä paremmat mahdollisuudet ennalta kerätä, koota ja saada tietoa kyberuhista ja niiden aiheuttajista kiin-

nittämällä samalla huomiota perusoikeuksina olemassa oleviin yksityisyyden suojaan ja luottamuksellisen viestin suojaan.

Linjauksessa tuodaan esiin yksityisen sektorin merkitys yhteiskunnan kriittisen infrastruktuurista ylläpitoon ja turvaamiseen. Yritykset toteuttavat suurelta osin kyberkyvykkyyden, osaamisen sekä palveluiden luomisen ja suojaamisen. Kybertoimintaympäristöä säätelevän kansallisen lainsäädännön tulee olla sellaista, että liiketoiminnan kehittämiselle on olemassa suotuisat edellytykset. Tämä mahdollistaa osaltaan kansainvälisesti tunnustetun, kilpailukykyisen ja vientimahdollisuudet omaavan kyberosaamisklusterin syntymisen. Samalla Suomesta kehittyy houkutteleva kyberturvallinen toimintaympäristö, johon kannattaa tehdä investointeja ja yritysten toimintojen sijoituspäätöksiä. (Kansallinen kyberturvallisuusstrategia, 10)

Poliisitoiminnan kannalta edellä mainitut tavoitteet sisältävät haasteen poliisin suorittamalle tiedonhankinnalle tietoverkoista. Vastakkain ovat kaksi eri intressitahoa. Toinen suojattava intressi on viranomaistoiminnan tehokkuus ja toisena on yksityisen sektorin liiketoiminnan tarvitsema yksityisyyden suoja, joka edistää kilpailukykyä ja turvaa yrityssalaisuutta. Vastakkain ovat siis viranomaistoiminta ja taloudellisen seikkojen suojaaminen ja sen ohessa yksityisyyden suoja. Kyse on tyypillisestä intressipunninnasta, kuinka paljon viranomaistoiminnalla voidaan puuttua yksityisyyden suojaan tavoiteltaessa yhteiskunnan turvallisuutta. Tämä on viime aikoina aiheuttanut muun muassa voimakasta keskustelua julkisuudessa eri medioissa.

Edellä mainittu viranomaistoiminnan ja kansalaisen yksityisyydensuoja vastakkainasettelu ovat olleet viime aikoina muun muassa lehtien otsikoissa. Poliisin ja Puolustusvoimien kansainvälisen tiedustelutoiminnan valtuuksia ja verkkovalvontaa pohtinut puolustusministeriön asettama työryhmä[36] on ehdottanut Suomeen tietoverkoissa tapahtuvaa tiedustelua koskevaa lainsäädäntöä, jota tällä hetkellä ei ole.

[36] Suomalaisen tiedustelulainsäädännön suuntaviivoja, Tiedonhankintalakityöryhmän mietintö 14.1.2015

Liikenne- ja viestintäministeriö on jättänyt eriävän mielipiteen työryhmän mietintöön, koska se vastustaa tietoverkkoliikenteen massavalvontaa. Sen mukaan tietoverkkovalvonta puuttuu kansalaisten perusoikeuksiin kuuluvaan yksityisyyden suojaan, sillä tiedustelun piirissä olisivat tahtomattaan kaikki Suomessa viestivät, myös viranomaiset, poliittiset toimijat, media ja yritykset. Kyseinen työryhmä on myös todennut, että verkkovalvonta edellyttäisi perustuslain muuttamista. Työryhmän mukaan tiedustelulla hankittaisiin Suomen ylimmälle johdolle kansallisen turvallisuuden kannalta välttämätöntä tietoa vakavista kansainvälisistä uhista. Uhat voisivat olla joko sotilaallisia tai siviililuontoisia.

Kannanotoissa on kyse myös poliittisista valinnoista: osallistuuko Suomi tiedustelulainsäädännöllä kybermaailman kilpavarusteluun vai etsitäänkö kilpailuetua siitä, että Suomi profiloituisi tietosuojan Sveitsiksi. Liikenne- ja viestintävirasto on tuonut esiin huolensa siitä, mitä vaikutuksia verkkovalvonnalla voi olla yritystoimintaan ja siihen, houkutteleeko Suomi esimerkiksi isoja konesali-investointeja. (Helsingin sanomat 11.1.2015 ja 13.1.2015)

Vielä yhtenä poliisitoimintaan vaikuttavana linjauksena strategiassa määritellään viranomaisille ja elinkeinoelämän toimijoille kyberturvallisuutta koskevat tehtävät ja palvelumallit sekä yhteiset perusteet kyberturvallisuuden vaatimusten hallinnalle. Kyberturvallisuuden kehittäminen vaatii selkeää vastuiden määrittelyä ja tehtävien jakoa strategisten linjausten mukaisesti. Käytännössä tämä edellyttää, että poliisissakin tehdään riskiarviointi ja kypsyysanalyysi, joiden avulla tunnistetaan kyberturvallisuuden kannalta merkittävät haavoittuvuudet ja riskit sekä niiden hallinnan taso. Saatujen tulosten perusteella laaditaan kunkin hallinnonalan toimeenpano-ohjelmat sekä tuetaan elinkeinoelämän toimeenpano-ohjelmien tekemistä yhteistoiminnassa huoltovarmuusorganisaation kanssa. (Kansallinen kyberturvallisuusstrategia, 10)

Kansallisessa kyberturvallisuusstrategiassa ministeriöt, virastot ja laitokset velvoitetaan sisällyttävän kyberturvallisuusstrategian toimeenpanon edellyttämät voimavarat omiin toiminta- ja taloussuunnitelmiinsa. Poliisin osalta

Kyberturvallisuusstrategiassa tai sen taustamuistiot jäävät ilman konkreettisia toimenpide-esityksiä. Siinä ei mainita, kuinka poliisitoiminta osaltaan huolehtii strategiassa viranomaisille annetuista vastuista ja tehtävistä, mitä rikosten ennalta estäminen ja paljastaminen kybermaailmassa tarkoittavat. (Leppänen & Kankaanranta, 65–66)

Valtioneuvoston periaatepäätös järjestäytyneen rikollisuuden torjunnan strategiasta

Pääministeri Jyrki Kataisen hallituksen hallitusohjelmaan vuosille 2001–2014 kirjattiin tarve tehostaa järjestäytyneen rikollisuuden torjuntaa sekä selvittää siihen liittyvän uuden erityislain tarve. Hallitusohjelmassa oli painopisteenä myös tietoverkkorikollisuuden torjunta osana järjestäytyneen rikollisuuden torjuntaa. Järjestäytyneen rikollisuuden torjuntastrategian tavoitteena on heikentää ja ennalta estää järjestäytyneen rikollisuuden toimintaedellytyksiä siten, että järjestäytynyt rikollisuus vähentyisi, eikä ilmiönä kehittyisi vakavampaan suuntaan. Erityisenä tavoitteena on estää järjestäytyneen rikollisuuden haitallista vaikutusta yhteiskunnan toimintaan, estää rikollisten järjestäytymistä ja korostaa sitä, että järjestäytyneeseen rikollisuuteen liittyvään toimintaan osallistuminen ei ole houkutteleva vaihtoehto. (Valtioneuvoston periaatepäätös järjestäytyneen rikollisuuden torjunnan strategiasta 2013, 3-4)

Järjestäytyneen rikollisuuden torjunnan strategiset linjauksina päätökseen on kirjattu muun muassa välttämätön tarve ottaa käyttöön uusia torjuntamenetelmiä, kuten hallinnollisten keinojen tehokas käyttö rikosten torjunnassa sekä tiivis yhteistyö viranomaisten ja yksityisen sektorin kanssa. Päätösasiakirja sisältää velvoitteen eri ministeriöille ryhtyä toimiin päätökseen kirjattujen 20 toimenpiteen osalta. (Valtioneuvoston periaatepäätös järjestäytyneen rikollisuuden torjunnan strategiasta 2013, 7)

Päätökseen on kirjattu toimenpide numero 17, jossa tietoverkkoja hyödyntävän rikollisuuden torjuntaan osana järjestäytyneen rikollisuuden torjuntaa tulee panostaa. Toimenpiteenä edellytetään selvittää tietoverkkorikollisuu-

den torjuntastrategian tarve Suomen kyberturvallisuusstrategian ja sen toimeenpano-ohjelman pohjalta sekä huolehtia siitä, että verkossa toimivat henkilöt pystyvät helposti ilmoittamaan rikolliseen toimintaan viittaavat tahot poliisille. Toimenpide edellyttää arviointia mahdollisuuksista, joilla viranomaiset voisivat torjua anonyymiverkoissa esiintyvää rikollisuutta. (Valtioneuvoston periaatepäätös järjestäytyneen rikollisuuden torjunnan strategiasta 2013, 10)

Tietoyhteiskuntakaari

Jäätteenmäen hallitusohjelmaan tehtyjen kirjausten johdosta vuonna 2015 astui voimaan Tietoyhteiskuntakaari – niminen lainsäädäntö, jonne on koottu keskeiset sähköistä viestintää koskevat säädökset. Lainsäädännön valmistelun yhteydessä Sisäasianministeriö ja Poliisihallitus korostivat teleyritysten ja viranomaisten välistä kulujen tasaamista aiemmasta voimassa olleesta tulkinnasta poiketen. Aiemmin viranomaiset joutuivat korvaamaan niin tekniset järjestelmät, laitteistot sekä ohjelmistot kuin tietokyselyistä aiheutuneet kustannukset.

Yhtenä keskeisenä seikkana Sisäasiainministeriö painotti lakiin kirjattavaksi selkeästi sen, että tiedonsaantipyyntöjä tarvitaan erityisesti rikosten tutkinnassa, ehkäisemisessä ja paljastamisessa. Edellä mainitut käyttötarpeet nähtiin tärkeinä kirjattavaksi selkeästi uuteen lakiin. Erityisesti ennalta estäminen ja rikosten ehkäiseminen nähtiin tärkeäksi, koska aiemmin rikosten ehkäisemiseen liittyen tiedonsaantipyyntöjen tulkinnassa oli ollut epäselvyyksiä teleoperaattoreiden ja poliisin välillä.

Edellä mainitut Sisäasiainministeriön ja Poliisihallituksen painotukset kirjattiin Tietoyhteiskuntakaareen seuraavasti. Tietoyhteiskuntakaaren 40 luvun 322 pykälässä on eräiden muiden viranomaisten tiedonsaantioikeudesta mainittu seuraavasti: ”Viranomaisten oikeudesta saada välitystietoja rikosten ennalta estämiseksi, paljastamiseksi tai selvittämiseksi säädetään poliisilaissa, rajavartiolaissa (578/2005), henkilötietojen käsittelystä rajavartiolaitoksessa annetussa laissa (579/2005), tullilaissa (1466/1994) ja pakkokeino-

laissa. Edellä 157 §:n perusteella säilytettäviä tietoja voivat saada säilytysvelvollisilta yrityksiltä ainoastaan ne viranomaiset, joilla on lain perusteella oikeus saada tiedot.”

Saman luvun 323 pykälään on kirjattu viranomaisen määräämän toimenpiteen ja tiedon luovutuksen maksuttomuus. ”Teleyrityksen on korvauksetta luovutettava viranomaiselle sellainen hallussaan oleva tieto: 1) joka on tarpeellinen laissa yleisen järjestyksen ja turvallisuuden ylläpitämiseksi, rikosten selvittämiseksi, paljastamiseksi tai estämiseksi taikka pelastustoiminnan ylläpitämiseksi säädetyn tehtävän suorittamisessa; ja 2) jonka saamiseen viranomaisella on erikseen säädetty oikeus. Teleyrityksen on tehtävä korvauksetta viranomaisen laissa säädetyn telekuunteluoikeuden mahdollistava toimenpide. Henkeä ja terveyttä välittömästi uhkaavissa tilanteissa tiedon luovuttaminen tai toimenpide on toteutettava kiireellisenä. Viranomainen toteuttaa kustannuksellaan järjestelmän, jolla se voi vastaanottaa ja käsitellä 1 momentissa tarkoitettuja tietoja tai toteuttaa 2 momentissa tarkoitetun telekuuntelun. Viranomainen vastaa myös viranomaisen järjestelmän yleiseen viestintäverkkoon ja -palveluun liittämisestä aiheutuneista kustannuksista. Teleyrityksen on kuitenkin toteutettava hätäliikenteen ohjausmuutokset maksutta. Viestintävirasto voi antaa tarkempia määräyksiä 1 ja 2 momentissa mainittujen toimenpiteiden ja tietopyyntöjen toteuttamisesta ja määräajoista.”

Edellä olevassa viitataan Tietoyhteiskuntakaaren 157 pykälään: ”Sen estämättä, mitä tässä osassa säädetään välitystietojen käsittelystä, sisäministeriön päätöksellään erikseen nimeämän teletoimintailmoituksen antaneen yrityksen (säilytysvelvollinen yritys) on huolehdittava jäljempänä säädetyin edellytyksin, että säilytysvelvollisuuden piiriin 2 ja 3 momentin mukaisesti kuuluvat tiedot säilytetään 4 momentissa säädettyjen säilytysaikojen mukaisesti. Säilytettäviä tietoja saa käyttää ainoastaan pakkokeinolain (806/2011) 10 luvun 6 §:n 2 momentissa tarkoitettujen rikosten selvittämiseksi ja syyteharkintaan saattamiseksi.

Säilytysvelvollisuus koskee tietoja, jotka liittyvät: 1) säilytysvelvollisen yrityksen tarjoamaan matkaviestinverkon puhelinpalveluun tai tekstiviestipalveluun mukaan lukien puhelut, joissa yhteys on saatu muodostettua, mutta puheluun ei vastattu tai puhelu on estynyt verkonhallintatoimenpiteestä johtuen; 2) säilytysvelvollisen yrityksen tarjoamaan internetpuhelinpalveluun, jolla tarkoitetaan palveluyrityksen tarjoamaa loppuasiakkaille asti internetyhteyskäytäntöön perustuvaa puhelun mahdollistavaa palvelua; 3) säilytysvelvollisen yrityksen tarjoamaan internetyhteyspalveluun.

Pykälään kirjattu velvoite, säilytettäviä tietoja saa käyttää ainoastaan pakkokeinolain (806/2011) 10 luvun 6 §:n 2 momentissa tarkoitettujen rikosten selvittämiseksi ja syyteharkintaan saattamiseksi, on osin ristiriidassa pykälän 322 kanssa. Nykyinen kirjaus ei huomioi rikosten ennalta estämistä tai paljastamista, mutta mikä näiden kirjausten tulkinta tulee jatkossa olemaan, jää nähtäväksi.

Suomalaisen tiedustelulainsäädännön suuntaviivoja

Puolustusministeriö asetti 13.12.2013 työryhmän kehittämään lainsäädäntöä turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista. Työryhmä toimi 31.12.2014 saakka ja sen tehtävänä oli arvioida Suomen lainsäädännön kehittämistarvetta siten, että Suomessa kyetään huolehtimaan kansallisesta turvallisuudesta tietoverkoissa esiintyvien uhkien torjumiseksi. Tehtävänä oli lisäksi koota yhteen näkemyksiä tietoverkkojen kautta Suomen turvallisuuteen kohdistuvista uhkista ja niiden vaikutuksista Suomen turvallisuudelle ja kilpailukyvylle, selvittää turvallisuusviranomaisten tiedonhankintaa koskeva nykytila ja kehittämisehdotukset, tarkastella tarvittavilta osin turvallisuusviranomaisten tiedonhankintaa koskevaa lainsäädäntöä eräissä muissa maissa, tuottaa vaikutusarviointi eri kehittämisvaihtoehdoista ja selvitetyn pohjalta tehdä lainsäädännön kehittämisehdotukset sekä esitys niiden toimeenpanon edellyttämistä toimista. (Suomalaisen tiedustelulainsäädännön suuntaviivoja, 7)

Työryhmä pääosin on käsitellyt tiedustelua tietoliikennetiedustelun näkökulmasta, joka on verkkovalvontaa. Verkkovalvonnasta käytetään myös nimitystä massavalvonta, sillä siinä on kyse teknisestä pääsystä kaikkeen tietoliikenteeseen. Työryhmätarkastelu ei siis koskenut tavanomaisena pidettävää verkkorikollisuuden torjuntaa, vaan se tarkasteli kansalliseen turvallisuuteen kohdistuvien vakavien uhkien havaitsemista ja tunnistamista sekä niiden torjunnan mahdollistamista. Tietoliikennetiedustelu voi yleisesti kohdistua valtion sisäiseen tai rajat ylittävään tietoliikenteeseen. Toiminnan toteuttaminen edellyttää, että tiedusteluviranomaisella on pääsy tietoliikennekaapeleiden liityntäpisteisiin. Tyypillisesti tiedustelutiedon hankintaa suunnataan tietoliikennettä seulovien automatisoitujen hakuehtojen avulla.

Työryhmä on kirjannut harkittavaksi, että hallitus käynnistäisi tarvittavat toimenpiteet tiedustelua koskevan säädösperustan luomiseksi. Tietoliikennetiedustelua koskevan lainsäädännön valmistelua harkittaessa on erityisesti otettava huomioon jokaiselle perus- ja ihmisoikeutena turvattu luottamuksellisen viestin salaisuuden suoja. Työryhmän mukaan tiedustelun tarkoituksena olisi hankkia kansallisen turvallisuuden kannalta välttämätöntä tietoa vakavista joko sotilaallisista tai siviililuontoisista kansainvälisistä uhista. Tiedustelu tukisi valtion ylimmän johdon päätöksentekoa, jotta se perustuisi oikeaan, ajantasaiseen ja luotettavaan tietoon. Työryhmän mietinnössä todetaan, että tietoliikennetiedustelun tekninen suorittaminen olisi tarkoituksenmukaista keskittää yhdelle viranomaiselle. Puolustusvoimille ja Suojelupoliisille tulisi harkita toimivaltuuksia ulkomaan tiedusteluun, jossa hankittaisiin tietoja henkilöiltä ja tietojärjestelmistä. (Suomalaisen tiedustelulainsäädännön suuntaviivoja, 1, 50, 80)

Mietinnössä lainsäädännön tarpeellisuutta on tarkasteltu suurelta osin Puolustusvoimien ja Suojelupoliisin toiminnan lähtökohdista, joka on yhteiskunnallisesti ja kansallisen turvallisuuden kannalta erittäin tärkeä. Kansallisen turvallisuuden turvaaminen valtion rajojen ulkopuolelta suuntautuvaa uhkaa vastaan laajan turvallisuuskäsityksen mukaan pitää sisällään myös kansainväliseltä ja järjestäytyneeltä rikollisuudelta suojautumisen eli sen torjumisen.

Mietinnön lähtökohtana on ollut tietoliikennetiedustelu, joka on verkkovalvontaa, josta voidaan käyttää myös nimitystä massavalvonta, koska kyse on teknisestä pääsystä kaikkeen tietoliikenteeseen. Tällöin verkkovalvonta kohdistuisi käytännössä kaikkeen tietoliikenteeseen. Mietinnössä ei ole otettu huomioon lainsäädäntöä, joka määrittelisi selkeämmin kohdennetun tietoverkoissa tapahtuvan tiedonhankinnan, joka poliisitoiminnan kannalta olisi tärkeää. Suomessa ilmenevä etenkin vakava rikollisuus on entistä enemmän kansainvälisiä yhteyksiä sisältävää, jossa tietoverkkoja joko käytetään rikoksentekovälineenä tai niitä hyödynnetään rikosten suunnittelussa tai rikollisten välisessä yhteydenpidossa. Koska vakava ja järjestäytynyt rikollisuus on lähes pelkästään piilorikollisuutta[37], sen paljastaminen edellyttää riittäviä toimivaltuuksia ja sääntelyä toiminnasta.

Kansallisen kyberturvallisuuden toimeenpano-ohjelma

Kansallisessa 24.1.2013 annetussa Kyberturvallisuusstrategiassa edellytettiin, että sen pohjalta laaditaan kansallinen kyberturvallisuuden toimeenpano-ohjelma[38]. Ohjelmassa esitetään keskeisimmät toimenpiteet strategiassa asetettujen tavoitteiden saavuttamiseksi: kyberturvallisuuskeskuksen toiminnan kehittäminen, valtion ympärivuorokautinen tietoturvatoiminta, salatun tiedonsiirron ja hallinnon turvallisuusverkon palveluintegraatiohanke, poliisin toimintakyky kyberrikollisuuden torjunnassa, kybertoimintaympäristöön ja – turvallisuuteen liittyvän lainsäädännön kehittäminen sekä tutkimus- ja koulutusohjelmat ja muu osaamisen vahvistaminen. Toimeenpano-ohjelmassa on yhteensä 74 toimenpidettä kyberturvallisuuden parantamiseksi, jotka on koottu hallinnonalojen ja huoltovarmuusorganisaation esityksistä. (Kansallisen kyberturvallisuuden toimeenpano-ohjelma, 2)

Poliisin osalta toimeenpano-ohjelmassa mainitaan rikostorjunnan kyberosaamisen kehittäminen, esitutkintaviranomaisen toimivaltuuksien selvittäminen kyberrikostorjunnassa, tietoverkkorikososaamisen liittäminen polii-

[37] Rikollisuus, joka ei tule poliisin tietoon ja jota siten ei rikoksina rekisteröidä.(Tilastokeskus 2015)

[38] Kansallisen kyberstrategian toimeenpano-ohjelma, Turvallisuuskomitea, 194/8.1.99/2013, 11.3.2014

sin 24/7 yhteyspisteeseen ja kansainvälisten palveluiden turvaaminen, kyberrikostilannekuvan ja – tiedonhankinnan kehittäminen sekä kyberrikostutkinnan järjestäminen ja resursointi. (Kansallisen kyberturvallisuuden toimeenpano-ohjelma, 18–22)

Kyberturvallisuuden toimeenpano-ohjelma sisältää laajan eri hallinnon aloja koskevan osaltaan yksityiskohtiin menevän yhteenvedon Kansallisen kyberturvallisuusstrategian jalkauttamiseksi.

Sisäministeriön ja poliisihallinnon ohjausasiakirjat

Tietotekniikkatutkinnan järjestäminen poliisissa

Sisäasiaministeriön poliisiosasto asetti työryhmän pohtimaan tietotekniikkatutkinnan järjestämistä ja laadun varmistamista ajalle 1.1.–31.12.2008, joka antoi loppuraporttinsa[39] 16.12.2008. Työryhmän tavoitteena oli tehdä ehdotus tietotekniikkatutkinnan järjestämisestä poliisin hallintorakenteen uudistamisen yhteydessä ja erityisesti tukea uusia poliisilaitoksia toimintoja järjestäessään. Ehdotusten tavoitteena oli, että tietotekniikkatutkinnan toiminnot järjestettäisiin mahdollisimman yhdenmukaisesti koko valtakunnassa. (Tietotekniikkatutkinnan järjestäminen poliisissa, loppuraportti, 2)

Työryhmän keskeiset ehdotukset liittyivät tietotekniikkatutkinnan organisatoriseen järjestämiseen, resursseihin, eri yksiköiden väliseen tehtävienjakoon, laatujärjestelmään sekä tietotekniikan käsitteisiin. Työryhmä käsitteli myös tietoverkkotiedustelua ja sen järjestämistä valtakunnan tasolla. Työryhmän näkemyksen mukaan poliisin tietotekniikkatutkinnan perustoimintojen organisointi ja resursointi tulisi olla ensisijainen tehtävä, ennen erityistoimintojen järjestämistä. (Tietotekniikkatutkinnan järjestäminen poliisissa, loppuraportti, 2)

Työryhmä esitti, että tietotekniikkatutkinnan palvelu tulisi muodostaa jokaiseen poliisilaitokseen ja resurssien niin vaatiessa alkuvaiheessa väliaikaises-

[39] Tietotekniikkatutkinnan järjestäminen poliisissa, loppuraportti, Poliisin ylijohdon julkaisusarja 7/2008

ti kahden tai useamman poliisilaitoksen yhteistoimintona. Toiminnolla tulisi olla asiantuntijuusstatus, sen tulisi olla päätoimista ja sen tulisi työskennellä yhden johdon alla. Lisäksi työryhmä esitti perustettavaksi tietotekniikkatutkinnan poliisin ylijohtoon sijoitettavan ohjausryhmän, jossa edustettuina olisivat ainakin poliisin ylijohto / poliisihallitus, keskusrikospoliisi, poliisiammattikorkeakoulu ja paikallispoliisi. Ohjausryhmän tehtävänä olisi työryhmän mukaan valvoa ja ohjata kansallista tietotekniikkatutkinnan järjestämistä, kehittämistä sekä laadunvalvontaa ja koulutusta asetettujen tavoitteiden saavuttamiseksi sekä ohjata laajalti koko tietotekniikkatutkinnan kehittämistä. (Tietotekniikkatutkinnan järjestäminen poliisissa, loppuraportti, 19–20, 23)

Työryhmän loppuraporttiin on kirjattu myös Keskusrikospoliisin ja paikallispoliisin tehtävät ja roolit tietotekniikkatutkinnan osalta, jossa kysymys oli lähinnä tietoverkkorikosten tutkinnasta. Suojelupoliisi nähtiin yhdeksi toimijaksi tietoverkkorikollisuuden kokonaistorjunnassa, mutta muuten Suojelupoliisia ei raportissa käsitellä. (Tietotekniikkatutkinnan järjestäminen poliisissa, loppuraportti, 30)

Raportti käsittelee ainoastaan poliisin tietoverkkorikosten tutkintaa ja siihen liittyviä järjestelyjä, tiedustelusta raporttiin ei ole kirjattu käytännössä mitään.

Järjestäytyneen rikollisuuden ja terrorismin torjunta

Pääministeri Matti Vanhasen toisen hallitusohjelman sisäiseen turvallisuuden ohjelmaan sisältyi muun muassa järjestäytyneen rikollisuuden ja terrorismin torjuntaan liittyvä työryhmäraportti[40]. Raportin laatineelle asiantuntijatyöryhmälle annettiin tehtäväksi valmistella poikkihallinnolliset strategiset linjaukset, tiivis nykytilan kuvaus sekä tavoitteet, toimenpiteet ja mittarit järjestäytyneen rikollisuuden ja terrorismin torjumiseksi ottaen huomioon

[40] Järjestäytyneen rikollisuuden ja terrorismin torjunta, Sisäisen turvallisuuden ohjelman valmisteluun osallistuneen asiantuntijaryhmän loppuraportti, Sisäasiainministeriö, 31.3.2008

keskeiset kansalliset ja kansainväliset kehityssuunnat ja uhka-arviot. Työryhmän tehtävänä oli myös arvioida yhteistyörakenteita ja resursseja sekä sen tuli laatia aihealueeltaan torjunnan tehostamiseen liittyviä toimenpide-ehdotuksia. Asiantuntijatyöryhmän raportissa tietoverkkorikollisuuden torjunnan osalta painopistealueeksi on linjattu yhteistyökulttuurin kehittäminen, yhteistyön esteiden poistaminen sekä piilorikollisuuden paljastaminen. (Järjestäytyneen rikollisuuden ja terrorismin torjunta, loppuraportti, 4-5)

Raporttiin on kuvattu yksityiskohtaiset toimenpide-ehdotukset tietoverkkorikollisuuden ja Internetin käyttöön liittyvien riskien ja uhkien torjumiseksi. Lainsäädännön kehittäminen on kirjattu yhdeksi toimenpide-ehdotukseksi. Raportissa on mainittu esteiksi tehokkaalle rikostorjunnalle lainsäädännölliset esteet, ilmiöiden tunnistaminen, toimintamallien ja vastuiden epäselvyys, yritysten kokema maineriski sekä Identiteettivarkauksiin liittyvät ilmiöt. (Järjestäytyneen rikollisuuden ja terrorismin torjunta, loppuraportti, 75)

Toisena kohtana raportissa mainitaan tietoverkkorikostorjunnan toiminta-edellytysten parantaminen vahvistamalla verkkovalvontaa ja -tarkkailua suorittavaa kansallista yksikköä ja tekemällä yhteistyötä muiden lainvalvontaviranomaisten kanssa. Raportin mukaan paljastettujen tietoverkkorikosten tutkintaresurssit tulisi turvata sekä tietoverkkorikostorjunnan ja verkkorikollisuuteen liittyvien ilmiöiden tunnistamisen tulisi perustua ajantasaiseen valvontaan ja reaaliaikaisen tiedon hyödyntämiseen, jotta torjuntatoimenpiteet voitaisiin kohdentaa oikea-aikaisesti ja tekojen haittavaikutukset kyettäisiin minimoimaan. (Järjestäytyneen rikollisuuden ja terrorismin torjunta, loppuraportti, 75–76)

Raportti kiinnittää huomiota kansalaisten mahdollisuuteen ilmoittaa viranomaisille epäillystä tai todetuista verkkoon kohdistuvista uhista, verkkoa hyväksikäyttävistä rikoksista tai muusta epäilyttävästä materiaalista. Tietoverkkorikostorjuntaa suorittavien viranomaisten riittävän ammatillisen osaamisen ylläpitämiseksi, kehittämiseksi ja laadukkaan tutkinnan varmistamiseksi tulisi viranomaisten sisällyttää ammatilliseen perus- ja jatkokoulutukseen tietotekniikkarikollisuutta käsitteleviä opintoja. Viranomaisten tulisi

järjestää myös erikoistumiskoulutusta, jotta lainvalvontaviranomaisilla olisi edellytykset vaikeiden ja laajojen tietotekniikkarikosten torjumiseksi, tutkimiseksi, syyteharkintaan saattamiseksi ja kansainväliseen yhteistyöhön. (Järjestäytyneen rikollisuuden ja terrorismin torjunta, loppuraportti, 77)

Vakavien tietoverkkorikosten torjunnan järjestäminen

Poliisihallitus on antanut 23.9.2013 määräyksen vakavien tietoverkkorikosten ja verkon kautta tapahtuvien rikosten tehokkaaseen ennalta estämiseen, paljastamiseen ja tutkintaan sekä vakaviin verkkorikosuhkiin liittyvään nopeaan reagointikyvyn varmistamiseen[41]. Määräys on turvaluokiteltu, ei julkinen asiakirja, joten sitä ei tässä tutkimuksessa käsitellä.

Poliisin kybertoimivaltuudet

Poliisihallitus asetti 25.3.2015 poliisin kybertyöryhmän[42], jonka tuli laatia yhteenveto ja kuvaus keskeisistä poliisin kybertoimintaympäristön toimivaltuustarpeista ja -muutoksista. Kyberturvallisuusstrategian toimeenpanosta ja tehtävistä annetussa sisäministeriön suunnitelmassa (SMDno/2013/901) edellytetään, että sisäministeriön hallinnonalan viranomaiset turvaavat valvonta- ja tilannekuvan muodostuskyvyn, johtamisen ja viranomaisyhteistyön sekä laissa määriteltyjen tehtäviensä kannalta välttämättömien tietoliikenne- ja tietojärjestelmien toiminnan kaikissa olosuhteissa kaikissa strategisissa tehtävissä. Raportti käsittelee tärkeimpiä toimivaltuustarpeita, jotka ovat poliisin ydintehtävien kannalta keskeisiä erityisesti tietoverkoissa tapahtuvien sekä niitä hyväksikäyttäen tehtävien rikosten osalta. (Poliisin kybertoimivaltuudet, 3)

Raportti sisältää 14 poliisin kiireellisintä käytännönongelmaa liittyen kybertoimivaltuuksien muutostarpeisiin. Raportin lähtökohtana on toimivaltuuksiin liittyvä lainsäädäntö, joka ei ole tämän tutkimuksen keskiössä, mutta se sisältää muun muassa kybertoimintaympäristöön liittyvien käsitteiden määrittelyn (muun muassa tietotekninen valvonta tietoverkoissa, tietoverkko-

[41] 2020/2013/3780, 23.9.2013
[42] Poliisin kybertoimivaltuudet, työryhmän loppuraportti, POL-2015–3879, 2.6.2015

tiedustelu ja turvallisuustiedustelu), joita ei aiemmin tämän tason asiakirjoissa ole tehty. (Poliisin kybertoimivaltuudet, 9-10)

Poliisin strategia

Poliisi julkaisi toukokuussa 2015 uuden strategian toiminnan uusiksi painopisteiksi. Strategian kärjessä ovat muun muassa kiireelliset hälytystehtävät, liikennevalvonta ja sen yhteydessä muiden rikosten paljastaminen, yhteistyö muiden viranomaisten kanssa erityisesti harva-alueilla, kyberosaamisen kehittäminen, vakavan rikollisuuden torjunta, sähköisten palveluiden kehittäminen sekä laadukas laillisuusvalvonta. (Poliisin strategia, Poliisin Internetsivut)

Strategisten päämäärien saavuttamiseksi strategiassa mainitaan yhtenä toimenpiteenä suunnata resursseja tietoverkkorikostorjuntaan sekä kehittää kyberosaamista. Tavoitteina mainitaan kyberrikollisuuden torjunnan osaamisen kasvattaminen, resurssien kohdistaminen kyberrikostorjunnan lisäksi omien toimintojen suojaamiseen kyberuhilta sekä tarve selvittää tietoverkoissa tapahtuvan tiedonhankinnan toimivaltuuksien kehittämistarpeet. (Poliisin strategia, 7)

Muita asiakirjoja

Keskusrikospoliisi on laatinut siellä sijaitsevaan Poliisin kyberturvallisuuskeskukseen liittyviä sisäisiä asiakirjoja, joita ei tarkemmin tässä tutkimuksessa käsitellä.

Poliisiammattikorkeakoulussa on käynnissä selvitys- ja kehittämishanke, jonka aikana kartoitetaan tietoverkkorikollisuuden tilannekuvatyön nykytilaa Suomessa. Hankkeen tavoitteena on koota kokonaiskuva siitä, miten tietoverkkorikollisuuden tilannekuvaa rakennetaan Suomessa. Hankkeessa tullaan esittämään kymmenen konkreettista ehdotusta tilannekuvatyön kehittämiseksi ja pidemmän aikavälin tavoitteena on saada aikaan pysyvä tietoverkkorikollisuuden tilannekuvatoiminnon prosessi, joka yhdistää viran-

omaiset, yksityiset ja akateemiset toimijat. Selvitys on osa poliisin kokonaisvaltaista kybersuunnitelmaa ja sen taustalla on hallitusohjelman tavoite luoda yhteinen tilannekuva tietoverkkojen ja tietoliikenteen turvallisuudesta. Hanke jatkuu helmikuuhun 2016 saakka eivätkä siitä saatavat tiedot ole vielä tässä tutkimuksessa käytettävissä. (Poliisiammattikorkeakoulun Internetsivusto)

4.3 Tutkimuksen tulokset

Tutkimuksessa asetin kaksi eri teemaa, joihin pyrin löytämään vastaukset asiaan liittyvän asiakirja-aineiston avulla. Tutkimuksen ensimmäinen teema on käsitellyt sitä, mitä asiakirjamateriaalia on laadittu ohjaamaan paikallispoliisin kyberympäristössä tapahtuvaa tiedustelutoimintaa ja tiedonhankintaa paikallispoliisin toiminnan järjestämiseksi.

Tutkimuksessa on tarkasteltu sekä EU-tasolla että kansallisesti laadittuja asiakirjoja, joista ilmenee vakavan ja järjestäytyneen rikollisuuden torjunnan hallinnollinen ohjaus tietojohtoisen poliisitoiminnan näkökulmasta tällä hetkellä. Tarkastelussa on keskitytty löytämään vastauksia siihen, ohjaavatko asiakirjat siihen, miten paikallispoliisin toiminta tulisi järjestää ja sen tulisi linkittyä muihin yksiköihin ja toimijoihin sekä millaisilla resursseilla toiminta tulisi järjestää.

Tutkimuksen asiakirja-aineiston perusteella yleisenä johtopäätöksenä voidaan todeta, että poliisin kyberrikostorjuntaa tai - tiedustelua vakavan ja järjestäytyneen rikollisuuden torjuntaan rikostiedustelun ja tietojohtoisen poliisitoiminnan lähtökohdista paikallispoliisin toiminnan ohjaukseen ei ole. Aineiston perusteella voi todeta, että 2000 – luvun alusta tähän päivään tutkimusaiheena oleva kyberrikollisuuden torjunta on nousemassa koko ajan merkittävämmäksi rikostorjunnan osa-alueeksi erityisesti kansallisissa sekä poliisin omissa ohjausasiakirjoissa, jonka johdosta toimintaa kehitetään koko ajan. Asiakirjoista on myös todettavissa, että niissä on alettu viime vuosina ottamaan mukaan rikostorjunnallinen näkökulma, joka on myös tämän tutkimuksen näkökulma. Poliittisissa asiakirjoissa (muun muassa Sipilän

hallitusohjelma) on nähtävissä kyberrikostorjunnan ohjauksen muuttuneen kohti konkreettisia linjauksia.

Ensimmäisiä eurooppalaisia poliisitoimintaa ohjaavia asiakirjoja on Euroopan neuvoston vuonna 2001 tekemä tietoverkkorikollisuutta koskeva yleissopimus, joka kehottaa jäsenmaita parantamaan tietoisuuttaan tietoverkkorikollisuudesta sekä kehittämään tietoverkkorikoksiin liittyvää lainsäädäntöään. Yhtenä merkittävänä asiana sopimuksessa on maininta, jossa kehotetaan ottamaan mukaan rikollisuuden torjuntaan myös yksityisen sektorin toimijat. Tämä seikka on vasta nyt viimeisten vuosien aikana noussut myös sekä kansallisiin että poliisin ohjausasiakirjoihin. Konkreettisia keinoja tai toimenpiteitä asian viemiseksi eteenpäin julkisissa asiakirjoissa toistaiseksi ei ole esitetty.

Euroopan Unionin oikeus- ja sisäasioiden yhteistyön kehittämiseen tähtäävät asiakirjat, niin sanottu Tampereen ohjelma vuosille 2000–2004 sekä niin sanottu Tukholman ohjelma vuosille 2010–2014 ovat strategiatason asiakirjoja, jotka ovat ohjanneet suomalaista kyberrikostorjuntaa. Tampereen ohjelmassa tietoverkkorikokset ja niiden torjunta mainitaan kiinteäksi osaksi muuta järjestäytyneen rikollisuuden torjuntaa. Kyberrikosten kytkentä osaksi järjestäytynyttä rikollisuutta antaa kyberrikollisuudelle saman yhteiskunnalle merkittävää vahinkoa tuottavan aseman kuin perinteisesti ymmärrettävä järjestäytynyt rikollisuus. Tukholman ohjelmassa tietoverkkorikollisuus ja sen torjunta on saanut vielä merkittävämmän aseman. Torjuntatoimia kehotetaan tehtävän myös Euroopan unionin ulkopuolisten maiden kanssa sekä ottamaan mukaan entistä kiinteämmin mukaan yksityisen sektorin toimijat. Ohjelma ottaa huomioon, ettei kyberrikollisuudella ole rajoja, vaan kyse on omasta toimintaympäristöstä, ”avaruudesta”, jossa toimiminen edellyttää viranomaisilta ja kansakunnilta laajaa panostusta monella eri rintamalla sen torjumiseksi.

Eurooppalaisesta poliittisen tason kirjauksista on luettavissa se, että kyberrikosten haitallisuus ja sen yhteiskunnille aiheuttama vahingollisuus on selkeästi havaittu. Kyberrikollisuuden torjunta edellyttää laajaa niin viranomais-

kuin yksityisen sektorin kanssa tehtävää yhteistyötä. Näillä poliittisilla päätöksillä on ollut merkittävä asema kyberrikostorjunnan kehittämisessä ja eteenpäin viemisessä. Euroopan neuvoston raportissa: Tackling digital crime through the establishment of a Cybercrime Centre- The way forward jalkautetaan edellä mainittuja päätöksiä. Raportissa määritellään Europolin yhteyteen perustetun Euroopan kyberkeskuksen pääasialliset tehtävät, jotka vaikuttavat myös Suomen poliisiin konkereettisella tasolla.

Ensimmäiseksi kansalliseksi poliittisen tason ohjausasiakirjaksi voidaan katsoa Lipposen hallituksen valmistelema hallitusohjelma vuosille 1999–2003. Hallitusohjelma ei sinällään vielä käsittele varsinaisesti kyberrikollisuutta tai sen torjuntaa, mutta siinä nostetaan tietoverkot ja tietoliikenne tarkasteltavaksi niiden turvallisen käytön näkökulmasta. Seuraavassa hallitusohjelmassa (2003–2007) kansalaisten tietoturva ja viestinnän yksityisyys oli keskiössä. Jo tuolloin yhteiskunnalliseen keskusteluun oli nostettu lainsäädäntötarve liittyen tietoverkkorikollisuuden torjuntaan. Kyseinen lainsäädäntö esimerkiksi tietoverkkotiedustelun osalta on vielä vuonna 2016 vasta valmisteluvaiheessa. Voidaan todeta, että kyberrikokset, niiden torjunta sekä yhteiskunnalle aiheutuva vahingollisuus ja uhka ovat edelleen vaikeasti ymmärrettäviä haasteita suomalaiselle yhteiskunnalle. Tämä osaltaan vaikuttaa yhteiskunnalliseen yhteisymmärryksen syntyyn. Tällä hetkellä on käynnissä muun muassa arvokeskustelu tiedustelulainsäädännön osalta ja siinä on vastakkain kansalaisen yksityisen suoja sekä yhteiskunnan turvaaminen esimerkiksi terrorismilta.

Tärkeä askel kyberrikosten torjunnan osalta suomalaisessa poliittisessa päätöksenteossa kirjattiin Kataisen hallitusohjelmaan vuosille 2011–2014. Yhtenä merkittävänä kirjauksena oli tavoitteena laatia kansallisen tietoverkkorikollisuutta koskeva kyberstrategia. Toisena keskeisenä kirjauksena voidaan pitää toteamusta tietoverkkorikollisuuden ja järjestäytyneen rikollisuuden liittymisestä yhteen, joka oli yhtenevä Euroopan Unionin niin sanotun Tukholman ohjelman kanssa. Voidaan todeta, että tällöin Suomessa oli havaittu kyberrikollisuuden uudet ja vaativat haasteet, jotka edellyttivät toimenpiteitä monilla eri tahoilla. Välillisesti ohjelmalla oli merkitystä poliisin

kyberrikostorjuntaan. On havaittavissa, että sen pohjalta alkoi myös poliisin kyberrikosten torjuntaan liittyvien ohjausasiakirjojen valmistelu, joka edelleen on käynnissä.

Sipilän hallitusohjelmaan (2015–2018) on kirjattu tietoverkkorikollisuuden torjuntaan tarvittavien resurssien, toimintatapojen sekä lainsäädännön tarkastelujen tarpeista. Hallitusohjelmassa edellytetään viranomaisten, oppilaitosten ja yritysten yhteisen osaamisen kehittämistä, yhteisen tilannekuvan luomista tietoverkkojen ja tietoliikenteen turvallisuudesta sekä turvallisesta tietojen vaihdosta toimijoiden välillä. Kirjaukset ovat aiempaa konkreettisempia ja kyberrikostorjuntaa eteenpäin vievää poliittista ohjausta.

Vuonna 2008 laadittiin Sisäisen turvallisuuden ohjelma, joissa tietoverkkorikollisuus kirjattiin keskeiseksi sisäisen turvallisuuden haasteeksi. Ohjelmaan kirjattiin asiaan liittyvän lainsäädännön ajantasaisuuden selvittäminen sekä poliisin resurssien parantaminen tietoverkkorikollisuuden tutkinnassa ja torjunnassa. Ohjelmaan tehdyt kirjaukset kertovat taustalla olevan tavoitteet ennalta estää tietoverkkorikollisuutta. Esiin nostettu torjuntanäkökulma edellyttää etupainotteista toimintaa ja tiedonhankintaa erilaisin tiedustelukeinoin.

Kansallisia muita kyberrikosten torjuntaa käsitteleviä asiakirjoja ovat ensimmäinen Suomen kyberturvallisuusstrategia vuodelta 2013 sekä sen toimeenpano-ohjelma vuodelta 2014. Vaikka poliisi on keskeisin sisäisen turvallisuuden toimija, strategia-asiakirja ei käsittele kyberrikosten torjuntaa poliisitoiminnan näkökulmasta kovinkaan tarkasti. Asiakirjassa kyllä mainitaan, että poliisilla tulee olla tehokkaat edellytykset ennalta ehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia sekä poliisin rooli keskeisenä rikosten torjujana. Poliisia koskevat kirjaukset jäävät melko yleiselle tasolle, lukuun ottamatta tiedustelulainsäädäntöä koskevat kirjaukset. Toimeenpano-ohjelmassa mainitaan poliisia koskien rikostorjunnan kyberosaamisen kehittäminen, esitutkintaviranomaisen toimivaltuuksien selvittäminen kyberrikostorjunnassa, tietoverkkorikososaamisen liittäminen poliisin 24/7 yhteyspisteeseen ja kansainvälisten

palveluiden turvaaminen, kyberrikostilannekuvan ja – tiedonhankinnan kehittäminen sekä kyberrikostutkinnan järjestäminen ja resursointi. Asiakirjassa mainittu kyberrikostilannekuvan kehittäminen kertoo jo selvästi toiminnan painopisteajattelun muuntumisesta kohti tiedustelulähtöistätoimintaa. Tilannekuvan ylläpito edellyttää tiedonhankintaa, analyysia ja johtopäätösten tekoa, joka eri tiedonhankintakeinoin on toteutettava.

Valtioneuvoston periaatepäätös järjestäytyneen rikollisuuden torjunnan strategiasta 2013, on poikkihallinnollinen ohjausasiakirja, jossa velvoitetaan eri ministeriöitä ryhtymään päätöksessä mainittuihin toimenpiteisiin järjestäytyneen rikollisuuden torjunnan tehostamiseksi. Yhdeksi toimenpiteeksi on kirjattu panostaminen tietoverkkoja hyödyntävän rikollisuuden torjuntaan osana järjestäytyneen rikollisuuden torjuntaa. Asiakirjan voidaan katsoa olevan strateginen ohjausasiakirja, jolla on erityinen vaikutus poliisin järjestäytyneen rikollisuuden torjuntaan ja sen yhtenä osa-alueena olevaan kyberrikostorjuntaan. Asiakirja osaltaan vahvistaa ymmärrystä kyberrikollisuuden laaja-alaisuudesta sekä sen haitallisuudesta. Strategiaa on jalkautettu poliisihallinnon sisällä 2014 työryhmä työskentelyn kautta ja sen pohjalta toimii työryhmä, jossa valmistellaan muun muassa sekä julkista että salaista osiota järjestäytyneen rikollisuuden torjunnan käsikirjaksi. Kyberrikollisuus osana järjestäytynyttä rikollisuutta on mukana torjuntatoimien suunnitelmissa.

Vuonna 2015 valmistui asiakirja Suomalaisen tiedustelulainsäädännön suuntaviivoja, joka otsikkonsa perusteella näyttäisi liittyvän keskeisesti poliisin kyberrikostorjuntaan. Asiakirja käsittelee tiedustelua tietoliikennetiedustelun näkökulmasta, jonka lähtökohta on kaikkeen tietoliikenteeseen kohdistuva valvonta. Mietintö ei suoranaisesti käsittele kyberrikostorjuntaa poliisin näkökulmasta poislukien Suojelupoliisi, jonka rooli ulkoisen turvallisuuden toimijana yhdessä Puolustusvoimien kanssa ovat asiakirjassa korostuneesti esillä. Asiakirja ei huomioi poliisin kyberrikostutkintaan ja – torjuntaan liittyviä lainsäädäntötarpeita, joissa lähtökohtana on kohdistettu tiedonhankinta ja sitä kautta rikosten ennalta estäminen, paljastaminen ja selvittäminen.

Poliisin vuonna 2008 julkaistussa raportissa Tietotekniikkatutkinnan järjestäminen poliisissa on laajasti käsitelty tietotekniikkatutkinnan järjestämistä Keskusrikospoliisissa ja paikallispoliisissa. Raporttiin on kirjattu useita konkreettia toimenpiteitä varsinaisesta tietoverkkorikosten tutkinnasta. Asiakirja ei sisällä kyberrikostorjunnan näkökulmaa eikä siihen liittyvää tiedustelullista elementtiä. Asiakirjan otsikkossa mainittu tietotekniikkatutkinta kertoo siitä ajattelusta, joka tuolloin vielä oli poliisissa vallalla. Asiaa lähestyttiin laitteisiin kohdistettavan teknisen tutkinnan näkökulmasta, joka linkittyi poliisi perinteiseen tekniseen tutkintaan. Yhtenä syynä siihen todennäköisesti on ollut se, että varsinaista kyberrikoksiin liittyvää tutkintaa tehtiin tuolloin melko vähäisissä määrin ja kyberrikosten torjuntanäkökulma koettiin vielä kaukaisempana asiana. Käytännössä päivittäinen työ kohdistui eri laitteisiin tehtävästä todistusaineiston etsinnästä ja keräämisestä.

Samana vuonna julkaistiin järjestäytyneen rikollisuuden ja terrorismin torjunnan sisäisen turvallisuuden ohjelman valmisteluun liittyvä asiantuntijatyöryhmän loppuraportti. Raportti sisältää yksityiskohtaisia toimenpideehdotuksia tietoverkkorikollisuuden ja Internetin käyttöön liittyvien riskien ja uhkien torjumiseksi. Asiakirja käsittelee tietoverkkorikostorjunnan toimintaedellytysten turvaamista ja osaamisen kehittämistä tietoverkkorikostorjunnan kehittämiseksi. Asiakirja on laadittu kyberrikostorjunnan näkökulmasta ja sen taustalla on näin ollen ennalta estävyyteen tähtäävää ja tiedustelullisia elementtejä sisältävää ajattelua.

Poliisin kybertoimivaltuuksia pohtinut työryhmä julkaisi raporttinsa 2015. Raportti sisältää 14 kiireellisintä lainsäädännön muutostarvetta käytännön ongelmiin liittyen. Raportissa on niiden lisäksi määritelty kybertoimintaympäristöön liittyviä käsitteitä, jonka johdosta asiakirjaa voidaan pitää merkittävä poliisin kyberrikostorjuntaa edistävänä ohjausasiakirjana. Aiemmissa asiakirjoissa kyseisiä määritelmiä ei ole tehty. Toinen poliisihallinnon tuoreimpia asiakirjoja on 2015 julkaistu Poliisin strategia, jossa kyberrikollisuuden torjunta on nostettu omaksi osa-alueekseen. Nämä kaksi hallinnon omaa asiakirjaa voidaan katsoa olevan jo selkeästi kyberrikostorjunnan ja ennalta estävästä näkökulmasta valmisteltuja.

Tutkimuksessa ei ole käsitelty Poliisihallinnon muutamia sisäisiä turvaluokiteltuja asiakirjoja, vaan ne on niiden sisällön vuoksi jouduttu jättämään tutkimusaineistosta pois. Asiakirjat sisältävät tietoja muun muassa vuonna 2015 aloittaneen Poliisin kyberrikoskeskuksen toiminnan organisoinnista, resursseista ja operatiivisesta toiminnasta. Yhteenvetona voidaan kuitenkin näiden osalta todeta, että niissä ei juurikaan käsitellä kyberrikostorjuntaa paikallispoliisin osalta.

Tutkimusaineistoon suoritetun analyysin pohjalta voidaan todeta, että eurooppalaiset asiakirjat ovat 2000 -luvun alkupuolelta lähtien alkaneet painottaa kyberrikollisuuden lainsäädäntömuutoksia, torjuntaa, sekä viranomais- että yksityisen sektorin kanssa tehtävää yhteistyötä. Suomalaisissa poliittisissa asiakirjoissa Vanhasen hallituksen ohjelmassa vuosille 2003–2007 mainittiin ensimmäisen kerran tietoverkkorikostorjunnan lainsäädäntötarve ja varsinaisesti vasta Kataisen hallitusohjelmaan (2011–2014) on kirjattu selkeästi tavoitteeksi kyberstrategian laatiminen. Poliisihallinnon sisäisissä asiakirjoissa vasta Sisäisen turvallisuuden ohjelman valmistelun yhteydessä vuonna 2008 on kirjattu toimenpide-ehdotukseksi kyberrikostorjunta ja sen toimintaedellytysten turvaaminen.

On todettava, että Poliisin omaa kyberrikostorjunnan strategiaa tai muuta poliisiyksiköiden tehtäviä, vastuiden jakoa ja niin edelleen kyberrikostorjuntaan tai – tiedusteluun liittyvää ohjausasiakirjaa ei ole julkaistu (helmikuu 2016). On tietysti otettava huomioon yhtenä puutteen selittävänä seikkana asiaan liittyvän selkeän lainsäädännön ja siihen pohjaavien toimivaltuuksien puute.

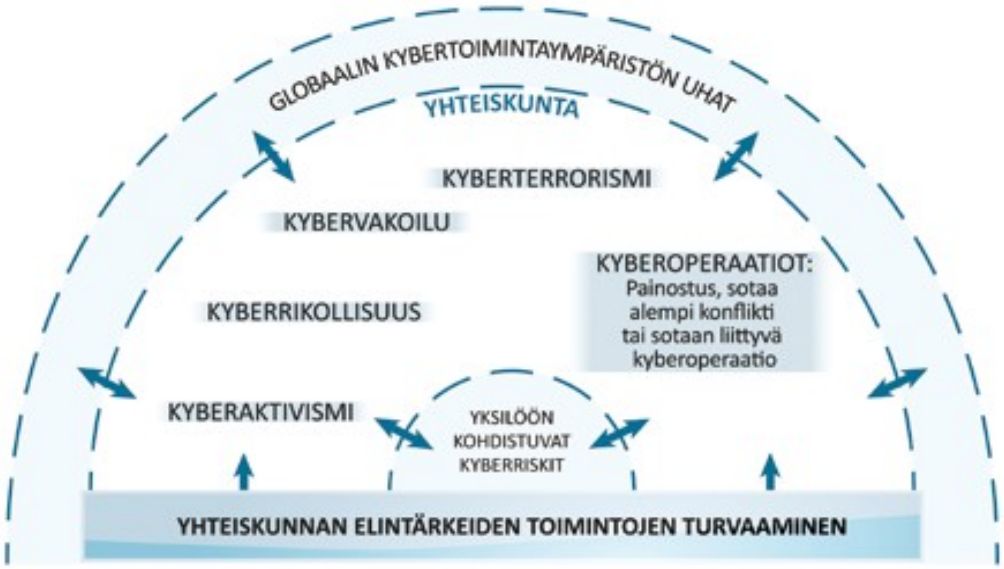
Toisena kysymyksenä tutkimuksessa tarkastelin sitä, Miten vakavan ja järjestäytyneen rikollisuuden kybertiedustelutoiminta tulisi paikallispoliisin näkökulmasta järjestää ottaen huomioon tietojohtoisen poliisitoiminnan vaatimukset? Tutkimuksen toisessa teemassa käsittelen sitä, miten tutkimuksen kohteena oleva toiminta tulisi paikallispoliisiin rakentaa siten, että se täyttäisi tietojohtoisen poliisitoiminnan kriteerit ja toimisi tehokkaasti ja tulok-

sekkaasti. Tarkastelussa pohjana käytän Itä-Uudenmaan poliisilaitoksen toimintaympäristöä sekä organisaatio- ja tehtävärakenteita, jotta tarkastelu voidaan tehdä paikallispoliisin näkökulmasta. Koska tutkimukseen ei ole käytettävissä tutkimusaihetta käsittelevää valmista asiakirja-aineistoa, asiaa on käsitelty tutkimuksen pohdintaosassa sivulla 92.

5 KYBERRIKOLLISUUS ILMIÖNÄ

Mistä kyberrikollisuudessa on kysymys ja miten se vaikuttaa nykyiseen poliisitoimintaan mukanaan tuomien uudenlaisten haasteiden johdosta? Tarkastelen ilmiötä edellä tekemieni käsitemäärittelyiden lähtökohdista.

Globaali kybertoimintaympäristö muodostuu monimutkaisesta ja – kerroksisesta maailmanlaajuisesta informaatioverkostosta, johon kuuluu kansallisia turvallisuusviranomaisten, muun julkishallinnon ja yritysmaailman kommunikaatioverkkoja sekä teollisuuden ja kriittisen infrastruktuurin valvonta- ja ohjausjärjestelmiä (Suomen kyberturvallisuusstrategia 2013, 17). Kyberrikollisuus on mainittu yhdeksi kyberuhaksi Suomen kyberturvallisuusstrategiassa. Kyberuhkamalli tarkoittaa kuvausta kyberuhkien aiheuttamista häiriöistä, uhkan vaikutusmekanismista, lähteestä, kohteesta ja vaikutuksesta kohteeseen. Uhkat voivat kohdistua suoraan tai välillisesti yhteiskunnan elintärkeitä toimintoja, kansallista kriittistä infrastruktuuria ja/tai kansalaisia vastaan maan rajojen sisältä tai ulkopuolelta (Suomen kyberturvallisuusstrategia 2013, 18)



KUVIO 3: Suomen kyberuhkamalli, (Suomen kyberturvallisuusstrategia 2013, 19)

Lainsäädännöllisistä haasteista huolimatta kyberrikollisuutta ja siihen vaikuttavia tahoja ja liittymäpintoja on kuvattu vuonna 2013 laaditussa kyberturvallisuusstrategiassa ja siihen liittyvässä kyberturvallisuusvisiossa. Siinä on mainittu, että 1) Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan, 2) kansalaisilla, viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti sekä 3) Vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa.

Kyberturvallisuusvision taustalla on muun muassa ajatus siitä, että Suomella on pienenä, osaavana ja yhteistyökykyisenä maana erinomaiset edellytykset nousta kyberturvallisuuden kärkimaaksi. Meillä on vahva osaamisperusta sekä pitkät perinteet tiivistä ja luottamuksellisesta yksityisen ja julkisen sektorin yhteistyöstä sekä hallinnon alojen välisestä yhteistyöstä. (Suomen kyberturvallisuusstrategia 2013, 3). Suomalaisen viranomaisyhteistyön toimivuus on todettu muun muassa Poliisiammattikoulun tuottamassa raportissa vuodelta 2014: ”Poliisin, tullin ja rajavartiolaitoksen, eli nk. PTR - viranomaisten yhteistyötä pidetään yhtenä sisäisen turvallisuuden kansallisena menestystarinana, joka on saanut myös kansainvälistä arvostusta” (Tietojohtoinen viranomaisyhteistyö ja sen vaikuttavuuden arviointi 2014, 4)

Tarkasteltaessa nykyistä kyberrikollisuuden määrittelyä, voidaan päätyä siihen, että kyberrikollisuuden käsite on vailla selkeää suomalaista määritelmää. Yhtenä siihen vaikuttavana tekijänä ovat lainsäädännölliset puutteet. Voimassa olevassa lainsäädännössä ei ole huomioitu tietoverkkorikollisuuden erityisasemaa tarkasteltaessa esimerkiksi rikoksen tapahtumapaikan määrittelyä. Kyberympäristössä rikoksen toteuttamiseen esimerkiksi haittaohjelmaa on voitu kierrättää palvelimilla ympäri maailmaa varsinaisten rikokseen syyllistyvien oleskellessa aivan eri maassa, samalla kun rikoksesta aiheutuvat vaikutukset ilmenevät useassa eri maassa[43]. Ongelmaksi tulee ri-

[43] Transnationaaliset tietotekniikkarikokset (Pihlajamäki 2004, 5)

koksen tekopaikan eli missä tapahtunut rikos tutkitaan. Kyse on siis perustavanlaatuisesta asiasta, johon voimassa olevasta lainsäädännöstä ei löydy yksiselitteistä vastausta. Järjestäytyneen ja rajat ylittävän kyberrikollisuuden torjuntaan ja tutkintaan liittyy monia muitakin lainsäädännöllisiä ongelmakohtia.

Tarkasteltaessa voimassa olevaa lainsäädäntöä järjestäytyneen rikollisuuden torjunnan ja tiedustelun näkökulmasta tilanne on vielä enemmän sääntelyä vailla olevaa. Niin sanottuun normaaliin toimintaympäristöön sovitettu lainsäädäntö ei sovi monelta osin suoraan kyberympäristöön. Toisin lainsäädännölliset puutteet ovat vain osa kyberrikollisuuteen liittyvää ongelmakenttää. Kyberrikollisuutta tulisi myös profiloida ja ymmärrystä sen toiminnasta ja vaikutuksista lisätä sekä harkita, millä retoriikalla kyberrikollisuutta tulisi lähestyä, kuten David S Wall on todennut (Wall 1998, 214).

Vuonna 1989, kun Euroopan lainsäädännön painopiste oli aineellisessa rikosoikeudessa, Euroopan neuvosto hyväksyi esityksen[44] tietoverkkorikollisuuden lainsäädännön laatimiseksi antamalla suuntaviivoja lainsäädäntöä varten jäsenmaille. 1990-luvun puolivälissä EU:n lainsäädännöstä käyty keskustelu alkoi sisältää prosessioikeudellisia elementtejä, esimerkkinä Euroopan neuvoston 1995 antama suositus[45] tietoverkkorikollisuuden huomioimiseksi rikosprosessioikeuden lainsäädännössä. 2000-luvun alussa osaksi EU:n lainsäädäntökeskustelua tuli mukaan kansainvälisen yhteistyön kehittäminen, jolloin alettiin valmistella Tietoverkkorikollisuutta koskevaa yleissopimusta[46], joka sisältyi vuonna 2001 Euroopan neuvoston yleissopimuksen III lukuun. (Europol IOCTA 2014, 77)

Kyberlainsäädännön kehittämiseksi Hallitus antoi vuonna 2014 esityksen eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia[47] koskevien sään-

[44] Expert Report on Computer-Related Crime' in 1989, Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies
[45] Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies
[46] Convention on Cybercrime, Council of Europe, ETS 185, Budapest, 23.11.2001
[47] Lainsäädäntö tuli voimaan 4.9.2015 (Säädöskokoelma 368/2015)

nösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi. Lakipaketti sisältää rikoslakia, pakkokeinolakia, poliisilakia ja sotilasoikeudenkäyntilakia koskevat muutokset. Lakimuutoksilla pantiin täytäntöön tietojärjestelmiin kohdistuvia hyökkäyksiä koskeva Euroopan parlamentin ja neuvoston direktiivi. Rikoslakiin tulleet uudet säännökset laajentavat sähköisessä muodossa olevan tiedon ja tiedonvälityksen rikosoikeudellista suojaa. Tietoverkkorikollisuuteen liittyvän lainsäädännön lähentäminen Euroopan unionin jäsenvaltioiden välillä saattaa jossain määrin edesauttaa Suomen viranomaisten mahdollisuuksia selvittää sellaisia rajat ylittäviä rikoksia, joiden vahingolliset seuraukset ilmenevät Suomessa. Tehokkaalla tietoverkkorikollisuuteen puuttumisella kattavien ja toimivien kriminalisointien avulla voidaan olettaa olevan myönteisiä yhteiskunnallisia ja taloudellisia vaikutuksia.

Kyberrikollisuus on osa vakavaa ja järjestäytynyttä rikollisuutta, jonka torjuntaan ja rikolliseen järjestöön kuulumista Suomessa ei ole kriminalisoitu erillislainsäädännöllä. Voimassa olevan rikoslain mukaan järjestäytyneen rikollisryhmän jäsenenä tehty rikos voi olla rangaistuksen koventamisperusteena. Hallitusohjelmaan vuosille 2011–2014 on kirjattu, että hallituskauden aikana tehostetaan järjestäytyneen rikollisuuden torjuntaa ja selvitetään erityslain tarve. Lisäksi tietoverkkorikollisuuden torjuntaan panostetaan osana järjestäytyneen rikollisuuden torjuntaa. Hallitusohjelman tehty kirjaus liittyy keskeisesti tiedonvaihdon ja yhteistyön kehittämiseen kansallisesti ja kansainvälisesti.

Oikeusministeriön johdolla valmisteltiin vuosina 2013–2014 Rikoslain 6 luvun 5 §:n 2 kohdan ja Rikoslain 17 luvun 1 a §:n sekä yksittäisten törkeitä tekomuotoja koskevien rikostunnusmerkistöjen järjestäytynyttä rikollisuutta koskevien määritelmien mahdolliset muutos- ja yhtenäistämistarpeet. Työryhmän mietinnön pohjalta annettiin hallituksen esitys vuonna 2014[48], joka johti 1.10.2015 voimaan tulleisiin lainsäädäntömuutoksiin (Säädöskokoelma 564/2015)

[48] HE 263/2014

Rikoslakia yhtenäistettiin järjestäytyneitä rikollisryhmiä koskevia säännöksiä. Järjestäytyneen rikollisryhmän toimintaan osallistumista koskevassa rangaistussäännöksessä oleva järjestäytyneen rikollisryhmän määritelmä siirrettiin rangaistuksen koventamisperusteita koskevaan rikoslain säännökseen. Muissa järjestäytyneitä rikollisryhmiä koskevissa säännöksissä viitataan tähän säännökseen. Tämän seurauksena kaikissa rikoslain järjestäytyneitä rikollisryhmiä koskevissa säännöksissä järjestäytyneellä rikollisryhmällä tarkoitetaan vähintään kolmen henkilön muodostamaa tietyn ajan koossa pysyvää rakenteeltaan jäsentynyttä yhteenliittymää, joka toimii yhteistuumin tehdäkseen tuossa määritelmäsäännöksessä mainittuja rikoksia. Yksittäisissä järjestäytyneitä rikollisryhmiä koskevissa säännöksissä on tämän lisäksi tarkemmin määritelty niiden soveltamiselta vaadittavat edellytykset.

Järjestäytyneitä rikollisryhmiä koskevissa säännöksissä on kysymys rikoksen tekemisestä osana järjestäytyneen rikollisryhmän toimintaa. Järjestäytyneitä rikollisryhmiä koskevan sääntelyn muuttaminen ei vaikuttanut säännöksen rangaistavuuden tai ankaruuden arviointiin. Tästä huolimatta käsitteistön yhtenäistämisen aiheuttaa joissakin kohdin pieniä säännösten soveltamisalojen muutoksia. Muutoksille ja sääntelyn yhtenäistämisellä on pyritty tehostamaan järjestäytyneen rikollisuuden torjuntaa.

Edellä mainitun lainsäädäntömuutoksen yhteydessä muutoksia tehtiin myös Rikoslain 38 luvun 6 (tieto- ja viestintärikoksista) ja 7 (törkeä tietojärjestelmän häirintä) pykäliin: jos rikos tehdään osana 6 luvun 5 §:n 2 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa ja rikos on myös kokonaisuutena arvostellen törkeä, rikoksentekijä on tuomittava törkeästä tietoliikenteen häirinnästä vankeuteen vähintään neljäksi kuukaudeksi ja enintään viideksi vuodeksi. Rikoslain 35 luvun 2 (törkeä vahingonteko) ja 3 b (törkeä datavahingonteko) pykäliin lisättiin kvalifioimisperusteeksi rikoksen tekemisen osana 17 luvun 1 a §:n 4 momentissa tarkoitetun järjestäytyneen rikollisryhmän toimintaa.

Lakimuutosten tarve oli todettu oikeuskäytäntöjen ja Korkeimman oikeuden tekemien päätösten johdosta. Aiemman lain soveltaminen ei ole johtanut lainvoimaisiin päätöksiin osin siksi, että järjestäytynyttä rikollisuutta koskevat säännökset on säädetty viimeisten neljänkymmenen vuoden aikana eri yhteyksissä. Sääntely on tämän johdosta muodostunut jossain määrin epäyhtenäiseksi. Taustalla on hallitusohjelma vuosille 2011–2014 ja valtioneuvoston 7.3.2013 antama periaatepäätös järjestäytyneen rikollisuuden torjunnan strategiasta.

Suomessa Rikollisuuden ammattimaistumista on tapahtunut 1970-luvun alusta lähtien. Tuolloin oli havaittavissa suomalaisten rikoksentekijöiden hierarkkista organisoitumista johtaviin ja rahoittaviin henkilöihin sekä ammattimaiseen suoritusportaaseen, mutta ammattimainen rikollinen toiminta oli lähinnä omaisuus- ja talousrikollisuutta. Huumausainerikollisuuden merkitys oli 1990-luvulle saakka melko pieni, mutta 1990-luvulla sen rooli ammattimaisen ja myöhemmin järjestäytyneen rikollisuuden piirissä on kasvanut selvästi. Nykyisin huumausainerikollisuus on yksi järjestäytyneen rikollisuuden päätoimialoista. Euroopan unionin laajentuminen ja siihen liittyvä vapaa liikkuvuus ovat tuoneet Suomeen myös uusia ulkomaisia, kansainvälisesti toimivia järjestäytyneitä rikollisryhmiä. Poliisin tietojen mukaan järjestäytyneeseen rikollisuuteen liittyvien ryhmien määrä on lisääntynyt viimeisten 10 vuoden aikana Suomessa. Keskusrikospoliisin arvion mukaan Suomessa toimii noin 80 järjestäytynyttä rikollisryhmää, ja näissä ryhmissä on jäseniä noin 1000. Tiedot perustuvat rikostuomioihin, tehtyihin rikosilmoituksiin ja esitutkintaviranomaisten vihjetietoihin, eivätkä kuvaa tehtyjen rikosten tai niistä tuomittujen määrää. (Valtioneuvoston periaatepäätös järjestäytyneen rikollisuuden torjunnan strategiasta 2013, 5)

Perinteiset järjestäytyneet rikollisryhmät mukaan lukien vanhat, mafiatyyliin rakenteen omaavat ryhmittymät ovat alkaneet käyttää toiminnassaan kyberympäristön tarjoamia mahdollisuuksia ostamalla tarvittavaa osaamista ulkopuoliselta toimijalta. Perinteinen järjestäytynyt rikollisuus pyrkii laajentamaan toimialaansa toteuttamalla tällä tavoin entistä monimutkaisempia rikoksia kyberympäristön avulla. Ulkopuoliselta taholta ostetut asiantuntija-

palvelut tarjoavat samalla järjestäytyneelle rikollisuudelle mahdollisuuden verkostoitua lailliseen liiketoimintaan ja tällä tavoin peittää laittomia liiketoimiaan.

Vakavan ja järjestäytyneen rikollisuuden toimintatavat ovat laajentumassa entistä voimakkaammin kyberympäristöön muokaten osaltaan järjestäytyneen rikollisuuden käsitettä. Samalla järjestäytynyt rikollisuus tulee entistä lähemmäksi tavallista kansalaista. Järjestäytyneen rikollisuuden toiminta kohdistuu tavalliseen kansalaiseen muun muassa identiteettivarkauksien, petosten, käyttäjätunnusten ja salasanojen kaappausten ja tietojen kalastelun[49] kautta. Koska esimerkiksi kaupankäynti siirtyy enenevässä määrin tietoverkkoihin[50], kansalaisten kiinnittyneisyys älypuhelinten ja tablettien avulla koko ajan kyberavaruuteen,[51] sosiaalinen media, Internetin tarjoamat anonyymiyden mahdollistavat viestintä- ja kaupankäyntifoorumit[52] ja virtuaalivaluutat[53], altistuvat kansalaiset helposti haavoitettaviksi järjestäytyneen rikollisuuden masinoimien rikosten uhreiksi. (Europol IOCTA 2014, 11–22)

Kybermaailma avaa ”online-rikollisjärjestöille” mahdollisuuden häivyttää muodolliset, hierarkiset organisaatiorakenteet ja liittyä toisiinsa asiayhteyksien kautta. ”Online-rikollisjärjestöjen” ei tarvitse olla rajattuja jäsenyyksien, toimintansa, kansallisten tai alueellisten rajojen tai kulttuurierojen osalta. Kybermaailmassa kulttuuri- ja maarajojen ylittämiseen riittävät asiayhteydet, jonka kautta organisaatiot muodostuvat. Järjestäytyminen ei edellytä ul-

[49] Phishing

[50] Vuonna 2012 erilaisilla maksukorteilla suoritettiin 3,5 triljoonan edestä maksusiirtoja, josta petosten osuus oli 1,33 biljoonaa (Europol IOCTA 2014, 35)

[51] Arvioiden mukaan maailmanlaajuinen älypuhelimen myynti yltää 1,2 miljardiin jo vuonna 2014. Luku on yhtä paljon kuin yhteenlaskettu väestön määrä Euroopassa ja Pohjois-Amerikassa. (Europol IOCTA 2014, 17)

[52] Esimerkiksi Tor- ja i2P- verkoissa toimivat Deep Web ja Darknet ovat niin sanottuja piilopalveluja, jotka mahdollistavat käyttäjälle lähes täydellisen anonymiteetin ja mahdollistavat tällä tavalla muun muassa laittomien tavaroiden ja palveluiden tarjonnan ja kysynnän. (Europol IOCTA 2014, 19)

[53] Muun muassa Bitcoin, joka on vertaisverkon avulla luotu virtuaalinen raha – vaihdannan väline, jota ei ole olemassa kolikkoina tai seteleinä. Vertaisverkossa välitettävä raha liikkuu käyttäjiensä välillä kuten esimerkiksi pankkikorttimaksu, mutta ilman välikäsiä, joita normaalissa rahaliikenteessä ovat pankit. Päinvastoin kuin perinteisissä maksuvälineissä, bitcoinin arvoa eivät määrittele eri maiden keskuspankit, vaan valuutan arvo määräytyy kysynnän ja tarjonnan perusteella. Bitcoin siirtyy vertaisverkossa henkilöltä toiselle, eikä sitä ole sidottu pankkien valuutanvaihtokursseihin. (Verottajan verkkosivut (Vero.fi): Virtuaalivaluuttojen tuloverotus)

koisia tunnusmerkkejä, kerhotiloja eikä muita perinteisten rikollisryhmien statusta vahvistavia elementtejä. Perinteisiä rikollisryhmiä toisiinsa tähän asti sitoneiden maantieteellisyyden ja hierarkisen jäykkyyden poistuminen mahdollistaa uusien koalitioiden syntymisen. Koalitioista koostuu tietoverkkorikollisten ja -järjestöjen jäsenistöltään hajanaisia, löyhästi jäsenneltyjä ryhmiä, jotka tulevat yhdessä hyödyntämään tietyntyyppisiin rikoksiin keskittyneitä ryhmiä. Koalitiot syntyvät tiettyihin tarkoituksiin ja ne toimivat niin kauan kuin niiden asettamat päämäärät tai tavoitteet on saavutettu. Sen jälkeen niiden toiminta lopetetaan. Kyberavaruudessa järjestäytyneen rikollisuuden edellyttämät monet toimintaprosessit voidaan automatisoida, jolloin rikollisjärjestöt voivat olla kyberavaruudessa tilannekohtaisia, asialiitännäisiä ja vain rajoitetun ajan koossapysyviä organisaatioita. (Brenner 2002, 47–50)

Lähtökohtaisesti voidaan ajatella kyberrikollisuuden torjunnan olevan tällä hetkellä osa perinteistä suomalaista rikostorjunta-ajattelua, joka lähtee pääosin lähipoliisitoiminnasta, jonka strateginen tausta-ajatuksena on poliisin perustehtävän hoitaminen kansalaisläheisesti, laadukkaasti ja tehokkaasti. Lähipoliisitoiminnan tavoitteena on tuottaa turvallisuutta ja turvallisuuden tunnetta, vähentää ja ehkäistä rikollisuutta sekä järjestyshäiriöitä ja siten myös säilyttää poliisin kuva myönteisenä ja poliisiin kohdistuva luottamus korkealla tasolla. Tässä mallissa lähipoliisitoiminnalla tarkoitetaan aluevastuulla ja ongelmasuuntautuneesti toimivaa poliisia. (Lähipoliisitoiminnan strategia 2010, 3)

Lähipoliisimallin rikostorjuntatyö perustuu keskeisesti suunnitelmalliseen ja ennakoivaan yhteistyöhön kansalaisten ja sidosryhmien kanssa, johon liittyy yhdessä toteutettujen toimenpiteiden vaikuttavuuden seuranta ja arviointi. Toimintamalli keskittyy ongelmien kokonaisvaltaiseen ratkaisuun yksittäisten tehtävien sijasta. Poliisin kannalta lähipoliisiajatus on siirtänyt painopistettä laillisuusvalvonnasta turvallisuustyön koordinoijaksi, jonka tavoitteena on palveluiden kehittäminen kansalaisläheisimmiksi (Virta 1998, 93–94). (Lähipoliisitoiminnan strategia 2010, 7)

Suomalaisen lähipoliisitoimintamallin ongelmasuuntautuneen poliisitoiminnan perusajatuksena on niiden olosuhteiden muuttaminen, jotka aiheuttavat uusiutuvia ongelmia. Toimintamallin toteuttaminen edellyttää syvällistä tutustumista ongelmien taustasyihin, niiden analysointia, sellaisten ratkaisumallien kehittämistä, joilla epäedulliset olosuhteet saadaan muuttumaan siten, ettei ongelmia enää tulevaisuudessa esiinny tai ainakin niiden määrää saadaan vähennettyä. Ongelmasuuntautuneen poliisitoiminnan tavoitteena on löytää kokonaisvaltaisia keinoja ongelmien poistamiseksi. (Hakaniemi 2012, 35)

Kybermaailmassa rikostorjunnan painopiste tulee olemaan Aasian ja Tyynenmeren alueella, koska siellä sijaitsee kyberrikollisuuden ”voimatoimijoita”, joihin vain kansainvälisellä torjuntatyöyhteistyöllä muun muassa yksityisen sektorin kanssa voidaan puuttua. Vaikuttamalla rikoksentekijän tilaisuuteen tehdä rikos, hänen motivaatioonsa tai rikoksen kohteeseen pystytään estämään rikollisuutta. Näiden peruselementtien tunnistamisen ja niihin kohdistettujen toimien lisäksi esimerkiksi kaupattavien tuotteiden tai sähköisen kaupankäynnin suunnittelussa rikostorjunnalliset näkökulmat ja riskien minimointi olisi otettava huomioon. (Broadhurst 2006, 9)

Rikostorjunnan ymmärtäminen ja toteuttaminen kybermaailmassa tai – avaruudessa, johon yhdistyy järjestäytynyt rajat ylittävä rikollisuus, edellyttää poliisitoiminnan tarkastelua globaalisti. Toimintaympäristön rajattomuus niin maantieteellisesti kuin asiallisesti tekee rikostorjunnasta vaikeasti hahmoteltavaa. Minne, milloin ja kuka kohdistaa torjuntatoimia ovat niitä kysymyksiä, joihin vastauksia on haettava niin lainvalvontaviranomaisten, muiden viranomaistahojen kuin yksityisen sektorin kanssa tehtävästä yhteistyöstä. Koska kyberrikollisuus aiheuttaa vakavia seurauksia ja on kaikkien valtioiden keskeinen rikostorjunnallinen haaste, kansainvälinen yhteistyö ei voi sivuuttaa kyberrikollisuuden torjuntaa, sillä se vain kannustaisi rikollisia ahneuteen ja vakavampien rikosten suunnittelun ja toteuttamiseen (Marion 2010, 11).

Poliisin tehokas ennalta estävä toiminta edellyttää asetetun tavoitteen saavuttamiseksi alueellisen ja paikallisen painopisteiden määrittämistä, kohderyhmien tunnistamista ja toiminnan kohdentamista sekä uusien toimintatapojen löytämistä. Tavoitteena on analysoidun tiedon pohjalta tehtävä ilmiöiden ja turvallisuutta vaarantavien tekijöiden tunnistaminen hyödyntäen asiakaslähtöisyyttä sekä moniviranomais- ja moniammatillista yhteistyötä. Kohderyhmänä ovat erityisesti sellaiset asiakasryhmät ja asiakkaat, joiden turvallisuusongelmien kokonaisvaltainen ratkaisu edellyttää perinteistä poliisitoimintaa laaja-alaisempaa lähestymistapaa tai moniammatillista työotetta ja jossa tarvitaan muun muassa kolmannen sektorin, kuten yritysten, järjestöjen ja yhdistysten osaamista. Ennalta estävän rikostorjunnan lähtökohtana ovat laadukas ja tehokas rikosten paljastaminen ja selvittäminen huomioiden rikostyyppien erityispiirteet. Tavoitteena on lisätä kiinnijäämisriskiä ja vähentää rikostenteon houkuttelevuutta. (Poliisin ennalta estävän toiminnan strategia 2014, 3-4)

Rikosten ennalta estäminen ei ole enää pelkästään poliisin monopolitoimintaa, vaan se edellyttää muita ei valtiollisten tahojen mukaan tuloa. Ymmärretään, että perinteinen hierarkinen, poliisilla käytössä ollut johtamismalli, ei toimi nykyisessä toimintaympäristössä ja täytä vaatimuksia nykyaikaisesta poliisitoiminnasta. Viimeisten vuosikymmenten aikana on jo luotu lukuisia yksityisiä ja yhteisöllisesti toimivia tahoja ja virastoja, jotka ehkäisevät ja estävät rikollisuutta, tutkivat rikoksia ja puuttuvat konflikteihin. Muiden toimijoiden toiminnasta on tullut konkreettista, yksityiset turvapalvelut osallistuvat rikosten ennalta estämiseen, kansalaiset suorittavat jalkapartiointia asuinalueillaan, rikollisuuden ehkäisyyn on perustettu yhdistyksiä ja valtakunnallisia tahoja[54] ja niin edelleen. Myös Suomessa on keskusteltu viime aikoina paljon poliisin roolista ja perinteisesti poliisin hoitamien tehtävien

[54] Esimerkkinä Rikoksentorjuntaneuvosto (1999 -), joka on oikeusministeriön yhteydessä toimiva valtioneuvoston asiantuntija- ja yhteistyöelin, joka suunnittelee ja toteuttaa toimia rikollisuuden ehkäisemiseksi. Tavoitteena on rikoksista aiheutuvien haittojen vähentäminen ja turvallisuuden edistäminen. Paikallista rikoksentorjuntaa edistetään antamalla asiantuntija-apua, osallistumalla oikeusministeriön myöntämän taloudellisen tuen jakoon ja tiedottamalla rikoksentorjunnan hyvistä käytännöistä. Rikoksentorjuntaneuvoston sihteeristönä toimivat oikeusministeriön kriminaalipoliittisen osaston tehtävään määrätyt virkamiehet. (Rikostorjuntaneuvoston verkkosivut 2015)

jakamista yksityiselle tai muille tahoille. On todettu, että poliisin resurssien vähetessä kaikki poliisille kuuluneet tehtävät eivät välttämättä enää olekaan poliisitoiminnan ydinaluetta. (Bailey 1996, 586–591)

Huolimatta lainsäädännöllisistä puutteista pystymme ennalta estämään kyberrikollisuutta yhdessä Internetin palveluntarjoajien kanssa ottamalla huomioon, että he eivät toimi viranomaisstatuksella. Kohdistamalla esimerkiksi toimenpiteitä vakaviin rikoksiin ja niiden taustalla toimiviin todellisiin toimijoihin pystytään hyödyntämään heillä olemassa olevaa ja poliisilta uupuvaa osaamispääomaa. Poliisin toimintaan kohdistettujen resurssien kannalta osaamisen hankkiminen, ylläpito ja kehittäminen hallinnon sisälle, ei ole kannattavaa eikä välttämättä kaikilta osin edes mahdollista. Osaamisen taso ja toiminnan tavoitteet nousevat liian korkeiksi. Yhteistyö yliopistojen kanssa tarjoaa tieteellisen näkökulman esimerkiksi ennalta estävien toimenpiteiden vaikuttavuudesta tai sen seurannasta sekä teknisen osaamisen hyödyntämismahdollisuuden. Sosiaalisen median hyödyntäminen entistä paremmin rikostutkinnan ja ennalta estävän toiminnan näkökulmasta laajentaa kybermaailmassa tapahtuvan ennalta estävän toiminnan mahdollisuuksia. Viestittämällä esimerkiksi huijausviesteistä välittömästi niiden tultua poliisin tietoon saatetaan säästää voimavaroja muiden rikosten tutkintaan. Vaikka kyberrikosten torjunta, tutkinta ja ennalta estävä toiminta keskitettäisiin järkevällä tavalla yhteen paikkaan, toiminnan organisointiin vaikuttavat kansalaisten tarpeet ja sen myötä paikallispoliisin osaaminen, resurssit ja siellä suoritettavat tehtävät. (The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime 2014, 25-27, 38, 42)

Vakavan ja järjestäytyneen rikollisuuden torjunta ja ennalta estäminen edellyttää tiedustelutoimintaa, koska se pääsääntöisesti on piilorikollisuutta. Suomessa poliisin suorittama tiedustelutoiminta on ollut perinteisesti luonteeltaan lähinnä rikostutkintaan liittyvää yksittäiseen rikoskokonaisuuteen kohdistuvaa tiedustelua. Rikostiedustelu on tiettyyn rikokseen, rikoksesta epäiltyyn tai rikoskokonaisuuteen liittyvää systemaattista tiedon keräämistä, tallentamista, käsittelyä ja analysointia. Rikostiedustelussa tiedonhankintamenetelminä käytetään kattavasti niitä lakitasoisia toimivaltuuksia, joita vi-

ranomaiselle on myönnetty sille säädettyjen tehtävien toteuttamiseksi. Tiedonhankinnan pääasiallisena kohteena on henkilö, jonka voidaan perustellusti olettaa syyllistyvän tai syyllistyneen rikokseen. Rikostiedustelun kohteena voi olla myös laite, menetelmä tai ohjelmisto. (Poliisin kybertoimivaltuudet 2015, 9)

Laajempaan tiedon keräämiseen, luokitteluun, analysointiin ja hyödyntämiseen on alettu vasta viime vuosina keskittää enemmän voimavaroja. Tiedustelu-elementti on sisältynyt suomalaiseen lähipoliisitoimintaan jo vuosia, samoin kuin tietojohtoisesta poliisitoiminnasta on käyty keskustelua. Varsinaisesti tiedustelun laajamittaista organisointia siten, että se ohjaisi poliisitoimintaa, ei kuitenkaan ole tehty eikä voimavaroja siihen ole kohdistettu. Suomalainen poliisitoiminta etenkin rikostutkinnan osalta on jo vuosikymmeniä perustunut perinteiseen ajatteluun, jossa rikosilmoitukset ohjaavat poliisin toimintaa ja toiminta on muutenkin reaktiivista. Tiedustelu-käsitteen jalkauttaminen paikallispoliisin arkeen ei ole vielä tapahtunut siten, että poliisitoimintaa todellisuudessa ohjaisi luotettava ja analysoitu tieto.

Tiedusteluun perustuva poliisitoiminta on ollut avainasemassa kaikessa Europolin toteuttamassa strategisessa arvioinnissa. Europol auttaa jäsenmaitaan muun muassa edistämällä kansallisten lainvalvontaviranomaisten välistä rikostiedustelu- ja muiden tietojen vaihtoa käyttäen apun Europolin tieto- ja analysointijärjestelmiä ja suojattua tiedonvaihtoverkkosovellusta (SIENA), tekemällä operatiivisten toimien analyysejä EU-maiden toimien tueksi, laatimalla strategisia selvityksiä (esim. uhka-arvioita) ja rikosanalyysejä itse keräämiensä, EU-maiden toimittamien tai muista lähteistä kerättyjen tietojen avulla, antamalla asiantuntija-apua ja teknistä tukea EU:ssa toteutettavaa tutkintaa ja operatiivista toimintaa varten EU-maiden valvonnassa ja oikeudellisella vastuulla. (Europolin verkkosivut 2015)

Suomessa valtakunnallinen rikostiedustelu on muodostettu yhteiseksi Poliisin, Tullin ja Rajavartiolaitoksen yhteistoiminnoksi (PTR)[55]. PTR -yhteistoiminta on rikostorjuntayhteistyön (PTR -rikostiedustelu- ja analyysitoiminta) ohella yhteispartiointia, valvonta- ja muun kaluston yhteiskäyttöä, koiratoimintaa ja koulutusta (Jukarainen & Laitinen 2014, 13).

PTR-toiminto muodostuu PTR-keskuksesta sekä Maa-, Meri- ja Ilmayksiköistä. PTR-keskus ohjaa ja koordinoi toimintaa ja kolme erillisyksikköä vastaa kukin nimensä mukaisesti eri liikennemuotoihin kohdistuvasta rajat ylittävän rikollisuuden torjunnasta. PTR-toiminnossa mukana olevat tahot toimivat omilla toimivaltasäännöksillään ja ovat omien hallinnonalojen ohjauksessa pois lukien päivittäinen työnjohto. PTR-toiminnon ohjausta varten on muodostettu eri tason toimijoista koostuvia työryhmiä, jotka ohjaavat toimintoa. Paikallispoliisiin sekä Tulliin ja Rajavartiolaitokseen on muodostettu toiminnot, jotka linkittyvät PTR-toimintoon ja yhdessä ne laativat muun muassa päivittäisen tilannekuvan valtakunnallisesta vakavasta ja järjestäytyneestä rikollisuudesta. Valtakunnallista tilannekuvaa laajentavat edellä mainittujen tahojen lisäksi Rikosseuraamuslaitos sekä Suojelupoliisi tuottaen tietoa omalta toimialaltaan. PTR -viranomaisten rikostorjunnalle Harmaan talouden selvitysyksikkö on tärkeä kumppani, joka auttaa paljastamaan ja tietoisuutta levittämällä ennaltaehkäisemään vakavaa ja järjestäytynyttä rikollisuutta. Harmaan talouden selvitysyksikkö toimii ikään kuin

[55] Laki poliisin, tullin ja rajavartiolaitoksen yhteistoiminnasta (687/2009). Lain tarkoituksena on edistää poliisin, tullin ja rajavartiolaitoksen (*PTR-viranomaiset*) yhteistoimintaa sekä PTR-viranomaisten yhteisten toimintalinjojen toteuttamista siten, että PTR-viranomaisille säädetyt rikosten estämiseen, paljastamiseen ja selvittämiseen (*rikostorjunta*), valvontaan sekä niitä koskevaan kansainväliseen yhteistyöhön liittyvät tehtävät ja yksittäiset toimenpiteet tulevat hoidetuiksi tarkoituksenmukaisesti, tehokkaasti ja taloudellisesti. Yhteistoiminnalla tarkoitetaan tässä laissa rikostorjuntaan, valvontatoimintaan tai kansainväliseen yhteistyöhön liittyvän toimenpiteen suorittamista toisen PTR-viranomaisen puolesta tai apuna tämän tehtäväalueella sekä toimimista yhteistyössä PTR-viranomaisten yhteisellä tehtäväalueella. PTR-viranomaisten tehtävistä ja niihin liittyvistä toimivaltuuksista on voimassa, mitä niistä on erikseen säädetty. (Laki poliisin, tullin ja rajavartiolaitoksen yhteistoiminnasta 1 §: Yleiset säännökset)

hallinnollisena, ei vain rikosoikeudellisena tiedusteluyksikkönä (Jukarainen & Laitinen 2014, 18).

Suomalainen lainvalvontaviranomaisten tiedustelumalli muodostuu pitkälti keskinäisestä viranomaisyhteistyöstä, koska kaikki tahot toimivat omilla toimivaltuuksillaan ja omassa tulosohjauksessa. Varsinaista strategista kumppanuutta toimijoiden välillä ei ole, koska strateginen kumppanuus edellyttää jäykkien toimivaltuusrajojen purkamista sekä jaettua, laajaa tulkintaa vakavasta ja järjestäytyneestä rikollisuudesta, jossa viranomaisten kaikkea toimintaa tukisi vahvemmin myös yhdessä jalostettu ja analysoitu strateginen ilmiötason tieto (Jukarainen & Laitinen 2014, 14–15).

Kyberrikollisuudesta puhuttaessa kyse on usein perinteisestä rikollisuudesta (esimerkiksi petokset, varkaudet, lapsiporno), joka on toteutettu tietoverkossa tai sitä hyödyntäen nopeasti aiheuttamalla suuri määrä rikoksen uhreja. Rikokset eivät ole enää välttämättä kansallisia, vaan valtioiden rajat ylittäviä, jolloin niiden torjuntaan eivät enää perinteiset yhteistyömuodot riitä, vaan ne ovat tehottomia. Kansainväliset tietoverkkoyhteydet ja – järjestelmät lainvalvontaviranomaisten välillä eivät enää ole riittäviä, vaan yhteistyötä vaaditaan myös yksityisen sektorin toimijoiden kanssa huomioimatta valtioiden rajoja. Esimerkiksi yksityiset turvallisuuspalvelut on merkittävä toimijoita maksukorttiteollisuudessa, muussa omaisuuteen tai varallisuuteen liittyvässä teollisuudessa ja lentoliikenneturvallisuudessa kuten osaltaan pankit ja televiestinnän tarjoajat ja niin edelleen, on siis olemassa valtava määrä maailmanlaajuisia toimijoita, joilla on merkitystä tietoverkkorikollisuuden torjunnassa. Tämä luo pakotteen poliisin yhteistyöhön näiden tahojen kanssa. Tehokkaan ja tuloksellisen kyberrikostorjunnan näkökulmasta poliisin tarvitsee strategisia kumppanuuksia[56] yksityisen sektorin toimijoiden kanssa. (Broadhurst 2006, 2-3, 11)

[56] Strateginen kumppanuus on kahden tai useamman yrityksen tai toimijan välinen toimintamalli, jossa osapuolet tekevät toisiaan täydentäviä, molempia hyödyttäviä toimenpiteitä ja investointeja yhteistyösuhteessa, jonka kustannukset, hyödyt, riskit ja haitat jaetaan osapuolten kesken. Kumppanuudet ovat luonteeltaan strategisia, koska ne koskettavat yritysten tai toimijoiden keskeisiä tutkimus ja kehitys-, tuotanto- tai markkinointitoimintoja ja niillä on keskeinen rooli yrityksen liiketoiminnan uudistumisen ja kilpailukyvyn kannalta. (Illman, Hokkanen, Pokela, Pursula, Luoma ja Gilbert 2013, 13)

Yhteistyötä on jo paljolti kehitetty, mutta vaatimukset lisääntyvät koko ajan teknologian kehittyessä tuoden uusia haasteita rikosten ennalta estämiseen ja tutkintaan. Kansainvälinen yhteisymmärrys siitä, mitä tietoverkkorikollisuuden torjunta tarkoittaa, miten sitä tulisi toteuttaa ja niin edelleen, on nykyisessä kaikkien valtioiden yhteisten ongelmien ilmapiirissä parantunut. Yhteistyö tarpeet myös kyberrikollisuuden torjunnan osalta on ymmärretty ja asiaan ollaan pureutumassa hallinnollisten, lainsäädännöllisin[57] sekä teknisten ongelmakysymysten osalta. Yhteistyö edellyttää globaalia keskustelua ja sopimista. Vuonna 1997 ensimmäisessä Manilassa pidetyssä kansainväliseen rikollisuuteen liittyvässä konferenssissa[58], jonka tavoitteena oli parantaa yhteistyötä rikosasioissa, saatiin aikaan merkittäviä edistysaskeleita. ASEAN-maiden ministerit sopivat, että kahdesti vuodessa järjestetään ministeritason kokouksia sekä asetettiin tavoitteeksi MLA-sopimusten[59] sekä muiden kahdenvälisten sopimusten ja yhteisymmärryspöytäkirjojen[60] allekirjoittaminen ASEAN-jäsenmaiden kesken. Lisäksi sovittiin perustettavaksi ASEAN:n kansainvälisen rikollisuuden keskus, jonka tehtäväksi tuli koordinoida tiedustelutiedon jakaminen kansainvälisestä rikollisuudesta yhdenmukaisesti poliittiselle päätöksentekotasolle sekä lainvalvontaviranomaisille torjuntatoimien suuntaamiseksi sekä sovittiin perustettavaksi korkean tason Ad-hoc -asiantuntijaryhmä, jonka tehtäväksi tuli kehittää toimintasuunnitelma kansainvälisen rikollisuuden torjumiseksi. (Broadhurst 2006, 18)

Valtiosopimuksessa Euroopan neuvoston tietoverkkorikollisuutta koskevasta yleissopimuksesta (60/2007) on määritelty tietoverkkoihin liittyviä käsit-

[57] Esimerkiksi kaksoisrangaistavuuden vaatimus: Milloin rikos on tehty vieraan valtion alueella, Suomen lain soveltaminen voidaan perustaa 5, 6 ja 8 §:ään vain, jos rikos myös tekopaikan lain mukaan on rangaistava ja siitä olisi voitu tuomita rangaistus myös tämän vieraan valtion tuomioistuimessa. Rikoksesta ei silloin Suomessa saa tuomita ankarampaa seuraamusta kuin siitä tekopaikan laissa säädetään. (Rikoslaki 1 luvun 11 §, 16.8.1996/626)

[58] ASEANin (Association of Southeast Asian Nations) varsinaiset jäsenmaat ovat Brunei, Kambodza, Indonesia, Laos, Malesia, Myanmar, Filippiinit, Singapore, Thaimaa, Vietnam. Tämän lisäksi myös Euroopan Unioni on ASEAin ulkoinen kumppani. (www.asean.org)

[59] Laki Euroopan unionin jäsenvaltioiden lainvalvontaviranomaisten välisen tietojen ja tiedustelutietojen vaihdon yksinkertaistamisesta tehdyn neuvoston puitepäätöksen lainsäädännön alaan kuuluvien säännösten kansallisesta täytäntöönpanosta ja puitepäätöksen soveltamisesta

[60] Niin sanotut MoU-sopimukset (Memorandum of understanding)

teitä sekä sovittu kansallisesta lainsäädännöstä (muun muassa Luvaton tunkeutuminen tahallisesti tietojärjestelmään, Datan vahingoittaminen ja Tietokoneavusteinen väärennös). Sopimuksessa on myös määritelty kansainvälistä yhteistyötä ja keskinäistä oikeusapua tietoverkkorikosten tutkintaan liittyen sekä sovittu kansallisten yhteyspisteiden järjestämisestä, joka on käytettävissä joka päivä 24 tuntia vuorokaudessa, sen varmistamiseksi, että oikeusapua voidaan antaa välittömästi tietojärjestelmiin ja datasiirtoon liittyvien rikosten tutkinnassa tai niitä koskevassa oikeudenkäynnissä tai rikokseen liittyvän sähköisessä muodossa olevan todistusaineiston keräämisessä. Tietoverkkotiedustelua Euroopan neuvoston tietoverkkorikollisuutta koskevassa sopimuksessa ei ole käsitelty, vaan tietoverkkorikollisuutta on tarkasteltu pelkästään rikostutkinnan näkökulmasta.

Kyberavaruudessa ”vellovan” valtavan tietomassan ja – liikenteen seasta kyberrikollisuuden torjuntaan tarvittavien elementtien seulonta edellyttää erityisesti kohdennettua ja täsmäohjattua tiedonhankintaa, joka on tietojohtoisen poliisitoiminnan yksi tukijalka. Yhtenä keskeisenä pääteemana tietojohtoisessa poliisitoiminnassa on ennakoivuus ja ennalta estäminen. Samalla se on tulevaisuuden suunnittelua, jotta ilmiöitä, tapahtumia, toimintaympäristömuutoksia ja niin edelleen, ei jouduttaisi kohtaamaan ilman ennakointia ja valmistautumista. Strategisten tulevaisuuteen tähtäävien analyysituotteiden tarkoituksena on tuottaa strateginen konteksti, joka auttaa ymmärtämään ilmitulevia uhkia, ennakoiva näkemys, joka mahdollistaa suunnattujen strategioiden suunnittelun ja luomisen, vähentää tulevaisuuteen liittyviä epävarmuustekijöitä sekä varmistaa, että tarkoituksen mukainen materiaali, tarkoituksen mukaisessa muodossa on oikealla päätöksentekijällä oikeaan aikaan käytössä (Hakaniemi 2012, 43–46).

Tietojohtoista poliisitoimintamallia on jalkautettu suomalaiseen poliisitoimintaan jo vuosia ja toiminnan kehittäminen jatkuu edelleen. Poliisitoiminnan toimintaympäristö on laajentunut viimeisten vuosien aikana ja mukaan on tullut Kybertoimintaympäristö ja sen myötä yhteiskuntaan kohdistuvat uhkat ovat muuttuneet vaikutuksiltaan aiempaa vaarallisemmiksi niin yksittäisten ihmisten, yritysten kuin koko yhteiskunnan kannalta. Kybertoimin-

taympäristössä tapahtuvat muutokset ovat nopeita ja vaikutuksiltaan vaikeasti ennakoitavia. Kyberympäristö tarjoaa erityisesti järjestäytyneelle ja vakavalle rikollisuudelle otollisen maaperän toimia. Tietojohtoisen poliisitoiminnan periaatteet ja toimintamallit on ulotettava koskemaan myös kyberrikollisuutta, jotta järjestäytynyttä ja vakavaa rikollisuutta voidaan tehokkaasti torjua ja ennalta estää kybertoimintaympäristössä[61]. David S Wall on todennut, että poliisin toiminta kybertoimintaympäristössä on vielä hahmottumatta ja rooli toimijana kyberympäristössä on ratkaistava kuten siellä tapahtuvan rikollisuuden torjuntaan kohdistettavat resurssit verrattuna ”normaaliin poliisitoimintaan” (Wall 2007, 17–21).

[61] Kybertoimintaympäristö on sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö (Suomen kyberturvallisuusstrategia 2013, 12).

6 POHDINTA

Tässä osiossa käsittelen toista tutkimuskysymystäni: Miten vakavan ja järjestäytyneen rikollisuuden kybertiedustelutoiminta tulisi paikallispoliisin näkökulmasta järjestää ottaen huomioon tietojohtoisen poliisitoiminnan vaatimukset? Asian käsittelyn konkretisoimiseksi käytän esimerkkinä Itä-Uudenmaan poliisilaitosta.

Itä-Uudenmaan poliisilaitoksessa tietoverkkorikostutkintayksikkö on sijoitettu poliisilinjan erityistutkintasektorille. Yksikköön kuuluu tutkinnanjohtaja, ryhmänjohtaja sekä neljä tutkijaa. Yksikkö vastaa elektronisen todistusaineiston keräyksestä ja käsittelystä sekä tietotekniikkarikosten tutkinnasta. Yksikkö ei itsenäisesti suorita tietoverkkorikostiedustelua pois lukien yksittäisiin rikoksiin liittyvää tiedonhankintaa avoimista lähteistä. Valtakunnallisessa tarkastelussa poliisilaitoksen toimintaedellytykset verrattuna muihin paikallispoliisin yksiköihin ovat hyvällä tasolla.

Tietojohtoinen poliisitoiminta edellyttää, että toimenpiteiden taustalla on reaaliaikainen tilannekuva, jonka perusteella tehdään analysoitujen tietojen pohjalta päätöksiä siitä, mihin toiminta kohdistetaan sen mukaisesti, mitkä ovat strategiset painopisteet ja valinnat. Näin myös tulisi toimia vakavan ja järjestäytyneen rikollisuuden torjunnassa. Vakava ja järjestäytynyt rikollisuus levittäytyy ja on jo siirtynyt toimimaan kyberavaruudessa hyödyntäen sen mahdollisuuksia. Perinteinen tiedonhankinta ja tiedustelutoiminta tulisi siirtää toimimaan tehokkaasti myös kybertoimintaympäristössä. Tämä asettaa useita haasteita poliisilaitoksissa sekä poliisin toimintarakenteissa ottaen huomioon muut poliisille annetut velvoitteet ja tehtävät.

Vakavan ja järjestäytyneen rikollisuuden torjunta kybertoimintaympäristössä edellyttää organisaatiolta uudenlaista ajattelua, rakenteita, reagointikykyä, osaamista ja resursointia. Rikosten paljastaminen ja selvittäminen edellyttävät toimimista kansainvälisesti ja nopeasti, koska rikollisten jäljet häviävät tai ne häivytetään mahdollisemman pian. Vakavan ja järjestäytyneen

rikollisuuden perinteiset hierarkiarakenteet eivät välttämättä enää toimi kybermaailmassa. Rikollisten yhteenliittymät syntyvät kulloisenkin tarpeen mukaan sen asian ympärille, johon toiminta kohdistuu. Tällä on vaikutuksia myös viranomaisten toimintaan, jo rikollisuuden tilannekuvan ylläpidon kannalta. Rikosten paljastamisen ja selvittämisen prosessit vaativat pohdintaa siitä, mihin jatkossa poliisin resurssit riittävät ja mihin toiminta kannattaa kohdistaa. Esimerkiksi perinteisen rikollisuuden yksi tehokas tutkintamalli, rikosten sarjoittaminen ei välttämättä enää sovellu kybertoimintaympäristöön tai siitä ei ole saatavissa vastaavaa hyötyä kuin reaalimaailmassa. Poliisiyksiköiden sisäiset ja keskinäiset organisaatiorakenteet, joissa toiminta on jaettu siiloihin ja lokeroihin saattaa kangistaa toimintaa. Johtamisrakenteiden ja resurssien käytön tulisi joustaa tarpeen mukaan, jolloin poliisitoiminta muuttuu entistä enemmän asiantuntijaorganisaation projektiluonteiseksi prosessin omaiseksi tekemiseksi.

Edellä mainittujen esimerkkien valossa paikallispoliisi ei jatkossa enää kykene vastaamaan läheskään täysipainoisesti kybermaailman haasteisiin. Poliisin rikostutkinta on edelleen järjestetty pitkälti samoilla periaatteilla kuin jo useita kymmeniä vuosia sitten, perinteisen ja reaalimaailman rikostutkinnan ehdoin. Rikosten ennalta estävä tai paljastava rikostiedustelu on pohjiltaan samanlaista kuin se on jo pitkään ollut. Tulisi ensinnäkin määritellä mitä tiedustelu kybertoimintaympäristössä tarkoittaa.

Tietoverkoissa olevista avoimista ja julkisista lähteistä on saatavissa paljon tietoa henkilöistä ja asioista, jotka ovat jokaisen tietoverkkoja käyttävän saatavilla. Näiden tietojen kerääminen ja hyödyntäminen on käytännössä sama, jos kyseiset tiedot saisi esimerkiksi lukemalla ne sanoma- tai muista paperilehdistä ja kirjoista. Kohdennettu rikostiedustelu tulisi määritellä siten, ettei sitä ”mystifioida” vain siksi, että se tapahtuu kyberavaruudessa. Rajapintojen määrittely olisi tärkeää, mikä on sellaista, jota kaikki voivat tehdä ja mikä edellyttää viranomaiselta erityisiä toimivaltuuksia tiedon saamiseksi. Jatkossa perinteinen ja kybermaailmassa tapahtuva tiedustelutoiminta tulisi olla johdettua ja kohdennettua toimintaa, joka etenee saumattomasti rikostutkintaan ja -prosessiin. Tällä hetkellä rikostiedustelun ja -tutkinnan rajapinnat

eivät läheskään aina kohtaa reaalimaailmassakaan johtuen osin toimimattomista työprosesseista. Kybertoimintaympäristössä toimiminen lisää haasteita, mutta toisaalta pakottaa uudistumiseen.

Jos esimerkkinä tarkastellaan Itä-Uudenmaan poliisilaitosta, edellä mainitut toimintaympäristön ja -kulttuurin muutokset vaatisivat jatkossa huolellisen pohdinnan siitä, miten poliisilaitos jatkossa täyttää kyberrikostorjunnan vaatimukset. Jotta tiedustelutoimintaa saataisiin parannettua, siihen kohdennettua resurssia tulisi lisätä, joka mahdollistaisi päätoimisen kyberrikostiedustelun. Toimijoiden osaamistasoa, käytettäviä laitteistoja ja ohjelmia tulisi hankkia, poliisilaitoksen ja yksikön roolit ja vastuut tulisi selkeästi määritellä suhteessa toisiinsa ja Keskusrikospoliisiin ja niin edelleen. Todennäköisesti näin menetellen rakennettaisiin organisaatiota tilkkutäkkimäisesti, yksittäisiä paloja toisiinsa yhdistellen, jolloin kokonaiskuva taustalta häviäisi.

Edellä kuvatut tarpeet ovat tällä hetkellä myös melko epärealistisia johtuen poliisin toimintaedellytyksistä ja toimintaympäristömuutoksista. Poliisihallinnon rahoituksen leikkaaminen on vähentämässä vajaat 900 poliisivirkaa vuodesta 2017 lähtien ja vuoden 2015 loppupuolella tapahtunut räjähdysmäinen nousu maahanmuuttajamäärissä on pakottanut koko poliisihallinnon ponnistelemaan tilanteen haltuun saamiseksi. Nyt näyttää siltä, että maahanmuuttoon liittyvät velvoitteet todennäköisesti tulevat työllistämään poliisia jatkossakin useiden vuosien ajan eteenpäin.

Poliisin roolia ja tehtäviä sekä koko kyberrikostiedustelun keskittämistä yhteen paikkaan tulisi miettiä laajemmin. On selvää, että poliisin käytettävissä olevat resurssit eivät tule lähivuosina lisääntymään. Tämä pakottaa hyödyntämään jo voimassa olevia resursseja ja toimijoita. Voisiko joku muu toimija kantaa osavastuun toiminnasta, vai tulisiko poliisin toiminta liittää osaksi muuta tai muita toimijoita? Poliisin lisäksi eri viranomaistahot (muun muassa Tulli, Rajavartiolaitos, Puolustusvoimat ja Viestintävirasto) ja yksityiset toimijat seuraavat omalla toimialallaan kyberavaruudessa tapahtuvaa viestiliikennettä, jolloin näitä rajapintoja poliisin toiminnan kanssa tulisi tarkastella laajemmassa kokonaisuudessa. Saisimmeko yhteistyön kanavoinnilla

hyödyntämällä resursseja ja osaamista kehitettyä rikostorjunnan kannalta tehokkaan toimijan?

Yhteenvetona tutkimuskysymykseen, miten vakavan ja järjestäytyneen rikollisuuden kyberrikostiedustelutoiminta tulisi paikallispoliisin näkökulmasta järjestää ottaen huomioon tietojohtoisen poliisitoiminnan vaatimukset, voidaan todeta, että koko kyberrikostiedustelutoimintaa tulisi tarkastella laajasti koko hallinnossa. Tiedustelutoiminnassa tulisi hyödyntää mahdollisuuksien mukaan eri tahojen vahvuus- ja osaamisalueita.

Tekemällä pieniä muutoksia ei pystyttäne vastaamaan siihen vaativaan haasteeseen, jonka kybertoimintaympäristö tuo mukanaan. Koska kyse olisi monien eri hallinnonaloilla tai tahoilla olevista toimijoista, asiaa tulisi pohtia lainsäädännön ja strategioiden kautta, mitä esimerkiksi tulevaisuudessa poliisin kyberrikostorjunta on ja mitkä ovat sen tavoitteet. Sama linjaus tulisi tehdä jokaisen toimijan osalta. Kyse olisi vaativasta haasteesta, joka edellyttäisi korkean tason päätöksentekoa sekä asenne- ja ajatusilmapiirien muokkaamista.

7 JOHTOPÄÄTÖKSET

Poliisin hallinnonalan kyberstrategia tulisi laatia mahdollisemman pikaisesti, koska sen puuttuminen estää määrätietoisen ja kokonaisvaltaisen toiminnan kehittämisen. Strategian tulisi sisältää keskeiset toimintalinjat ja keinot kyberturvallisuuden kehittämiseksi ja sisäisen turvallisuuden toteuttamiseksi. Strategian tulisi määritellä myös tietoverkkotiedustelu ja sen toteuttamismuoto, mitä sillä tavoitellaan sekä painopisteet, joihin poliisin tulisi tiedustelutoiminta tietojohtoisen poliisitoiminnan näkökulmasta suunnata.

Tietoverkkotiedustelun toteuttaminen poliisissa edellyttää harkintaa siitä, miten tehokas ja tuottava toiminta tulisi organisoida. Toimintona tietoverkkotiedustelu tarvitsee ympärilleen laajalti eri toimijoita niin viranomaisista kuin yksityiseltä sektorilta. On pohdittava, tulisiko koko toiminto keskittää yhteen paikaan ja miten se tulisi sijoittaa ottaen huomioon Kyberturvakeskus, joka on keskeinen tietoverkoissa operoiva viranomainen.

Merkittävänä osa-alueena on yhteistyö muiden viranomaisten ja yksityisen sektorin kanssa. Tämä edellyttää verkostomaista työskentelyä ja sitä kautta tapahtuvan torjuntatyön johtamista toimijoiden yhteisen tilannekuvan kautta. Tulisi miettiä mallia, millä tavalla asiantuntija- ja verkostojohtaminen soveltuisi tietojohtoisen poliisitoiminnan lähtökohdista tietoverkoissa tapahtuvan rikostorjunnan johtamiseen. Lähtötavoitteena tulisi olla kyky muodostaa reaaliaikainen tilannekuva kyberrikosmaailmasta ja sen torjunnasta. Ilman sitä toiminnan suuntaaminen oikea-aikaisesti ja oikein kohdennetusti ei perustu suunnitelmalliseen, johdettuun ja tehokkaaseen torjuntatoimintaan, vaan reagoivaan suunnittelemattomaan ajelehtimiseen kyberavaruudessa.

Keskeinen kysymys on myös se, vastaavatko nykyiset poliisin organisaatiorakenteet ja erityisesti poliisin rikostutkinnan järjestelyt kyberrikostorjunnan vaatimuksia. Poliisin heikkenevät resurssit ja toimintaympäristön muutokset (esimerkiksi 2015 alkanut maahanmuuton räjähdysmäinen kasvu) herättävät myös kysymyksen siitä, kuinka poliisi ylipäätään pystyy jat-

kossa kantamaan vastuuta kyberrikostentorjunnasta. Lähitulevaisuudessa nämä asiat saattavat tulla pakonomaisesti ratkaistaviksi, jonka johdosta poliisihallinnossa tultaneen toteuttamaan uudelleen järjestelyjä tilanteen hallitsemiseksi ja yhteiskunnan antamien tehtävien hoitamiseksi. Nämä asiat muodostavat oman laajan kokonaisuuden ja niihin tulisi paneutua muissa tulevaisuudessa tehtävissä tutkimuksissa.

8 LÄHTEET

Arjen turvaa. Sisäisen turvallisuuden ohjelma 2004–2007, Sisäasiainministeriön julkaisusarja 44/2004, ISBN 951-734-763-4

Bayley David H. 1996: *The Future of Policing*, Law & Society Review, Vol. 30, No. 3. (1996), pp. 585-606

Brenner Susan W. 2002: *Article: Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships*, North Carolina Journal of Law & Technology, Volume4, and Issue1: Fall 2002

Broadhurst Roderick 2006: *Developments in the global law enforcement of cyber-crime*, Policing: An International Journal of Police Strategies and Management 29(2): pp. 408-433

BROWN, Steven David 2007: International Journal of Police Science & Management Volume 9 number 4 2007, pp. 336 – 340

Bryant Robin, Bryant Sarah: *Policing Digital Crime.* 2014 Dorchester, ISBN 987-1-4094-2343-0

Chesbro Michael 2010: *Introducing Criminal Intelligence*, Inside Homeland Security, Fall 2010

Convention on Cybercrime, Council of Europe, ETS 185, Budapest, 23.11.2001

Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa 7.2.2013, 6342/13

Ehdotus neuvoston päätelmiksi vakavan ja järjestäytyneen rikollisuuden torjuntaa koskevien EU:n painopisteiden asettamisesta vuosiksi 2014–2017 28.5.2013, 9849/13

Esitutkintalaki 22.7.2011/805

Euroopan komission muistio: *Komissio ehdottaa uusia EU:n toimenpiteitä eurooppalaisten suojelemiseksi*, Bryssel 22. marraskuuta 2010, IP/10/1535

Euroopan neuvoston julkaisema Europa-portaali Internetissä, Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus 2001, ETS 185, 23.11.2001.

Europol 2014: *The Internet organized crime threat assessment (iOCTA),* ISBN: 978-92-95078-96-3

Europol 2013: *EU Serious and Organised Crime Threat Assessment (SOCTA)*, 19.3.2013 Haag, ISBN: 978-92-95078-79-6

Expert Report on Computer-Related Crime' in 1989, Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies

Grabar Anton 2012: *Toimintakykyinen ja oppiva henkilötiedusteluoperaattori*, Maanpuolustuskorkeakoulu

Grönfors Martti 2011 (1985): *Laadullisen tutkimuksen kenttätyömenetelmät*, (toim.) Vilkka Hanna, Hämeenlinna, ISBN 978-952-93-0048-8

Hakaniemi Jussi 2012: *Analyysitoiminta ja päätöksenteko paikallispoliisissa, tietojohtoisen poliisitoiminnan sovelluksia*, Pro Gradu

Helminen Klaus, Kuusimäki Matti, Rantaeskola Satu 2012: *Poliisilaki*, Talentum, ISBN 978-952-14-1924-9

Helsingin Sanomien artikkelit: *Viestintäministeriö tyrmää verkkovalvonnan. Työryhmä ehdottaa Puolustusvoimille ja suojelupoliisille tiedusteluvaltuuksia. Liikenne- ja viestintäministeriö vastustaa verkkovalvontaa.* 11.1.2015 ja *Tiedusteluvaltuudet pitää punnita tarkoin*13.1.2015

Hirsjärvi Sirkka, Remes Pirkko ja Sajavaara Paula 2007: *Tutki ja kirjoita*, 13. painos, Otavan kirjapaino Oy, Keuruu, ISBN 978-951-26-5635-6

Illman Julia, Hokkanen Niina, Pokela Pekka, Pursula Tiina, Luoma Päivi ja Gilbert Ylva 2013: *Kumppanuudesta kilpailuetua, Strategiset yrityskumppanuudet vesi-, metsä- ja kemian alan tulevaisuuden kilpailuedun rakentajina*, Tekesin katsaus 298/2013, Helsinki, ISBN 978-952-457-560-7

Jukarainen Pirjo ja Laitinen Kari 2014: *Tietojohtoinen viranomaisyhteistyö ja sen vaikuttavuuden arviointi – Tapaustutkimus poliisin, tullin ja rajavartiolaitoksen rikostorjuntayhteistyöstä* (PTR -rikostiedustelu- ja analyysitoiminnasta), Poliisiammattikorkeakoulun katsauksia 6/2014, Tampere, ISBN 978-951-815-828

Järjestäytyneen rikollisuuden ja terrorismin torjunta, Sisäisen turvallisuuden ohjelman valmisteluun osallistuneen asiantuntijaryhmän loppuraportti, Sisäasiainministeriö, 31.3.2008

Kansallisen kyberstrategian toimeenpano-ohjelma, Turvallisuuskomitea, 194/8.1.99/2013, 11.3.2014

Metsämuuronen Jari 2003: *Tutkimuksen tekemisen perusteet ihmistieteissä*, 2. uudistettu painos, Gummerus, Jyväskylä, ISBN 952-5372-15-4

Mälkiä, Matti ja Kiehelä, Hannu 1999: *Lähipoliisi lähestymistapana*, poliisiammattikorkeakoulun oppikirjat 4, toimittajat Kiehelä Hannu & Sirpa Virta, OY Edita Ab, Helsinki

Komission tiedonanto Euroopan parlamentille ja neuvostolle, Viimeinen kertomus vuosien 2010–2014 sisäisen turvallisuuden strategian täytäntöönpanosta, 20.6.2014 Bryssel

Laki Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta, 539/2007

Leppänen Anna ja Kankaanranta Terhi 2013: Kosmopolis-lehden artikkeli; *Tietoverkkorikollisuus kyberuhkana: strategiat ja julkinen ilmiöseuranta Suomessa*, KOSMOPOLIS – Vol. 43:3/2013

Leppänen Anna ja Virta Sirpa 2014: *Kohti systeemiälykästä kyberturvallisuuden hallintaa - kyberrikollisuus ja sen torjunta*, Futura 2/2014, ISSN 0785–5494 Vammala

Lähipoliisitoiminnan strategia, Lähipoliisitoiminnan ja turvallisuusyhteistyön kehittämisen strategiset linjaukset ja tavoitteet, Poliisin ylijohdon julkaisusarja 1/2007, ISBN 952-491-076-4 (nid.)

Lähipoliisitoiminnan strategia, Lähipoliisitoiminnan ja turvallisuusyhteistyön kehittämisen strategiset linjaukset ja tavoitteet 2010, Poliisihallitus, ISBN 978-952-491-514-4 (nid.)

Marion Nancy E. 2010: *The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation*, International Journal of Cyber Criminology Vol 4 Issue 1&2 January - July 2010 / July - December 2010

Neuvoston päätelmät komission ja Euroopan unionin ulkoasioiden ja turvallisuuspolitiikan korkean edustajan yhteisestä tiedonannosta "Euroopan unionin kyberturvallisuusstrategia: Avoin, turvallinen ja vakaa kybertoimintaympäristö" 7.2.2013, 12109/13

Oikeusministeriö 2014: Järjestäytynyttä rikollisuutta koskevan käsitteistön yhtenäistäminen, Mietintöjä ja lausuntoja 23/2014, ISBN (pdf) 978–952-259-363-4

Palo Sanna 2010: *Järjestäytyneet rikollisryhmät ja rikosvastuu*, Yliopistopaino, Helsinki, ISBN 978-952-10-5536-2 (PDF)

Pihlajamäki Antti 2004: *Tietojenkäsittelyrauhan rikosoikeudellinen suoja*, Gummerus Kirjapaino Oy, Jyväskylä, ISBN 951-855-233-9

Poliisilaki 22.7.2011/872

Poliisin ennalta estävän toiminnan strategia vuosille 2014 – 2018 vuonna 2014, Sisäministeriön julkaisu 2/2014, Helsinki, ISBN 978-952-491-899-2

Poliisin kybertyöryhmän loppuraportti 2015: Poliisin kybertoimivaltuudet, POL-2015–3879

Poliisin strategia 2015, Poliisin internetsivut

Ratcliffe, Jerry H 2008: *Intelligence-Led Policing*, Willan Publishing, Devon EX15 3AT, United Kingdom

Ratcliffe Jerry H ja Guidetti Ray 2008: *State police investigative structure and the adoption of intelligence-led policing*, Policing: An International Journal of Police Strategies and Management, Vol. 31 Iss: 1, pp.109 – 128

Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies

Safety & Security Studies: *Cybercrime and the Police*. 2013 Haag, ISBN 987-94-6236-069-3

Sipilän strateginen hallitusohjelma vuosille 2015–2018; Ratkaisujen Suomi 29.5.2015, Hallituksen julkaisusarja 10/2015 Helsinki, ISBN PDF 978–952-287-181-7

Sisäministeriön verkkosivut

Suomen kyberturvallisuusstrategia ja taustamuistio. Valtioneuvoston periaatepäätös 24.1.2013 Helsinki, ISBN 978-951-25-2434-1
Suomen Rikoslaki, 19.12.1889/39

Suomalaisen tiedustelulainsäädännön suuntaviivoja,
Tiedonhankintalakityöryhmän mietintö 14.1.2015 Helsinki, 978–951-25-2624-6

Terveyden ja hyvinvoinnin laitos 2014, *Huumetilanne Suomessa 2014*, THL – Raportti 1/2015, Juvenes Print – Suomen Yliopistopaino Oy, Tampere, ISBN 978-952-302-414-4 (verkkojulkaisu)

Tietojohtaminen 2013, Tampereen teknillinen yliopisto, tietojohtamisen tutkimuskeskus Novi, Juvenes print, Tampere, ISBN 978-952-15-3058-6

Tietotekniikkatutkinnan järjestäminen poliisissa, Poliisin ylijohdon julkaisusarja 7/2008, Helsinki, ISBN 978-952-491-104-7 (nid.)

The Police Executive Research Forum 2013: *Compstat: Its Origins, Evolution, and Future In Law Enforcement Agencies*, Washington, ISBN: 978-1-934485-23-1

The Role of Local Law Enforcement Agencies In Preventing and Investigating Cybercrime 2014, Critical issues in policing series, Police executive research forum, USA, ISBN: 978-1-934485-24-8

Tietotekniikkatutkinnan järjestäminen poliisissa, Poliisin ylijohdon julkaisusarja 7/2008, ISBN 978-952-491-104-7

Tietoyhteiskuntakaari 7.11.2014/917

Tietoyhteiskuntakaaren lainsäädäntövalmisteluasiakirjat vuosilta 2011–2013

Turvallinen elämä jokaiselle. Sisäisen turvallisuuden ohjelma 2007–2011, Sisäasiainministeriön julkaisusarja 16/2008, ISBN 978-952-491-347-8

Turvallisempi huominen. Sisäisen turvallisuuden ohjelma 2012–2015, Sisäasiainministeriön julkaisusarja 26/2012, ISBN 978-952-491-760-5

Valtioneuvoston periaatepäätös järjestäytyneen rikollisuuden torjunnan strategiasta 2013

Verottajan verkkosivut (Vero.fi) 2015: *Virtuaalivaluuttojen tuloverotus*, 28.8.2013, A83/200/2013

Wall David S 1998: *Catching Cybercriminals: Policing the Internet*, International Review of Law, Computers and Technology, vol. 12, Number 2, pages 201-2018

Wall, D.S. 2007: *Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace* (Revised May 2010), *Police Practice & Research: An International Journal*, 8(2):183 205

Wall, D.S. 2008: *Cybercrime, Media and Insecurity: the shaping of public perceptions of cybercrime*, International Review of Law, Computers and Technology, vol. 22, nos. 1-2, pp. 45–63 (ISSN 0965-528X)

Willa Kirsi ja Uusitupa Seppo 2007: *Tietoliikenneaapinen*, TTK.

Virta, Sirpa 2005: *Tavoitteena turvallisuus*, Tampereen yliopistopaino Oy – Juvenes Print, Tampere

Yhteiskunnan turvallisuusstrategia, Valtioneuvoston periaatepäätös 16.12.2010 Helsinki, ISBN 978-951-25-2170-8

Yhteinen tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Euroopan unionin kyberturvallisuusstrategia 7.2.2013, 6225/13

Yhteiskunnan turvallisuusstrategia, Valtioneuvoston periaatepäätös 2011, Puolustusministeriö, Vammalan kirjapaino, ISBN: 978–951-25-2170-8