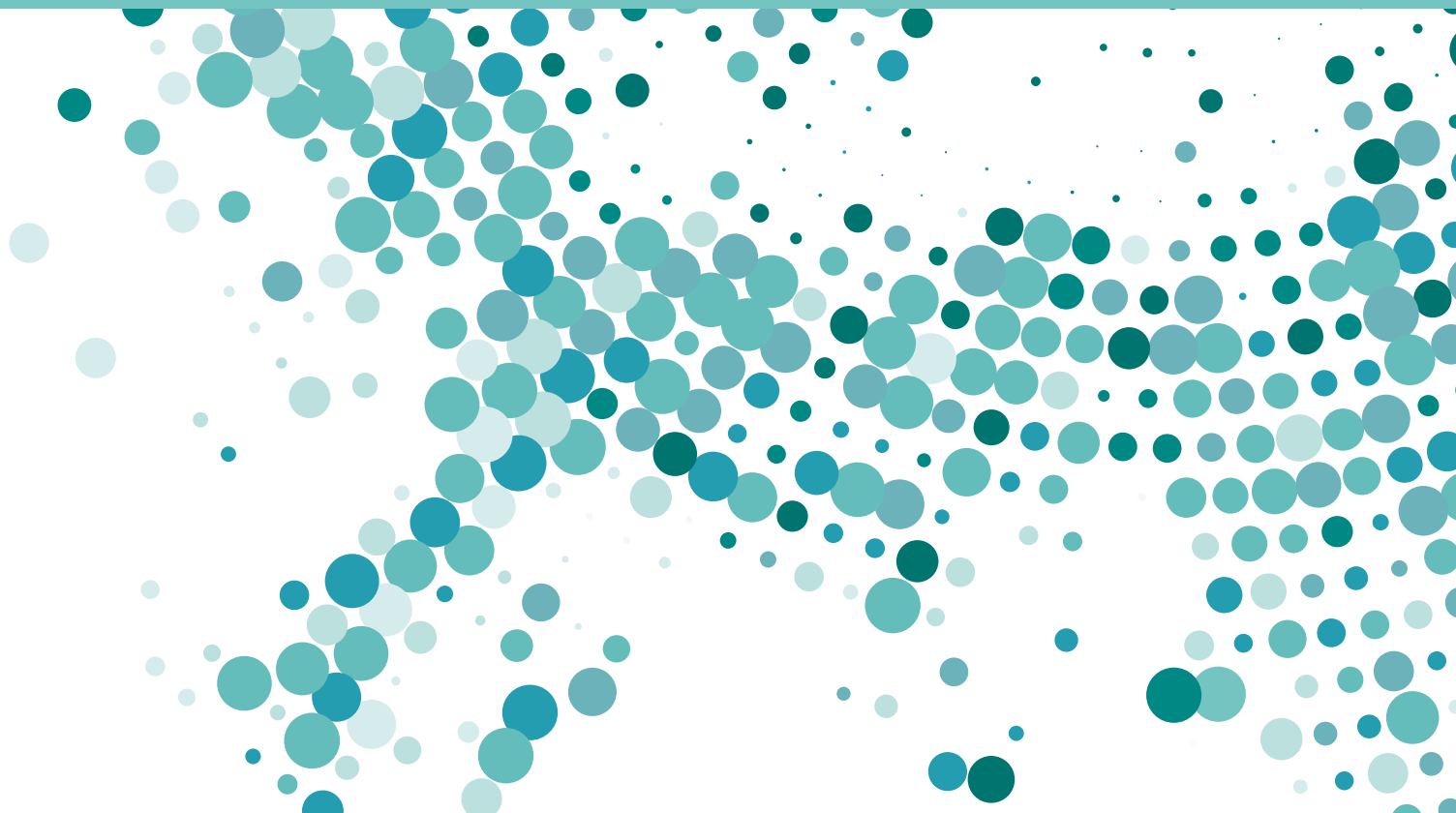
SISÄMINISTERIÖ
INRIKESMINISTERIET

Tietoverkkorikollisuuden torjuntaa koskeva selvitys

SISÄMINISTERIÖN JULKAISU 14/2017

Sisäinen turvallisuus



Sisäministeriön julkaisu 14/2017

Tietoverkkorikollisuuden torjuntaa koskeva selvitys

Sisäministeriö, Helsinki 2017

Sisäministeriö

ISBN: 978-952-324-135-0 (nid.)
978-952-324-136-7 (PDF)

ISSN: 2341-8524

Taitto: Valtioneuvoston hallintoyksikkö/
Tietotuki- ja julkaisuyksikkö/Anitta Türkkan

Helsinki 2017

Sisältö

TIIVISTELMÄ

Tietoverkkorikosten määrät ovat lisääntyneet ja tulevat lisääntymään edelleen merkittävästi. Tuottoisin rikollisuus toimii tietoverkossa ja etenkin verkossa tapahtuvien petosrikosten määrät ovat kasvaneet. Esineiden internet[1] (IoT, internet of things) tulee muuttamaan erilaisten vahingontekorikosten toteutusmenetelmiä. Tietoverkkorikollisuus on suurelta osin rajat ylittävää rikollisuutta. Globalisoituneessa ja keskinäisriippuvaisessa maailmassa uhat ovat monimuotoistuneet ja perinteisten uhkien rinnalle on noussut uudenlaisia, nopeasti syntyviä ja vaikutuksiltaan vaikeasti ennakoitavia tilanteita. Hybridi kuvaa konfliktien monimuotoisuutta ja yllättävyyttä. Vanhaa ja uutta yhdistämällä rikolliset luovat jatkuvasti uusia tekotapoja. Lennokkien käyttöön liittyvät rikollisuusuhat ovat nousseet Suomessakin. Niiden avulla on mahdollista toteuttaa vakoilua, skannata ja saastuttaa verkkoja sekä hyödyntää haavoittuvia laitteita langattomasti.

Rikollisten hyödyntämien verkkofoorumeiden toiminta on johtanut rikollisuuden teollistumiseen ja voidaankin puhua ns. palveluun perustuvasta rikollisesta teollisuudesta. Tietoverkossa toimiva rikollinen palveluteollisuus muuttaa järjestäytyneen rikollisuuden rakenteita. Rikollisten kyky toteuttaa tavoitteensa kohteessa on usein selvästi parempi ja kehittynyt nopeammin kuin kohdeorganisaatioiden kyky havaita tunkeutujia. Globaali kyberympäristö mahdollistaa ääriryhmien välisen verkottumisen, tiedonvaihdon ja terroristisen materiaalin levittämisen.

Osaamisen kehittäminen on eräs tärkeimmistä poliisihallinnon tehtävistä kyberturvallisuusstrategian saavuttamisessa. Kyberturvallisuusstrategian linjaus huolehtia poliisin tehokkaista kyberrikostorjunnan edellytyksistä pitää sisällään muun muassa sen periaatteen, että poliisilla tulee olla osaava ja motivoitunut henkilöstö, joka hoitaa kybertoimintaympäristössä tapahtuvien rikosten ennaltaehkäisemisen, taktisen esitutkinnan sekä digitaalisen todistusaineiston käsittelyn ja analysoinnin oikeusvarmalla tavalla. Esitutkinta- ja turvalli-

1 Esineiden internetiä kuvaa se että tietoteknologia on sulautunut arkisiin esineisiin kuten kodin laitteisiin, joita pystyy internetin yli seuraamaan ja ohjaamaan tietokoneella, puhelimella tai muilla laitteilla, kuten tabletilla.

suusviranomaisilla tulee olla uhan vakavuus huomioon ottaen riittävät toimivaltuudet ennalta estää, paljastaa ja selvittää kyberrikoksia sekä torjua kyberuhkia. Jatkuvasti muuttuva toimintaympäristö edellyttää lainsäädännön arviointia ja kehittämistä jatkuvana ja pysyväisluonteisena toimintana.

Poliisin suorituskykyä ja lainsäädännöllisiä edellytyksiä torjua rikoksia tietoverkkoympäristössä tulee edelleen kehittää. Ennalta estävän ja tietojohtoisen poliisitoiminnan toteuttamiseksi poliisin päätöksentekijöillä tulee olla käytettävissään reaaliaikaista ja analysoitua tietoa. Poliisin kiireellisimmät ja tärkeimmät lainsäädännön kehitystarpeet tulevat jatkossa arvioitaviksi selvityksen toimenpidesuositusten mukaisesti.

Oikea ja ajantasainen tilannetietoisuus on edellytys tietojohtoiselle poliisitoiminnalle. Tilannekuvan avulla viranomaisilta ja yrityksiltä saadut operatiivisen toiminnan havainnot yhdistetään laajempiin, ilmiötason havaintoihin – sekä toisin päin – viestitään tarvittaville tasoille niin organisaation sisällä kuin ulkopuolisille sidosryhmille. Yhteistyö muiden viranomaisten ja elinkeinoelämän kanssa on tärkeää, koska tietoverkkorikollisuus ja kyberuhkat ilmiönä ylittävät rajat valtioiden rajat ja torjunta kuuluu monen eri viranomaisen ja lainkäytön piiriin.

Poliisiammattikorkeakoulun roolia kehitetään kyberrikostorjuntaosaamisen nostamisessa muun muassa lisäämällä kyberasioiden opetusta poliisin peruskoulutukseen, tarjoamalla kyberrikostorjuntaan erikoistuville laadukasta erityiskoulutusta, kehittämällä koulutus- ja tutkimusyhteistyötä viranomaisten, yliopistojen, korkeakoulujen kanssa sekä lisäämällä kyberalan tutkimusta.

Poliisin tietoverkkorikollisuuden torjunnan resurssitarpeet liittyvät erityisesti tietoteknisen tutkinnan eli digitaaliforensiikan kehittämiseen, vakavan tietoverkkorikollisuuden torjuntaan sekä tiedonhankintaan tietoverkoista.

Tämä selvitys on laadittu yhteistyössä sisäministeriön, poliisihallituksen asettaman työryhmän, Suojelupoliisin sekä Keskusrikospoliisin kanssa. Selvityksessä on lisäksi hyödynnetty tietoverkkorikollisuuden tilannekuvan parantamista koskevaa valtioneuvoston rahoittaman (VNTEAS) hankkeen kehittämisehdotuksia sekä Europolin internetin järjestäytynyttä rikollisuutta koskevaa uhka-arviota (Europol iOcta2015). Selvitys on ollut laajalla lausuntokierroksella huhtikuussa 2016.

1 Johdanto

Pääministeri Juha Sipilän hallitusohjelman mukaan hallitus selvittää tietoverkkorikollisuuden torjuntaan tarvittavat resurssit, toimintatavat ja lainsäädäntötarpeet vuoden 2015 loppuun mennessä. Hallitusohjelman mukaan tehostetaan viranomaisten, oppilaitosten ja yritysten yhteistä osaamisen kehittämistä. Lisäksi luodaan yhteinen tilannekuva tietoverkkojen ja tietoliikenteen turvallisuudesta sekä varmistetaan luotettava ja turvallinen tietojen vaihto eri toimijoiden välillä.

Kyberympäristö on olennainen osa rikollisuuden ja rikostorjunnan toimintaympäristöä, sillä tahallisesti toteutetun kyberympäristöön kohdistuvan poikkeaman taustalla on lähes aina rikos. Tietoverkkorikollisuudesta on tullut hyvin kattava rikollisuuden osa-alue ja sen vaikutukset kohdistuvat niin valtioihin, yksityisiin kansalaisiin kuin liiketoimintaankin. Tietoverkko on sekä rikollisille edullisempi, että myös riski-hyöty ja riski-vahinko – suhteessa entistä houkuttelevampi ympäristö toteuttaa rikoksia, joilla on taloudellinen tai jopa terroristinen tavoite. Turvallisuusympäristön muutoksen myötä turvallisuutta vaarantavat, normaaliajan tilanteessa tapahtuvat uhkat kuten hybridivaikuttaminen, kyberhyökkäykset ja terrorismi ovat lisääntyneet. Myös vakavimman ja yhteiskunnan kriittisiin toimintoihin kohdistuvan rikollisuuden tekotavat ovat tehostuneet ja uhkat kasvaneet. Laajoilla kyberhäiriöillä voi olla vaikutuksia yhteiskuntajärjestykseen ja sitä kautta sisäisen turvallisuuden viranomaisten toimintaan poliisi-, pelastus-, raja- tai maahanmuutontehtävien kasvavina määrinä.

Valtioneuvoston periaatepäätöksenä 24.1.2013 annetun Suomen kansallisen kyberturvallisuusstrategian mukaan poliisilla tulee olla keinot ja osaaminen tunnistaa tietoverkkoihin liittyviä rikollisuusilmiöitä, ennalta estää verkossa tapahtuvia rikoksia, paljastaa verkossa toimivia rikollisia ja selvittää verkkoihin liittyviä epäiltyjä rikoksia. Poliisin tulee myös pystyä tunnistamaan ja torjumaan verkossa tapahtuvaa terroristisen ja muiden yhteiskuntajärjestystä vaarantavien rikosten valmistelua, rahoitusta, johtamista sekä niihin liittyvää propagandistista tiedottamista ja mielipiteen muokkaamista sekä kyetä selvittämään epäillyt rikokset. Lisäksi poliisilla tulee olla kyberturvallisuusstrategian mukaan taito ja kyky sekä riittävät oikeudelliset mahdollisuudet vaihtaa tietoja ja tehdä yhteistyötä eri

viranomaisten, yksityisen sektorin ja kansalaisten kanssa rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi.

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 ja yhteiskunnan elintärkeiden toimintojen strategiassa määritellyissä strategisissa tehtävissä.

Poliisihallitus asetti poliisin kybertyöryhmän 25.3.2015 (POL-2015-3879) poliisin kokonaisvaltaisen kybersuunnitelman laatimiseksi. Työryhmän tavoitteena oli koota viranomaisten toimivaltuuksista, poliisin toimintaympäristöstä, vastuista, tehtävistä, osaamisesta ja kehittämisestä suunnitelma poliisin toiminnan ohjaamiseksi kybertoiminnassa. Työryhmän ensisijaisena tehtävänä oli luoda kattava, yhteinen ja yhtenäinen lainvalvontaviranomaisen käsitys tietoverkkorikollisuuden ja tietoturvallisuuden tilasta sekä niitä koskevista toimenpiteistä ja organisatorisesta vastuunjaoista ja tarpeista. Tässä selvityksessä on huomioitu työryhmässä laadittujen raporttien suosituksia.

Valtioneuvoston rahoittamassa (VNTEAS) Tietoverkkorikollisuuden tilannekuvahankkeessa kartoitettiin tietoverkkorikollisuuden tilannekuvatyön nykytila. Hankkeeseen osallistuivat Poliisiammattikorkeakoulu, Keskusrikospoliisin kyberrikostorjuntakeskus, Kyberturvallisuuskeskus ja Tampereen yliopisto. Tämän selvityksen toimenpidesuositukset tietoverkkorikollisuuden tilannekuvan parantamiseksi perustuvat hankkeessa esiin tuotuihin kehittämisehdotuksiin.

Selvityksessä on hyödynnetty Keskusrikospoliisin laatimia uhka-arvioita.

Selvityksestä pyydettiin lausunnot seuraavilta tahoilta: liikenne- ja viestintäministeriö, maa- ja metsätalousministeriö, oikeusministeriö, opetus- ja kulttuuriministeriö, puolustusministeriö, sosiaali- ja terveysministeriö, työ- ja elinkeinoministeriö, ulkoasiainministeriö, valtioneuvoston kanslia, valtiovarainministeriö, ympäristöministeriö, puolustusvoimat, Tulli, Viestintävirasto, Valtion palvelukeskus VALTORI, Elinkeinoelämän keskusliitto, Finanssialan keskusliitto, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, Finnish Information Security Cluster ry FISC, SM/Hallinto- ja kehittämisosasto, SM/Maahanmuutto-osasto, SM/Pelastusosasto, SM/Kansainvälisten asioiden yksikkö, Rajavartiolaitos, Hätäkeskuslaitos, Hallinnon tietotekniikkakeskus HALTIK, Maahanmuuttovirasto.

Lausunnoissa selvitystä pidettiin kattavana. Elinkeinoelämän roolia tietoverkkorikosten ennalta estämisessä pidettiin tärkeänä. Lisäksi lausunnoissa korostettiin sitä, että tietoverkkorikollisuuden torjunnan koko rikostorjuntaketju esitutkinnasta aina tuomion antamiseen tulee olla varmistettu. Perusoikeuksien ja Suomea koskevien ihmisoikeusvelvoitteiden huomioon ottamista korostettiin tietoverkkorikostutkinnan toimivaltuuksia tarkasteltaessa. Erityisesti suhteellisuus-periaate, laillisuusperiaate ja luottamuksellisen viestin suoja ovat tietoverkkorikostutkinnan toimivaltuuksia tarkasteltaessa korostetusti esillä. Salaisten tiedonhankintakeinojen ja salaisten pakkokeinojen käytön osalta tuotiin esille se, että olennaista on hahmottaa, mitä mainitut keinot ovat, minkälaisia toimenpiteitä ne mahdollistavat, miten ne suhtautuvat toisiinsa ja minkälaisen kokonaisuuden ne muodostavat. On myös huomioitava, että poliisilain (872/2010) ja pakkokeinolain (806/2010) kokonaisuudistukset ovat varsin tuoreita. Niissä on pyritty ottamaan huomioon myös tekninen kehitys. Kaiken kaikkiaan tietoverkkoverkkorikosselvityksen toimeenpanosuosituksia pidettiin hyvinä ja lausunnossa korostettiin tietoverkkorikosten torjunnan tärkeyttä.

Tietoverkkorikosselvitys käsiteltiin ja sisällöllisesti hyväksyttiin sisäisen turvallisuuden ja oikeudenhoidon ministerityöryhmässä 1.3.2017. Selvityksen resurssitarpeet käsitellään kuitenkin normaalissa talousarvio- ja kehysvalmisteluprosessissa.

2 Tietoverkkorikollisuuden käsitteistä

2.1 Tietoverkkorikollisuuden määritelmät

Tietoverkkorikoksesta ei ole vakiintunutta määritelmää. Määritelmissä on korostettu teknologiaa tekovälineenä, kohteena tai ympäristönä. Rikoslain esitöissä käytetään termiä tietoverkkorikollisuus ja synonyymiä tietotekniikkarikos käännöksenä englanninkieliselle käsitteelle cybercrime. Poliisissa tietoverkkorikokset[2] (nykyisin käytetään myös termiä kyberrikos) on perinteisesti jaettu tietoverkkoympäristöön[3] *kohdistuviin* rikoksiin eli ns. puhtaisiin tietoverkkorikoksiin ja tietoverkkoympäristöä *hyväksi käyttäen* tehtyihin rikoksiin.

Kun rikos kohdistuu tietoverkkoympäristöön, on kyse sellaisista rikosten tekomuodoista, joita esiintyy ainoastaan tietoverkoissa tai tietojärjestelmissä ja rikos kohdistuu tietoverkkoon, tietojärjestelmään tai siinä olevaan dataan. Näin ollen tietoverkkorikoksia ovat ensinäkin *palvelunestohyökkäykset*, jolloin kohteena olevan tietojärjestelmän toimintaa tarkoituksellisesti estetään tai hidastetaan. Tietokoneeseen voidaan tartuttaa *haittaohjelma* (virus, mato tai troijalainen tms.), jolloin tietojärjestelmä tekee ei-toivottuja toimia tietokoneessa, esimerkiksi vakoilee tai lähettää tietoa tietylle komentopalvelimelle. *Hakkeroinnin* avulla taas voidaan tunkeutua luvatta tietoverkkoon tai tietojärjestelmään (tietomurto) ja esimerkiksi tuhota tietojärjestelmässä olevia tietoja tai käyttää järjestelmää omiin tarkoituksiin.

2 Kyberrikos, tietotekniikkarikos ja tietoverkkorikos ovat tässä selvityksessä synonyymejä ja tarkoittavat samaa kuin englanninkielinen cybercrime. Nykyään käytetään myös termiä digitaalinen rikos (Digital Crime)

3 Tässä selvityksessä verkkoympäristö, tietoverkkoympäristö, digitaalinen toimintaympäristö, kybertoimintaympäristö, kyberavaruus ja sähköinen toimintaympäristö ovat toistensa synonyymejä ja tarkoittavat samaa kuin englanninkielinen käsite cyberspace. Kansallisen kyberturvallisuusstrategian mukaan kybertoimintaympäristöllä ymmärretään keskinäisriippuvaista sähköisessä muodossa olevan tiedon käsittelyyn tarkoitettua tietojärjestelmistä muodostuvaa toimintaympäristöä. Tietoverkkoympäristöön voidaan katsoa kuuluvan tietojärjestelmien, tietoverkkojen, ohjausjärjestelmien ja laitteiden lisäksi loputon joukko sovelluksia, mediaa, pelejä ja virtuaalitodellisuuksia, jotka kehittyneissä maissa läpäisevät modernin elämäntavan kokonaisuudessaan.

Lähes kaikki rikokset voidaan tehdä tietoverkkoympäristöä hyödyntäen. Tietoverkkorikollisuuden voidaankin katsoa olevan luonteeltaan horisontaalista. Esimerkiksi maksuvälinepetoksista suurin osa tehdään nykyään tietoverkkoympäristöä hyväksikäyttäen.

2.2 Kyber-käsitteistä

Kun internetin käyttö laajeni voimakkaasti 1990-luvulla, huomio kiinnittyi erityisesti kehittyneissä maissa siihen, että lähes kaikki yhteiskunnan sektorit olivat tulleet riippuvaiseksi sähköisestä tiedonkäsittelystä, viestintäverkoista ja näitä toimintoja tukevasta infrastruktuurista. Kyber-alkuisten käsitteiden käyttö alkoi Yhdysvalloissa nykyisessä merkityksessään kriittiseen infrastruktuurin suojaamiseen liittyvässä toiminnassa 1990-luvun loppupuolella. Kriittiseen infrastruktuuriin liittyvät uhkat jaettiin tällöin kahteen kategoriaan: fyysisiin uhkiin ja kyberuhkiin (cyberthreats).

Kyber -etuliitteellä varustetut termit kuten kyberturvallisuus, kyberrikos, kyberhyökkäys ja kybersota tulivat laajempaan käyttöön Suomessa sen jälkeen kun kansallisen kyberstrategian laatiminen aloitettiin vuonna 2011.

Kyber – etuliite on yleiskielessä ainakin osin korvannut aiemman tieto- ja tietoverkko-etuliitteen. Kyber – termin käyttöönotolla on kuitenkin pyritty kuvaamaan toimintaympäristön muutosta, jossa tietotekninen ympäristö on globaali ja josta modernit yhteiskunnat ovat voimakkaasti keskinäisriippuvaisia. Eri merkityssisällöistä voidaan esimerkkinä käyttää tietoturvallisuus- ja kyberturvallisuuskäsitteiden eroa. Tietoturvallisuus kuvaa olemassa olevan ja varastoidun tiedon (niin fyysisen kuin digitaalisen) luottamuksellisuuden, käytettävyyden ja eheyden turvaamista. Kyberturvallisuus taas kuvaa koko sähköisen toimintaympäristön turvallisuutta, johon kuuluu tiedon lisäksi myös esimerkiksi digitaaliset ohjausjärjestelmät, jotka kontrolloivat ja ohjaavat yhteiskunnan monia elintärkeitä infrastruktuureita ja koko muu infrastruktuuri tietoverkoista sovelluksiin.

3 Tietoverkko rikollisten toimintaympäristönä

Digitaalinen toimintaympäristö on olennainen osa rikollisuuden ja rikostorjunnan toimintaympäristöä, sillä tietoverkkoympäristössä tehdään tänä päivänä yhä suurempi osa poliisin tietoon tulleista rikoksista. Globalisoituneessa ja keskinäisriippuvaisessa maailmassa uhat monimuotoistuneet ja perinteisten uhkien rinnalle on noussut uudenlaisia, nopeasti syntyviä ja vaikutuksiltaan vaikeasti ennakoitavia tilanteita. Hybridi kuvaa konfliktien monimuotoisuutta ja yllättävyyttä.

Rikollisuuden maailmanlaajuinen teollistuminen verkon rikollisuuspalveluiksi muuttaa rikollisuuden toimintarakenteita. Internetissä toimii laittomiin tarkoituksiin erityisesti suunnattuja Darknettejä sekä tavanomaisten hakukoneiden tavoittamattomissa olevia Deep Webejä ja muita foorumeita. Ne ovat rikollisuuden markkina- ja kohtauspaikkoja.

Perinteisten massarikosten tyyppisten, yksinkertaisten tekojen toteuttamiseen tarvittavia helppokäyttöisiä välineitä, dataa ja palveluita on saatavissa edullisesti. Kokeneiden ja ammattimaisesti toimivien rikollisten on verkon palveluiden ansiosta helppo tehostaa toimintaansa ulkoistamalla ne toiminnan vaiheet, jotka eivät kuulu heidän omaan ydinosaamiseensa. Etenkin tietoteknologiaa hyödyntävät petokset ja laskutuspetokset ovat lisääntyneet. Tyypillisimmät petosrikokset ovat maksukorttipetoksia, nettikauppapetoksia ja massamarkkinointipetoksia.

Darkneteissä[4] oli vuoden 2014 puolivälissä EU-maiden poliisipäälliköille tehdyn selvityksen mukaan yli 8 000 rikollisesti toimivaa sivustoa, eniten lapsiin kohdistuvaa seksuaalista hyväksikäyttöä sisältävää aineistoa markkinoivaa, huumausaineisiin keskittyviä sekä maksukorttirikollisuutta palvelevia sivuja.

4 TOR (The Onion Router, alun perin Yhdysvaltain ilmavoimien viestintätarpeisiin kehitetty ”Sipuliverkko”) sekä I2P-darknetit.

Laittomaan toimintaa soveltuvien tuotteiden ja palveluiden helppo saatavuus mahdollistaa entistä joustavammat, nopeasti muuttuvat ja projektikohtaiset rikollisorganisaatiot, jotka eivät juurikaan enää muistuta järjestäytyneen rikollisuuden perinteisesti tyypillisiä rakenteita. Europol puhuukin ”palveluun perustuvasta rikollisesta teollisuudesta”. Rikollisuuden teollistumiseen kuuluu, että alamaailman verkkofoorumeilla on tarjolla erikoistunutta rahansiirto- ja pesupalvelua. Käteisrahan kaltainen anonymiteetti on tehnyt ns. virtuaalivaluutoista rikollisten suosimia maksamisen ja rahanpesun välineitä. Virtuaalivaluutat asettavat uudenlaisia vaatimuksia rikostutkinnalle ja rikoshyödyn jäljittämiselle. Huumaus-, doping- ja lääkeaineita välittäviä verkkofoorumeita hyödyntävät sekä yksittäiset tilaajat että välittäjät. Netistä hankittujen huumeiden myynti voi olla hyvin tuottoisaa sekä oman käytön rahoittamiseksi että järjestäytyneen rikollisuuden tarkoituksiin.

Sosiaaliset keinot (social engineering) ovat toimintatapoja, joilla uhri manipuloidaan toimimaan rikollisten haluamalla tavalla esimerkiksi haittaohjelmien ujuttamiseksi uhrin käyttämiin järjestelmiin. Europolin uhka-arvio (iOcta2015) nostaa esille sen, että kyberrikolliset ovat yhä ammattimaisempia. Hyökkäykset on suunniteltu hyvin ja niissä käytetään uusia ja innovatiivisia menetelmiä. Tietoverkkorikolliset ovat tulleet aggressiivisemmiksi ja he ottavat entistä useammin suoraan yhteyttä uhreihinsa, mikä lisää käyttäjien pelkoa ja epävarmuutta. Erityisesti kiristys tekotapana, tapahtuipa se kohdistettuja palvelunestohyökkäyksiä tai kiristysohjelmia käyttäen, on yleistynyt nopeasti. Osa kiristyshaittaohjelmista kykenee selvittämään uhrin varallisuustasoa. Myös yritykset ovat olleet kiristyshaittaohjelmien kohteena. Pahimmillaan kiristyshaittaohjelma on levittynyt yrityksen sisäverkkoon jolloin yrityksen verkkolevyt ja jopa pilvipalvelut on salattu kiristyshaittaohjelman avulla. Sisäpiiri hyökkäyskanavana ja liiketoiminnan tuhoamiseen pyrkivät kyberhyökkäykset ovat yleistyneet.

Mobiiliyhteyksiin liittyy kasvavassa määrin rikoksentekomahdollisuuksia. Europolin uhka-arvioiden mukaan tietoverkkohyökkäysten painopiste siirtyneekin mobiililaitteisiin, sillä ne sopivat hyvin haittakoodien levittämiseen ja toimivat väylänä kiinteisiin laitteisiin. Monet haittaohjelmat mahdollistavat kohdelaitteiden täyden hallinnan. Mobiilialustoihin voi kohdistua tulevaisuudessa myös kaappauksia bottiverkkoon, jolloin kaapattuja alustoja voidaan hyödyntää hyökkäyksissä.

4 Kriittiseen infrastruktuuriin kohdistuvat uhkat

Yhteiskunnan kriittiset tuotantoprosessit ovat entistä riippuvaisempia automaatiojärjestelmistä. Nykyisin valtaosa kriittisestä infrastruktuurista ja sen palveluista on yksityisen sektorin omistamaa ja tuottamaa. Vakavissa kyberrikoksissa on usein vahva kansainvälinen ulottuvuus sekä vakava uhka yhteiskunnalle ja sen elintärkeille tietojärjestelmille. Vakavimman ja yhteiskunnan kriittisiin toimintoihin kohdistuvan rikollisuuden tekotavat ovat tehostuneet ja uhkat kasvaneet. Aalto-yliopiston tutkimuksessa löydettiin Suomen tietoverkosta lähes 3 000 teollisuuden automaatiojärjestelmiin, kiinteistöautomaatioon, sähkönhallintaan ja järjestelmien etäkäyttöön liittyvää laitetta, jotka olivat internetissä näkyvillä. Ääritapauksissa kriittistä infrastruktuuria kohtaan voidaan hyökätä terroristisessa tarkoituksessa perinteisten tapojen lisäksi myös kyberiskuin. Vuonna 2016 Ukrainan sähköverkkoon tehtiin kyberhyökkäyksiä, jotka lamauttivat osittain sähköverkon toiminnan.

Kohdistetut haittaohjelmahyökkäykset ovat lisääntyneet selvästi. Vuonna 2014 nähtiin aktiivinen haittaohjelmakampanja, jolla pyrittiin selvittämään eurooppalaisen energian jalostus- ja jakeluverkoston tarkkaa teknistä rakennetta. Hyökkääjä keräsi haittaohjelman avulla muun muassa tietoa sähköverkon ohjauslaitteista ja niiden ohjelmistoversioista. Teko voidaan nähdä esimerkiksi valmistautumisena vihamieliseen sähköverkon toimintaan vaikuttamiseen. Kriittisten tahojen alihankkijoiden riski joutua hyödynnetyksi hyökkäysten toteuttamisessa kasvaa, koska niillä on rikollisia kiinnostavaa tietoa. Europolin arvion (IOcta2014) mukaan järjestäytyneen rikollisuuden, vihamielisten valtioiden tai terroristi- ja äärijärjestöjen verkkohyökkäyksistä EU-maiden kriittiselle infrastruktuurille koituva uhka on merkittävä.

Asiattomien pääsy käsiksi teollisuusjärjestelmiin voi olla hyvin tuhoisaa ja vain kokeilumielessäkin tehty tunkeutuminen voi aiheuttaa vaurioita järjestelmässä sekä sen hallitsemassa fyysisessä ympäristössä. Haavoittuvuusriskejä lisää myös liiketoiminnan osien ulkoistaminen tahoille, joiden toiminta ei täytä kyseisen liiketoiminnan turvallisuusvaatimuksia.

Terveystoimialaan liittyvät hyökkäykset ovat yleistyneet. Viranomaisten ja muiden toimijoiden tietojärjestelmiin tallennettujen arkaluonteisten tietojen kuten esimerkiksi terveystietojen tai poliisin järjestelmiin tallennettujen tietojen laajamittainen tietomurto ja tietojen saattaminen julkisesti saataville loukkaisi merkittävästi perusoikeuksia ja saattaisi vaarantaa viranomaisen toiminnan.

5 Kybervakoilu

Tietoverkkojen kautta tapahtuva vakoilu ja luvaton tiedustelutoiminta ovat yhä suurempi uhka ja siihen liittyvä havainnointikyky on Suomessa puutteellinen. Vieraan valtion tiedustelupalveluiden tavoitteena on muun muassa haittaohjelmien avulla murtautua tietojärjestelmiin ja päästä käsiksi kaikkeen sellaiseen luottamukselliseen ja salaiseen tietoon, jolla voi olla merkitystä omien kansallistensa etujen ajamiseksi. Kohdistettua verkon yli toteutettua lähinnä ulko- ja turvallisuuspoliittiseen päätöksentekoon ja korkean teknologian tuotekehitykseen kohdistuvaa oikeudetonta tiedonhankintaa on paljastunut viime vuosina yhä enemmän. Kyseessä voi olla niin poliittinen, sotilaallinen, taloudellinen tai tieteellis-tekninen tieto. Vakoilulla aiheutetut vahingot voivat olla Suomen kansalliselle turvallisuudelle korvaamattomia. Toisena ulottuvuutena on kohdevaltion kriittiseen infrastruktuuriin kohdistuva ennakoiva tiedustelutoiminta, jonka tavoitteena on varautua sen lamauttamiseen tai haavoittamiseen esimerkiksi kriisitilanteessa.

Vaikka valtion organisoima kybervakoilu sinänsä täyttää useammankin rikoksen tunnusmerkistön, tekoa ei käytännössä voida selvittää rikosoikeuden kontekstissa, sillä tekijähenkilöiden selvittäminen edellyttäisi oikeusapua valtiolta, josta käsin he toimivat. Jos vakoilijat toimivat sijaintivaltionsa lukuun, oikeusapua ei ole odotettavissa.

6 Väkivaltainen ekstremismi tietoverkoissa

Väkivaltaiseen ekstremismiin kytkeytyvät henkilöt ja terroristiset toimijat käyttävät kyberympäristöä laajamittaisesti propaganda- ja terroristisen materiaalin levittämiseen, uusien jäsenten rekrytointiin ja väkivaltaiseen radikalisoimiseen. Kyberympäristöä voidaan hyödyntää lisäksi terroristisen toimijoiden väliseen yhteydenpitoon ja toiminnan, kuten terroriteon, suunnitteluun.

Tietoverkoissa voidaan häirinnän ja hyökkäyksellisen toiminnan lisäksi pyrkiä vaikuttamaan mielipiteisiin ja päätöksentekoon. Viharikoksiin puututaan (mukaan lukien vihapuhe netissä) ja tutkitaan matalalla kynnyksellä, mutta on hyvä huomioida, että vihapuhe ja viharikollisuus ovat eri asioita (vihamotiivi on rangaistuksen koventamisperuste). Osa vihapuheesta kuuluu sananvapauden piiriin (joskin voi olla huonoa tai asiatonta käytöstä) ja osa taas on viharikollisuutta (kunnianloukkauksia, kiihottaminen kansanryhmää vastaan, jne.). Poliisi pyrkii puuttumaan jatkossa entistä tehokkaammin varsinkin internetissä kirjoitettuihin vihapuheisiin ja saamaan niiden kirjoittajat vastuuseen teoistaan.

7 Seksuaalinen hyväksikäyttö tietoverkoissa

Verkkoympäristö on lisännyt rikoksentekomahdollisuuksia lapsiin ja nuoriin kohdistuvassa seksuaalisessa hyväksikäytössä. Hyväksikäyttömahdollisuudet ovat lisääntyneet internetin käytön laajetessa. Seksuaaliseen hyväksikäyttöön tähtääviä kontakteja potentiaalisiin uhreihin voidaan tehdä netin keskustelupalstojen yms. avulla suuria määriä, jolloin tekijöiden on mahdollista löytää itselleen helpoimmat uhrit. Internetissä ja sen kautta tapahtuvaa seksuaalista hyväksikäyttöä kartoittaneiden tutkimusten[5] mukaan varsinaiseen fyysiseen kanssakäymiseen johtaneita tapauksia on suhteellisen vähän, mutta verkossa tapahtuva ahdistelu on monimuotoista ja joissakin muodoissaan hyvin yleistä.

Aineistojen etävarastoinnin ja –käsittelyn mahdollistavien pilvipalveluiden käyttö lapsiin kohdistuvaa hyväksikäyttöä sisältävää aineistoa levittävässä rikollisuudessa on yleistynyt. Rikollisuudenalan uhrit ovat olleet vuosi vuodelta yhä nuorempia – maailmanlaajuisesti noin 80 prosenttia uhreista on alle kymmenenvuotiaita – ja levitettävässä aineistossa on todettu yhä äärimmäisempää ja sadistisempaa hyväksikäyttöä. Lasten hyväksikäyttöön keskittyvien seksirikollisten Euroopassa suosimissa darknet-foorumeissa aineistoa voidaan katsoa ja levittää hyvin riskittömästi.

5 Rikollisuustilanne 2014 - Rikollisuuskehitys tilastojen ja tutkimusten valossa: Kriminologian ja oikeuspolitiikan instituutin vuosikatsaus Katsauksia 4/2015

8 Kansainväliset sopimukset ja velvoitteet

Euroopan neuvoston 23.11.2011 tehty Budapestin yleissopimus on ainoa erityisesti tietoverkkorikollisuutta käsittelevä kansainvälinen sopimus. Se on avoin myös Euroopan neuvoston ulkopuolisille maille. Sopimuksen on ratifioinut noin 40 maata, ml. Suomi. Kiina ja Venäjä eivät ole liittyneet sopimukseen, eikä Pohjoismaista myöskään Ruotsi. EU:n ja Suomenkin kantana on ollut se, että Euroopan neuvoston Budapestin sopimuksen tulisi olla tietoverkkorikollisuuden vastaisen toiminnan globaali viitekehys eikä tarvetta uudelle yleiselle tietoverkkorikossopimukselle esimerkiksi YK:n piirissä ole. Pelkona on ollut, että tietyt maat haluaisivat internetin monitoimijamallin tilalle valtiokeskeisemmän kybertoimintaympäristön.

Euroopan unionin tavoitteena on entisestään lähentää jäsenvaltioiden rikosoikeudellisia säännöksiä ja parantaa jäsenvaltioiden viranomaisten välistä yhteistyötä tietoverkkorikollisuuden tehokkaaksi torjumiseksi. Tietojärjestelmiin kohdistuvista hyökkäyksistä annettiin Euroopan Unionin neuvoston puitepäätös vuonna 2005.[6] Puitepäätös korvattiin Euroopan neuvoston parlamentin ja neuvoston direktiivillä vuonna 2013.[7] Sekä puitepäätös että direktiivi on Suomessa pantu täytäntöön rikoslain muutoksilla, joista viimeisin tuli voimaan 4.9.2015.

EU:n sisäisen turvallisuuden strategian yksi tärkeimmistä painopistealueista on tietoverkkorikollisuuden torjunta. Joulukuussa 2014 komissio antoi päätelmät EU:n sisäisen turvallisuuden linjauksiksi 2015-2020. Päätelmien mukaan tärkeimmät yhteiset uhat ja haasteet tuleviksi vuosiksi sisäisen turvallisuuden alalta ovat vakava ja järjestäytynyt rikollisuus, terrorismi, radikalisoituminen, värvääminen ja terrorismiin liittyvä rahoitus, tietoverkkorikollisuus ja kansalaisten, yritysten ja julkisten laitosten verkkoturvallisuus, uudesta teknologiasta johtuvat uhat ja haasteet, uudet ja kehittyvät uhat ja kriisit sekä luonnon tai ihmisten aiheuttamat katastrofit. Päätelmien mukaan uhkiin varautuminen edellyttää

6 (2005/222/YOS).

7 2013/40/EU

kokonaisvaltaisen ja johdonmukaisen toimintatavan lujittamista sekä horisontaalisesti että vertikaalisesti seuraavien avulla: eurooppalaisen turvallisuusmallin edelleen kehittäminen, kokonaisvaltainen, monialainen ja yhdennetty toimintatapa, tiedusteluperusteinen toimintatapa, tietojen käyttö, saatavuus ja vaihto, rikosten ja terrori-iskujen estäminen ja ennakointi, uuden teknologian tehokas käyttö, tutkinta- ja syytetoimien koordinointi, yhteistyön tehostaminen, rajaturvallisuuden lujittaminen jne.

EU on tiivistänyt yhteistyötään myös muutoin. EU:n kyberturvallisuusstrategia hyväksyttiin vuonna 2013 ja EU:n kyberdiplomatiaa koskevat päätelmät helmikuussa 2015. Myös hybridiuhkiin varautumista ja vastaamista on EU:ssa ryhdytty tehostamaan vuoden 2015 alusta lähtien. Toukokuussa 2015 ulkoasiainneuvosto totesi hybridikeinojen käytön lisääntyneen erityisesti EU:n lähialueilla sekä valtiollisten että ei-valtiollisten toimijoiden toimesta. Euroopan komissio ja unionin ulkoasioiden ja turvallisuuspolitiikan korkea edustaja hyväksyivät 6.4.2016 yhteisen kehyksen hybridiuhkien torjumiseksi ja EU:n, sen jäsenvaltioiden ja kumppanimaiden kestokyvyn (resiliessi) parantamiseksi.

OSA-neuvostossa on tammikuussa 2016 pidetty tilannekatsaus siitä, miten varmistetaan tehokas rikosoikeus digitaalisella aikakaudella. Digitalisaation seurauksena rikolliset voivat toimia verkossa nopeasti ja valtioiden rajat ylittäen. Samalla todistusaineisto digitalisoituu ja on entistä helpompi kätkeä tai tuhota. On tärkeää, että tähän muutokseen kyetään vastaamaan rikosoikeuden keinoin, tutkintakeinot ja oikeudellinen yhteistyö mukaan lukien.

9 Tietoverkkorikollisuuden tilannekuva

9.1 Tietoverkkoihin tai tietojärjestelmiin kohdistuvat rikokset

Europolin uhka-arvion mukaan (iOcta2015) tietoverkkoihin kohdistuvissa rikoksissa haittaohjelmat ovat edelleen suurin uhka. Tietoverkkohyökkäyksissä käytetään usein hyökkäysalustoina haittaohjelmien saastuttamia koneita, joita komennetaan ja ohjataan tietoverkon yli ns. komentopalvelimen kautta. Haittaohjelman kaappaaman koneen omistaja voi olla itse ns. ”identiteettivarkauden uhri” tai hänen konettaan on voitu käyttää hyväksi muun, johonkin toiseen järjestelmään kohdistuneen rikoksen esim. tietoverkkohyökkäyksen, tekemisessä.

Tietojärjestelmähyökkäysten kohteena ovat olleet useimmiten finanssialan asiakkaat, mutta myös terveystoimiala, julkinen sektori, vähittäiskauppa, majoitusala ja julkiset palvelut joutuvat usein tietomurtorikosten kohteeksi. Vahingot voivat olla hyvin suuria: esimerkiksi vuonna 2013 Yhdysvaltalaiseen Target-kauppaketjuun kohdistuneessa tietomurrossa vietiin 70 miljoonan asiakkaan ja 40 miljoonan luottokortin tiedot.

Tietokoneen tiedostoja salaavat kiristysohjelmat (Ransomware) edustavat laajuudessaan ja vaikutuksiltaan yhtä tärkeimmistä uhista, joita EU:n liiketoiminta ja kansalaiset raportoivat lainvalvontaviranomaisille. Keskusrikospoliisi on tutkinut useita Cryptolocker- ja Cryptowall-kiristyshaittaohjelmiin liittyviä rikosilmoituksia. Näissä tekijä salaa haittaohjelman avulla saastuneen koneen kiintolevyt ja siihen liitetyt verkkolevyt, jolloin koneen käyttäjä ei enää pääse mihinkään sisältöönsä käsiksi. Tämän jälkeen tekijä vaatii uhria maksamaan bitcoineina (virtuaaliraha) tietyn summan. Summaa vastaan tekijä väittää toimittavansa purkavan avaimen. Kiristyksessä välineenä käytetään tiedostojen salaamisen lisäksi palvelunestohyökkäyksen tai yksityisyyttä koskevan tiedon levityksen uhkaa.

Kohdistetut hyökkäykset ovat lisääntyneet. Kohdistetussa hyökkäyksessä on yleensä kyseessä poliittinen vakoilu, talousvakoilu tai sotilasvakoilu. Kohdistetuissa hyökkäyksissä hyökkäävän tahon tarkoituksena on usein organisaation kriittisen tiedon haltuun saaminen. Tiivistyneen kansainvälisen ja kansallisen yhteistyön sekä aktiivisen viranomaistoi-

minnan seurauksena on saatu paljastettua useita vieraiden valtioiden toteuttamia haittaohjelmakampanjoita, joilla on pyritty ja osin jopa onnistuttu hankkimaan salassa pidettävää tietoa Suomen viranomaisten järjestelmistä. Suomessa vakavin tapaus on ollut ulkoministeriötä koskeva tietovuoto.

9.2 Digitaalista toimintaympäristöä hyödyntäen tehdyt rikokset

Tietoverkkoja tai tietojärjestelmiä hyödyntäen tehtyjen rikosten määrät ovat kasvaneet. Tyypillistä verkkoa hyödyntäville rikoksille on se, että ne ovat yksittäisinä yleensä vähäisiä, mutta uhreja on runsaasti ja vahingot ovat kokonaisuudessaan suuria. Tietoverkkoa hyödyntäen tehtyjen rikosten suurimmat ryhmät ovat omaisuusrikokset – lähinnä petokset ja maksuvälinepetokset, mutta myös rahanpesu ja kiristysrikokset. Tietotekniikan kehittyminen on luonut uusia mahdollisuuksia petoksiin ja muuhun rikolliseen toimintaan. Internetissä tehtyjen maksuvälinepetosten määrä on jatkanut voimakasta kasvuaan. Petosrikoksia oli vuonna 2016 yhteensä noin 2 900 ja kasvua niissä oli lähes kahdeksan prosenttia vuoteen 2015 verrattuna. Maksuväline- ja lieviä maksuvälinepetoksia oli vuonna 2015 yhteensä 5 574, mutta viime vuonna jo 8 782 kappaletta.

Kasvu johtuu esimerkiksi siitä, että omistajat ovat ilmoittaneet korttitietojaan netissä oleville huijaussivustoille, joissa on mainostettu vaikkapa euron matkapuhelimia. Tyypillisessä verkkokauppahuijauksessa asiakas houkutellaan maksamaan tuote etukäteen ”myyjän” väärennetyillä henkilötiedoilla avaamalle pankkitilille, mutta asiakas ei koskaan saa tilaamaansa tuotetta.

Ns. verkkourkinnassa (phishing) taas yritetään huijausviestein saada käsiin verkkopankkien käyttäjätunnuksia ja salasanoja, jotta päästäisiin käsiksi asiakkaan tileillä oleviin varoihin. Kysymyksessä ovat usein ulkomailta käsin toimivat rikolliset. Esimerkiksi vuonna 2015 Keskusrikospoliisi on tutkinut laajaa kansainvälistä petosrikoskokonaisuutta, jossa satojen suomalaisten yksityishenkilöiden ja pienyritysten pankkitileiltä onnistuttiin vuosina 2011-2013 siirtämään rahaa uhrien tietokoneet saastuttaneen ja pankkitunnukset kalastelleen haittaohjelman avulla. Tutkintaa tehtiin yhteisessä kansainvälisessä tutkintaryhmässä (Joint Investigation Team) muun muassa Itävallan, Belgian, Hollannin ja Norjan lainvalvonta-viranomaisten kanssa lähes kolmen vuoden ajan. Myös Eurojust ja Europol ovat olleet mukana rikoskokonaisuuden tutkinnassa.

Kriminologian ja oikeuspolitiikan instituutin tutkimuksen[8] mukaan RTST-tietokannan[9] tietojen perusteella tehty petosrikosten tarkempi luokittelu osoittaa verkossa tehtyjen rikosten lisääntyneen merkittävästi viime vuosina. Kuudensadan petosrikoksen otokseen perustuvan tarkastelun mukaan vuonna 2007 noin 17 prosenttia lievistä petoksista ja petoksista tapahtui erilaisissa verkkokaupoissa sekä osto- ja myyntisivustoilla. Tällaisten tapausten osuudet vuonna 2010 olivat 23 prosenttia ja vuonna 2013 luku oli 31 prosenttia. Törkeissä petoksissa trendi oli samansuuntainen, mutta osuudet olivat pienempiä. Osittain samaa kehitystä kuvastaa havainto, että yksityishenkilöihin kohdistuneiden petosten osuus lisääntyi 51 prosentista (2007) 73 prosenttiin (2013). Toisen henkilön henkilötietoja käyttämällä tehdyt petokset (esimerkiksi pikalainojen nostaminen ja tuotteiden tilaaminen verkkokaupasta) yleistyivät myös, ja vuoden 2013 lievistä petoksista ja petoksista noin joka neljäs oli tätä tyyppiä (vuoden 2007 osuus 14 prosenttia). Viranomaisten tietoon tulevan rikollisuuden määrään ja rakenteeseen vaikuttaa muun muassa ilmoitusalttius, kirjaamisalttius ja poliisin kontrollitoiminnan kohdistaminen.

Suomessa tehdyt nettipetokset saadaan tutkinnassa pääosin selvitettyä, mutta rikokset, jotka tehdään ulkomailta käsin, mutta joiden seuraukset ilmenevät Suomessa, tutkinta on huomattavan haasteellista.

9.3 Tietoverkkorikollisuuden tilastointi

Tietoverkkorikosten tilastointimahdollisuudet ovat puutteelliset niin Suomessa kuin muuallakin maailmassa, sillä nimikkeitä on runsaasti ja rajanvedot epäselviä. Lainvalvontaviranomaisten tietokannoista suoraan saatavista tilastoista ei voi juurikaan tehdä päätelmiä tietoteknologiaa hyödyntävien rikosten trendeistä. Tietoverkkoihin, tietojärjestelmiin sekä viestintään liittyvistä rikosnimikkeistä saatava ilmiökuva on myös puutteellinen ja antaa väärän kuvan määristä, sillä tietoverkkorikollisuus on isolta osin piilorikollisuutta ja ilmoitusmäärät ovat pieniä. Esimerkiksi Helsingissä tutkittiin törkeää tietomurtoa, jossa uhreja oli 50 000, mutta siitä kirjattiin vain yksi rikosilmoitus.

Tietoverkkorikostorjunnan tehostamiseksi tarvitaan tietoa poliisin tutkittavaksi tulleiden tietoverkkorikosten lukumääristä, tekotavoista ja rikoksella aiheutettujen vahinkojen määristä. Tällä hetkellä poliisin raportointijärjestelmistä ei pystytä tuottamaan luotettavia tilastoja edellä mainituista tiedoista. Pelkästään rikosnimikkeiden perusteella ei tarvittavia tietoja pystytä tuottamaan, sillä iso osa samoilla rikosnimikkeillä kirjattavista teoista voidaan

8 Rikollisuustilanne 2014-Rikollisuuskehitystilastojen ja tutkimusten valossa. Katsauksia 4/2015. Kriminologian ja oikeuspoliittisen instituutti

9 Kriminologian ja oikeuspolitiikan instituutin luoma Rikosten teonpiirteiden seuranta- ja tutkimusrekisteri (RTST)

tehdä joko reaalimaailmassa tai tietoverkkoympäristössä. Ohessa on tilastotietoa puhtaista tietoverkkoon, tietojärjestelmään tai sen sisältämiin tietoihin kohdistuvista rikoksista. Sen sijaan tietoverkkoympäristöä hyväksikäyttäen tehtyjen rikosten määristä ei ole saatavissa tilastotietoa edellä mainituista syistä.

Taulukko 1. Tietojenkäsittelyä ja viestintää koskevia poliisin tietoon tulleita rikoksia rikosnimikkeittäin vuosilta 2010-2016. Lähde: Polstat helmikuu 2017

Ilmoitettu kpl	2010	2011	2012	2013	2014	2015	2016
Törkeä viestintäsalaisuuden loukkaus	1	1	6	3	4	0	3
Salassapitorikos	29	57	45	48	40	48	41
Tietoliikenteen häirintä	25	79	50	93	57	85	67
Henkilörekisteririkos	36	91	148	119	488	122	105
Vaaran aiheuttaminen tietojenkäsittelylle	2	7	1	6	36	4	4
Viestintäsalaisuuden loukkaus	295	297	268	279	297	298	414
Viestintäsalaisuuden loukkauksen yritys	1	0	1	0	0	1	3
Lievä tietoliikenteen häirintä	8	3	5	9	5	6	9
Tietoliikenteen häirinnän yritys	0	1	1	0	0	1	0
Tietoliikenteen lievän häirinnän yritys	0	1	0	0	0	0	0
Törkeä tietoliikenteen häirintä	2	4	7	13	6	3	9
Tietomurto	292	410	503	580	339	347	409
Törkeä tietomurto	1	8	14	5	6	3	8
Suojauksen purkujärjestelmärikos	0	0	0	0	2	0	0
Tietoverkkorikosvälineen hallussapito	2	1	0	2	4	2	3
Sähköisen viestinnän tietosuojarikkomus	2	0	1	3	1	0	2
Tietokoneohjelman suojauksen poistovälineen luvaton levittäminen	0	0	0	0	0	0	0
Datavahingonteko	0	0	0	0	0	2	14
Datavahingonteon yritys	0	0	0	0	0	0	1
Lievä datavahingonteko	0	0	0	0	0	1	0
Törkeä datavahingonteko	0	0	0	0	0	0	3
Tietojärjestelmän häirinnän yritys	0	0	0	0	1	4	0
Tietojärjestelmän häirintä	3	3	9	11	11	30	38
Törkeä tietojärjestelmän häirintä	0	0	0	0	3	7	16
YHTEENSÄ	**699**	**963**	**1 059**	**1 171**	**1 300**	**964**	**1 149**

10 Tietoverkkorikostorjunnan keskeiset toimijat ja niiden tehtävät

Tietoverkkorikosten ennalta estämisessä, selvittämisessä ja syyteharkintaan saattamisessa toimivaltaisena viranomaisena toimii pääsääntöisesti poliisi yhteistyössä muiden lainvalvontaviranomaisten kanssa. Myös Tulli ja Rajavartiolaitos suorittavat toimialoillaan rikostutkintaa ja niihin liittyen tietoverkkoja ja tietotekniikkaa hyväksi käyttävien rikosten tutkintaa.

Tietoverkkorikostorjunnan poliisin sisäistä tehtävänjakoa käsitellään Poliisihallituksen antamassa ohjeessa vakavien tietoverkkorikosten torjunnan järjestämisestä (2020/2013/3780) sekä määräyksessä Keskusrikospoliisin ja muiden poliisiyksiköiden välisestä tehtävänjaosta sekä yhteistyöstä rikostorjunnassa (2020/2013/4613). Näissä on määritetty tietoverkkorikostorjunnan koordinointia ja tutkintavastuita poliisin eri yksiköiden välillä. Erityisesti painotetaan verkostoitumista tietoverkkorikosten esitutkintaan ja tietotekniseen tutkintaan erikoistuneiden tutkijoiden välillä.

Poliisin tietoverkkorikostorjunnan pääasialliset tehtävät voidaan jaotella seuraavalla tavalla:

- Tietoverkkorikosten ja tietoverkkoympäristöä hyödyntävien rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen
- Digitaaliforensiikka (todisteiden esille haku tietoteknisistä laitteista)
- Tiedonhankinta (rikostiedustelu tietoverkossa)
- Poliisin ennalta estävä toiminta tietoverkoissa

Poliisilaitosten päivittäistutkinnan yksiköissä hoidetaan valtaosa tietoverkkoympäristössä tehdyistä petoksista, kunnianloukkauksista ym. jutuista. Vaativammat ja laajemmat kokonaisuudet tutkitaan poliisilaitosten päivittäistutkinnassa ns. projektitutkintana tai pitkäkestoisen ja keskitetyn rikostutkinnan yksiköissä.

Keskusrikospoliisissa toimii maaliskuussa 2015 perustettu tietoverkkorikosten esitutkintaan erikoistunut yksikkö, kyberrikostorjuntakeskus, jossa tutkitaan pääasiallisesti tietoverkkoympäristössä tehtyjä laajempia kansainvälisiä rikoskokonaisuuksia. Kyberrikostorjuntakeskuksen perustamisella on pyritty varmistamaan paitsi tietoverkkorikosten torjuntakyky, myös poliisihallinnon toimintakyky kybertoimintaympäristössä tapahtuvissa vaativissa poliisitoiminnallisissa tilanteissa sekä törkeiden rikosten estämisessä, paljastamisessa ja selvittämisessä. Kyberrikostorjuntakeskus on vakiinnuttanut asemansa ja osoittautunut tarpeelliseksi lyhyen toimintansa aikana. Sisäisen turvallisuuden muutokset vaikuttavat kyberrikostorjuntakeskukseen toimintaan monin tavoin, mutta erityisesti tiedonhankintaan internetistä.

Kyberrikostorjuntakeskuksella on kaksi toisistaan poikkeavaa tehtäväkokonaisuutta. Keskus vastaa ensinnäkin tietoverkkorikostorjunnasta. Näihin rikoksiin kuuluu niin sanottuja hakkerijuttuja, palvelunestohyökkäyksiä sekä muita vakavia ja kansainvälisiä tietojärjestelmiin kohdistuneita rikoksia. Keskus toimii yhteistyössä muiden poliisiyksiköiden kanssa myös tietoverkoissa tapahtuvan lasten seksuaalisen hyväksikäytön ja maksukorttirikollisuuden torjunnassa. Nämä rikollisuuden osa-alueet ovat samat, joista myös Europolin European Cyber Crime Center (EC3) vastaa.

Toinen merkittävä tehtävä on tarjota poliisihallinnolle kybertoimintaympäristön palveluja. Nämä palvelut pitävät sisällään kaikki ne tehtävät, jotka kohdistuvat tietoteknisiin laitteisiin tai tietoverkkoihin. Keskeisimmät näistä ovat digitaaliforensiikka ja tietoverkkoihin liittyvä tiedonhankinta. Keskuksen tehtävänä on viestiä aktiivisesti poliisin kybertoimintaympäristön asioissa sekä luoda uusia palveluita kuten tietoverkkorikosten tilannekuvatoiminto ja poliisilaitosten neuvontapalvelu tietoverkkorikosasioissa.

Kaikissa poliisilaitoksissa toimii tänä päivänä digitaalisen todistusaineiston käsittelyyn ja analysoimiseen (digitaaliforensiikkaan) erikoistuneita yksiköitä. Keskusrikospoliisissa tietoteknisen tutkinnan yksikkö on osa kyberrikostorjuntakeskusta. Lisäksi rikostekninen laboratorio palvelee teknistä erityisosaamista ja -resursseja edellyttävissä tapauksissa koko poliisihallintoa.

Suojelupoliisin rooli tietoverkkorikostorjunnassa seuraa sen yleisestä toimialamääritelmästä. Viraston tehtävänä on ennalta estää ja paljastaa terrorismia, laitonta tiedustelutoimintaa ja valtion turvallisuutta vaarantavaa ääriliikkeiden toimintaa sekä tutkia vakoilurikoksia, tapahtui tämä toiminta sitten reaalimaailmassa taikka tietoverkoissa. Lisäksi Suojelupoliisi tekee ennalta estävää turvallisuustyötä kyberuhkien torjunnassa lisäämällä uhkia koskevaa tietoisuutta viranomaisissa ja yksityisen sektorin organisaatioissa. Suojelupoliisi selvittää haittaohjelmahyökkäyksiä yhteistyössä muiden viranomaisten kanssa sekä tarvittaessa yksityisen sektorin kanssa. Poliisiammattikorkeakoulu vastaa poliisialaan liittyvästä tutkinto- ja täydennyskoulutuksesta sekä tutkimus- ja kehitystoiminnasta.

Liikenne- ja viestintäministeriön alaiseen Viestintävirastoon perustettiin Suomen kansallisen kyberturvallisuusstrategian linjausten mukaisesti Kyberturvallisuuskeskus palvelemaan viranomaisia, elinkeinoelämää, ja muita toimijoita kyberturvallisuuden ylläpitämiseksi ja kehittämiseksi. Kyberturvallisuuskeskus on poliisille erittäin tärkeä yhteistyökumppani sekä tietoverkkorikosten tutkinnassa että kybertilannekuvan ylläpitämisessä. Myös muut viranomaiset kuten puolustusvoimat, valtioneuvoston kanslian tilannekuvatoiminto (VNTIKE) sekä valtiovarainministeriö valtion omien tietojärjestelmien osalta ovat tärkeitä yhteistyökumppaneita tietoverkkorikollisuuden ennalta estämisessä, paljastamisessa ja selvittämisessä.

Viranomaisten lisäksi myös yksityisillä toimijoilla on merkittävä rooli tietoverkkorikollisuuden torjunnassa. Organisaatioiden tasolla yhteistyö on pisimmällä finanssisektorin kanssa. Muutoin poliisin ja elinkeinoelämän välinen säännöllinen tietoverkkorikollisuuden torjuntaa koskeva yhteistyö ja tiedonvaihto ovat Suomessa vasta alkuvaiheessa. Monilla tietoturva-alan yrityksillä, esimerkiksi SOC-toimijoilla (security operation center) on kiinteä kontakti asiakasorganisaatioihinsa ja ovat ensimmäinen taho, jonka puoleen asiakas kääntyy poikkeamahallintatilanteessa. Näille tietoturva-alan yrityksille kertyy erittäin hyvä tilannekuva suomalaisiin yrityksiin kohdistuvista uhista. Yhteistyötä tulisikin merkittävästi edelleen tiivistää.

11 Kansainvälinen yhteistyö

Suomi osallistuu aktiivisesti EU:ssa sekä kansainvälisillä foorumeilla tapahtuvaan yhteistyöhön tietoverkkorikosten torjunnassa. Suomi on pyrkinyt edistämään kansainvälistä yhteistyötä tietoverkkorikostorjunnassa kehittämällä tiedonvaihtoa sekä jakamalla parhaita käytäntöjä, kokemuksia ja asiantuntemusta.

Poliisin kannalta keskeinen toimija on Alankomaihin perustettu Europolin European Cyber Crime Center (EC3), johon Suomen poliisi on lähettänyt kansallisen asiantuntijan. Suomi osallistuu täysimääräisesti ja aktiivisesti yhteistyöhön Europolin kanssa sen mandaatin ja yhteistyömahdollisuuksien puitteissa. Europolin kanssa tehdään kansainvälistä operatiivista yhteistyötä EU:n alueella ja saadaan tukea operatiiviseen yhteistyöhön sekä kontaktit EC3 kumppaneihin. EC3 on aloittanut operatiivisen tiiviin yhteistoiminnan Joint Cybercrime Action Task Force (J-CAT), johon useat eri Euroopan maat ovat lähettäneet yhdysmiehen ja johon myös USA, Kanada, Australia ja Kolumbia osallistuvat.

EU:n yhteisten arviointien työryhmä (GENVAL) arvioi EU-jäsenvaltioiden kyberrikollisuutta koskevien politiikkojen käytännön täytäntöönpanoa. Sisäministeriöstä on ilmoitettu arviointeihin mukaan kaksi asiantuntijaa. Suomi on arvioitu syksyllä 2016. Poliisi on ottanut vastuuta myös EU:n toimintapoliittisen syklin Cybercrime (EMPACT) tavoitteissa. European Union Cybercrime Task Force (EUCTF) on Euroopan Unionin jäsenmaiden tietotekniikka- ja tietoverkkorikostorjunnan asiantuntijoiden yhteistyöryhmä. Työryhmän työskentelyyn osallistuvat eri maiden kansallisten tietotekniikkarikosyksiköiden päälliköt (Head of National Units). Suomen edustaja on Keskusrikospoliisista. Keskusrikospoliisi on Euroopan neuvoston tietoverkkorikollisuutta koskevan (Budapestin sopimuksen) yleissopimuksen 35 artiklan mukainen 24/7/365 periaatteella toimiva yhteyspiste ja verkosto.

Suomi osallistuu täysimääräisesti ja aktiivisesti yhteistyöhön mahdollisuuksiensa puitteissa Singaporeen perustetun INTERPOLin Global Complex for Innovation (IGCI) kanssa. Interpolin IGCI tekee kansainvälistä operatiivista yhteistyötä globaalisti muun muassa tietoverkkorikollisuuden torjunnassa (Digital Crime Center) ja avustaa jäsenmaita tietoverkkorikostorjunnassa sekä tukee niiden osaamisen kehittämisessä. Keskusrikospoliisin kyberrikostor-

juntakeskus osallistuu asiantuntijatyöryhmän toimintaan, jonka tarkoituksena on auttaa ja osallistua Interpolin toimintaan tietoverkkorikostorjunnassa.

Suorat kahdenväliset yhteydet ovat tärkeitä erityisesti maiden kanssa, jotka eivät ole Europolin EC3:n viitekehyksessä mukana ja joilla on merkittävä rooli Suomeen kohdistuvan tai täällä toteutuvan tietoverkkorikollisuuden kanssa. Myös pohjoismaista yhteistyötä on tehty tietoverkkorikostorjunnassa useita vuosia. Yksi tämän yhteistyön tuloksista on yhteispohjoismainen koulutusohjelma tietoteknisessä tutkinnassa. Pohjoismaiden poliisipäälliköillä on yhteistyöryhmä, jonka työhön Suomi osallistuu. Poliisipäälliköiden aloitteesta on perustettu yhteispohjoismaisia alatyöryhmiä mm. tietoverkkorikollisuuden tehtäväalueelle.

Poliisitoiminnan kannalta yksi merkittävimmistä työryhmistä, joka on vaikuttanut merkittävästi alan toimijoiden kansainväliseen verkostoitumiseen, on ollut Interpolin Euroopan alueen jäsenmaiden tietotekniikka- ja tietoverkkorikostorjunnan asiantuntijoiden yhteistyöryhmä. Se on ollut toiminnassa jo vuodesta 1991. Työryhmän tehtävinä oli alun perin yhteistyökanavan perustaminen, alan koulutus ja verkostoituminen. Työryhmän aloitteesta onkin järjestetty runsaasti alan koulutusta eri puolilla maailmaa.

Suomi osallistuu myös YK:n kriminaalipoliittisen toimikunnan työhön. YK:n järjestäytyneen kansainvälisen rikollisuuden vastainen yleissopimus (UNTOC) sekä useat yleiskokouksen ja ECOSOC:in päätöslauselmat antavat mahdollisuuksia kansainväliselle yhteistyölle. YK:n huume- ja rikosvirasto UNODC on valmistellut muun muassa ohjelman tietoverkkorikostorjuntaan (Global Programme on Cybercrime).

12 Tietoverkkorikostorjunnan nykytilan arviointi

12.1 Arvioinnin laatimiseen osallistuneet tahot

Tietoverkkorikollisuuden nykytilaa ja kehittämistä on arvioitu vuonna 2015 Poliisihallituksen asettamassa poliisin kybertyöryhmässä ja sen alaisissa viidessä alatyöryhmässä. Työn tavoitteena on ollut tuottaa poliisin kokonaisvaltainen kybersuunnitelma. Poliisihallitus on järjestänyt keskustelutilaisuuden tietoverkkorikollisuuden lainsäädäntötarpeista. Myös Keskusrikospoliisin kyberrikostorjuntakeskuksen ja Viestintäviraston Kyberturvallisuuskeskuksen kanssa on pidetty yhteinen työpaja, joka keskittyi keskusten väliseen yhteistyöhön ja sen parantamiseen.

Tietoverkkorikollisuuden tilannekuvaa koskeva selvityshanke toteutettiin syksyllä 2015. Selvityksessä kartoitettiin tietoverkkorikollisuuden tilannekuvatyön nykytila ja luotiin pohja tietoverkkorikollisuuden tilannekuvatyön kehittämiselle poliisissa. Hanke rahoitettiin valtioneuvoston päätöksentekoa tukevan selvitys- ja tutkimustoiminnan määrärahoista (VN TEAS). Toteuttajatahot olivat Poliisiammattikorkeakoulu, Poliisin kyberrikostorjuntakeskus, Viestintäviraston kyberturvallisuuskeskus ja Tampereen yliopiston johtamiskorkeakoulu.

Valtakunnallisessa valmiusharjoituksessa VALHA15-16 on harjoiteltu hybridiuhkiin varautumista. Osana harjoitusta on kehitetty valtiovarainministeriön johtaman VIRT-yhteistyöryhmän (virtual incident response team) puitteissa valtiohallinnon yhteistoimintakykyä vakavien kyberhäiriötilanteiden ja poikkeusolojen hallinnassa.

Tämän selvityksen toimenpide-ehdotukset perustuvat edellä mainituissa työryhmissä, työpajoissa ja hankkeissa esiin nostettuihin toimenpidesuosituksiin.

12.2 Tietoverkkorikostutkinnan vahvuudet, heikkoudet, uhat ja mahdollisuudet

VAHVUUDET

- Lainsäädäntöön on saatu joitain uusia pakkokeinoja vaikka edelleen puutteita onkin.
- Tietoverkkorikostutkijoita on vähän mutta he ovat **motivoituneita** ja **ammattitaitoisia**.
- Tietoverkkorikostutkijat ovat hyvin **verkostoituneita** kansainvälisesti ja kansallisesti. Hyvä yhteistyö **Kyberturvallisuuskeskuksen** sekä finanssisektorin kanssa.
- Suomen kansallisen **Kyberturvallisuusstrategian** toimeenpanoehdotukset tukevat tietoverkkorikostorjunnan kehittämistä.
- Keskusrikospoliisiin on perustettu **poliisin Kyberrikostorjuntakeskus** ja sinne on panostettu resursseja
- Poliisilla on edelleen myönteinen julkisuuskuva ja kansalaiset luottavat poliisiin.

HEIKKOUDET

- **Lainsäädännössä on puutteita** liittyen tiedon tallentamiseen ja käsittelyyn (uhkien paljastaminen, ennaltaehkäisy)
- **Resurssit ovat jakautuneet** epätasaisesti eikä toiminnan kehittämiseen ole osoittaa määrärahoja
- **Osaamisvajetta** on erityisesti tietoverkkorikostutkijoiden ulkopuolisilla tahoilla sekä osin myös ydinryhmässä
- Tietoteknisen tutkinnan **työprosessit** ja raportointikäytännöt ovat epäyhtenäisiä
- Tietoteknisen tutkinnan **työvälineet** epäyhtenäisiä (ml. palvelin- ja verkkoympäristö)
- **Tiedonhankinta** tietoverkoista
  - Lainsäädännön haasteet
  - Osaamishaasteet
  - Organisointi ja välineet epäyhtenäiset
- Verkkoa hyödyntävien rikosten esim. petosrikosten **käsittely hajanaista**
- **Syyttäjien** erikoistumisen hajanaisuus ja työkuorma
- **Oikeusapuprosessi** on hidas ja kansainvälisen järjestäytyneen tietoverkkorikollisuuden torjunnan haasteet **kansallisen oikeudenkäytön** osalta

MAHDOLLISUUDET

- Kansallisten ja kansainvälisten **yhteistyöverkostojen hyödyntämisen** kehittäminen ja syventäminen
- **Ennalta estävän toiminnan** kehittäminen tuo jatkossa hyötyä
- Poliisin tietoverkkorikollisuuden **tilannekuvatyötä** kehitetään
- **Kansalaisten ja yritysten valistaminen ja kouluttaminen** vähentää riskiä joutua tietoverkkorikollisuuden uhriksi.
- Sidosryhmillä ja yhteistyökumppaneilla on tahtoa tehdä yhteistyötä Suomen poliisin kanssa

UHAT TÄLLÄ HETKELLÄ

- **Poliisipula**, ei saada koulutettua henkilöstöä ja henkilöstö uupuu
- Koulutettu ja kokenut **henkilöstö menetetään** yksityiselle sektorille paremman palkkauksen ja valtavan työkuorman takia. Palkkauskäytäntöjen kirjavuus yksiköiden välillä
- Valmistuneet **jutut eivät** etene syyttäjien ylikuormituksen vuoksi
- **Tutkinta vaikeutuu** teknisten syiden vuoksi (krypto, TOR, jne)
- Tuomioistuimien **erikoistumisen puute**
- Järjestäytyneiden tietoverkkorikollisten ns. **foorumshoppailu** (rikos toteutetaan sellaisesta maasta käsin, joka on rikosvastuun toteutumisen suhteen rikollisille edullinen) sekä **rikosvastuun toteutumisen haasteet**

12.3 Nykytilan arviointi ja toimenpide-ehdotukset

Poliisilaitoksien ja Keskusrikospoliisin rikostorjuntatehtävissä haetaan tietoja tietoverkoista (ns. avoimet lähteet) rikosten ja rikoskokonaisuuksien selvittämiseksi, estämiseksi ja paljastamiseksi. Poliisin salaisesta tiedonhankinnasta on säädetty erikseen. Tällä hetkellä ei ole käytettävissä keskitettyä tiedonhankintajärjestelmää eikä yhtenäisiä toimintatapoja tiedonhankinnan osalta, mitä on pidettävä merkittävänä puutteena.

Ennalta estävä toiminta on poliisin, sidosryhmien sekä yhteisöjen ja asukkaiden välistä yhteistyötä turvallisuuden parantamiseksi. Osana ennalta estävän toiminnan kokonaisuutta poliisi toteuttaa johdettua nettipoliisitoimintaa, jonka vaikuttavuutta kehitetään koko poliisitoimintaa tukevista lähtökohdista.

Suurin osa tietoverkkorikollisuudesta jää tulematta poliisin tietoon ja rikokset, joista poliisi käynnistää esitutkinnan jäävät usein selvittämättä tai selviävät vain osittain. Poliisin on sen vuoksi syytä painottaa ennalta estävää toimintaa tässä rikoslajissa nykyistä enemmän. Tällä hetkellä ennalta estävää tiedottamista tehdään siinä vaiheessa kun esitutkinta on aloitettu jostain sellaisesta tietoverkkorikostapauksesta, jossa on vaara uusien ihmisten ja yritysten joutuminen rikoksen uhriksi. Poliisiin tulee laatia ennalta estävän toiminnan suunnitelma tietoverkkorikollisuuden torjuntaan.

Tietotekniikkarikostutkinnan menetelmiä ja prosesseja ei ole kuvattu yhteisen laatuohjelman muotoon. Myös käytössä olevat tutkintainfrastruktuurit ovat kirjavia. Näihin tekijöihin tulee kiinnittää huomiota joskin pääpiirteissään toimintatavat ovat eri yksiköiden välillä melko yhtenevät.

Tällä hetkellä poliisin tietoverkkorikostorjunnan sidosryhmäyhteistyöstä puuttuu kokonaisvaltainen suunnitelmallisuus. Tämän vuoksi tulisi laatia kansallinen sidosryhmäyhteistyösuunnitelma sekä harkita, tulisiko keskeisimpien toimijoiden kanssa laatia yhteistyösopimukset (MoU).

Työpajoissa nousi esille monia yritysten ja kansalaisten tietoverkkorikosten torjuntaan liittyviä toimenpide-ehdotuksia. Verkossa tapahtuvan petosrikollisuuden ehkäisyyn tarvitaan yhteistyötä eri tahojen kanssa. Kauppiaiden ja kansalaisten tulisi panostaa verkossa ostamisen turvallisuuteen entisestään. Yritysten ja kansalaisten tulisi tehdä aktiivisemmin väärinkäytöksistä rikosilmoitus. Yksi pohdittava asia olisi avata poliisin kyberrikostorjuntakeskuksen neuvontanumero yritysten tiedusteluille. Tavoitteena on myös opastaa tietoturva-alan yrityksiä neuvomaan asiakkaita tekemään rikosilmoitus. Toimenpiteenä voisi olla myös valita 1-2 yritystyyppiä (esim. SOC), joiden kanssa aloitetaan säännölliset, yhteistä ilmiötilannekuvaa tukevat tapaamiset. Yrityksille voitaisiin antaa koulutusta rikosten tunnistamiseen ja analyysin kehittämiseen.

Laadukkaan ja tehokkaan kyberrikostutkinnan turvaamiseksi on syytä kehittää aihepiiriin liittyvää syyttäjäyhteistyötä. Kyberrikosten tutkinnassa on tavallisesti mukana kansainvälisiä elementtejä, jolloin yhteistyötarve esitutkinnan aikana korostuu. Lisäksi kyberrikosten tutkinta edellyttää usein syvällistä perehtymistä aihepiiriin.

Ennakkoilmoitusmenettelyyn ja sen mahdollisimman tarkoituksenmukaiseen hyödyntämiseen tulee kiinnittää huomiota. Suomen kansallisen kyberturvallisuusstrategian taustamuistiossa todetaan tehokkaan kyberrikostorjunnan edellyttävän, että viranomaisten, syyttäjien ja tuomareiden osaamista parannetaan kehittämällä alan koulutusta. Tämä edellyttää eri osapuolten osaamisen kehittämistarpeiden tunnistamista ja tarpeiden mukaisen koulutuksen järjestämistä. Valtakunnansyyttäjänvirasto on valinnut syksyllä 2014 neljä kihlakunnansyyttäjää kouluttautumaan kyberosaajiksi. He tulevat jatkossa vastaamaan muiden syyttäjien valtakunnallisesta koulutuksesta muun muassa elektronisen todistusaineiston käsittelyyn liittyen. Yhteistyö kyseisten syyttäjien kanssa on erittäin tärkeää kyberosaamisen kehittämistarpeita arvioitaessa.

Kybertoimintaympäristöä tulee suojata terroristiselta toiminnalta. Terroristiseen toimintaan tietoverkoissa varaudutaan muun muassa kansallisessa terrorismintorjunnan strategiassa kuvattujen toimenpiteiden (toimenpiteet 14 ja 15) mukaisesti eli varmistetaan viranomaisten toimintakyky- ja valtuudet vastata terrorismintorjunnan kyberuhkiin. Jatkossa kansallisesti tulisi arvioida tulisiko rikoslain 34 a luvun 1 §:n luetteloon terroristisessa tarkoituksessa tehdyistä rikoksia lisätä tietyn tyyppisiä kyberympäristölle aiheutuvia rikoksia, jolloin terrorismin torjumista koskevat eri mekanismit olisivat käytössä. Parhaillaan Euroopan unionin toimielimissä on käsiteltävänä komission ehdotus Euroopan parlamentin ja neuvoston direktiiviksi terrorismin torjumisesta sekä terrorismin torjumisesta tehdyn neuvoston puitepäätöksen 2002/475/YOS korvaamisesta. Työryhmävalmistelussa on päädytty siihen, että direktiivin terrorismirikoksia koskevan 3 artiklan 2 kohtaan otettaisiin i alakohta, jonka mukaan terrorismirikoksia olisivat myös terroristisessa tarkoituksessa tehtävät vakavimmat tietojärjestelmän häirinnät ja datavahingonteot. Riippuen lopputuloksesta, asia saattaa tulla käsiteltäväksi direktiivin täytäntöönpanovaiheessa.

Viranomaisten välistä yhteistyötä ja koulutusta tulee kehittää kyberympäristössä tapahtuvan terroristisen toiminnan paljastamiseksi ja estämiseksi. Poliisin osallistuu myös kansainväliseen yhteistyöhön terroristisen materiaalin leviämisen estämiseksi tietoverkoissa. Jatkossa on arvioitava viranomaisten terrorismintorjunnan toimintakyky kyberympäristössä ja päättää mihin toimenpiteisiin tulisi ryhtyä.

Tietoverkkorikostorjunnan kehittämiseksi esitetään seuraavia toimenpide-ehdotuksia:

1) Muodostetaan poliisin sisäinen tietoverkkorikostorjunnan yhteistyöverkosto, joka toimii seuraavien asioiden valmisteluryhmänä:

a) Tietoverkkorikollisuuden ennalta estävä toiminta

b) Kansallisen sidosryhmäyhteistyön kehittäminen

c) Kansainvälisen yhteistyön koordinoiminen

d) ICT-rikostutkinnan infrastruktuurin yhtenäistäminen

e) Kyberrikostorjuntatyön mittareiden ja raportoinnin kehittäminen

f) Vuotuisen laajapohjaisen tietoverkkorikostorjunnan strategiatyöpajan järjestäminen ennakoivan osaamisen kehittämisen tueksi

Vastuutaho: Poliisihallitus

2) Kehitetään yliopistojen, korkeakoulujen ja muiden toimijoiden välistä yhteistyötä tietoverkkorikostorjunnan osaamisen nostamisessa.
Vastuutaho: Poliisiammattikorkeakoulu

3) Laaditaan tietoteknisen tutkinnan laatuohjelma.

Vastuutaho: Poliisihallitus

4) Kehitetään kyberrikostorjunnan syyttäjäyhteistyötä tarjoamalla syyttäjille tietoverkkorikostorjuntaan liittyvää koulutusta ja toisaalta syyttäjät voisivat antaa rikostutkijoille tietoverkkorikostorjuntaan liittyvää juridista koulutusta.

Vastuutaho: Poliisiammattikorkeakoulu

5) Suojataan kybertoimintaympäristöä terroristiselta toiminnalta varmistamalla viranomaisten toimintakyky- ja valtuudet vastata kyberuhkiin.

6) Asetetaan viranomaisten ja elinkeinoelämän yhteistyöryhmä yrityksiin kohdistuvien rikosten ennalta estämisen ja torjunnan tehostamiseksi. Ryhmän erityiseksi painopisteeksi asetetaan tietoverkkorikollisuuden torjunta.

Vastuutaho: sisäministeriö.

12.4 Tietoverkkorikostorjunnan koulutukseen liittyvä arviointi ja toimenpide-ehdotukset

Poliisihallituksen asettama kyberohjausryhmä asetti koulutuksen ja tutkimuksen alatyöryhmän tekemään konkreettisia toimenpide-esityksiä kyberturvallisuuden ja -rikostorjunnan koulutuksen ja tutkimuksen kehittämiseksi.

Suomen kansallinen kyberturvallisuusstrategian toimeenpano-ohjelma edellyttää poliisia lisäämään kyberalan tutkimusta ja yhteistyötä yliopistojen ja korkeakoulujen kanssa. Tutkimus- ja koulutusyhteistyöhön panostamisen voidaan nähdä olevan poliisin kannalta lähes välttämätöntä, jotta kyberturvallisuusstrategian tavoite ajantasaisesta, korkealaatuisesta ja kustannustehokkaasta kyberrikostorjuntakoulutuksesta voidaan saavuttaa. Poliisin kyberrikostorjuntatietoisuutta ja -osaamista on viimeisten kahden vuosikymmenen aikana kehitetty eri menetelmillä. Koulutusta on järjestetty kotimaassa niin poliisioppilaitosten kuin muiden poliisiyksiköiden ja sidosryhmien toimesta. Osaamisen kehittäminen kyberrikostorjunnan osalta ei ole ollut poliisihallinnossa kokonaisuutena erityisen suunnitelmallista eikä koordinoitua. Useita kursseja on järjestetty esiin tulleen tietyn koulutustarpeen kattamiseen ad hoc -periaatteella. Sen sijaan koko hallinnon kattavaan asiantuntijuuden rakentamiseen tähtäävää suunnitelmallisuutta ei ole ollut.

Kotimaisen koulutustarjonnan niukkuudesta johtuen on erittäin merkittävänä osaamisen kehittämiskeinona ollut ulkomaisille kursseille, koulutustilaisuuksiin ja seminaareihin osallistuminen. Poliisiyksiköt ovat kuitenkin kouluttaneet virkamiehiään etenkin ulkomailla varsin vaihtelevasti. Näistä seikoista johtuen osaamisen alueellinen kattavuus ei ole ollut paras mahdollinen.

Poliisin perustutkintokoulutuksessa on viime vuosina tiettyjen opintojaksojen sisällä kuulunut lyhyitä katsauksia poliisin toiminnasta kybertoimintaympäristössä esimerkiksi yksittäisten luentojen ja harjoitustehtävien muodossa. Kokonaisia opintojaksoja aihepiiristä ei ole ollut tarjolla. Poliisin alipäällystö- ja päällystökoulutuksissa aihepiirin käsittely on ollut tätäkin vähäisempää rajoittuen lähinnä yksittäistapauksina esiin nousseeseen keskusteluun sekä muutamien aiheeseen liittyvien opinnäytetöiden tarkasteluihin.

Poliisin perustutkintokoulutukseen hakeutuu säännöllisesti henkilöitä, joilla on aiempaa koulutustaustaa ja/tai työkokemusta ICT-alalta. Tällaiset henkilöt kasvattavat jo sinällään hallinnon tietopääomaa kyberturvallisuuden osa-alueella, mutta toistaiseksi heidän potentiaaliaan ei ole pyritty hyödyntämään erityisen suunnitelmallisesti.

Poliisiammattikorkeakoulun kurssivalikoimaan on kuulunut muutamia tietotekniikkarikostutkinnan opintojaksoja, jotka ovat vaativuudeltaan olleet enimmäkseen perustasoa. Vaativan tason koulutusta ei ole juurikaan tarjottu. Tästä johtuen kyberrikostorjunnan asian-

tuntijatehtävissä pitemmän aikaa toimineille virkamiehille ei ole juurikaan ollut osaamisen kehittämistä edistävää kurssitarjontaa. Opetuksesta kursseilla ovat vastanneet enimmäkseen Keskusrikospoliisin, Suojelupoliisin ja paikallispoliisin edustajat.

Kyberrikostorjunnan asiantuntijatehtävissä toimivat virkamiehet ovat suorittaneet lukuisia, enimmäkseen ulkomaisia, kursseja. Ulkomaisten koulutusta tarjoavien tahojen kursseja on myös järjestetty Suomessa. Poliisiyksiköt ovat arvioineet tällaisen koulutuksen tarpeellisuutta ja hyödyllisyyttä varsin eri tavoin, minkä seurauksena virkamiesten mahdollisuudet kehittää osaamistaan ovat olleet eriarvoisia eri virastojen välillä. Pohjoismaiden digitaalifo-rensiikkaa työnään tekevät poliisit voivat osallistua yhteispohjoismaiseen alan koulutusohjelmaan, joka toteutetaan yhteistyössä norjalaisen yliopiston kanssa. Toiminta on aloitettu ensin Norjassa ja Tanskassa, jotka olleet mukana laatimassa alan koulutusohjelmaa. Suomi tuli myöhemmin mukaan. Useat suomalaiset poliisimiehet ovat tällä hetkellä suorittamassa ko. koulutusohjelmaa.

Poliisiammattikorkeakoulussa on vuosina 2009-2011 kertaalleen toteutettu tietotekniikkarikostutkinnan erikoistumisopinnot (EOP), jossa Poliisiammattikorkeakoulun kurssitarjonnasta koostettiin opintokokonaisuus, joka palvelisi parhaiten kyseisissä tehtävissä toimivien virkamiesten osaamisen kehittämistä. EOP:in suorittaneiden antaman palautteen mukaan kurssitarjonta ei suurelta osin tukenut tietotekniikkarikostutkijan ydinosaamisen kehittämistä.

Edellä luetellut kyberrikostorjuntaan liittyvät täydennyskoulutukset ovat olleet luonteeltaan pääasiallisesti teknistä ICT-rikostutkintaa palvelevia. Viime vuosina on enenevissä määrin noussut esiin tarve osaamisen kehittämiselle myös vaativan taktisen kyberrikostorjunnan osa-alueella. Tähän mennessä taktisille tutkijoille on tarjottu lähinnä mahdollisuutta osallistua koulutukseen, joka on alun perin kohdennettu teknistä kyberrikostorjuntaa suorittaville tutkijoille. Poliisiammattikorkeakoulu on lisäksi järjestänyt ensisijaisesti taktisille tutkijoille suunnattua tietotekniikkarikostutkinnan peruskurssia. Teknisten kurssien sisältö ei ole optimaalinen kun huomioidaan vaativan taktisen kyberrikostorjunnan tarpeet.

Jatkossa tuli selvittää "Insinööristä poliisiksi"-koulutusohjelmamallia huomioiden mallin tarveharkinnan, edellytykset ja vaatimukset. Kyseisen koulutusohjelman keskeisenä ideana on rekrytoida soveltuvan teknisen koulutuksen omaavia henkilöitä suorittamaan koulutusta, joka antaisi hakukelpoisuuden poliisivirkoihin eri yksiköissä. Kyseessä olisi erityisesti kyberturvallisuuden tehtäviin räätälöity kokonaisuus, jossa annettaisiin riittävät tiedot ja taidot toimia poliisiviroissa sellaisissa tehtävissä, joiden pääasiallinen toimenkuva liittyy kyberrikostorjuntatyöhön. Vastaavan kaltaisia koulutusohjelmia on suunnitteilla eräissä Euroopan maissa.

Edellä mainittujen koulutusten lisäksi on syytä nostaa esiin kyberturvallisuuden verkkokoulutukset, joiden suorittamista on edellytetty suurimmalta osalta poliisihallinnon työntekijöistä. Kyseisen kaltaisissa koulutuksissa on tarvittaessa mahdollista nostaa esiin sellaisia kyberrikostorjuntaan liittyviä seikkoja, joiden voidaan katsoa kuuluvan poliisihallinnon henkilöstön yleistietämykseen.

Poliisiammattikorkeakoulussa on valmisteilla kyberturvallisuuteen liittyvä turvallisuushallinnon väitöstutkimushanke. Tämän lisäksi on viime aikoina ollut suunnitteilla tutkimusyhteistyötä eri korkeakoulujen ja lähinnä poliisin valtakunnallisten yksiköiden välillä.

Tietorikollisuuden torjunnan koulutukseen liittyvät toimenpidesuositukset:

1) Kartoitetaan tietoverkkorikostorjunnan henkilöstö ja osaamisen kehittämistarpeet sekä järjestetään tarpeiden mukaisesti koulutusta. Kehitetään myös kyberrikostorjunnan osaamisen kehittämistä tukevia jatko-opintomahdollisuuksia poliisihallinnossa.

Vastuutaho: Poliisiammattikorkeakoulu.

2) Poliisiammattikorkeakoulu tekee tarvittavat muutokset AMK- ja YAMK -tutkinto-ohjelmiinsa. Tämä tarkoittaa mm. kyberrikostorjunnan perusteiden sisällyttämistä opetussuunnitelmiin.

Vastuutaho: Poliisiammattikorkeakoulu

3) Lisätään kyberrikostorjunnan täydennyskoulutustarjontaa. Yksittäisten täydennyskoulutuksen opintojaksojen lisäksi tarjotaan kyberrikostorjuntaan erikoistuville mahdollisuutta kokonaisvaltaisemman erikoistumisopintokokonaisuuden suorittamiseen.

Vastuutaho: Poliisiammattikorkeakoulu.

4) Poliisi liittyy täysivaltaiseksi jäseneksi mukaan yhteispohjoismaiseen NCFI-koulutusohjelmaan (Nordic Computer Forensic Investigators).

Vastuutaho: Poliisiammattikorkeakoulu

5) Selvitetään "Insinööristä poliisiksi"-koulutusohjelmamallia huomioiden mallin tarveharkinnan, edellytykset ja vaatimukset.

Vastuutaho: Poliisiammattikorkeakoulu

12.5 Tietoverkkorikollisuuden tilannekuvaan liittyvä arviointi

Suomen kansallisessa kyberturvallisuusstrategiassa yhtenä tavoitteena on parantaa eri toimijoiden tilannetietoisuutta tarjoamalla niille ajantasaista, koottua ja analysoitua tietoa haavoittuvuuksista, häiriöistä ja niiden vaikutuksista. Myös Sipilän hallitusohjelmaan on kirjattu tavoite kehittää tilannekuvatyötä.

Valtioneuvoston rahoittamassa (VNTEAS) Tietoverkkorikollisuuden tilannekuva-hankkeessa kartoitettiin tietoverkkorikollisuuden tilannekuvatyön nykytila. Tämän selvityksen toimenpidesuositukset perustuvat hankkeessa esiin tuotuihin kehittämisehdotuksiin. Tietojohtoinen poliisitoiminta on johtamismalli, jossa päätöksenteko nojaa rikostiedustelutietoon ja analyysiin. Oikea ja ajantasainen tilannetietoisuus on edellytys tietojohtoiselle poliisitoiminnalle. Tilannekuvan avulla operatiivisen toiminnan havainnot yhdistetään laajempiin, ilmiötason havaintoihin – sekä toisin päin – viestitään tarvittaville tasoille niin organisaation sisällä kuin ulkopuolisille sidosryhmille. Yhteistyö muiden viranomaisten ja elinkeinoelämän kanssa on tärkeää, koska tietoverkkorikollisuus ja kyberuhkat ilmiönä ylittävät rajat paitsi valtioiden myös viranomaisten välillä.

Poliisin tilannekuva tietoverkkorikollisuudesta pitäisi olla myös osa Viestintäviraston Kyberturvallisuuskeskuksen laatimaa yhdistettyä kybertilannekuvaa. Tietoverkkorikollisuuden osalta Keskusrikospoliisin kyberrikostorjuntakeskus vastaa tilannekuvan laatimisesta. Myös Suojelupoliisi pitää yllä tilannekuvaa toimivaltaansa kuuluvista tietoverkkorikoksista.

Tietoverkkorikollisuuden tilannekuvaa poliisin kyberrikostorjuntakeskuksessa kokoaa pääasiassa tiedonhankintatiimi, jonka ensisijainen tehtävä on tukea rikostutkintaa tekemällä tietoverkkorikostiedustelua poliisin Kyberrikoskeskuksen tutkinnassa oleviin juttuihin liittyen. Tietoverkkorikollisuuden tilannekuvatyön kehittäminen aloitettiin syksyllä 2015. Tyypilliset tiedonkeruun lähteet ovat erilaisia verkkolähteitä. Twitter, verkkofoorumit ja poliisin oma Nettivinkki-palvelu, jonne kansalaiset voivat ilmoittaa rikosepäilyistään, ovat esimerkkejä säännöllisesti seurattavista lähteistä. Sosiaalisen median kautta voi seurata niin tietoturva-alan toimijoiden ja viranomaisten kuin rikollisten toimia. Poliisin kyberrikostorjuntakeskus käyttää myös muiden viranomaisten, erityisesti Kyberturvallisuuskeskuksen, toimittamia kyberturvallisuuden raportteja sekä säännöllisiä tilannekuvatuotteita oman tilannetietoisuutensa ylläpitämisessä. Kotimaisten tahojen lisäksi tietoa vastaanotetaan kansainvälisiltä kumppaneilta esimerkiksi raportteina, sähköpostiviesteinä ja tiedustelutietona. Säännöllistä ja järjestelmällistä tilannetietoisuuden lisäämiseen pyrkivää tiedonvaihtokulttuuria kotimaisten poliisilaitosten kanssa ei toistaiseksi ole.

Tietoverkkorikollisuuden tilannekuvaa välitetään tällä hetkellä kotimaisille viranomaisille lähinnä suullisesti viikoittaisissa palavereissa (Poliisin kyberrikostorjuntakeskus, Kyberturvallisuuskeskus, Suojelupoliisi, Valtioneuvoston tilannekeskus ja Puolustusvoimat) sekä tarpeen mukaan tapahtuvin yhteydenotoin esimerkiksi yhteisten pikaviestintäpalveluiden kautta, sähköpostitse tai puhelimitse. Myös erilaiset seminaarit, harjoitukset, tapaamiset, lausunnot sekä yhteistyöryhmät ovat keino välittää ja saada ilmiötason tilannekuvaa.

Yhtenä tavoitteena on osoittaa, mitä hyötyä tilannekuvayhteistyöstä on yrityksille. Poliisilla tulisi olla tarjota riittävän hyvin yrityksiä palveleva tiedonvaihtomekanismi, jotta yritykset kokisivat tiedonvaihdon hyödylliseksi. Erityisesti yritysvakoilun rajapintaa lähestyttäessä myös Suojelupoliisi voi osallistua ja olla mukana tukemassa yrityksiä. Tietoverkkorikollisuuden tilannekuvahanke suositteli kohdistamaan viestintää yritysten johtotasolle, jotta se näkisi, mitä konkreettista hyötyä rikostutkinnasta on ollut. Esimerkiksi on voitu löytää toimintatapoja, joilla ennaltaehkäistään rikoksia tulevaisuudessa.

Viranomaisten yhteisen tilannetietoisuuden parantamiseksi kehitetään Viestintäviraston alusta yhteiseksi tiedonvaihtoalustaksi. Tilannekuvahanke suositteli laatimaan yhteistyöasiakirjat poliisin ja Kyberturvallisuuskeskuksen kanssa, jossa sovittaisiin menettelytavat yhteistyölle ja tiedonvaihdolle. Yhteistyöasiakirja poliisin ja Kyberturvallisuuskeskuksen välillä allekirjoitettiin huhtikuussa 2016. Poliisin ja tutkimusyhteisön välistä yhteistyötä tulisi kehittää esimerkiksi asettamalla yhteisiä tutkimus- ja kehityshankkeita, joissa poliisi osallistuu tutkimuksen toteuttamiseen tai on loppukäyttäjän roolissa. Tietoverkkorikollisuuden tilannekuvan kehittämishanke on tällaisesta toimintatavasta loistava esimerkki.

Tietoverkkorikollisuuden tilannekuvaan liittyvät toimenpidesuositukset:

1) Määritellään poliisin oman tilannekuvatyön tavoitteet, resurssit, keinot ja toimenpiteiden aikataulu.

Vastuutahot: Poliisihallitus ja Keskusrikospoliisi

2) Tehdään tietoverkkorikollisuuden tilannekuvasta koko poliisin kyberrikostorjuntakeskuksen, poliisilaitosten ja soveltuvissa määrin Suojelupoliisin yhteinen asia.

Vastuutaho: Keskusrikospoliisi

12.6 Lainsäädäntöön ja kansainväliseen tutkintaa liittyvien tarpeiden arviointi ja toimenpide-ehdotukset

Poliisihallituksen asettama työryhmä poliisin kybertoimivaltuuksista antoi loppuraporttinsa 27.5.2015. Raportissa on tuotu poliisin näkökulmasta esille tärkeimpiä toimivaltuustarpeita, jotka ovat poliisin ydintehtävien kannalta keskeisiä erityisesti tietoverkoissa tapahtuvien sekä niitä hyväksikäyttäen tehtävien rikosten tutkinnan osalta. Muutostarpeita oli muun muassa laite-etsintää ja telepakkokeinoja koskeviin säännöksiin sekä rikostiedusteluun liittyen.

Lisäksi sisäisen turvallisuuden selonteon linjausten mukaisesti tulee tarkastella muun muassa esitutkinnan rajoittamismahdollisuuksien käytön lisäämistä osana esitutkinnan tehostamistoimenpiteitä.

Suomen turvallisuusympäristö on muuttunut nopeasti johtuen muun muassa globalisoitumisesta ja digitalisaation voimakkaasta kehityksestä. Jatkuvasti muuttuva toimintaympäristö edellyttää lainsäädännön arviointia ja kehittämistä jatkuvana ja pysyväisluonteisena toimintana. Yleinen kansainvälistymis- ja digitalisoitumiskehitys on tärkeää ja väistämätöntä. Turvallisuusviranomaisillamme pitää olla riittävät toimivaltuudet kehittyvissä tietoverkoissa. On erittäin tärkeää, että tietoverkkorikollisuuden torjunnassa koko rikostorjuntaketju esitutkinnasta aina tuomion antamiseen on varmistettu. Tässä esimerkiksi syyttäjien ja tuomioistuimen rooli on esitutkintaviranomaisten ohella tärkeässä asemassa.

Tammikuussa 2014 tuli voimaan poliisilain (872/2010) ja pakkokeinolain (806/2010) kokonaisuudistukset, joissa pyrittiin ottamaan huomioon myös tekninen kehitys. Lainsäädännössä pyrittiin tekniikkaneutraaliin lainsäädäntöön, jotta lainsäädäntöä ei teknisen kehityksen takia tarvitse lyhyin väliajoin muuttaa. Säännösten tulisi kuitenkin kyetä vastaamaan toimintaympäristön muutoksiin.

Erityisesti kohteelta salaa tapahtuvan tiedonhankinnan ja salaisten pakkokeinojen kannalta merkityksellisiä ovat perustuslailliset, varsinkin luottamuksellisen viestin suojaan liittyvät näkökohdat, sekä suhteellisuusperiaate. Usein on kysymys punninnasta, jossa perus- ja ihmisoikeuksien suojaa tarkastellaan rikosoikeuden tehokkuusvaatimuksia vastaan. Suhteellisuusperiaatteesta seuraa, että jonkin tutkintakeinon käyttöä rikoksen estämisessä, paljastamisessa ja selvittämisessä ei ratkaise yksinään se, onko keinosta hyötyä, vaan huomioon on otettava se, puuttuuko keino, ja jos puuttuu, millä tavoin perustuslailla suojattuihin oikeuksiin, ja se, kuinka vakava kysymyksessä oleva rikos on. Merkityksellisiä ovat perustuslakivaliokunnan esimerkiksi pakkokeino- ja poliisilainsäädännön kokonaisuudistuksen yhteydessä esittämät kannanotot (PeVL 66/2010 vp ja PeVL 67/2010 vp).

Poliisilakia koskevassa hallituksen esityksen (224/2010) yleisperusteluissa todetaan, että suoja ja tehokas rikostorjunta eivät ole toistensa poissulkevia, sillä erityisesti rikosten ja vahingollisten tapahtumien estämisellä suojataan samalla myös perus- ja ihmisoikeuksia. Lisäksi kysymys on rikostorjunnan tehokkuuden suojaamisesta siten, että taktisten ja teknisten menetelmien teho heikkenee, kun tietoisuus niiden käyttötavasta tai teknisistä ominaisuuksista leviää.

Salaisten tiedonhankintakeinojen ja salaisten pakkokeinojen käytön osalta on tärkeää sen hahmottaminen, mitä mainitut keinot tarkkaan ottaen ovat, minkälaisia toimenpiteitä ne jo nykyisin mahdollistavat, miten ne suhtautuvat toisiinsa ja minkälaisen kokonaisuuden ne muodostavat. Ennen mahdollisiin lainsäädännön muuttamistoimenpiteisiin ryhtymistä on huolellisesti selvitettävä, mitä kaikkea jo voimassa olevat säännökset mahdollistavat. Tältä kannalta tärkeässä asemassa on myös koulutus.

Euroopan ihmisoikeustuomioistuimen (EIT) ratkaisuilla on ollut ratkaiseva vaikutus kun salaisia tiedonhankintatoimenpiteitä uudistettiin. Tuomioistuimen ratkaisukäytännössä on korostettu erityisesti laillisuusperiaatetta.

Rikostiedustelun kannalta lainsäädännön keskeisimmät ongelmat ovat henkilötietojen käsittelyä koskevassa sääntelyssä. Tietoverkoissa tehtävän tiedonhankinnan toimivaltuuksia tulisi parantaa, jotta tietoverkkorikosten ennalta estämiseen ja paljastamiseen olisi tehokkaampia keinoja. Tiedustelutiedolla on suurta merkitystä rikosten estämisen esiedellytyksenä. Jatkovalmistelussa on täsmentynyt, että poliisin kiireellisimmät ja tärkeimmät toimivaltuustarpeet koskevat erityisesti rikosanalyysia tukevaa tietojenkäsittelyä sekä tietojen keräämistä ja tallettamista tietoverkkojen avoimista lähteistä. Sisäministeriö on käynnistänyt 28.1.2016 lakihankkeen poliisin henkilötietojen käsittelyä koskevan lain kokonaisuudistuksesta niin, että se vastaa uudistuvaa Euroopan unionin tietosuojalainsäädäntöä. Lisäksi hankkeen asettamiskirjeen mukaan erityisesti kyberrikollisuuden ja järjestäytyneen rikollisuuden torjunta edellyttää mahdollisuutta tiedustelutiedon ja niin sanotuista avoimista lähteistä saatavan tiedon hyödyntämiseen ja tallettamiseen.

Hallitus on käynnistänyt kolme erillistä lainsäädäntöhanketta, joissa esitetään säädösperustaa ulkomaantiedustelulle ja tietoliikennetiedustelulle. Valmistelun yhteydessä kiinnitetään huomiota perus- ja ihmisoikeuksien toteutumiseen. Sisäministeriö johtaa siviilitiedustelua koskevaa hanketta, puolustusministeriö sotilastiedustelua koskevaa ja oikeusministeriö perustuslain mahdollista muuttamista koskevaa hanketta. Hankkeita valmistelee kolme erillistä työryhmää kiinteässä yhteistyössä. Siviilitiedustelua koskevan lainsäädäntöhankkeen keskeisin tavoite on kansallisen turvallisuuden parantaminen. Sisäministeriön johtaman työryhmän työ painottuu suojelupoliisin tehtäviin ja toimivaltuuksiin. Suojelupoliisin tärkeimpänä tehtävänä on yhteistyössä muiden turvallisuusviranomaisten, erityisesti keskusrikospoliisin, kanssa ennalta estää ja paljastaa terrorismiin, laittomaan tiedus-

telutoimintaan, joukkotuhoaseiden levittämiseen ja ääriliikkeisiin sekä valtion turvallisuutta vaarantavaan järjestäytyneeseen rikollisuuteen kytkeytyviä hankkeita.

Kansainvälinen ulottuvuus digitaalisen todistusaineiston keräämisessä

Tietoverkkorikokset ovat hyvin usein rajat ylittäviä rikoksia. Laite-etsintää tehtäessä tulkintaongelmia on aiheuttanut erityisesti pilvessä sijaitsevan datan luonne. Tietoverkossa oleva data on helposti siirrettävissä lainkäyttöalueelta toiselle, se saattaa olla pirstoutuneena useammalle lainkäyttöalueelle tai sen sijaintia ei ole mahdollista lainkaan selvittää. Lisäksi datan sijainti jossakin valtiossa ei tarkoita sitä, että samassa valtiossa sijaitseva luonnollinen tai juridinen henkilö myös hallinnoisi ko. dataa. Tietoverkossa olevan datan luonteeseen nimittäin kuuluu, että sitä voi lähtökohtaisesti hallinnoida mistä päin maailmaa tahansa. Tällöin huomio kiinnittyy tiedonhankinnan mahdolliseen rajat ylittävään luonteeseen, jolloin on huomioitava se, ettei tutkinnassa mennä toisen valtion viranomaisten toimivaltaan. Erityisesti kysymys kuuluu milloin ylipäätänsä lainvalvontaviranomaisten tulee kiinnittää huomiota tiedon hankinnan rajat ylittävään luonteeseen.

Kansainvälisen yhteistyön perustana oleva kansainvälinen oikeusapu, jonka taustalla ovat kansainväliset sopimukset ja muut instrumentit sekä niihin perustuva kansallinen lainsäädäntö. Määräyksiä kansainvälisestä oikeusavusta sisältyy paitsi Euroopan neuvoston tietoverkkorikollisuutta koskevaan yleissopimukseen (ns. Budapestin sopimus), myös Euroopan neuvoston keskinäistä oikeusapua rikosasioissa koskevaan sopimukseen ja sen lisäpöytäkirjoihin. Euroopan unionissa keskeinen rikosoikeusapuinstrumentti on eurooppalaista tutkintamääräystä koskeva direktiivi, joka korvaa pääosin vuoden 2000 Euroopan unionin oikeusapusopimuksen ja siihen tehdyn pöytäkirjan. Lisäksi Euroopan unionilla ja jäsenvaltioilla on kahdenvälisiä oikeusapusopimuksia kolmansien maiden kanssa, kuten USA:n kanssa. Viimeksi mainittua sopimusta ollaan päivittämässä. Eurojustilla on myös keskeinen rooli oikeusapumenettelyn helpottamisessa ja koordinoinnissa.

Kansainvälisistä sopimuksista merkittävin on Euroopan neuvoston tietoverkkorikollisuutta koskeva yleissopimus (ns. Budapestin sopimus). Budapestin sopimus edesauttaa osaltaan kyberrikostutkintaprosessin nopeuttamista valtionrajat ylittävien tutkintatoimenpiteiden osalta, mutta sitä voidaan luonnollisesti soveltaa ainoastaan sopimuksen ratifioineiden valtioiden välillä. T-CY komitea edustaa Budapestin tietoverkkorikollisuutta koskevan yleissopimuksen jäsenvaltioita sopimusta koskevissa asioissa. T-CY -komitea (Cybercrime Convention Committee) on perustanut kaksi työryhmää käsittelemään rajan ylittävän tiedon käsittelyä. Transborder Group ja Cloud Evidence Group. Sähköisessä muodossa oleva tieto voidaan jakaa tilaajatietoihin, liikennetietoihin ja sisältötietoihin. Näistä erityisesti sisältötiedot ovat yksityisyyden suojan kannalta merkityksellisintä tietoa. Rikostutkinnan etenemisen kannalta taas tilaajatiedolla on suuri merkitys. T-CY:ssä on parasta aikaa käsittelyssä yleissopimuksen 18 artiklan 1 kappaleen b kohtaa (tilaajatietoa koskeva esittämismääräys)

koskeva tulkintaohje, jolla pyritään tehostamaan tilaajatietojen saamista suoraan palvelutarjoajalta. Lisäksi seuraavassa T-CY:n kokouksessa kesäkuussa 2017 on tarkoitus tehdä päätös lisäpöytäkirjan laatimisesta koskien nimenomaan rajat ylittävää digitaalista todisteiden hankintaa.

Suomi osallistuu aktiivisesti T-CY komitean työhön ja näkee tärkeänä, että kansainvälisiä oikeusapuinstrumentteja tehostetaan ja rajat ylittävän digitaalisen todisteiden keräämistä koskevia menettelyjä selvennetään.

Suomi osallistuu aktiivisesti myös siihen työhön, jota Euroopan unionissa tehdään rikosoikeuden käytön parantamiseksi verkkoavaruudessa. Tietoverkkorikollisuuden torjunnan haasteisiin on kiinnitetty erityistä huomiota jo siitä alkaen, kun huhtikuussa 2015 hyväksyttiin turvallisuusagenda. Aihe on ollut prioriteettina Brysselin terrori-iskuista 22.3.2016 lähtien.

OSA -neuvosto hyväksyi 9.6.2016 päätelmät rikosoikeuden käytön parantamisesta verkkoavaruudessa. Päätelmien ensimmäinen jakso koskee yhteistyön parantamista palveluntarjoajien kanssa, toinen jakso koskee keskinäisen oikeusavun menettelyjen virtaviivaistamista ja olemassa olevien instrumenttien nopeata ja tehokasta täytäntöönpanoa ja kolmas jakso koskee tarvetta tarkastella verkkoavaruuden tutkintatoimivallan sääntöjä. Päätelmien toteuttamisesta vastaa komissio, joka esitti edistymisraportin OSA -neuvoston kokouksessa 8.12.2016. Työn tulokset on tarkoitus esittää kesäkuussa 2017.

Tietojen salaukseen (kryptaus) liittyviä rikosoikeuden haasteita on ryhdytty käsittelemään Euroopan unionissa vuoden 2016 jälkipuoliskolla. Puheenjohtajavaltion järjestämän kyselyn jälkeen tarvittavista toimenpiteistä on keskusteltu unionin toimielimissä. OSA -neuvosto hyväksyi kokouksessaan 8.12.2016 puheenjohtajan ehdottaman käytännön toimenpiteisiin painottuvan lähestymistavan, joka kiinnittää huomiota muun ohessa teknisen asiantuntemuksen parantamiseen, tietojen ja hyvien käytäntöjen vaihtamiseen sekä koulutukseen ja kapasiteetin rakentamiseen.

Toimenpidesuositukset lainsäädännön kehittämiseksi:

1) Arvioidaan yhdessä oikeusministeriön kanssa poliisilakia ja pakkokeinolakia koskevien säännösten muutostarpeita sekä tarvittaessa valmistellaan pakkokeinojen käyttöä ohjaavan suhteellisuusperiaatteen ja perustuslakivaliokunnan pakkokeinojen käyttöä koskevien kannanottojen asettamissa rajoissa lainsäädäntömuutoksia niin, että poliisilla on riittävät toimivaltuudet tietoverkkoympäristöön kohdistuvien rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi.

Vastuutahot: sisäministeriö ja oikeusministeriö

2) Arvioidaan yhdessä oikeusministeriön kanssa poliisin esitutkinnan toimittamista koskevien säännösten muutostarpeita sekä tarvittaessa valmistellaan lainsäädäntömuutoksia niin, että tutkintavoimavarat voidaan kohdistaa asianmukaisesti ottaen huomioon tietoverkkoympäristöön kohdistuvien rikosten laatu ja asianomistajan asema.

Vastuutahot: sisäministeriö ja oikeusministeriö

3) Poliisin henkilötietojen kokonaisuudistusta valmistelemaan asetetussa hankkeessa arvioidaan rikosanalyysiä tukevan tietojenkäsittelyyn sekä tietojen keräämistä ja tallettamista tietoverkkojen avoimista lähteistä liittyvät säädöstarpeet sekä säädetään asiasta tarvittaessa.

Vastuutaho: sisäministeriö

4) Osallistutaan aktiivisesti Euroopan neuvostossa ja Euroopan unionissa tehtävään työhön, jossa etsitään tehokkaampia keinoja digitaalisen todistusaineiston keräämiseksi.

Vastuutahot: sisäministeriö ja oikeusministeriö

12.7. Tietoverkkorikostorjunnan resurssitarpeiden arviointi ja esitys resursseiksi

Poliisin (pl. Suojelupoliisi) kyberiin ja tietoverkkorikostorjuntaan liittyvät lisäresurssitarpeet toimintamenoihin momentille 26.10.01 (siirtomääräraha 2v)

Esitys liittyy kansalliseen kyberturvallisuusstrategiaan ja sen täytäntöönpano-ohjelmaan sekä Sipilän hallitusohjelmaan. Resurssit tulee mitoittaa kyberrikollisuuden Suomelle aiheuttamiin riskeihin ja tietoverkkorikostorjunnalle asetettaviin tavoitteisiin. Poliisin sisällä toimintaa ohjaa "ohje vakavien tietoverkkorikosten torjunnan järjestämisestä".

Poliisin tietoverkkorikollisuuden (kyberrikollisuuden) torjunnan resurssitarpeet jakautuvat kolmen erillisen toiminnon kesken sekä taloudellisiin että henkilöresursseihin. Tehtäväalueet ovat seuraavat:

1) Tietotekninen tutkinta (ns. digitaaliforensiikka)

Digitaaliforensiikka tarkoittaa todisteiden esille hakua erilaisista tietoteknisistä laitteista, esimerkiksi tietokoneista, muistilaitteista ja navigaattoreista. Toiminto on rikoslajineutraalia, sillä digitaalisen todistusaineiston esille haku voi liittyä varsinaisiin kyberrikoksiin, mutta myös muihin rikoksiin kuten esimerkiksi henkirikoksiin tai talousrikoksiin.

2) Vakavien tietoverkkorikosten esitutkinta

Vakavia tietoverkkorikoksia ovat:

- rikollisryhmien tekemät verkkorikokset (esim. poliisin nimissä tehdyt kiristyshaittaohjelmarikokset)
- teot, jotka aiheuttavat merkittäviä vahinkoja, kuten mittavat verkkopetokset
- verkkorikokset, jotka aiheuttavat uhreille vakavaa haittaa (esim. lasten seksuaalinen hyväksikäyttö tietoverkkoja hyödyntäen)
- verkkorikokset, jotka kohdistuvat kriittiseen infrastruktuuriin ja tietojärjestelmiin (esim. pankkijärjestelmät, sähkön- tai vedenjakelujärjestelmät ym.)

3) Tiedonhankinta tietoverkoista (rikostiedustelu tietoverkoissa)

Poliisin operatiivisessa toiminnassa tiedonhankinnan ja tietoverkoissa tapahtuvan tiedustelun tavoitteena on seurata ja hankkia tietoa, jolla voidaan arvioida olevan merkitystä poliisitoiminnallisesti joko ennalta ehkäisevässä, paljastavassa tai rikostutkinnallisessa merkityksessä. Toiminto on rikoslajineutraalia.

Tietoverkkorikollisuuteen ja kybertoimintaympäristöön liittyvät tehtävät ja vastuut kuuluvat kaikkien poliisiyksikköjen tehtäviin siten kun poliisiyksikköjen välisestä tehtävänjaosta on määrätty. Tietoverkkouhkien torjunta on kaikkien viranomaisten yhteinen asia. Valtion ja kuntien merkittävien tietojärjestelmien turvallisuudesta ja toimivuudesta on huolehdittava kaikissa olosuhteissa. Myös yksisyissektorin tietojärjestelmien ja kansalaisten järjestelmien toiminta on pystyttävä turvaamaan. Tietojärjestelmien ja tietoverkkojen ylläpidosta vastaavilla on erityinen velvollisuus huolehtia omien järjestelmiensä turvallisuudesta. Tietoverkkorikollisuuden ja tietoverkkouhkien torjunta ja mahdollisten tapausten selvittäminen kuuluu rauhan aikana pääasiallisesti poliisin tehtäviin. Tehtävän hoitamiseksi poliisille on annettu oikeudet käyttää lainsäädännössä säädettyjä toimivaltuuksia uhkien torjumiseksi tietoverkoissa, tietoverkkorikosten estämiseksi tai selvittämiseksi.

Tietoverkkorikollisuus ja sen eri tekomuodot ovat jatkuvassa kasvussa. Selvitäkseen rikosten määrän noususta sekä toimintaympäristön jatkuvasta muuttumisesta poliisi tarvitsee lisähenkilöstöä, uusia teknisiä laitteita ja järjestelmiä sekä osaamisen kasvattamista koulutuksella.

Poliisin kyberrikollisuuden torjunta ja kybertoimintaympäristön kehittämiseen tarvittavat lisäresurssit on kuvattu alla olevassa taulukossa. Samaan kokonaisuuteen liittyvä Suojelupoliisin esitys on kirjattu Suojelupoliisin toimintamenomomentin alle.

Poliisin kyberrikollisuuden torjunta ja kybertoimintaympäristön kehittäminen	S 2018	S 2019	S 2020	S 2021
Henkilöresurssit lisäys: sijoitus poliisiyksiköihin 11 virkaa tietotekninen tutkinta 25 virkaa taktiseen tutkintaan 30 virkaa tietoverkkotiedusteluun Tarve aiheutuu tietoverkkorikosten määrän kasvusta sekä toiminnan tehostamistarpeesta	3 480 000	3 480 000	3 480 000	3 480 000
Tietoteknistä tutkintaa koskevan tietojärjestelmän päivittäminen vastaamaan toiminnan vaatimuksia.				
Tämä pitää sisällään palvelimet, tietoverkot ja sovellukset				
Jatkuva tarve johtuen toimintaympäristön muutoksesta.	2 000 000	2 000 000	400 000	400 000
Alan koulutuksen järjestäminen teknisen ja taktisen tutkinnan osalta (mm. Encase, FTK, XRY, Cellebrite, Oxcygen, verkkojäljet, haittaohjelmat, taktinen verkkorikostutkinta)				
Osaamisen kehittäminen on jatkuvaa	250 000	250 000	300 000	300 000
Teknisen tietojärjestelmäalustan hankkiminen (investoinnit, palvelut ja ylläpito) tiedonhankintaan tietoverkoista.				
Toiminnan tehostamistarve	600 000	300 000	230 000	230 000
Tiedonhankinnan sovellusten ja työkalujen hankkiminen (mm. sosiaalinen media, tiedonhankinta, tekstianalyysi, laitetarkkailu jne.)				
Toiminnan tehostamistarve	600 000	600 000	700 000	700 000
Kyberrikostorjuntakeskus				
Keskusrikospoliisiin perustetun kyberrikostorjuntakeskuksen toiminnan vahvistaminen ja laajentaminen, yht. 18 htv	1 800 000	1 800 000	1 800 000	1 800 000
YHTEENSÄ	**8 730 000**	**8 430 000**	**6 910 000**	**6 910 000**

Suojelupoliisin kyberiin ja tietoverkkorikostorjuntaan liittyvät lisäresurssitarpeet toimintamenot momentille 26.10.02 (siirtomääräraha 2v)

Esitys liittyy kansalliseen kyberturvallisuusstrategiaan ja sen täytäntöönpanoesityksiin sekä Sipilän hallitusohjelmaan. Poliisin, pl. Suojelupoliisin tietoverkkorikollisuuden (kyberrikollisuuden) torjunnan resurssitarpeet on esitetty momentin 26.10.01 Poliisitoimen toimintamenot alla.

1) Tietotekninen tutkinta

Suojelupoliisin digitaaliforensiikan tarpeet ovat lisääntyneet merkittävästi erityisesti terrorismin torjunnan sektorilla. Suojelupoliisi osallistuu entistä enemmän myös valtionhallinnon siviiliviranomaisten tietojärjestelmien suojaukseen. Viranomaispoolin toiminnalla selvitetään tietoturvapoikkeamia ja estetään lisävahinkojen syntymistä organisaatioissa sekä organisaatioiden välillä.

2) Tietoverkossa tapahtuvien vakoilurikosten esitutkinta

Suojelupoliisi suorittaa toimialaansa kuuluvien vakavien tietoverkkorikosten esitutkinnan. Suojelupoliisin omalla toimialalla tapahtuva tietoturvapoikkeamien- sekä verkkovakoiluesitutkinnat vaativat riittävää resursointia.

3) Tiedonhankinta tietoverkoista (tietoliikennetiedustelu)

Suojelupoliisin kybertoiminnolla tulee olemaan merkittävä rooli valtakunnallisesti kohdistetussa tietoliikennetiedustelussa sen operatiivisten yksiköiden tarpeiden toteuttamisessa. Kohdistetun tietoliikennetiedustelun toteuttaminen edellyttää henkilöstöä operointiin sekä analyysiin.

4) Koulutus

Suojelupoliisin toimialalla tapahtuva digitaaliforensiikka sekä haittaohjelmatutkinta vaatii erityisen syvällistä osaamista käytettyjen tekniikoiden kehittyneisyydestä johtuen. Tämä edellyttää jatkuvaa kouluttautumista. Tällaista koulutusta hankintaa myös alan erityisosaamista tarjoavista kansainvälisistä yrityksistä.

5) Tietojärjestelmien alustat ja tiedonhankinnan sovellukset ja työkalut

Kohdistetussa tietoliikennetiedustelussa viraston tulee integroida järjestelmiään muiden organisaatioiden järjestelmiin toiminnallisuutta ja oikeusturvaa tukevalla tavalla. Tällä on väistämättömiä kustannusvaikutuksia Suojelupoliisille kehyskauden aikana. Käytettävien tietojärjestelmien alustoille ja työkaluille sekä sovelluksille voidaan antaa vain alustavia kustannusarvioita. Kokonaislisäystarve noudattelee edellisen kehysesityksen tarve-esitystä, koska on oletettavaa, että tietoliikenne-tiedustelun osalta Suojelupoliisi joutuu hankkimaan omat järjestelmänsä, mutta rikostiedustelun tiedonhankinnassa lienee mahdollista tukeutua poliisin järjestelmiin. Tietojärjestelmien alustojen osalta kokonaislisäystarve on, 1,36 milj. €.

Suojelupoliisin tietoverkkorikostorjunta ja kybertoimintaympäristön kehittäminen	S 2018	S 2019	S 2020	S 2021
Henkilötyövuodet	5	10	14	17
Muut kulut €	1 050 000	675 000	625 000	640 000
YHTEENSÄ €	**1 350 000**	**1 275 000**	**1 465 000**	**1 660 000**

Oikeusministeriön hallinnonalan lisäresurssitarpeet

Lisäresurssitarpeita arvioitaessa huomioon on otettava se, että koko rikostorjuntaketjun esitutkinnasta aina tuomion antamiseen tulee olla varmistettu. Tietoverkkorikollisuuden tehokkaan torjunnan kannalta ei ole riittävää, että huomiota kiinnitetään vain poliisin lisäresurssitarpeisiin, vaan tärkeää on myös syyttäjien ja tuomareiden riittävien resurssien turvaaminen.

Poliisin tietoverkkorikollisuuden torjuntaan arvioidusta henkilöstölisäyksestä aiheutuu vuosittain 5,28 milj. euron menot. Oikeusministeriön hallinnonalalla lisämäärärahan tarve on tällä perusteella oikeusavun osalta 0,64 milj. euroa, tuomioistuinten osalta 1,64 milj. euroa ja syyttäjien osalta 0,69 milj. euroa. Mainittu arvio perustuu eri viranomaisten osuuksiin rikostorjunnan kustannuksista. Poliisin rikostorjunnan osuus rikosprosessin kustannuksista on noin 42 prosenttia. Vuonna 2013 poliisin rikostorjunnan kustannukset olivat 345 milj. euroa, syyttäjälaitoksen 46 milj. euroa, oikeusavun 41 milj. euroa, tuomioistuinten 107 milj. euroa ja rangaistusten täytäntöönpanon 278 milj. euroa. Jokaista poliisin rikostorjuntaan käyttämää euroa kohden aiheutuu siten oikeusministeriön hallinnonalalle kustannuksia keskimäärin 1,36 euroa, josta syyttäjien osuus on 0,13 euroa, oikeusavun 0,12 euroa, tuomioistuinten 0,31 euroa ja rangaistusten täytäntöönpanon 0,8 euroa. Tietoverkkorikosasiat voivat olla rajat ylittävien vaikutusten vuoksi syyttäjiä ja tuomioistuimia poikkeuksellisesti työllistäviä ja erityisosaamista vaativia.

Tässä tapauksessa ei ole arvioitu aiheutuvan rangaistusten täytäntöönpanosta aiheutuvia lisäkustannuksia.

13 Yhteenveto toimeenpanosuosituksista

Suomen kansallisen kyberturvallisuuden poliisia koskevien strategisten linjausten mukaiseen tavoitetilaan pääsemiseksi esitetään seuraaviin kokonaisuuksiin liittyviä toimenpidesuosituksia:

Tietoverkkorikostorjunnan kehittämiseksi esitetään seuraavia toimenpide-ehdotuksia:

1) Muodostetaan poliisin sisäinen tietoverkkorikostorjunnan yhteistyöverkosto, joka toimii seuraavien asioiden valmisteluryhmänä:

a. Tietoverkkorikollisuuden ennalta estävä toiminta

b. Kansallisen sidosryhmäyhteistyön kehittäminen

c. Kansainvälisen yhteistyön koordinoiminen

d. ICT-rikostutkinnan infrastruktuurin yhtenäistäminen

e. Kyberrikostorjuntatyön mittareiden ja raportoinnin kehittäminen

f. Vuotuisen laajapohjaisen tietoverkkorikostorjunnan strategiatyöpajan järjestäminen ennakoivan osaamisen kehittämisen tueksi

Vastuutaho: Poliisihallitus

2) Kehitetään yliopistojen, korkeakoulujen ja muiden toimijoiden välistä yhteistyötä tietoverkkorikostorjunnan osaamisen nostamisessa.

Vastuutaho: Poliisiammattikorkeakoulu

3) Laaditaan tietoteknisen tutkinnan laatuohjelma.

Vastuutaho: Poliisihallitus

4) Kehitetään kyberrikostorjunnan syyttäjäyhteistyötä tarjoamalla syyttäjille tietoverkkorikostorjuntaan liittyvää koulutusta ja toisaalta syyttäjät voisivat antaa rikostutkijoille tietoverkkorikostorjuntaan liittyvää juridista koulutusta.

Vastuutaho: Poliisiammattikorkeakoulu

5) Suojataan kybertoimintaympäristöä terroristiselta toiminnalta varmistamalla viranomaisten toimintakyky- ja valtuudet vastata kyberuhkiin.

6) Asetetaan viranomaisten ja elinkeinoelämän yhteistyöryhmä yrityksiin kohdistuvien rikosten ennalta estämisen ja torjunnan tehostamiseksi. Ryhmän erityiseksi painopisteeksi asetetaan tietoverkkorikollisuuden torjunta.

Vastuutaho: sisäministeriö.

Tietorikollisuuden torjunnan koulutukseen liittyvät toimenpidesuositukset:

1) Kartoitetaan tietoverkkorikostorjunnan henkilöstö ja osaamisen kehittämistarpeet sekä järjestetään tarpeiden mukaisesti koulutusta. Kehitetään myös kyberrikostorjunnan osaamisen kehittämistä tukevia jatko-opintomahdollisuuksia poliisihallinnossa.

Vastuutaho: Poliisiammattikorkeakoulu.

2) Poliisiammattikorkeakoulu tekee tarvittavat muutokset AMK- ja YAMK -tutkinto-ohjelmiinsa. Tämä tarkoittaa mm. kyberrikostorjunnan perusteiden sisällyttämistä opetussuunnitelmiin.

Vastuutaho: Poliisiammattikorkeakoulu

3) Lisätään kyberrikostorjunnan täydennyskoulutustarjontaa. Yksittäisten täydennyskoulutuksen opintojaksojen lisäksi tarjotaan kyberrikostorjuntaan erikoistuville mahdollisuutta kokonaisvaltaisemman erikoistumisopintokokonaisuuden suorittamiseen.

Vastuutaho: Poliisiammattikorkeakoulu.

4) Poliisi liittyy täysivaltaiseksi jäseneksi mukaan yhteispohjoismaiseen NCFI-koulutusohjelmaan (Nordic Computer Forensic Investigators).

Vastuutaho: Poliisiammattikorkeakoulu

5) Selvitetään "Insinööristä poliisiksi"-koulutusohjelmamallia huomioiden mallin tarveharkinnan, edellytykset ja vaatimukset

Vastuutaho: Poliisiammattikorkeakoulu

Tietoverkkorikollisuuden tilannekuvaan liittyvät toimenpidesuositukset:

1) Määritellään poliisin oman tilannekuvatyön tavoitteet, resurssit, keinot ja toimenpiteiden aikataulu.

Vastuutahot: Poliisihallitus ja Keskusrikospoliisi

2) Tehdään tietoverkkorikollisuuden tilannekuvasta koko poliisin kyberrikostorjuntakeskuksen, poliisilaitosten ja soveltuvissa määrin Suojelupoliisin yhteinen asia.

Vastuutaho: Keskusrikospoliisi

Toimenpidesuositukset lainsäädännön kehittämiseksi:

1) Arvioidaan yhdessä oikeusministeriön kanssa poliisilakia ja pakkokeinolakia koskevien säännösten muutostarpeita sekä tarvittaessa valmistellaan pakkokeinojen käyttöä ohjaavan suhteellisuusperiaatteen ja perustuslakivaliokunnan pakkokeinojen käyttöä koskevien kannanottojen asettamissa rajoissa lainsäädäntömuutoksia niin, että poliisilla on riittävät toimivaltuudet tietoverkkoympäristöön kohdistuvien rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi.

Vastuutahot: sisäministeriö ja oikeusministeriö

2) Arvioidaan yhdessä oikeusministeriön kanssa poliisin esitutkinnan toimittamista koskevien säännösten muutostarpeita sekä tarvittaessa valmistellaan lainsäädäntömuutoksia niin, että tutkintavoimavarat voidaan kohdistaa asianmukaisesti ottaen huomioon tietoverkkoympäristöön kohdistuvien rikosten laatu ja asianomistajan asema.

Vastuutahot: sisäministeriö ja oikeusministeriö

3) Poliisin henkilötietojen kokonaisuudistusta valmistelemaan asetetussa hankkeessa arvioidaan rikosanalyysiä tukevan tietojenkäsittelyyn sekä tietojen keräämistä ja tallettamista tietoverkkojen avoimista lähteistä liittyvät säädöstarpeet sekä säädetään asiasta tarvittaessa.

Vastuutaho: sisäministeriö

4) Osallistutaan aktiivisesti Euroopan neuvostossa ja Euroopan unionissa tehtävään työhön, jossa etsitään tehokkaampia keinoja digitaalisen todistusaineiston keräämiseksi.

Vastuutahot: sisäministeriö ja oikeusministeriö

Poliisin ja Suojelupoliisin sekä oikeusministeriön lisäresurssitarpeet toimintamenoihin:

1) Myönnetään esityksen mukaisesti tietoverkkorikostorjuntaan ja kybertoimintaympäristön kehittämiseen esitetyt lisämäärärahat.

Sisäministeriö PL 26, 00023 Valtioneuvosto

Inrikesministeriet PB 26, 00023 Statsrådet

www.intermin.fi

SISÄMINISTERIÖ
INRIKESMINISTERIET