Euroopan unionin
neuvosto

Bryssel, 11. syyskuuta 2017
(OR. en)

8178/1/17
REV 1 DCL 1

GENVAL 40
CYBER 55

TURVALLISUUSLUOKITUKSEN POISTAMINEN

Asiakirja:	ST8178/1/17 REV 1 RESTREINT UE/EU RESTRICTED
Päivämäärä:	4. syyskuuta 2017
Muuttunut jakelu:	Julkinen
Asia:	Seitsemännen keskinäisen arviointikierroksen arviointikertomus "Kyberrikollisuuden ehkäisemistä ja torjumista koskevien eurooppalaisten politiikkojen käytännön täytäntöönpano ja toimivuus" – Suomea koskeva kertomus

Valtuuskunnille toimitetaan oheisena toisinto asiakohdassa mainitusta asiakirjasta, jonka turvallisuusluokitus on poistettu.

Tämän asiakirjan teksti on sama kuin edellisen toisinnon teksti.

Euroopan unionin
neuvosto

Bryssel, 4. syyskuuta 2017
(OR. en)

8178/1/17
REV 1

RESTREINT UE/EU RESTRICTED

GENVAL 40
CYBER 55

SELVITYS

Asia:	Seitsemännen keskinäisen arviointikierroksen arviointikertomus "Kyberrikollisuuden ehkäisemistä ja torjumista koskevien eurooppalaisten politiikkojen käytännön täytäntöönpano ja toimivuus" – Suomea koskeva kertomus

Sisällysluettelo

1. TIIVISTELMÄ

Suomen viranomaiset olivat organisoineet arviointivierailun hyvin ja sen aikana tavattiin asiaankuuluvia toimijoita, jotka vastaavat kyberrikosten ehkäisemisestä ja torjumisesta sekä eurooppalaisten politiikkojen täytäntöönpanosta ja toiminnasta: esimerkiksi Suomen kyberturvallisuuskeskus, sisäministeriö, oikeusministeriö, valtakunnansyyttäjän virasto, keskusrikospoliisi, poliisihallitus sekä liikenne- ja viestintäministeriö.

Suomen viranomaiset antoivat arviointiryhmälle täydelliset tiedot ja selvitykset kyberrikostorjunnan, rajat ylittävän yhteistyön ja EU:n virastojen kanssa tehtävän yhteistyön ja kyberstrategian oikeudellisista ja operatiivisista yksityiskohdista.

Suomen kyberturvallisuusstrategia hyväksyttiin vuonna 2013 ja siinä määritellään keskeiset tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin uhkiin ja varmistetaan sen toimivuus. Siinä keskitytään pääasiassa poliisin rooliin, eikä oikeuslaitoksen rooliin. Strategiaa ei ole tarkastelu uudelleen sen hyväksymisen jälkeen, eikä viranomaisilla myöskään vaikuta olevan suunnitelmia tehdä niin lähitulevaisuudessa.

Suomessa on yksi keskitetty tietokanta poliisiraporteille, jossa noudatetaan omanlaistaan luokittelua. Tallettaessaan raportteja järjestelmään monet poliisit eivät kuitenkaan käytä järjestelmää oikein ja luokitteluun tulee virheitä. Näin ollen arviointiryhmä katsoi, että kyberrikollisuuden laajuudesta Suomessa on vaikea saada kokonaiskuvaa yksin poliisin tilastojen pohjalta. CERT-FI -tilastoja, Viestintäviraston välittämien tapausten lukumäärää tai poliisin taikka oikeuslaitoksen luotettavia tilastoja ei ollut saatavilla. Tämä johtopäätös vastaa kyberturvallisuuskeskuksen ilmaisemia yleisiä näkemyksiä. Näin ollen arviointiryhmä katsookin, että kyberrikokset ovat aliraportoituja, minkä vuoksi järjestelmän kestokyvyn arvioiminen on vaikeaa.

Suomi on pannut täytäntöön kyberrikollisuutta koskevat eurooppalaiset välineet ja niihin perustuvat toimenpiteet.

Lainsäädäntö sisältää yleisiä säännöksiä, jotka koskevat tutkintaan, pakkokeinoihin ja poliisityöhön liittyviä menettelyjä. Erityisiä kyberrikollisuutta koskevia säännöksiä ei ole. Kyberrikollisuuden erityispiirteiden vuoksi arviointiryhmä totesi, että lainsäädäntöä on yhdenmukaistettava kyberrikostutkintaan soveltuvan toimivallan takaamiseksi poliisille.

Poliisi on toimivaltainen viranomainen kyberrikollisuuden ennaltaehkäisyn ja siihen liittyvän tutkinnan osalta sekä toimittamaan tapaukset syyttäjälle. Poliisi tekee yhteistyötä muiden lainvalvontaviranomaisten kanssa. Poliisihallitus on sisäministeriön alaisuudessa toimiva poliisin keskushallintoviranomainen. Poliisihallitus suunnittelee, hallinnoi, kehittää ja valvoo poliisin työtä ja siihen liittyviä toimintoja. Maininnan arvoista on poliisihallituksen hallinnoima erillinen budjetti, joka on omistettu poliisiyksiköille tarjottavaan kyberrikollisuuden alan koulutukseen ja laitteistohankintoihin. Arviointiryhmä katsoo tämän osoittavan, että poliisihallitus tunnustaa kyberrikostorjunnan merkityksen sekä kansallisella että aluetasolla.

Suomen keskusrikospoliisi vaikuttaa olevan hyvin valmistautunut kyberrikollisuuden torjuntaan Suomessa, mutta tietoja ja osaamista on parannettava alue- ja paikallistasolla. Arviointiryhmä totesi keskusrikospoliisin luoneen järjestelmän, jossa se avustaa lievempien kyberrikosten tukinnassa sen sijaan, että se ottaisi tutkinnan kokonaan omalle vastuulleen. Arviointiryhmä kuitenkin suositteli, että kaikkien poliisilaitosten yleisellä, ei-teknisellä henkilöstöllä olisi oltava mahdollisuus osallistua koulutukseen yhtenäisen ja johdonmukaisen näkökannan varmistamiseksi kyberrikollisuuteen kautta koko maan.

Oikeuslaitoksen puitteissa erikoistuminen on puutteellista. Arviointiryhmä katsoo, että kyberrikollisuuteen erikoistuneiden syyttäjien lukumäärä ei ole riittävä tämänhetkisen työmäärän käsittelemiseksi. Syyttäjäviranomaisilla ei myöskään ole minkäänlaista erillistä rakennetta kyberrikostorjuntaa varteen. Koska ilmi tulleiden kyberrikostapausten lukumäärä kasvaa, on perusteltua nimetä erikoistunut ryhmä syyttäjiä käsittelemään näitä tapauksia.

Viestintävirasto ylläpitää sähköisten viestintäverkkojen toimivuuden ja tietoturvan tilannekuvaa ja tiedottaa mahdollisista tietoturvauhkista. Viestintäviraston ja poliisin väliset yhteydet vaikuttavat säännöllisiltä ja epämuodollisilta. Yhteisymmärryspöytäkirjan tekeminen ja allekirjoittaminen niiden välillä olisi nähtävä ensimmäisenä askeleena kohti näiden kahden sidosryhmän tulevan yhteistyön virallistamista. Koska kyberrikokset ovat aliraportoituja, arviointiryhmä suosittelee vakavasti harkitsemaan pakottavamman ilmoitusjärjestelmän käyttöönottoa erityisesti vakavien rikosten osalta (esim. kriittisiin infrastruktuureihin tai pankkeihin kohdistuvat hyökkäykset).

Erityisesti on mainittava poliisin perustama yksi yhteyspiste kansainvälisten palveluntarjoajien kanssa käytävää viestintää varten. Näin on helpompi ylläpitää viranomaisten ja yksityisten yritysten välisiä luottamukseen ja keskinäiseen kunnioitukseen perustuvia suhteita.

Alan toimijat tuntevat Europolin/EC3:n ja Eurojustin, ja niiltä pyydetään apua. Suomi on käyttänyt yhteisiä tutkintaryhmiä suhteellisen usein. Arviointiryhmä totesi, että Suomen viranomaisten kokemukset ovat hyvin myönteisiä ja ne kannustavat yhteisten tutkintaryhmien käyttöä rajat ylittävässä tutkinnassa johtuen niistä mahdollisuuksista, joita nämä puitteet tarjoavat.

Arviointiryhmä pitää Pohjoismaiden välistä alueellista yhteistyötä tehokkaana parhaana käytäntönä. Esimerkkejä tästä yhteistyöstä ovat muun muassa pohjoismainen pidätysmääräys, yhteyshenkilöiden jakaminen ja pohjoismainen koulutusfoorumi. Yhteistyö on erinomaista myös Baltian maiden kanssa.

Kyberrikollisuuteen liittyvä asiantuntemus on rajallista oikeuslaitoksen puitteissa. On olemassa suunnitelmia lisätä syyttäjille tarjottavaa alan peruskoulutusta, mutta tuomareille ei ole nyt tarjolla järjestelmällistä koulutusta. Syyttäjien mielestä on selvää, että syyttäjät ja tuomarit tarvitsevat lisää koulutusta kyberrikollisuuteen liittyvissä kysymyksissä. Alueellisten ja paikallisten poliisivoimien osalta asiantuntemus ja työkalujen saatavuus riippuu pääasiassa yksittäisistä poliisilaitoksista. Suomen viranomaiset voisivat myös harkita järjestelmällisen koulutuksen tarjoamista erikoistuneille poliiseille hyödyntämällä ulkoisten lähteiden, kuten Euroopan kyberrikollisuuden tutkinnan koulutusryhmän (ECTEG) ja CEPOLin, kautta saatavilla olevia koulutusmahdollisuuksia.

Vaikuttaa siltä, että suurelle yleisölle on suunnattu hyvin rajallisia ja satunnaisia ehkäisykampanjoita ja muita toimia lasten hyväksikäytöstä ja yleisemmin internetin turvallisuudesta. Arviointiryhmä katsoo, että Kyberrikoskeskuksella, Kyberturvallisuuskeskuksella, kyberturvallisuusyrityksillä ja kansalaisjärjestöillä olisi mahdollisuus täyttää tämä aukko yhdistämällä resurssejaan ja toteuttaa näkyviä ja kestäviä kampanjoita, joilla pyrittäisiin lisäämään suuren yleisön tietoisuutta tästä ilmiöstä.

Ottaen huomioon kyberrikostorjunnan alan kunnianhimoisen lähestymistavan ja siihen osoitetut resurssit, arviointiryhmän näkemyksen mukaan Suomen tilanne on myönteinen ja lupaava.

2. JOHDANTO

Yhteinen toiminta 97/827/YOS[1] hyväksyttiin 5. joulukuuta 1997 ja sen nojalla perustettiin järjestäytyneen rikollisuuden torjuntaan liittyvien kansainvälisten sitoumusten kansallisen tason soveltamista ja täytäntöönpanoa koskeva arviointijärjestelmä. Yhteisen toiminnan 2 artiklan nojalla yleisten kysymysten työryhmä (GENVAL) päätti 3. lokakuuta 2013, että seitsemännellä keskinäisellä arviointikierroksella olisi käsiteltävä kyberrikollisuuden ehkäisemistä ja torjumista koskevien eurooppalaisten politiikkojen käytännön täytäntöönpanoa ja toimivuutta.

Jäsenvaltiot olivat tyytyväisiä kyberrikollisuuden valitsemiseen seitsemännen keskinäisen arviointikierroksen aiheeksi. Sovittiin kuitenkin, että koska termi "kyberrikollisuus" kattaa niin monenlaisia rikoksia, arvioinnissa keskityttäisiin niihin rikoksiin, jotka vaativat jäsenvaltioiden mielestä erityistä huomiota. Tästä syystä arvioinnissa keskitytään pääasiassa kolmeen erityisalueeseen, jotka ovat kyberhyökkäykset, lasten seksuaalinen hyväksikäyttö / lapsipornografia verkossa ja korttipetokset verkossa. Siinä olisi tarkasteltava kattavasti oikeudellisia ja operatiivisia näkökohtia, jotka liittyvät kyberrikollisuuden torjuntaan, rajatylittävään yhteistyöhön ja yhteistyöhön asiaankuuluvien EU-virastojen kanssa. Erityisen relevantteja ovat lasten seksuaalisen hyväksikäytön ja seksuaalisen riiston sekä lapsipornografian torjumisesta annettu direktiivi 2011/93/EU[2] (määräaika saattamiselle osaksi kansallista lainsäädäntöä 18. joulukuuta 2013) ja tietojärjestelmiin kohdistuvista hyökkäyksistä annettu direktiivi 2013/40/EU[3] (määräaika saattamiselle osaksi kansallista lainsäädäntöä 4. syyskuuta 2015).

1 Yhteinen toiminta 5 päivältä joulukuuta 1997 (97/827/YOS), EYVL L 344, 15.12.1997, s. 7–9.
2 EUVL L 335, 17.12.2011, s. 1.
3 EUVL L 218, 14.8.2013, s. 8.

Lisäksi kesäkuussa 2013 hyväksytyissä neuvoston päätelmissä EU:n kyberturvallisuusstrategiasta[4] toistetaan tavoite tietoverkkorikollisuudesta 23. marraskuuta 2001 tehdyn Euroopan neuvoston yleissopimuksen (Budapestin yleissopimus)[5] pikaisesta ratifioimisesta. Päätelmien johdanto-osassa painotetaan, että "EU ei kannata uusien kansainvälisten säädösten luomista kyberkysymyksissä". Yleissopimusta täydentää pöytäkirja, joka koskee muukalaisvihaan ja rasismiin syyllistymistä tietokonejärjestelmien välityksellä.[6]

Aikaisemmista arvioinneista saadut kokemukset osoittavat, että asianomaisten säädösten täytäntöönpanossa ollaan eri jäsenvaltiossa eri vaiheissa, ja tämä arviointi voisi olla hyödyksi myös niille jäsenvaltioille, jotka eivät ehkä vielä ole panneet täytäntöön eri säädösten kaikkia osia. Arvioinnin on kuitenkin tarkoitus olla laaja ja monialainen, eikä siinä ole tarkoitus keskittyä ainoastaan kyberrikollisuuden torjuntaan liittyvien eri välineiden täytäntöönpanoon, vaan pikemminkin operatiivisiin näkökohtiin jäsenvaltioissa.

Näin ollen arvioinnissa käsitellään syyttäjäviranomaisten kanssa tehtävän yhteistyön lisäksi poliisiviranomaisten yhteistyötä Eurojustin, Euroopan unionin verkko- ja tietoturvaviraston (ENISA) sekä Europolin / Euroopan kyberrikostorjuntakeskuksen (EC3) kanssa sekä sitä, miten näiden toimijoiden antama palaute kanavoidaan asianmukaisille poliisi- ja sosiaaliviranomaisille. Arvioinnissa painotetaan niiden kansallisten politiikkojen täytäntöönpanoa, jotka liittyvät kyberhyökkäysten ja petosten estämiseen sekä lapsipornografiaan. Arvioinnissa käsitellään myös jäsenvaltioiden operatiivisia käytäntöjä kansainvälisessä yhteistyössä sekä kyberrikollisuuden uhreille tarjottavaa tukea.

[4] 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

[5] CETS nro 185; avattiin allekirjoittamista varten 23. marraskuuta 2001, tuli voimaan 1. heinäkuuta 2004.

[6] CETS nro 189; avattiin allekirjoittamista varten 28. tammikuuta 2003, tuli voimaan 1. maaliskuuta 2006.

GENVAL-työryhmä hyväksyi 1. huhtikuuta 2014 järjestyksen, jossa jäsenvaltioissa vieraillaan. Suomi oli 27. jäsenvaltio, jota arvioitiin tällä arviointikierroksella. Puheenjohtajavaltio on yhteisen toiminnan 3 artiklan mukaisesti laatinut luettelon arvioinneissa käytettävissä olevista asiantuntijoista. GENVAL-työryhmän puheenjohtajan 28. tammikuuta 2014 toimittaman kirjallisen pyynnön perusteella jäsenvaltiot ovat ilmoittaneet asiantuntijoita, joilla on perusteellinen käytännön kokemus arvioinnin kohteena olevalla alalla.

Arviointiryhmät koostuvat kolmesta kansallisesta asiantuntijasta, joita avustaa kaksi neuvoston pääsihteeristön työntekijää sekä tarkkailijoita. GENVAL-työryhmä sopi puheenjohtajavaltion ehdotuksen pohjalta, että Euroopan komissio, Eurojust, ENISA ja Europol / EC3 olisi kutsuttava tarkkailijoiksi seitsemännellä keskinäisellä arviointikierroksella.

Suomea koskevan arvioinnin toteuttaneet asiantuntijat olivat Timothy Zammit (Malta), Aneta Trojanowska (Puola) ja Henrik Olin (Ruotsi). Läsnä oli myös kaksi tarkkailijaa: Michael Schmid (Eurojust) ja Sławomir Buczma neuvoston pääsihteeristöstä.

Asiantuntijaryhmä laati tämän kertomuksen neuvoston pääsihteeristön avustuksella niiden tulosten perusteella, joita saatiin Suomeen 6.–9. syyskuuta 2016 järjestetyn arviointivierailun aikana, sekä Suomen yksityiskohtaisten vastausten pohjalta, joita se toimitti arviointikyselyyn sekä näiden vastausten perusteella esitettyihin jatkokysymyksiin.

3. YLEISET KYSYMYKSET JA RAKENTEET

3.1. Kansallinen kyberturvallisuusstrategia

Suomen kyberturvallisuusstrategia hyväksyttiin valtioneuvoston periaatepäätöksellä 24. tammikuuta 2013. Strategiassa määritellään keskeiset tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin uhkiin ja varmistetaan sen toimivuus. Yksi kyberturvallisuusstrategian kymmenestä strategisesta linjauksesta on huolehtia, että poliisilla on riittävät valmiudet ennaltaehkäistä, paljastaa ja selvittää kyberrikoksia. Lisäksi huolehditaan, että poliisilla on riittävät toimivaltuudet, resurssit sekä motivoitunut henkilöstö kyberrikollisuuden ennaltaehkäisyyn, taktiseen esitukintaan sekä sähköisen todistusaineiston käsittelyyn ja analysointiin.

Kyberturvallisuusstrategiassa painotetaan kansainvälisen operatiivisen yhteistyön merkitystä sekä tiedonvaihdon jatkamista ja syventämistä EU:n ja muiden maiden vastaavien lainvalvontaviranomaisten kanssa, esimerkiksi Europolin kanssa.

Kyberturvallisuusstrategian kansallinen toimeenpano-ohjelma julkistettiin 11. maaliskuuta 2014. Kyberturvallisuuden parantamiseksi toimeenpano-ohjelmassa esitettiin kaikkiaan 74 hallinnonalojen ja Huoltovarmuuskeskuksen ehdottamaa toimenpidettä.

Liikenne- ja viestintäministeri hyväksyi Suomen tietoturvastrategian maaliskuussa 2016. Strategiassa esitetään, miten taloudellista hyvinvointia voidaan tukea rakentamalla luotetumpi ja kestokykyisempi digitaalinen ympäristö.

3.2. Kyberrikollisuuden torjunnan kansalliset painopisteet

Kun Suomen kyberturvallisuusstrategia laadittiin vuonna 2013, poliisin valmiudet todettiin yhdeksi kehittämistä vaativaksi alaksi. Yksi strategisista linjauksista kuuluu seuraavasti: "huolehditaan, että poliisilla on tehokkaat edellytykset ennalta ehkäistä, paljastaa sekä selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia". Tämän strategian pohjalta on laadittu toimeenpano-ohjelma. Ohjelma sisältää kaikkiaan 74 eri hallinnonaloja koskevaa toimenpidettä. Useilla ohjelman sisältämillä toimenpiteillä pyritään parantamaan poliisin valmiuksia kyberrikollisuuden torjunnassa.

18	Poliisiammattikorkeakoulu kehittää koulutustarjontaansa kyberrikollisuuteen liittyvien aiheiden osalta.
45	Laaditaan selvitys poliisin oikeudellisista toimivaltuuksista ennaltaehkäistä, paljastaa ja selvittää kyberrikoksia.
46	Varmistetaan, että keskusrikospoliisin kansallisella 24/7-yhteyspisteellä on kyberrikollisuuteen liittyvät valmiudet, jotta se pystyy vastaamaan kansallisiin ja kansainvälisiin tarpeisiin.
47	Varmistetaan Suomen kyberrikostilannekuvan laatiminen sekä internetiin liittyvän tiedustelutiedon hankkimisen ja hallinnoinnin parantaminen.
48	Kyberrikollisuuden torjunnan järjestäminen ja resurssointi.

Edellä mainittujen toimenpiteiden osalta on jo ryhdytty useisiin toimiin.

18	Poliisiammattikorkeakoulu rekrytoi toukokuussa 2015 henkilön kehittämään kyberrikollisuuteen liittyvää koulutustarjontaa. Tuloksista lisätietoja jäljempänä.
45	On laadittu selvitys poliisin toimivaltuuksista ennaltaehkäistä, paljastaa ja selvittää kyberrikoksia ja siitä on julkaistu raportti.
46	Keskusrikospoliisin kansallisen 24/7-yhteyspisteen resursseihin on lisätty kyberalan päivystäviä virkamiehiä.
47	On laadittu selvitys poliisin lähestymistavasta Suomen kyberrikosilmiön tilannekuvaan. Se sisältää ehdotuksia tavoista luoda kattava tilannekuva yhteistyössä valtionhallinnon toimijoiden ja yksityissektorin kanssa. Internetiin liittyvää tiedustelutiedon hankkimista ja hallinnointia on tehostettu.
48	Poliisihallitus vahvisti kyberrikosten torjuntaa koskevat ohjeet. Keskusrikospoliisiin perustettiin kyberkeskus 15.4.2015.

Vuonna 2015 otettiin käyttöön poliisin uusi strategia. Yksi strategian päämääristä on resurssien suuntaaminen tietoverkkorikostorjuntaan ja kyberosaamisen kehittäminen. Toimenpiteet päämäärän saavuttamiseksi:

- Lisätään osaamista kyberrikollisuuden torjunnasta.
- Kohdistetaan enemmän resursseja kyberrikostorjuntaan mutta myös poliisin omien järjestelmien kyberturvallisuuden varmistamiseen.
- Selvitetään, miten eri tietoverkoissa tapahtuvan tiedonhankinnan toimivaltuuksia olisi lisättävä.

Kyberrikollisuuden torjumiseksi vakavan rikollisuuden toimintaedellytyksiä olisi heikennettävä kiinnittäen erityistä huomiota kansainvälisiin painopisteisiin. Toimenpiteet päämäärän saavuttamiseksi:

- Seurataan sekä rikosilmiöiden kehittymistä että kansainväliselle kyberrikostorjunnalle asetettuja tavoitteita osana EU-ohjausjaksoa ja hyödynnetään ne etukäteisesti ja tarkoituksenmukaisesti kansallisessa toiminnassa.
- Torjutaan Suomeen suuntautuvaa kansainvälistä kyberrikollisuutta tavoitteena kyberrikosten paljastaminen ja estäminen ennalta sekä rikosvastuun toteutuminen jo lähtömaassa.

Suomen kyberturvallisuusstrategian ansiosta, mutta myös lainvalvontaviranomaisten operatiivisten tarpeiden vuoksi kyberkysymykset on tunnustettu kaikilla poliisitoiminnan tasoilla. Poliisin strategiassa todetaan, että ennaltaehkäisy on äärimmäisen tärkeää vakavan rikollisuuden kohdalla.

Keskusrikospoliisin uusi kyberrikostorjunnan keskus aloitti toimintansa 1. huhtikuuta 2015. Keskuksen pyrkimyksenä on parantaa poliisin valmiuksia torjua ja tutkia vakavia rikoksia. Kyberrikollisuuden torjumisen lisäksi uusi keskus osallistuu tiedustelutiedon hankintaan internetistä ja uhka-arvioiden laatimiseen.

Suomen kyberturvallisuusstrategiassa asetettujen tavoitteiden saavuttamiseksi poliisihallitus perusti 25. maaliskuuta 2015 työryhmän laatimaan poliisille kattavan kyberstrategian; toimeksianto päättyi vuoden 2016 lopulla. Työryhmä kokoaa yhteen kyberrikollisuuden ja kyberturvakysymysten asiantuntijoita poliisivoimien eri yksiköistä.

Tämän lisäksi poliisihallitus on antanut kirjallisia määräyksiä ja ohjeita poliisin tietojärjestelmien käytöstä ja ylläpidosta, tietoturvasta, tietoturvahäiriöiden hallinnoinnista ja luottamuksellisen tiedon käsittelystä. Näitä ohjeita ei ole käännetty englanniksi.

Poliisihallitus toteuttaa kattavaa kyberrikosten torjuntaohjelmaa läheisessä yhteistyössä paikallisten poliisiyksiköiden, keskusrikospoliisin ja sisäministeriön kanssa. Ohjelma sisältää useita toteutettavia toimia tavoitteiden saavuttamiseksi.

Poliisi osallistuu myös Nordic Computer Forensic Investigators -koulutuksiin, mitkä sisältävät tietokoneforensiikan kursseja. Poliisi on käynnistänyt erityisen laatuohjelman, jolla pyritään parantamaan sähköisen todistusaineiston analysointia oikeusvarmalla tavalla. Kyberrikostutkintaan osallistuvien viranomaisten, syyttäjien ja tuomareiden osaamista on myös parannettu järjestämällä asiaankuuluvaa koulutusta.

Suomessa tarkistetaan parhaillaan tiedon keräämiseen ja käsittelyyn liittyvää lainsäädäntöä, jotta varmistetaan riittävät resurssit ja toimivaltuudet kyberrikosten ennaltaehkäisemiseksi, paljastamiseksi ja selvittämiseksi.

Suomen kansalliset painopisteet vastaavat EU:n kyberrikollisuuden alan painopisteitä. Suomi osallistuu toimijana Euroopan monialaisen rikosuhkien torjuntafoorumin (EMPACT) kyberrikoksia käsittelevän osioin kaikkiin kolmeen painopistealueeseen (kyberiskut, maksukorttipetokset ja lasten seksuaalinen hyväksikäyttö).

Suomi on osallistunut aktiivisesti kyberrikollisuudesta käytävään keskusteluun sekä Euroopan neuvostossa että EUssa. Oikeusministeriö on myös perustanut horisontaalisen työryhmän, joka käsittelee rikosasioissa tehtävän kansainvälisen yhteistyön käytännön kysymyksiä. Työryhmään osallistuu oikeus- ja sisäministeriöiden edustajien lisäksi syyttäjien ja lainvalvontaviranomaisten sekä tuomareiden ja Rikosseuraamusviraston edustajia. Työryhmä on vuosien kuluessa osoittautunut hyödylliseksi foorumiksi vaihtaa näkemyksiä ja käytäntöjä ja tiedottaa lainsäätäjille ja alan toimijoille uudesta lainsäädännöstä ja muusta kehityksestä tällä alalla.

3.3. Kyberrikollisuutta koskevat tilastot

3.3.1. Kyberrikollisuuden alan tärkeimmät kehityssuuntaukset

Suomen viranomaiset ovat ilmoittaneet, että verkkopankkipetosten (haittaohjelmien avulla tehtävät petokset sähköisissä pankkipalveluissa) määrä on laskenut ja viimeisten kahden vuoden aikana esiin on tullut joitakin irrallisia tapauksia tapausta. Verkossa tapahtuvien maksukorttipetosten määrän on taas todettu kasvaneen merkittävästi viime vuodesta lähtien (vuoden 2016 ensimmäisellä vuosineljänneksellä 174,6 prosentin kasvu vuoden 2015 vastaavaan neljännekseen).

Verkkourkintakampanjoita esiintyy jatkuvasti ja ne ovat lisäksi entistä huolellisemmin suunniteltuja ja toteutettuja. Käyttäjän manipulointi eri tavoin on nykyään yleisempää kuin muutamia vuosia sitten. Viime aikoina on uutena ilmiönä todettu useita CEO fraud -tapauksia (tekeytyminen yrityksen johtohenkilöksi).

Haittaohjelmista, erityisesti kiristysohjelmista, on tullut aikaisempaa vakavampi ongelma, kun tarkastellaan niiden kykyä aiheuttaa vahinkoa.

3.3.2. Rekisteröityjen kyberrikollisuustapausten määrä

Suomen tilastokeskus toimitti vuoden 2013 ja 2014 tilastot. Datavahingontekoa (rikoslain 35 luvun 3 a, 3 b ja 3 c §) ja identiteettivarkauksia (rikoslain 38 luvun 9 a §) koskevat määräykset tulivat voimaan 4. syyskuuta 2015 ja näin ollen näiden määräysten kattamia rikoksia ei ole tässä käsitelty. Monet tässä yhteydessä relevantit rikokset eivät ole ainoastaan kyberrikoksia, vaan voivat olla myös muita rikoksia (esimerkiksi väärennös- tai petosrikoksia). Näitä rikoksia koskevilla tilastotiedoilla ei ole merkitystä tässä yhteydessä. Seuraavat luvut koskevat käräjäoikeuksissa annettuja tuomioita:

	2013	2014
Vaaran aiheuttaminen tietojenkäsittelylle (34:9 a)	2	3
Viestintäsalaisuuden loukkaus (38:3)	6	9
Törkeä viestintäsalaisuuden loukkaus (38:4)	1	2
Tietoliikenteen häirintä (38:5)	6	10
Törkeä tietoliikenteen häirintä (38:6)	1	4
Lievä tietoliikenteen häirintä (38:7)	-	-
Tietojärjestelmän häirintä (38:7 a)	1	1
Törkeä tietojärjestelmän häirintä (38:7 b)	-	-
Tietomurto (38:8)	2	4
Törkeä tietomurto (38:8 a)	1	-
Suojauksen purkujärjestelmärikos (38:8 b)	-	-

3.4. Kyberrikollisuuden ehkäisemiseen ja torjumiseen osoitetut kansalliset määrärahat ja EU-rahoitteinen tuki

Näitä rikollisuuden aloja varten ei ole erityisesti osoitettu määrärahoja. Poliisihallituksella on kuitenkin erillinen budjetti (420 000 euroa vuonna 2016) poliisiyksiköiden tukemiseksi tietokoneforensiikan alan koulutusta ja laitteiston hankkimista varten. Poliisiyksiköt vastaavat pääasiassa itse omista operaatioistaan, koulutuksestaan ja laitteiston hankkimisesta.

Kyberkeskuksen organisatorisesta rakenteesta johtuen keskusrikospoliisilla ei ole keskukselle erityistä operatiivista budjettia. Operatiivinen budjetti on osoitettu niille kolmelle keskusrikospoliisin osastolle, joilla kyberkeskuksen henkilöstö työskentelee.

Kyberkeskus on matriisiorganisaatio. Vaikka kyberrikollisuuden torjuntaan ei ole osoitettu erillisiä määrärahoja, keskusrikospoliisin osaston hyödyntävät aktiivisesti resurssejaan tällä alalla.

Kyberrikollisuuden torjuminen ja poliisin tietotaidon varmistaminen kyberrikostutkinnan ja kyberforensiikan aloilla on sisällytetty sisäisen turvallisuuden rahaston kansalliseen ohjelmaan ja sen täytäntöönpanosuunnitelmaan. Keskusrikospoliisin kyberkeskus on hakenut (poliisihallituksen kautta) ja sille on myönnetty varoja EU:n sisäisen turvallisuuden rahastosta keskuksen perustamista ja teknisten valmiuksien kehittämistä varten (1 288 913 euroa vuosina 2015 - 2016).

3.5. Päätelmät

- Suomella on ollut kyberturvallisuusstrategia vuodesta 2013 lähtien. Siinä kuvataan Suomen kyberturvallisuuden visio, toimintamalli ja strategiset linjaukset. Siinä mainitaan tietyt julkishallinnon yksiköt ja kuvataan niiden tehtävät. Lisäksi siinä painotetaan ennakoivan toiminnan merkitystä, jolla pyritään parantamaan yhteiskunnan tietoisuutta virtuaalimaailman uhkista.

- Suomen kyberturvallisuusstrategian on tarkoitus kattaa kaikki kyberturvallisuuden näkökohdat. Siinä keskitytään kuitenkin pääasiassa poliisin rooliin, eikä oikeuslaitoksen rooliin. Tästä johtuu osittain se, että pääpaino on kyberrikollisuuden torjumisella ja kyberrikoksista seuraavaa rikosoikeudellista vastuuta tuskin mainitaan. Arviointiryhmä katsoo, että tätä valintaa olisi harkittava uudelleen.

- Strategiaa varten on laadittu myös toimeenpano-ohjelma. Toimeenpano-ohjelmaa tarkastellaan säännöllisesti uudelleen, mutta itse strategiaa ei. Arviointiryhmä katsoo, että kyberturvallisuusstrategiaa olisi tarkasteltava uudelleen, jotta se vastaisi tämänhetkisiä tarpeita, mukaan lukien muun muassa oikeuslaitoksen tarpeet.

- Suomessa on yksi keskitetty tietokanta poliisiraporteille. Tietokannassa noudatetaan omanlaistaan luokittelua. Tallettaessaan raportteja järjestelmään monet poliisit eivät kuitenkaan käytä järjestelmää oikein ja luokitteluun tulee virheitä. Arviointiryhmä katsoo, että tilastojen keräämiseen sovellettavaa laadunvalvontaa olisi parannettava.

- Lisäksi CERT-tilastoja, Viestintäviraston välittämien tapausten lukumäärää tai poliisin taikka oikeuslaitoksen luotettavia tilastoja ei ole saatavilla. Tilastotietojen avulla esitetty kokonaiskuva määrittelee kyberrikollisuuden ongelman laajuuden Suomessa. Ongelman laajuutta on vaikea määritellä ilman täydellisiä tietoja / tilastoja. Tämä päätelmä vastaa suoraan Suomen kyberturvallisuusstrategiassa esitettyjä yleisiä näkemyksiä. Näin ollen arviointiryhmä katsookin, että kyberrikokset ovat aliraportoituja, minkä vuoksi yleiskuvan saaminen ilmiön laajuudesta on vaikeaa.

- Paikan päälle tehdyn vierailun aikana kerätyn tiedon mukaan poliisi ei saanut minkäänlaista lisäbudjettia kyberturvallisuusstrategian julkistamisen jälkeen; strategiassa annetaan poliisille tehtäviä, mutta ei resursseja. Yleisvaikutelma on, että oikeuslaitokselta ja poliisilta puuttuu resursseja, jotka ne katsovat tarvitsevansa torjuakseen kyberrikollisuutta tehokkaasti. On laadittava tarveanalyysi sen varmistamiseksi, että resurssit ovat saatavilla. Käytännön toimijoiden (poliisi) tasolla tunnutaan ymmärtävän erittäin hyvin rajoitteet ja mahdolliset ratkaisut, jotka liittyvät kyberrikollisuuden käsittelyyn. Arviointiryhmä sai kuitenkin sen käsityksen, että käytännön toimijoiden mielestä aiheen "arvostus" ei ole sama strategisella tasolla.

- Arviointiryhmä oli tyytyväinen poliisihallituksen hallinnoimaan erilliseen budjettiin, joka on omistettu poliisiyksiköille tarjottavaan kyberrikollisuuden alan koulutukseen ja laitteistohankintoihin. Se toteaa, että poliisihallitus tunnustaa tämän rikosilmiön torjunnan merkityksen sekä kansallisella että alueellisella tasolla.

4. KANSALLISET RAKENTEET

4.1. Oikeuslaitos (syyttäjäviranomaiset ja tuomioistuimet)

4.1.1. Sisäinen rakenne

Yksikään syyttäjäviranomainen tai tuomioistuin ei käsittele ainoastaan kyberrikollisuutta. Paikallisten syyttäjäviranomaisten sisällä useimmat kyberrikostapaukset käsittelee tietty ryhmä syyttäjiä, mutta heillä on myös muita tehtäviä. Heille ei ole osoitettu erityisiä toimivaltuuksia.

Valtakunnansyyttäjä on nimennyt neljä syyttäjää, jotka erikoistuvat kyberrikollisuuteen liittyviin ongelmiin. Nämä eivät kuitenkaan ole heidän ainoita tehtäviään. Heidän odotetaan tulevaisuudessa tarjoavan apua ja koulutusta muille syyttäjille. Valtakunnansyyttäjänvirasto on myös järjestänyt joitakin seminaareja aiheista kuten kybervaluutta, lasten hyväksikäyttöön liittyvä materiaali jne. Syyttäjille on myös tarjottu mahdollisuus osallistua poliisin järjestämille kursseille.

Suomessa rikosten esitutkinnasta vastaa poliisi. Tutkinta tapahtuu läheisessä yhteistyössä tapausta käsittelemään määrätyn syyttäjän kanssa aivan tutkinnan alusta saakka, koska kaikki päätökset vaikuttavat syyttäjän tuleviin mahdollisuuksiin esittää todisteita ja varmistaa onnistunut oikeuskäsittely.

4.1.2. Onnistuneeseen syytteeseenpanoon liittyvät valmiudet ja esteet

Suomen viranomaisten mainitsemat vaikeudet johtuvat siitä, että maassa ei ole virallisia syyttäjiä, jotka käsittelisivät ainoastaan kyberrikoksia. Valtakunnansyyttäjänvirastossa ei ole valtionsyyttäjää, joka vastaisi kyberrikoksista. Koska kyberrikollisuuden odotetaan lisääntyvän ja monimutkaisiin kyberrikostapauksiin yleensä liittyy kansainvälistä yhteistyötä ja epäselviä oikeuskysymyksiä, virallisten syyttäjien työmäärä on valtava. Näin ollen nykyiset syyttäjäresurssit eivät todennäköisesti ole riittävät käsittelemään kyberrikostapauksia tulevaisuudessa. Poliisin tasolla investoituja resursseja ei myöskään voida hyödyntää täysimääräisesti, jos resurssit eivät ole riittävät tapausten syytteenpanemiseksi.

Suomen viranomaiset totesivat, että kyberrikollisuuden määritteleminen on vaikeaa. Tämä voi johtaa ongelmiin, koska kyberrikoksiin erikoistuneet poliisit tai syyttäjät eivät suorita tutkintaa ja syytteeseenpanoa tapauksissa, joihin liittyy kyberrikollisuuden elementtejä. Esimerkiksi Tor-verkossa tapahtunutta huumeiden salakuljetusta käsittelisi normaalisti huumausainerikoksiin erikoistunut syyttäjä; Tor-verkossa tapahtunutta lapsipornografian levittämistä käsittelisi lapsiin kohdistuviin rikoksiin erikoistunut syyttäjä; verkossa olevan tekijänoikeussuojatun aineiston / liikesalaisuuksien luvatonta jakamista tai käyttöä käsittelisi talousrikoksiin erikoistunut syyttäjä; identiteettivarkautta tai lievää kyberpetosta käsittelisi nuorempi syyttäjä. Ongelmia voi syntyä siitä, että kaikki edellä mainitut tapaukset edellyttävät erityistietämystä kyberrikoksista. Onnistuneen syytteeseenpanon esteenä on siis se, että tapauksia eivät välttämättä käsittele sellaiset henkilöt, joilla on riittävät tiedot kyberrikollisuudesta.

Esteenä mainittiin myös käräjäoikeuden tuomareiden riittämättömät yleistiedot kyberrikoksista. Tämä on johtanut tuomioihin, joissa vaikuttaa siltä, että todistusaineistoa ei ole täysin ymmärretty. Jotkut tuomarit vaikuttavat myös haluttomilta käsittelemään kyberrikostapauksia, koska eivät tunne teknisiä aspekteja. Niin syyttäjien kuin tuomareidenkin erikoistuminen olisi suotavaa. Joitakin vaikeuksia aiheuttaa myös se, että tuomioistuimilta puuttuu käytännön kokemusta monista kyberrikoksista.

Lisäksi Suomen rikosprosessissa otettiin tammikuussa 2015 käyttöön syytetingintä, mutta vaikuttaa siltä, ettei sitä voida kovin hyvin soveltaa kyberrikollisuuteen. Tämä voi johtua siitä, että kun uhreja on tuhansia ja usein uhrien kotipaikka on ulkomailla, on mahdotonta saada kaikkien uhrien suostumusta.

Kyberrikosten onnistuneen tutkinnan suurin este ovat pitkäkestoiset menettelyt, etenkin jos todisteita on hankittavat keskinäisen oikeusavun kautta.

4.2. Lainvalvontaviranomaiset

Suomessa on yksi poliisiorganisaatio, joka toimii sisäministeriön alaisuudessa. Suojelupoliisi on sisäministeriön alainen valtakunnallinen poliisiyksikkö. Poliisihallitus suunnittelee, johtaa ja ohjaa poliisitoimintaa. Suomen 11 poliisilaitosta vastaavat yleisen järjestyksen ja turvallisuuden ylläpitämisestä ja rikosten ennalta ehkäisemisestä omilla alueillaan. Keskusrikospoliisi ja Poliisiammattikorkeakoulu ovat Suomen poliisin valtakunnalliset yksiköt, joita johtaa ja ohjaa Poliisihallitus.

Valtioneuvosto ohjaa poliisitoimintaa hallitusohjelmaan sisältyvien tavoitteiden ja valtioneuvoston periaatepäätösten avulla.

Poliisi on tulosohjattu organisaatio. Sisäministeriö vastaa ohjauksesta ja valvonnasta. Poliisin organisaatio on kaksiportainen: sisäministeriön alainen Poliisihallitus johtaa ja ohjaa operatiivista poliisitoimintaa sisäministeriön alaisuudessa toimivaa Suojelupoliisia lukuun ottamatta.

Poliisin keskeiset tehtävät, toiminnan yleiset periaatteet ja toimivaltuudet on säädetty laissa. Lakien ja valtioneuvoston asetusten lisäksi poliisiin sovelletaan sisäministeriön asetuksia, määräyksiä ja ohjeita. Suomen poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennaltaehkäiseminen ja selvittäminen. Poliisi toimittaa esitutkinnan ja tekee tiivistä yhteistyötä rajavartio- ja tulliviranomaisten kanssa, jotka ovat oman toiminta-alansa esitutkintaviranomaisia.

Kyberrikostutkintaan erikoistunut elin Kyberrikostorjuntakeskus perustettiin vuonna 2015, mutta kaikki poliisilaitokset ovat myös vastuussa kyberrikostutkinnasta. Keskus vastaa kansainvälisistä, järjestäytyneistä, teknisesti haastavista ja laajemmista kyberrikoksista. Poliisilaitokset ovat vastuussa kaikista niiden alueilla tapahtuneista tapauksista. Kyberkeskus (keskusrikospoliisi) ja poliisilaitokset pystyvät yleensä helposti sopimaan, mikä yksikkö hoitaa minkäkin tapauksen. Jos ne eivät pääse sopimukseen, asian päättää poliisihallitus.

Kaikilla poliisilaitoksilla on omat tietokoneforensiikan ryhmänsä. Kyberrikosten esitutkinnan organisoinnissa on suuria eroja poliisilaitosten välillä. Monilla poliisilaitoksilla ei ole erikoistuneita tutkijoita. Kyberkeskus myös tukee kaikkia poliisi yksiköitä kyberrikostutkinnassa, tietokoneforensiikan alan tutkimuksissa, internettiedusteluissa ja kansainvälisessä yhteistyössä.

Suojelupoliisi vastaa kyberrikoksista omalla toiminta-alueellaan, mutta niiden tutkinnasta vastaa poliisi.

Budapestin yleissopimuksen mukaisten sitoumusten osalta keskusrikospoliisin viestintäkeskus on kansainvälisten pyyntöjen 24/7-yhteyspiste. Suurin osa 24/7-toiminnoista on Suomessa keskitetty yhteen yksikköön. Viestintäkeskus sijaitsee samassa paikassa kuin Interpol Helsinki, Suomen Sirene-toimisto ja Europolin kansallinen yksikkö. Rikostiedustelu- ja internettiedusteluyksiköiden edustajat ovat myös paikalla viestintäkeskuksessa lähes kellon ympäri. Tämän lisäksi johtava poliisiviranomainen päivystää aina ja voi tarvittaessa hyödyntää kaikkia viestintäkeskuksen resursseja. Päivystäjällä on oikeudellinen toimivalta päättää esimerkiksi tietojen turvaamisesta, etsinnästä ja takavarikosta sekä pidätyksistä.

Poliisi totesi, että todisteiden hankkiminen hitaan keskinäisen oikeusapumenettelyn avulla on tärkein kyberrikostutkinnan este. Tietojen nopea takavarikoiminen on kriittisen tärkeä seikka rikostutkinnassa yleensä, mutta erityisesti kyberrikostutkinnassa. On hyvin yleistä, että keskinäisen oikeusapupyynnön toteutuminen kestää vähintään 2-3 kuukautta. Ei ole harvinaista, että toteutumisessa kestää vuoden ja joskus jopa pidempään. Ongelmasta tulee erittäin vaikea, jos keskinäisen oikeusavun kautta saadut tulokset antavat aiheen uuteen keskinäiseen oikeusapupyyntöön. Toinen este on se, että läheskään kaikilla mailla (edes Budapestin yleissopimuksen sopimuspuolilla) ei ole laillista mahdollisuutta toteuttaa tietojen turvaamismääräystä.

4.3. Muut viranomaiset / laitokset / julkisen ja yksityisen sektorin kumppanuus

Suomen viestintävirasto toimii liikenne- ja viestintäministeriön alaisuudessa. Viestintävirasto ylläpitää sähköisten viestintäverkkojen toimivuuden ja tietoturvan tilannekuvaa ja tiedottaa mahdollisista tietoturvauhkista. Tavoitteena on myös lisätä kansalaisten ja yritysten tietoturvaosaamista muun muassa ohjeistuksen avulla. Viestintävirasto varmistaa myös viestintäverkkojen ja -palveluiden yhteentoimivuuden.

Kansallinen kyberturvallisuuskeskus on viestintäviraston ulkoinen toimiala.
Kyberturvallisuuskeskuksen käsittelemät aiheet:

- teleyritysten varautuminen sekä viestintäverkkojen ja -palveluiden toimivuushäiriötilanteissa ja poikkeusoloissa
- yksityisyyden suoja sähköisessä viestinnässä
- sähköinen tunnistaminen ja allekirjoitukset
- viranomaisvaatimukset hätäliikenteessä, telekuuntelussa ja -valvonnassa
- kansallisen tietoturvallisuusviranomaisen (NCSA-FI) tehtävät
- fi-verkkotunnuksen hallinnointi.

Viestintäviraston CERT-FI ja NCSA-FI -toiminnot on yhdistetty osaksi kansallista kyberturvallisuuskeskusta.

Kyberturvallisuuskeskus on kansallinen tietoturvaviranomainen. Se kehittää ja valvoo viestintäverkkojen ja -palveluiden toimintavarmuutta ja turvallisuutta. Sen CERT-toimintoihin kuuluu tietoturvaloukkausten ennaltaehkäisy, havainnointi, ratkaisu sekä tietoturvauhkista tiedottaminen. Kyberturvallisuuskeskuksen NCSA-toiminto vastaa turvaluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä turvallisuusasioista.

NCSA-FI -toiminnon kansainvälisiin tietoturvavelvoitteisiin kuuluvat tehtävät:

- kansalliseen turvallisuustoimintaan liittyvä ohjeistus- ja sopimusvalmistelu;
- kansainvälisen turvaluokitellun tietoaineiston käsittelemiseen liittyvä ohjeistus;
- salausteknisen aineiston jakeluverkon hallinnointi, kirjanpito sekä ohjeistus aineiston turvalliseen käsittelyyn (CDA);
- salaustuotteiden hyväksyntä kansainvälisen turvaluokitellut tiedon suojaamiseksi Suomessa (CAA);
- kansainvälistä turvaluokiteltua tietoa käsittelevien tietojärjestelmien hyväksyntä (SAA) (Menettelyn piiriin kuuluvat valtionhallinnon järjestelmät niiltä osin, kun ne liittyvät kansainvälisten tietoturvallisuusvelvoitteiden täyttämiseen, sekä sellaiset kansainvälisiin tarjouskilpailuihin osallistuvien yritysten järjestelmät, joilta edellytetään kansallisen tietoturvaviranomaisen hyväksyntää.);
- Kansallisen TEMPEST-toiminnan koordinointi ja ohjeistus (NTA).

Keskuksen toiminta tähtää yleisten viestintäverkkojen ja viestintäpalveluiden turvallisen ja häiriöttömän toiminnan varmistamiseen sekä yhteiskunnan elintärkeiden toimintojen turvaamiseen. Huoltovarmuuskeskuksen kanssa solmitun sopimuksen mukaisesti Kyberturvallisuuskeskus vastaa osaltaan huoltovarmuuden kannalta elintärkeiden teknisten järjestelmien toimivuuden turvaamisesta. Kyberturvallisuuskeskus haluaa kehittää ja monipuolistaa tietoturvapalvelujaan muun muassa kehitystyön ja laajojen yhteistyöverkostojen avulla.

Lisäksi Viestintävirasto vastaa useista kansallisiin tietoturvavelvoitteisiin liittyvistä tehtävistä:

- teleyritysten tietoturvallisuuden hallinnan ohjaus- ja valvontatehtävät, muun muassa tietoturvallisuusmääräyksen (M47) valvonta;
- vahvan sähköisen tunnistamisen ja laatuvarmennetoiminnan ohjaus- ja valvontatehtävät, muun muassa viestintäviraston antamien määräysten M7 ja M8 valvonta sekä laatuvarmennetoiminnan vuotuiset auditoinnit;
- viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arviointi;
- tietoturvallisuuden arviointilaitoksien hyväksyminen;
- yhteistyö kansainvälisten ja kansallisten turvallisuustoimijoiden kanssa.

4.4. Yhteistyö ja koordinointi kansallisella tasolla

4.4.1. Lakisääteiset tai toimintapoliittiset velvoitteet

Keskusrikospoliisin uusi kyberrikoskeskus keskittyy poliisin valmiuksien parantamiseen ehkäistä ja tutkia vakavia rikoksia. Kyberrikollisuuden torjumisen, tutkinnan ja digitaalisen forensiikan lisäksi keskus osallistuu tiedustelutiedon hankintaan internetistä ja uhka-arvioiden laatimiseen. Kyberrikoskeskus tuottaa ja ylläpitää kyberturvallisuuden analysoitua tilannekuvaa ja välittää sen muille toimijoille osana Suomen yhdistettyä kyberturvallisuuden tilannekuvaa. Suomen suojelupoliisi ylläpitää oman toiminta-alansa tilannekuvaa.

Yksi poliisin strategiaan sisältyvistä toimenpiteistä on syventää yhteistyötä muiden turvallisuusviranomaisten kanssa sekä hyödyntää tietojohtoisuutta parantamalla poliisin analyysiosaamista ja -työkaluja. Kyberturvallisuusjärjestelyissä noudatetaan viranomaisten, yritysten ja organisaatioiden välistä säädösten ja sovittujen yhteistyömallien mukaista tehtävänjakoa.

Kaikkien rikosten, kyberrikokset mukaan lukien, tutkinta tapahtuu läheisessä yhteistyössä tutkintaviranomaisten ja sen syyttäjän välillä, jonka käsiteltäväksi tapaus on osoitettu. Tutkintaviranomaisten on ilmoitettava syyttäjäviranomaiselle kaikista rikoksista, joihin liittyy ulkomaalaisia yhteyksiä tai muita yhteistyöperusteita. Syyttäjällä on oikeus määrätä toteutettavia tutkintatoimenpiteitä. Syyttäjälle on myös annettava tiedoksi kaikki toisen valtion esittämät keskinäistä oikeusapua koskevat pyynnöt.

Poliisin tärkein yhteistyökumppani kyberrikosten ehkäisemis- ja torjuntatyössä on kansallisen kyberturvallisuuskeskus (NCSC-FI). Keskuksen CERT-toimintoihin kuuluu tietoturvaloukkausten ennaltaehkäisy, havainnointi, ratkaisu sekä tietoturvauhkista tiedottaminen. Kyberturvallisuuskeskus myös ylläpitää kansallista kyberturvallisuuden tilannekuvaa.

Kyberturvallisuuskeskuksen tehtävissä on monia päällekkäisiä alueita poliisin kanssa, mutta osapuolten roolit ovat selkeät. Lyhyt kuvaus näistä rooleista: poliisin tärkeimmät tehtävät ovat rikollisten paljastaminen ja kyberrikoksia koskeva esitutkinta ja kyberturvallisuuskeskuksen tärkeimmät tehtävät ovat tilannetietoisuus, ennaltaehkäisy sekä yritysten ja valtion virastojen, etenkin elintärkeiden infrastruktuurien tukeminen turvallisuushäiriöiden (ei ainoastaan rikosten) ratkaisemisessa. Kyberturvallisuuskeskus ja poliisi neuvottelevat parhaillaan yhteistyötä koskevasta yhteisymmärryspöytäkirjasta. Yhteistyötä pidetään avoimena ja sujuvana, etenkin operatiivisella tasolla. Tulevan yhteisymmärryspöytäkirjan avulla tullaan syventämään yhteistyötä muillakin aloilla (viestintä, tutkimus ja kehitys, osaamisen kehittäminen jne.).

4.4.2. Yhteistyön parantamiseen osoitetut resurssit

Keskusrikospoliisissa kaikki poliisit ovat yhdessä vastuussa tästä omilla aloillaan. Yhteistyön parantamista pidetään hyvin tärkeänä ja etenkin johtotason henkilöt ovat investoineet paljon vaivaa ja aikaa hyvien yhteistyösuhteiden luomiseen yksityisen sektorin toimijoiden kanssa.

Suomen viranomaisten mukaan tarvitaan lisää työkaluja erilaisten rikollisten toimintatapojen testaukseen, jotta voidaan tarvittaessa suorittaa niitä koskeva tutkinta ja jotta voidaan parantaa tietämystä tällä alalla. Rikolliset kehittävät menetelmiään nopeasti ja lainvalvontaviranomaiset ovat aina niitä jäljessä poliisiorganisaatioiden reaktiivisesta luonteesta johtuen. Suomen viranomaisten mukaan esimerkiksi NFC-lähimaksutekniikan heikkoudet tulevat todennäköisesti joutumaan rikollisten hampaisiin tulevaisuudessa.

4.5. Päätelmät

- Suomessa ei tällä hetkellä ole syyttäjäviranomaisia tai tuomioistuimia, jotka käsittelisivät ainoastaan kyberrikollisuutta.

- Valtakunnansyyttäjänvirastossa tehdään rakenneuudistus vuoden 2018 alussa. Erikoistuneet syyttäjät jaetaan kolmeen alueeseen: henkilöt (mukaan lukien lasten seksuaalinen hyväksikäyttö ja ihmiskauppa), talous (mukaan lukien veropetokset) ja turvallisuus (mukaan lukien terrorismi ja kyberrikokset). Syyttäjien lukumäärä on ollut jo vuosia laskussa. Pullonkaulojen välttämiseksi valtakunnansyyttäjän viraston resursseja on lisättävä samaan tahtiin kuin poliisin resursseja.

- Arviointiryhmä pani merkille suunnitelman parantaa syyttäjäviranomaisten tarjoamaa palvelua organisaation rakenneuudistuksella ja lisäämällä kyberrikostapauksia käsittelevien erikoistuneiden syyttäjien lukumäärää. Ottaen huomioon, että myös poliisi ilmoitti aikeistaan osoittaa lisäresursseja tämän ilmiön käsittelyyn sekä nykyisen työmäärän, arviointiryhmä pelkää, että suunniteltu lisäys ei edelleenkään riitä välttämään syyttäjäviranomaisen tasolla syntyvää pullonkaulaa.

- Ainoastaan erikoistuneiden syyttäjien määrän lisääminen ei kuitenkaan ratkaise Suomen viranomaisten mainitsemia kyberrikoksen määritelmään liittyviä ongelmia. Arviointiryhmä katsoo, että asia voidaan ratkaista kaksiosaisella lähestymistavalla: (1) lisäämällä yleistä osaamistasoa kautta linjan myös niiden syyttäjien keskuudessa, jotka käsittelevät perinteisiä tapauksia, joihin liittyy kyberrikollisuuden elementtejä ja (2) ottamalla käyttöön järjestelmä, jonka ansiosta tällaisia tapauksia käsittelevät syyttäjät voivat pyytää erikoistuneiden kyberrikossyyttäjien apua.

- Suomen keskusrikospoliisi vaikuttaa olevan hyvin valmistautunut kyberrikollisuuden torjuntaan, mutta on selvää, että tietoa ja osaamista on parannettava alue- ja paikallistasolla. Vaikuttaa siltä, että vain kaikkiaan yhdestätoista poliisilaitoksesta vain neljän tutkijoilla on "riittävät" tiedot kyberrikollisuudesta. Muissa poliisilaitoksissa tietokoneforensiikan alan henkilöstö voi olla hyvin perillä teknisistä kysymyksistä, mutta tutkijat eivät ole. Näin ollen arviointiryhmä katsoo, että tutkijoille olisi kautta maan tarjottava koulutusta kyberrikollisuuteen liittyvistä yleisistä kysymyksistä.

- Kyberrikostorjunnan rakenteet ovat kehittyneet. Kaikissa poliisilaitoksissa on tietokoneforensiikkaan erikoistunut yksikkö. On kuitenkin hankittava asianmukaiset laitteet ja tarjottava erikoistunutta koulutusta rikosteknisen tutkinnan alalla, erityisesti lapsipornografian ja maksukorttipetosten alalla.

- Keskusrikospoliisin kyberkeskuksen tapa olla ottamatta hoitaakseen kokonaisia tapauksia, vaan paikallisten poliisiviranomaisten avustaminen ongelman ratkaisemiseksi on maininnan arvoista. Näin toimivaltaisille paikallisille rikostutkijoille tarjotaan oppimiskokemus.

- Samaa tavoitetta tuetaan myös poliisihallituksen määrärahoilla, jotka on erikseen osoitettu kyberrikollisuuden alan koulutukseen ja laitteisiin: Arviointiryhmä panee tämän myönteisesti merkille.

- Kyberrikostorjunnasta ja kyberturvallisuudesta vastaavat sekä lainvalvontaviranomaiset että tietotekniikka-ala. Vaikka yhteistyön laajuudesta ja luonteesta ei olekaan paljon virallisia asiakirjoja, vaikuttaa siltä, että toiminta on ammattimaista.

- Olisi kuitenkin suotavaa valmistella tiettyjä standardeja uhkien laajuutta ja luonnetta koskevan tiedon keräämistä ja jakamista varten. Tällaisen tiedon perusteella voitaisiin esimerkiksi perustaa ehkäiseviä ohjelmia tai yhteiskunnallisia kampanjoita internetin käyttäjien tietoisuuden parantamiseksi kyber- ja muita uhkia koskevista perustavanlaatuisista turvallisuussäännöistä.

- Viestintäviraston ja poliisin väliset yhteydet vaikuttavat säännöllisiltä ja epämuodollisilta. Niiden välisen yhteisymmärryspöytäkirjan tekeminen ja allekirjoittaminen olisi nähtävä ensimmäisenä askeleena kohti näiden kahden erittäin tärkeän sidosryhmän yhteistyön vahvistamista edelleen.

5. OIKEUDELLISET NÄKÖKOHDAT

5.1. Kyberrikoksiin liittyvä aineellinen rikosoikeus

5.1.1. Tietoverkkorikollisuutta koskeva Euroopan neuvoston yleissopimus

Suomi on ollut tietoverkkorikollisuutta koskevan Budapestin yleissopimuksen sopimuspuoli vuodesta 2007.

5.1.2. Kansallisen lainsäädännön kuvaus

A/ Neuvoston puitepäätös 2005/222/YOS tietojärjestelmiin kohdistuvista hyökkäyksistä ja direktiivi 2013/40/EU tietojärjestelmiin kohdistuvista hyökkäyksistä

Neuvoston puitepäätös 2005/222/YOS tietojärjestelmiin kohdistuvista hyökkäyksistä on saatettu osaksi Suomen lainsäädäntöä. Suomi on saattanut myös tietojärjestelmiin kohdistuvista hyökkäyksistä annetun direktiivin 2013/40/EU osaksi kansallista lainsäädäntöä. Tässä yhteydessä rikoslakia ja erityisesti tieto- ja viestintärikoksia koskevaa 38 lukua muutettiin (laki 368/2015). Muutokset tulivat voimaan 4. syyskuuta 2015.

Suomella on siis kattava kyberrikoksia koskeva säännöstö[7]. Seuraavat teot on kriminalisoitu: tietomurto ja törkeä tietomurto (38 luvun 8 - 8 a §); törkeä tietoliikenteen häirintä, lievä tietoliikenteen häirintä, tietojärjestelmän häirintä ja törkeä tietojärjestelmän häirintä (38 luvun 5 - 7 b §); datavahingonteko, törkeä datavahingonteko ja lievä datavahingonteko (35 luvun 3 a - 3 c §); viestintäsalaisuuden loukkaus ja törkeä viestintäsalaisuuden loukkaus (38 luvun 3 ja 4 §); vaaran aiheuttaminen tietojenkäsittelylle ja suojauksen purkujärjestelmärikos (34 luvun 9 a § ja 38 luvun 8 b §).

[7] Suuren sivumäärän vuoksi raportissa ei esitetä yksityiskohtaista kuvausta. Lisätietoja on liitteessä D.

Rikoslaissa eritellään lieventämis- ja koventamisperusteet. Suomen lainsäädännön nojalla sekä tekijät että avunantajat voidaan asettaa rikosoikeudelliseen vastuuseen. Oikeushenkilöt voidaan asettaa rikosoikeudelliseen vastuuseen rikoksista, jotka on tehty oikeushenkilön toiminnan yhteydessä, sen edun mukaisesti tai sen puolesta. Rikoslain 9 luku sisältää määräyksiä oikeushenkilön rangaistusvastuusta. Sen 1 §:n mukaan yhteisö, säätiö tai muu oikeushenkilö, jonka toiminnassa on tehty rikos, on syyttäjän vaatimuksesta tuomittava rikoksen johdosta yhteisösakkoon, jos se on tässä laissa säädetty rikoksen seuraamukseksi. Rikoslain 9 luvun 5 §:n mukaan yhteisösakko tuomitaan määräeuroin. Alin yhteisösakon rahamäärä on 850 ja ylin 850 000 euroa.

B/ Direktiivi 2011/93/EU lasten seksuaalisen hyväksikäytön ja seksuaalisen riiston sekä lapsipornografian torjumisesta

Suomen viranomaiset ilmoittivat, että lasten seksuaalisen hyväksikäytön ja seksuaalisen riiston sekä lapsipornografian torjumisesta annetun direktiivin 2011/93/EU täytäntöönpano ei ole edellyttänyt lainsäädäntötoimia, koska asiaankuuluva lainsäädäntö on jo direktiivin mukaista. Rikoslakia (laki 540/2011) ja tiettyjä muita lakeja muutettiin jo 1. kesäkuuta 2011 lasten suojelemisesta seksuaalista riistoa ja seksuaalista hyväksikäyttöä vastaan annetusta Euroopan neuvoston yleissopimuksesta johtuvien velvoitteiden suhteen. Suomi on ollut tämän yleissopimuksen sopimuspuoli vuodesta 2011.

Lapsipornografiaan liittyvät kyberrikokset

Näitä rikoksia ovat *sukupuolisiveellisyyttä loukkaavan kuvan levittäminen, törkeä sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan levittäminen* ja *sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan hallussapito* (rikoslain 17 luvun 18, 18 a ja 19 §). Nämä säännökset ovat luonteeltaan yleisiä ja kattavat kaikki näiden rikosten tekotavat.

Lasten houkuttelemiseen liittyvät kyberrikokset

Kyseinen rikos on *lapsen houkutteleminen seksuaalisiin tarkoituksiin* (rikoslain 20 luvun 8 b §). Säännökset ovat luonteeltaan yleisiä ja kattavat kaikki näiden rikosten tekotavat.

C/ Korttipetokset verkossa

Verkossa toteutetut vilpilliset rahoitustoimet ovat Suomen lain vastaisia. Kyberpetokset ja kybervääreennykset on rikoslaissa määrätty rangaistaviksi.

Kyberpetokset

Näitä rikoksia ovat *petos, törkeä petos, lievä petos, maksuvälinepetos, törkeä maksuvälinepetos* ja *lievä maksuvälinepetos* (rikoslain 36 luvun 1 - 3 § ja rikoslain 37 luvun 8 - 10 §).

Kybervääreennykset

Näitä rikoksia ovat *väärennys, törkeä väärennys* ja *lievä väärennys* (rikoslain 33 luvun 1 - 3 §). Nämä säännökset ovat luonteeltaan yleisiä ja kattavat kaikki näiden rikosten tekotavat[8].

[8] Näiden rikosten kuvaukset ovat liitteessä D.

D/ Muut kyberrikollisuuden ilmiöt

Identiteettivarkaus on kriminalisoitu rikoslaissa (38 luvun 9 a §).

38 luku, 9 a § - Identiteettivarkaus
Joka erehdyttääkseen kolmatta osapuolta oikeudettomasti käyttää toisen henkilötietoja, tunnistamistietoja tai muuta vastaavaa yksilöivää tietoa ja siten aiheuttaa taloudellista vahinkoa tai vähäistä suurempaa haittaa sille, jota tieto koskee, on tuomittava *identiteettivarkaudesta* sakkoon.

Vaikka Suomen viranomaiset painottivat, että ei ole täysin selvää, mitä roskapostilla tarkoitetaan, roskasähköpostien ja ei-toivottujen massasähköpostien katsotaan kuuluvan tämän käsitteen piiriin. Roskapostiin liittyvät teot vastaavat rikoksia, joihin viitataan käsitteellä 'viestintärauhan rikkominen' (rikoslain 24 luvun 1 a §).

24 luku, 1 a § – Viestintärauhan rikkominen
Joka häirintätarkoituksessa toistuvasti lähettää viestejä tai soittaa toiselle siten, että teko on omiaan aiheuttamaan tälle huomattavaa häiriötä tai haittaa, on tuomittava *viestintärauhan rikkomisesta* sakkoon tai vankeuteen enintään kuudeksi kuukaudeksi.

5.2. Menettelykysymykset

5.2.1. Tutkintatekniikat

- **tietojärjestelmän / datan etsintä ja takavarikointi**

Laitteessa olevaa tietosisältöä koskevat säännökset on esitetty pakkokeinolain 8 luvun 20 - 29 §:ssä. Tällaisen etsinnän määritelmät ja edellytykset ovat 20 ja 21 §:ssä:

8 luku, 20 § - Laite-etsinnän määritelmä

(1) *Laite-etsinnällä* tarkoitetaan tietokoneessa, telepäätelaitteessa tai muussa vastaavassa teknisessä laitteessa tai tietojärjestelmässä etsinnän toimittamishetkellä olevaa tietosisältöön kohdistettavaa etsintää.

(2) Laite-etsintää ei saa kohdistaa sellaiseen luottamukselliseen viestiin, jota koskevasta telekuuntelusta, televalvonnasta ja teknisestä tarkkailusta säädetään 10 luvussa.

8 luku, 21 § - Laite-etsinnän edellytykset

(1) Laite-etsintä saadaan toimittaa, jos:

(1) on syytä epäillä, että on tehty rikos, josta säädetty ankarin rangaistus on vähintään kuusi kuukautta vankeutta, tai selvitettävänä ovat yhteisösakon tuomitsemiseen liittyvät seikat; ja

(2) etsinnässä voidaan olettaa löytyvän tukittavana olevaan rikokseen liittyvä 7 luvun 1 §:n 1 tai 2 momentissa tarkoitettu takavarikoitava asiakirja tai tieto taikka 7 luvun 2 §:n nojalla jäljennettävä asiakirja.

(2) Laite-etsintä voidaan toimittaa myös laitteen palauttamiseksi siihen oikeutetulle, jos on syytä olettaa, että se on rikoksella joltakulta viety.

(3) Päätös paikkaan kohdistuvan etsinnän toimittamisesta saadaan ulottaa koskemaan myös etsinnän toimittamispaikassa olevaa teknistä laitetta tai tietojärjestelmää, jos kyseessä ei ole paikkaan kohdistuva etsintä henkilön löytämiseksi.

Laite-etsintä ei ole salainen pakkokeino. Todisteiden hankkiminen kohteelta salassa on kuitenkin mahdollista pakkokeinolain 10 luvun 23 §:n nojalla:

10 luku, 23 § - Tekninen laitetarkkailu ja sen edellytykset

(1) *Teknisellä laitetarkkailulla* tarkoitetaan tietokoneen tai muun vastaavan teknisen laitteen taikka sen ohjelmiston toiminnan, sisältämien tietojen tai yksilöintitietojen muuta kuin yksinomaan aistinvaraista tarkkailua, tallentamista tai muuta käsittelyä rikoksen selvittämiselle merkityksellisen seikan tutkimiseksi.

(2) Teknisellä laitetarkkailulla ei saa hankkia tietoa viestin sisällöstä eikä 6 §:n 1 momentissa tarkoitetuista tunnistamistiedoista.

(3) Esitutkintaviranomainen saa kohdistaa teknistä laitetarkkailua rikoksesta epäillyn todennäköisesti käyttämään 1 momentissa tarkoitettuun tietokoneeseen tai muuhun vastaavan tekniseen laitteeseen taikka sen ohjelmistoon, kun tätä on syytä epäillä 16 §:n 3 momentissa tarkoitetusta rikoksesta.

16 §:n 3 momentti kattaa rikokset, joista säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta, sekä tietyt lievemmät rikokset.

Pakkokeinolain 7 luvussa säädetään takavarikoimisesta. Kun takavarikoinnin kohde on asiakirja (joka voi olla myös datan muodossa), päärikos on kopioiminen.

7 luku, 1 § - Takavarikoimisen edellytykset

(1) Esine, omaisuus tai asiakirja voidaan takavarikoida, jos on syytä olettaa, että:

(1) sitä voidaan käyttää todisteena rikosasiassa;

(2) se on rikoksella joltakulta viety; tai

(3) se tuomitaan menetetyksi.

(2) Mitä 1 momentissa säädetään, koskee myös tietoa, joka on teknisessä laitteessa tai muussa vastaavassa tietojärjestelmässä taikka sen tallennusalustalla (*data*). Tässä luvussa asiakirjasta säädettyä sovelletaan myös datan muodossa olevaa asiakirjaan.

7 luku, 2 § - Asiakirjan jäljentäminen

(1) Asiakirjan takavarikoiminen 1 §:n 1 momentin 1 kohdan mukaisesti todisteena käytettäväksi on korvattava sen jäljentämisellä, jos jäljennös on riittävä todistelun luotettavuuden kannalta.

(2) Asiakirja on jäljennettävä ilman aiheetonta viivytystä sen haltuunottamisen jälkeen. Jäljentämisen jälkeen asiakirja on viipymättä palautettava sille, jolta se on otettu haltuun.

(3) Jos asiakirjaa ei voida viivytyksettä jäljentää asiakirjan tai asiakirja-aineiston laadun tai laajuuden vuoksi, asiakirja on takavarikoitava.

- **liikennetietojen / viestin sisällön reaaliaikainen sieppaus/kerääminen**

Telekuuntelun ja televalvonnan määritelmät ja edellytykset on esitetty pakkokeinolain 10 luvun 3 ja 6 §:ssä:

10 luku, 3 § - Telekuuntelu ja sen edellytykset

(1) *Telekuuntelulla* tarkoitetaan viestintämarkkinalaissa tarkoitetun yleisen viestintäverkon tai siihen liitetyn viestintäverkon kautta teleosoitteeseen tai telepäätelaitteeseen vastaanotettavan taikka siitä lähetetyn viestin kuuntelua, tallentamista ja muuta käsittelyä viestin sisällön ja siihen liittyvien 6 §:ssä tarkoitettujen tunnistamistietojen selvittämiseksi. Telekuuntelua saadaan kohdistaa vain rikoksesta epäillyltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin.

(2) Esitutkintaviranomaiselle voidaan antaa lupa kohdistaa telekuuntelua rikoksesta epäillyn hallussa olevaan tai hänen oletettavasti muuten käyttämäänsä teleosoitteeseen tai telepäätelaitteeseen, jos epäiltyä on syytä epäillä:

(1) joukkotuhonnasta, joukkotuhonnan valmistelusta, rikoksesta ihmisyyttä vastaan, törkeästä rikoksesta ihmisyyttä vastaan, sotarikoksesta, törkeästä sotarikoksesta, kidutuksesta, kemiallisen aseen kiellon rikkomisesta, biologisen aseen kiellon rikkomisesta, jalkaväkimiinakiellon rikkomisesta;

(2) Suomen itsemääräämisoikeuden vaarantamisesta, sotaan yllyttämisestä, maanpetoksesta, törkeästä maanpetoksesta, vakoilusta, törkeästä vakoilusta, turvallisuussalaisuuden paljastamisesta, luvattomasta tiedustelutoiminnasta;

(3) valtiopetoksesta, törkeästä valtiopetoksesta, valtiopetoksen valmistelusta;

(4) törkeästä sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan levittämisestä;

(5) lapsen seksuaalisesta hyväksikäytöstä, törkeästä lapsen seksuaalisesta hyväksikäytöstä;

(6) taposta, murhasta, surmasta, rikoslain 21 luvun 6 a §:ssä tarkoitetusta kyseisen luvun 1, 2 tai 3 §:n mukaisesta törkeän henkeen tai terveyteen kohdistuvan rikoksen valmistelusta;

(7) törkeästä laittoman maahantulon järjestämisestä, törkeästä vapaudenriistosta, ihmiskaupasta, törkeästä ihmiskaupasta, panttivangin ottamisesta, panttivangin ottamisen valmistelusta;

(8) törkeästä ryöstöstä, törkeän ryöstön valmistelusta, törkeästä kiristyksestä;

(9) törkeästä kätkemisrikoksesta, ammattimaisesta kätkemisrikoksesta, törkeästä rahanpesusta;

(10) tuhotyöstä, liikennetuhotyöstä, törkeästä tuhotyöstä, törkeästä terveyden vaarantamisesta, ydinräjähderikoksesta, kaappauksesta;

(11) rikoslain 34 a luvun 1 §:n 1 momentin 2–7 kohdassa tai 2 momentissa tarkoitetusta terroristisessa tarkoituksessa tehdystä rikoksesta, terroristisessa tarkoituksessa tehtävän rikoksen valmistelusta, terroristiryhmän johtamisesta, terroristiryhmän toiminnan edistämisestä, koulutuksen antamisesta terrorismirikoksen tekemistä varten, värväyksestä terrorismirikoksen tekemiseen, terrorismin rahoittamisesta;

(12) törkeästä vahingonteosta tai törkeästä datavahingonteosta;

(13) törkeästä petoksesta, törkeästä kiskonnasta;

(14) törkeästä rahanväärennyksestä;

(15) törkeästä ympäristön turmelemisesta; tai

(16) törkeästä huumausainerikoksesta.

(3) Lupa telekuunteluun voidaan antaa myös, kun jotakuta on syytä epäillä liike- tai ammattitoimintaan liittyvästä:

(1) törkeästä lahjuksen antamisesta;

(2) törkeästä kavalluksesta;

(3) törkeästä veropetoksesta, törkeästä avustuspetoksesta;

(4) törkeästä väärennyksestä;

(5) törkeästä velallisen epärehellisyydestä, törkeästä velallisen petoksesta;

(6) törkeästä lahjuksen ottamisesta, törkeästä virka-aseman väärinkäyttämisestä;

(7) törkeästä säännöstelyrikoksesta;

(8) törkeästä sisäpiirintiedon väärinkäytöstä, törkeästä markkinoiden vääristämisestä; tai

(9) törkeästä tulliselvitysrikoksesta.

(4) Edellä 3 momentissa tarkoitetun luvan antamisen edellytyksenä on lisäksi, että rikoksella on tavoiteltu erityisen suurta hyötyä ja rikos on tehty erityisen suunnitelmallisesti.

(5) Lupa telekuunteluun voidaan antaa myös, kun on syytä epäillä jotakuta törkeästä parituksesta, jossa on tavoiteltu erityisen suurta hyötyä ja rikos on tehty erityisen suunnitelmallisesti tai jota tarkoitetaan rikoslain 20 luvun 9 a §:n 1 momentin 3 kohdassa. (1180/2014)

10 luku, 6 § - Televalvonta ja sen edellytykset

(1) *Televalvonnalla* tarkoitetaan tunnistamistietojen hankkimista viestistä, joka on lähetetty 3 §:ssä tarkoitettuun viestintäverkkoon kytketystä teleosoitteesta tai telepäätelaitteesta taikka vastaanotettu tällaiseen osoitteeseen tai laitteeseen sekä teleosoitteen tai telepäätelaitteen sijaintitiedon hankkimista taikka teleosoitteen tai telepäätelaitteen käytön tilapäistä estämistä. *Tunnistamistiedolla* tarkoitetaan sähköisen viestinnän tietosuojalain 2 §:n 8 kohdassa tarkoitettua tilaajaan tai käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

(2) Esitutkintaviranomaiselle voidaan antaa lupa kohdistaa televalvontaa rikoksesta epäillyn hallussa olevaan tai hänen oletettavasti muuten käyttämäänsä teleosoitteeseen tai telepäätelaitteeseen, jos epäiltyä on syytä epäillä:

(1) rikoksesta, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta;
(2) teleosoitetta tai telepäätelaitetta käyttäen tehdystä rikoksesta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta;
(3) teleosoitetta tai telepäätelaitetta käyttäen tehdystä, automaattiseen tietojenkäsittelyjärjestelmään kohdistuneesta luvattomasta käytöstä;
(4) seksikaupan kohteena olevan henkilön hyväksikäytöstä, lapsen houkuttelemisesta seksuaalisiin tarkoituksiin tai parituksesta;
(5) huumausainerikoksesta;
(6) terroristisessa tarkoituksessa tehtävän rikoksen valmistelusta, kouluttautumisesta terrorismirikoksen tekemistä varten, terroristiryhmän rahoittamisesta tai matkustamisesta terrorismirikoksen tekemistä varten;
(7) törkeästä tulliselvitysrikoksesta;
(8) törkeästä laittoman saaliin kätkemisestä;
(9) panttivangin ottamisen valmistelusta; taikka
(10) törkeän ryöstön valmistelusta. (369/2015)

(3) Verkkoviestin tunnistamistietojen luovuttamisesta säädetään sananvapauden käyttämisestä joukkoviestinnässä annetun lain (460/2003) 17 §:ssä.

- **datan tallentaminen**

  Datan säilyttämismääräyksestä ja määräyksen kestosta on säädetty pakkokeinolain 8 luvun 24 ja 25 §:ssä:

8 luku, 24 § – Datan säilyttämismääräys

(1) Jos ennen laite-etsinnän toimittamista on syytä olettaa, että data, jolla voi olla merkitystä tutkittavana olevan rikoksen selvittämiselle, häviää tai sitä muutetaan, pidättämiseen oikeutettu virkamies voi antaa datan säilyttämismääräyksen. Sillä määrätään dataa hallussaan tai määräysvallassaan pitävä, ei kuitenkaan rikoksesta epäiltyä, säilyttämään se muuttumattomana. Määräys voi koskea myös dataa, jonka voidaan olettaa tulevan laitteeseen tai tietojärjestelmään määräyksen antamista seuraavan kuukauden aikana. Määräyksestä on pyynnöstä annettava kirjallinen todistus, jossa yksilöidään määräyksen kohteena oleva data.

(2) Mitä 1 momentissa säädetään, koskee myös tietojärjestelmän välityksellä siirrettyyn viestiin liittyvää tietoa viestin alkuperästä, määränpäästä, reitistä ja koosta sekä viestinnän ajankohdasta, kestosta, laadusta ja muista vastaavista seikoista *(liikennetieto)*. (1146/2013)

(3) Esitutkintaviranomaisella ei ole 1 momentissa tarkoitetun säilyttämismääräyksen nojalla oikeutta saada tietoonsa viestin, liikennetiedon tai muun tallennetun tiedon sisältöä. Jos 2 momentissa tarkoitetun viestin välittämiseen on osallistunut useampi palveluntarjoaja, esitutkintaviranomaisella on oikeus saada tietoonsa palveluntarjoajien tunnistamiseksi tarvittavat liikennetiedot. (1146/2013).

8 luku, 25 § – Datan säilyttämismääräyksen kesto

Datan säilyttämismääräys annetaan kolmeksi kuukaudeksi kerrallaan. Määräys voidaan uudistaa rikoksen tutkinnan sitä edellyttäessä. Määräys on kumottava niin pian kuin se ei enää ole tarpeen.

- **tallennettuja liikennetietoja / viestin sisältöä koskeva määräys**

Tallennettuja liikennetietoja koskeva määräys voi koskea myös luvan antamista edeltänyttä aikaa (pakkokeinolain 10 luvun 9 §:n 3 momentti) - *Televalvonnasta ja sijaintitietojen hankkimisesta päättäminen*

(3) Lupa voidaan antaa ja päätös tehdä enintään kuukaudeksi kerrallaan ja lupa tai päätös voi koskea myös luvan antamista tai päätöksen tekemistä edeltänyttä aikaa, joka voi olla kuukautta pidempi.

Tallennetuista viestisisällöistä säädetään pakkokeinolain 10 luvun 4 §:ssä - *Tietojen hankkiminen telekuuntelun sijasta*

(1) Jos on todennäköistä, että 3 §:ssä tarkoitettua viestiä ja siihen liittyviä tunnistamistietoja ei ole enää saatavissa telekuuntelulla, esitutkintaviranomaiselle voidaan antaa 7 luvun 4 §:ssä säädetystä kiellosta huolimatta lupa takavarikoida tai jäljentää ne tämän luvun 3 §:ssä säädetyillä edellytyksillä teleyrityksen tai yhteisötilaajan hallusta.

(2) Jos tietojen hankkiminen kohdistetaan viestin sisällön selvittämiseksi telepäätelaitteeseen välittömästi yhteydessä olevaan viestin lähettämiseen ja vastaanottamiseen soveltuvaan henkilökohtaiseen tekniseen laitteeseen tai tällaisen laitteen ja telepäätelaitteen väliseen yhteyteen, esitutkintaviranomaiselle voidaan antaa lupa tietojen hankkimiseen telekuuntelun sijasta, jos 3 §:ssä säädetyt edellytykset täyttyvät.

Syyttäjälaitoksesta annetun lain 25 §:n mukaisesti:

(1) Syyttäjällä on salassapitosäännösten estämättä oikeus maksutta saada viranomaiselta ja julkista tehtävää hoitamaan asetetulta yhteisöltä virkatehtävien suorittamista varten tarpeelliset tiedot ja asiakirjat, jollei sellaisen tiedon tai asiakirjan antamista syyttäjälle tai tietojen käyttämistä todisteena ole laissa kielletty tai rajoitettu.

(2) Syyttäjällä on oikeus saada virketehtävien suorittamista varten tarpeelliset tiedot yhteisön jäsentä, tilintarkastajaa, hallituksen jäsentä tai työntekijää velvoittavan yritys-, pankki- tai vakuutussalaisuuden estämättä.

- **käyttäjätietoja koskeva määräys**

Asianomaiset säännökset sisältyvät poliisilain (872/2011) 4 luvun 3 §:ään - *Tietojen saanti yksityiseltä yhteisöltä tai henkilöltä*

(1) Poliisilla on päällystöön kuuluvan poliisimiehen pyynnöstä oikeus saada rikoksen estämiseksi tai selvittämiseksi tarvittavia tietoja yhteisön jäsentä, tilintarkastajaa, toimitusjohtajaa, hallituksen jäsentä tai työntekijää velvoittavan yritys-, pankki- tai vakuutussalaisuuden estämättä. Poliisilla on sama oikeus saada 6 luvussa tarkoitetussa poliisitutkinnassa tarvittavia tietoja, jos tärkeä yleinen tai yksityinen etu sitä vaatii.

(2) Poliisilla on yksittäistapauksessa oikeus pyynnöstä saada teleyritykseltä ja yhteisötilaajalta yhteystiedot sellaisesta teleosoitteesta, jota ei mainita julkisessa luettelossa, taikka teleosoitteen tai telepäätelaitteen yksilöivät tiedot, jos tiedot ovat tarpeen poliisille kuuluvan tehtävän suorittamiseksi. Poliisilla on vastaava oikeus saada postitoimintaa harjoittavalta yhteisöltä jakeluosoitetietoja.

Seuraavat seikat ovat tärkeitä erityisesti tietokoneforensiikan kannalta:

- Laitteiden (kuten matkapuhelinten) haltuun ottaminen, kun niiden turvakoodi on auki
- Lisätietojen hankkiminen kohteesta internetin avulla selvittämällä mahdollinen sosiaalisen median tai pilvipalveluiden käyttö, salasanat jne. (julkisiin lähteisiin perustuva tiedustelu)
- Datan laillinen sieppaaminen ennen pidätystä, jos mahdollista
- Datan laillisen sieppaamisen lisäksi saattaisi olla hyödyllistä käyttää muita keinoja, jotka mainitaan teknistä laitetarkkailua koskevissa pakkokeinolain pykälissä
- Viranomaisten tehokas yhteistyö (poliisi, tulli, rajavartiosto, viestintäviraston kyberturvallisuuskeskus, puolustusvoimat)
- Poliisin ja yksityisen sektorin tehokas yhteistyö (esimerkiksi rahoitusala)
- kansainvälinen yhteistyö (esimerkiksi yhteiset tutkintaryhmät).

5.2.2. Rikostekninen tutkinta ja salaus

Rikosten esitutkinnan puitteissa hankitaan sähköistä todistusaineistoa ja analysoidaan toistettua dataa. Sähköistä todistusaineistoa käytetään kaikkien rikosten tutkinnassa, kyberrikokset mukaan lukien. Etäetsintä, esim. datan kopioiminen pilviasemalta, on mahdollista Suomessa. Rajat ylittävää etäetsintää ei ole vielä suoritettu ja pyrkimyksenä on lainsäädäntöjen yhdenmukaistaminen.

Viranomaiset mainitsivat seuraavat salaukseen liittyvät ongelmat:

- salauksen lisääntynyt käyttö, esim. matkapuhelimen muistin salaus;
- vahva salaus ja vahvat salasanat;
- haittaohjelmiin liittyä salaus;
- verkkoliikenteen salaus.

Nämä ongelmat pyritään kyberrikostutkinnassa ja tietokoneforensiikassa ratkaisemaan seuraavasti:

- Laitteiden (kuten matkapuhelinten) haltuun ottaminen, kun niiden turvakoodi on auki
- Hankitaan lisää laskentatehoa ja parempia salasanahakemistoja
- Tutkitaan salausmenetelmien haavoittuvaisuuksia
- Dataliikenteen sieppaamisen lisäksi olisi tutkittava tapoja valvoa aktiivisessa tilassa olevien tietokoneiden tai mobiililaitteiden käyttöä.

Keskusrikospoliisin kyberrikoskeskus on aloittanut salauksen alalla yhteistyön Suomen puolustusvoimien tutkimuslaitoksen kanssa, joka on asiantuntijakeskus.
Lisäksi kyberrikoskeskus on vaihtanut salaukseen liittyvää tietoa viestintäviraston kansallisen kyberturvallisuuskeskuksen kanssa.

Haittaohjelmiin liittyvien kokoonpanotiedostojen salauksia on purettu yhteistyössä yksityisten yritysten kanssa vain muutamia kertoja.

5.2.3. Sähköiset todisteet

Sähköisiä todisteita ei sinällään ole määritelty Suomen lainsäädännössä. Oikeudenkäymiskaaressa säädetään yleisellä tasolla periaatteesta, jonka mukaan tuomioistuin arvioi todisteet vapaalla todistusharkinnalla. *17 luvun 1 §:n* (732/2015) mukaan tuomioistuimen on arvioitava esitettyjen todisteiden näyttöarvo. Tähän liittyen lainvalvontaviranomaisten tai yksityisen sektorin yritysten on dataa kerätessään, tallentaessaan ja siirtäessään dokumentoitava toiminta asianmukaisesti. Todisteiden kerääminen on tärkein vaihe. Useimmissa tapauksissa lainvalvontaviranomaisten yleisimmin käyttämät ohjelmistot ja työkalut luovat aikaleimoja, lokeja ja protokollia, joilla datan eheys varmistetaan. Kun yksityisen sektorin toimijat keräävät dataa, datan todentaminen saattaa edellyttää toisessa maassa olevien todistajien kuulemista, ja lisäksi on olemassa riski, että todisteiden keräämisen yhteydessä ei noudateta poliisin tai jopa lainsäädännön standardeja.

Tällä hetkellä sähköinen todistusaineisto toimitetaan syyttäjille eri keinoin: muistitikuilla, DVD-levyillä jne. Kehitteillä oleva uusi asianhallintajärjestelmä (AIPA) tulee mahdollistamaan datan siirtämisen sähköisesti. Tosiasiassa esimerkiksi tavallinen valokuva tai ruutukaappaus paperilla tai pdf-tiedostona johtaa merkittävään datan menetykseen. Joissakin tapauksissa poliisi on kopioinut verkkosivuja sisältöineen ja linkkeineen ja toimittanut kaiken syyttäjälle DVD-levyllä. Suomen viranomaisten mukaan tätä käytäntöä voitaisiin hyödyntää useammin. Nykyisessä asianhallintajärjestelmässä (SAKARI) ei ole mahdollista toimittaa sähköistä todistusaineistoa poliisilta syyttäjälle tai syyttäjältä tuomioistuimelle. Syyttäjä tai poliisi huolehtii sähköisen todistusaineiston jakamisesta muille oikeudenkäyntiin osallistuville osapuolille ottamalla aineistosta tarvittavia kopioita. Monissa tapauksissa tämä laaja aineisto ei ole hyvin organisoitua. Sähköisen todistusaineiston analysointiin ei ole riittävästi työvoimaa ja poliisin syyttäjälle toimittamat pöytäkirjat sisältävät usein epäselviä asiakirjoja ilman todellista todisteluaihetta. Analyytikkoresurssien puute on suuri ongelma.

Lisäksi puolustus voi haastaa syyttäjän, jos todisteiden keräämistä ei ole dokumentoitu asianmukaisesti. Verkkotutkinnan välineet (esim. poliisin haittaohjelmat) pidetään usein salassa mahdollisimman pitkään, ja joskus näitä tekniikoita ei selitetä selkeästi pakkotoimista päättävälle tuomarille.

Suomen viranomaiset katsovat, että kybertiedustelutiedon vaihtaminen rahat ylittävässä oikeudellisessa yhteistyössä on hyvin vaikeaa luottamuspulan vuoksi. Joskus näillä tutkintatekniikoilla on suuri kaupallinen arvo (kuten nollapäivähaavoittuvuus). Jos yksityiset yritykset keräävät todistusaineistoa, niiden tutkintatekniikoista tiedetään hyvin vähän. Ratkaisevan todistusaineiston osalta heikko dokumentointi voi merkittävästi huonontaa aineiston arvoa ja johtaa vapauttavaan tuomioon.

Sähköiseen todistusaineistoon ei sovelleta mitään erityisiä hyväksyttävyyssääntöjä.

5.3. Ihmisoikeuksien/perusvapauksien suojeleminen

Kyberrikoksia koskevat lainsäädäntötoimet, kansainvälisten kriminalisointivelvoitteiden täytäntöönpano mukaan lukien, on toteutettu ihmisoikeuksia ja perusvapauksia sekä oikeusvaltioperiaatetta suojelevalla tavalla. Suhteellisuusperiaate ja tarpeellisuus demokraattisessa yhteiskunnassa on otettu huomioon. Laillisuusperiaatteen mukaisesti säännökset ovat täsmällisiä, tarkkoja ja ennakoitavia.

Tutkintatoimien osalta on löydettävä tasapaino ihmisoikeuksien ja perusvapauksien suojelemisen sekä rikostutkinnan tehokkuuden välillä. Tutkinnassa käytettävillä toimenpiteillä, joista säädetään pakkokeinolaissa (806/2011), puututaan ihmisoikeuksien ja perusvapauksien käyttämiseen. Sellaiset pakkokeinot, joilla puututaan merkittävästi näihin oikeuksiin, ovat yleensä sallittuja vain vakavien rikosten tutkinnassa.

Vastaajalla on käytössään oikeussuojakeinoja. Pakkokeinojen käytöstä päättää käräjäoikeus (esimerkiksi monet salaiset pakkokeinot). Jos pakkokeinon määrää poliisi tai joissakin harvoissa tapauksissa syyttäjä, tuomioistuimen on asianomaisen pyynnöstä päätettävä, säilyykö pakkokeino voimassa (esimerkiksi matkustuskielto ja takavarikointi). Lisäksi tuomioistuimen on asianomaisen pyynnöstä harkittava uudelleen, säilyykö pakkokeino voimassa (esimerkiksi tutkintavankeus ja takavarikointi). Kaikkiin tuomioistuimen tekemiin pakkokeinoja koskeviin päätöksiin voidaan hakea muutosta varsinaisin tai ylimääräisin muutoksenhakukeinoin (ei aikarajaa ja kiireellinen käsittely).

Rikostutkinnassa käytettävillä pakkokeinoilla puututaan ihmisoikeuksiin ja perusvapauksiin eri tavoin, riippuen asianomaisen pakkokeinon luonteesta. Pakkokeinolaki sisältää säännöksiä esimerkiksi kiinniottamisesta, pidättämisestä ja vangitsemisesta (2 ja 3 luku), yhteydenpidon rajoittamisesta (4 luku; kattaa kiinniotetut, pidätetyt ja vangitut henkilöt), matkustuskiellosta (5 luku), vakuustakavarikosta sakon, vahingonkorvauksen tai hyvityksen taikka valtiolle menetettäväksi tuomittavan rahamäärän maksamisen turvaamiseksi (6 luku), takavarikoimisesta ja asiakirjan jäljentämisestä (7 luku), etsinnästä (8 luku) ja salaisista pakkokeinoista (telekuuntelu, tukiasematietojen hankkiminen, asuntokuuntelu, tekninen tarkkailu jne.).

Sellaiset pakkokeinot, joilla puututaan merkittävästi ihmisoikeuksiin ja perusvapauksiin, ovat yleensä sallittuja vain vakavien rikosten tutkinnassa ja niiden käytöstä päättää käräjäoikeus. Salaisia pakkokeinoja koskevat säännökset sisältävät joitakin pakkokeinokohtaisia lisäedellytyksiä, kuten "erittäin tärkeä merkitys rikoksen selvittämiselle" tai "välttämätöntä rikoksen selvittämiseksi". Tietyt periaatteet on otettava huomioon kaikkien pakkokeinojen käytöstä tehtävien päätösten yhteydessä. Pakkokeinolain 1 luvun 2 §:ssä vahvistetun suhteellisuusperiaatteen mukaisesti pakkokeinoja saadaan käyttää vain, jos pakkokeinon käyttöä voidaan pitää puolustettavana ottaen huomioon tutkittavana olevan rikoksen törkeys, rikoksen selvittämisen tärkeys sekä rikoksesta epäillylle tai muille pakkokeinon käytöstä aiheutuva oikeuksien loukkaaminen ja muut asiaan vaikuttavat seikat. Pakkokeinolain 1 luvun 3 §:n 1 momentin (vähimmän haitan periaate) mukaisesti pakkokeinon käytöllä ei kenenkään oikeuksiin saa puuttua enempää kuin on välttämätöntä käytön tarkoituksen saavuttamiseksi.

5.4. Lainkäyttövalta

5.4.1. Kyberrikostutkintaan sovellettavat periaatteet

Kyberrikoksiin ei sovelleta mitään erityisiä toimivaltasääntöjä. Rikoslain 1 lukua sovelletaan kaikkiin rikoksiin. Lähtökohtana on, että Suomessa tehtyyn rikokseen sovelletaan Suomen lakia (1 luvun 1 §). Rikos katsotaan tehdyksi sekä siellä, missä rikollinen teko suoritettiin, että siellä, missä rikoksen tunnusmerkistön mukainen seuraus ilmeni (10 §:n 1 momentti). Suomen rikoslakia sovelletaan myös joihinkin alueen ulkopuolella tehtyihin rikoksiin. Näitä ovat esimerkiksi suomalaiseen alukseen liittyvät rikokset, Suomeen kohdistuneet rikokset, suomalaiseen kohdistuneet rikokset sekä suomalaisen tekemät rikokset (2, 3, 5 ja 6 §). Kun rikos on tehty Suomen ulkopuolella, monissa tapauksissa edellytetään kaksoisrangaistavuuden vaatimuksen täyttymistä.

5.4.2. Toimivaltaristiriitoja koskevat säännöt ja tapauksen antaminen Eurojustin käsiteltäväksi

Rikosoikeudenkäyntejä koskevien toimivaltaristiriitojen ehkäisemisestä ja ratkaisemisesta 30. marraskuuta 2009 annettu neuvoston puitepäätös 2009/948/YOS on saatettu osaksi kansallista lainsäädäntöä. Toimivaltaristiriidoista ei kuitenkaan ole kokemusta.

Jos rikos on tehty Suomen ulkopuolella, tutkintaan sovellettavista järjestelyistä neuvotellaan asianomaisen maan kanssa. Tähän mennessä toimivaltaristiriidat on ratkaistu tutkimalla tapaukset tekijän asuinvaltiossa. Eurojustin välityksellä käydään keskusteluja myös asianomaisten valtioiden oikeusviranomaisten välisistä suorista neuvotteluista.

5.4.3. Lainkäyttövalta pilvipalveluissa tehtyjen kyberrikosten osalta

Suomen rikoslain toimivaltaa koskevat säännökset (1 luku) ovat vuodelta 1996. Kyberrikosten osalta toimivaltakysymykset saattavat olla vaikeita ratkaista tavallisiin rikosasioihin verrattuna.

Suomi on vahvistanut toimivaltansa tilanteissa, joissa rikoksen tekijä tai uhri on suomalainen, mutta näissä tapauksissa syyttäjän on selvitettävä, käsitteleekö toinen valtio (tai toiset valtiot) tapausta, ja saatava sen valtion viranomaisilta, missä rikos tehtiin, kyseisen valtion asiaankuuluvat säännökset sisältävä asiakirja. Rikoksen tekopaikan maantieteellinen sijainti saattaa olla vaikea määritellä. Näihin tilanteisiin olisi varauduttava ja harkittava tapoja parantaa käytäntöjä siten, että varmistetaan tehokas syytteeseenpano, mutta vältytään positiivisilta toimivaltaristiriidoilta.

Todisteiden keräämiseen liittyy seuraavanlaisia ongelmia: jos todistusaineisto vaihtaa paikkaa nopeasti, tutkivien viranomaisten pitää hyvin nopeasti pystyä lähettämään pyyntöjä moniin eri maihin. Kybertoimintaympäristön rajaton luonne synnyttää erityisiä haasteita lainvalvonta- ja oikeusviranomaisille. Sähköistä todistusaineistoa, joka on nykyään ratkaisevan tärkeää tutkinnan ja oikeusviranomaisten kannalta, voidaan tallentaa, muuttaa ja tuhota sekunneissa mistä tahansa maailman kolkasta. Sähköistä todistusaineistoa voidaan myös sekunneissa siirtää, tuhota ja kontrolloida taikka pirstaloida useille lainkäyttöalueille kaikkialla maailmassa.

Keskinäisen oikeusavun nykyisiä menettelyjä on lisäksi nopeutettava ja tehostettava. Jos data siirretään paikkoihin, jotka ovat lainvalvonta- tai oikeusviranomaisten ulottumattomissa, tämä haittaa keskinäisen oikeusavun yhteistyömekanismeja, koska nämä mekanismit perustuvat alueperiaatteeseen, eli datan sijaintiin. On todettu, että keskinäisen oikeusavun menettelyt ovat tietyissä tapauksissa liian hitaita ja raskaita toimiakseen tehokkaasti kyberrikostutkinnassa. Joskus ei tiedetä, mistä maasta oikeusapua tulisi pyytää (keskinäinen oikeusapu on mahdotonta esimerkiksi tilanteissa, joissa datan sijainti on täysin tuntematon).

Näin ollen on tärkeää löytää ratkaisuja kysymyksiin siitä, missä olosuhteissa tietty valtio voi tutkia kyberrikosta ja toteuttaa tutkintatoimia ja minkälainen yhteys pitää olla tapauksen ja rikosta tutkivan valtion välillä. Tässä yhteydessä olisi otettava erityisesti huomioon muut yhdistävät tekijät kuin datan sijainti (esim. epäillyn kansalaisuus tai vakinainen asuinpaikka taikka rikoksen uhrin sijainti.

Datan fyysinen sijainti on nykyään vähemmän olennaista. Kysymys ei ole ainoastaan datan saatavuudesta yli rajojen, vaan kysymys liittyy myös puhtaasti kansallisiin toimenpiteisiin. Tehokkaiden ratkaisujen saavuttamiseksi on kehitettävä yhteisiä näkemyksiä. Tätä työtä aloitellaan EU-tasolla.

Pilvipalvelujen osalta Suomessa keskustellaan siitä, onko poliisilla laillinen oikeus kirjautua tilille tai profiiliin suoraan ilman vieraan valtion ja haltijan suostumusta tilanteessa, jossa tutkijalla on käyttäjätunnus ja salasana, ja *laite-etsinnän toimittamisen etäetsintänä* ja *asiakirjan jäljentämisen* (takavarikoiminen) kansalliset edellytykset täyttyvät.

5.4.4. Suomen näkemys kyberrikostorjunnan oikeuskehyksestä

Datan sijainti on perinteisesti ollut ratkaiseva tekijä lainkäyttövallan kannalta kyberrikoksissa. Sijainnin merkitys on vähentynyt vaiheittain, erityisesti esim. sen johdosta, että internetpalveluntarjoajat pystyvät määrittämään, missä dataa hallinnoidaan ja missä se on saatavilla. Toinen tähän vaikuttanut seikka on se, että datan sijaintia saattaa olla vaikeaa tai jopa mahdotonta selvittää. Tämä kaikki on johtanut tilanteeseen, jossa keskinäistä oikeusapua pyydetään usein siltä maalta, missä dataa hallinnoidaan, sen maan sijasta, missä data todellisuudessa sijaitsee. Internetpalveluntarjoajien lisäksi vastaava lähestymistapa tämän kysymyksen käsittelemiseksi olisi ulotettava koskemaan myös luonnollisia henkilöitä ja oikeushenkilöitä. Datan sijainti ei enää voi olla ainoa tekijä, joka määrittää valtion lainkäyttövallan datan suhteen, jota voidaan sattumanvaraisesti tallentaa eri paikkoihin tai peilata taikka siirtää ympäri maailman kybertoimintaympäristössä.

Riippumattomuus sijainnista on pilvipalveluiden avainominaisuus. Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen komitean laatiman pilvipalveluiden määritelmän mukaan erityispiirteenä on, että dataa ei yleensä säilytetä tietyllä laitteella tai suljetuissa verkoissa, vaan se jaetaan eri palveluihin, eri palveluntarjoajille, eri sijainteihin ja usein eri lainkäyttöalueillekin. Kybertoimintaympäristössä sijaitsevan todistusaineiston saatavuuden turvaamiseksi on kehitettävä yhteinen käsitys rajattomasta internetistä, missä ratkaiseva tekijä on se, kuka dataa hallinnoi ja mistä sitä hallinnoidaan (rekisteröidyn (epäilty/syytetty) sijainti/kansalaisuus), eikä se, missä data tosiasiassa sijaitsee. On kehitettävä yhteiset puitteet, erityisesti seuraavia kahta tilannetta varten: 1) kun palveluntarjoaja hallinnoi dataa jostakin muualta kuin sieltä, missä data tosiasiassa sijaitsee, ja tarvitaan keskinäistä oikeusapua datan saamiseksi ulkomaiselta lainkäyttöalueelta sekä 2) kun keskinäistä oikeusapua ei voida käyttää (datan sijainti on tuntematon tai epäselvä, kuten pilvipalveluiden kohdalla yleensä on) tai kun se ei ole järkevä tapa edetä asiassa (data voidaan saada muulla tavalla).

Tässä asiassa on avainkysymyksenä se, että jos valtiolla on kiistaton toimivalta tutkia tietty rikos, voiko sen toimivalta saada sähköistä todistusaineistoa muuttua tai jopa lakata riippuen siitä, missä data milloinkin sijaitsee tai miten se on tallennettu. Vastaus on usein kielteinen, koska datan sijaintia koskevaa kysymykseen ei ole rationaalista vastausta tai vastaus on epäoleellinen, sillä keskinäistä oikeusapupyyntöä ei voida onnistuneesti osoittaa maalle, missä data sijaitsee.

Parhaiden mahdollisten tulosten saavuttamiseksi valtioiden on varmistettava, että keskinäisen oikeusavun välineitä ja vastavuoroiseen tunnustamiseen perustuvia välineitä käytetään täysimääräisesti ja tehokkaasti ja erityisesti mahdollisimman nopeasti. Yhteistyötä voidaan parantaa monin tavoin, esim. vahvistamalla 24/7-verkostojen välistä yhteistyötä oikeusviranomaisten välinen yhteistyö mukaan lukien, kehittämällä tiedoksiantomenettelyjä tai muita valvontamenettelyjä kiireellisiä tilanteita varten sekä kehittämällä yhdenmukaisia sähköisesti toimitettavia pyyntöjä.

Kysymys suorasta rajat ylittävästä yhteistyöstä palveluntarjoajien kanssa on arkaluonteinen. Kummankin valtion viranomaisten valvonta-aspekti on tärkeää perusoikeuksien, tietosuojan ja suvereniteettikysymysten vuoksi. Sekä pyynnön esittävä että pyynnön vastaanottava valtio voivat hyväksyä suorat yhteydet, ja yhteiset säännöt voitaisiin laatia tältä pohjalta. Tällaiset menettelyt voivat olla paikallaan tiettyjen tilanteiden tai tietyn datan, kuten tilaajatietojen osalta. On kuitenkin järkevää kehittää kevyempiä järjestelyjä tilaajatietoja varten, koska se on rikosoikeudellisissa menettelyissä eniten pyydetty datan laji, eikä se liity luottamukselliseen viestintään kuten sisältö- ja liikennetiedot.

Datan rajat ylittävä saatavuus on olennaista vain niissä tapauksissa, joissa rikostutkinnasta vastaavalla viranomaisella on syytä uskoa, että datan hankkimiseen liittyy rajan ylittäminen. Tämä lähtökohta olisi otettava huomioon. Kun käsitellään rajat ylittäviä tapauksia, tarvitaan yhteinen oikeudellinen kehys niitä tilanteita varten, joissa keskinäinen oikeusapu ei ole mahdollista. Viranomaisten olisi täsmennettävä, milloin tällaiseen tilanteeseen joudutaan. Olisi katettava ainakin tilanteet, joihin liittyy "sijainnin menettäminen", eli joissa sähköinen todistusaineisto on tallennettu pilvipalveluun tai on jopa jatkuvassa liikkeessä pilvipalvelussa. Näissä tilanteissa voitaisiin sallia datan rajat ylittävä saatavuus, jos se on teknisesti mahdollista. Asianomaisen viranomaisen olisi noudatettava samoja menettelyjä kuin kansallisissakin tapauksissa.

Tehokkaiden ratkaisujen löytämiseksi on tärkeää kehittää yhteisiä näkemyksiä. Koska tätä työtä on tehty EU:n tasolla, on järkevää välttää päällekkäisyyksiä. Kun on keskusteltu mahdollisista tulevista EU-toimista on monissa tapauksissa voitu hyödyntää Euroopan neuvoston puitteissa jo tehtyä työtä. Budapestin yleissopimukseen liittyvä Euroopan neuvoston ad hoc -työryhmä (Cloud Evidence Group) tutkii parhaillaan ratkaisuja sähköisen todistusaineiston saatavuuden parantamiseksi laatimalla esimerkiksi ohjeita tai jopa lisäpöytäkirja.

5.5. Päätelmät

- Suomi ratifioi Euroopan neuvoston yleissopimuksen tietoverkkorikollisuudesta vuonna 2007. Neuvoston puitepäätös 2005/222/YOS tietojärjestelmiin kohdistuvista hyökkäyksistä ja direktiivi 2013/40/EU tietojärjestelmiin kohdistuvista hyökkäyksistä on saatettu osaksi Suomen lainsäädäntöä.

- Suomi on ollut lasten suojelemisesta seksuaalista riistoa ja seksuaalista hyväksikäyttöä vastaan annetun Euroopan neuvoston yleissopimuksen sopimuspuoli vuodesta 2011 lähtien. Suomen viranomaisten mukaan lasten seksuaalisen hyväksikäytön ja seksuaalisen riiston sekä lapsipornografian torjumisesta annetun direktiivin 2011/93/EU täytäntöönpano ei ole näin ollen edellyttänyt lainsäädäntötoimia, koska asiaankuuluva lainsäädäntö on jo direktiivin mukaista.

- Kyberpetokset ja kyberväärennykset on rikoslaissa määrätty rangaistaviksi.

- Salauskysymyksiä pidetään haasteellisina. Viranomaiset mainitsivat verkkoliikenteen salauksen ja koko kovalevyn salauksen sellaisina alueina, joilla salaukseen liittyviä ongelmia ei vielä ole kyetty ratkaisemaan tehokkaasti.

- Sähköistä todistusaineistoa ei määritellä kansallisessa lainsäädännössä, eikä siihen sovelleta mitään erityisiä hyväksyttävyyssääntöjä. Sähköiseen todistusaineistoon sovelletaan samoja todisteita koskevia sääntöjä kuin paperiasiakirjoihinkin, ja sähköiset todisteet hyväksytään oikeudenkäymiskaaressa.

- Lainsäädäntö sisältää yleisiä säännöksiä, jotka koskevat tutkintaan, pakkokeinoihin ja poliisityöhön liittyviä menettelyjä. Kyberrikostutkintaa varten ei kuitenkaan ole mitään erityisiä säännöksiä. Nykyisten tutkintatoimien riittämättömyys syytteeseenpanon varmistamiseksi kyberrikosten osalta vaikuttaa olevan Suomessa merkittävin ongelma tällä alalla. Tiettyjen pakkokeinojen, kuten telekuuntelun käyttö on rajattu koskemaan joukkoa erikseen lueteltuja rikoksia. Tässä luettelossa ei ole törkeän verkkopetoksen lisäksi yhtään rikosta, joka kuuluu kyberrikoksiin. Ottaen huomioon kyberrikosten erityisluonteen ja niiden tutkijoille asettamat vaatimukset, arviointiryhmän mielestä olisi hyödyllistä tarkastella, voitaisiinko tätä luetteloa laajentaa erityisesti kyberrikoksiin tai voitaisiinko löytää muita tapoja mahdollistaa näiden pakkokeinojen käyttö tällaisessa tutkinnassa. Lisäksi voitaisiin harkita tiettyjen tutkintatoimien lisäämistä, joita voimassa oleva tutkintatoimien luettelo ei tällä hetkellä sisällä.

- Kyberrikoksiin ei sovelleta mitään erityisiä toimivaltasääntöjä ja rikoslain 1 lukua sovelletaan kaikkiin rikoksiin. Pilvipalveluihin liittyvän lainkäyttövallan osalta Suomessa keskustellaan siitä, onko poliisilla laillinen oikeus kirjautua tilille tai profiiliin suoraan ilman vieraan valtion ja haltijan suostumusta tilanteessa, jossa tutkijalla on käyttäjätunnus ja salasana, ja *laite-etsinnän toimittamisen etäetsintänä* ja *asiakirjan jäljentämisen* (takavarikoiminen) kansalliset edellytykset täyttyvät. Rajat ylittävää etäetsintää ei ole vielä suoritettu ja pyrkimyksenä on lainsäädäntöjen yhdenmukaistaminen.

- Arviointiryhmä katsoo, että Suomen viranomaisten mainitsemat ongelmat, jotka liittyvät lainkäyttövaltaan ja sähköisen todistusaineiston keräämiseen pilvipalveluista, ovat samankaltaisia kuin useimpien muiden jäsenvaltioiden ongelmat. Näin ollen tarvitaan yhteinen EU-tason ratkaisu. EU:n toimielimiä olisi kannustettava etsimään ratkaisuja oikeudellisiin ongelmiin, jotka liittyvät lainkäyttövaltaan ja sähköisen todistusaineiston keräämiseen pilvipalveluista.

6. OPERATIIVISET NÄKÖKOHDAT

6.1. Kyberhyökkäykset

6.1.1. Kyberhyökkäysten luonne

Suomessa on tutkittu seuraavia kyberhyökkäyksiä:

- hajautetut palvelunestohyökkäykset valtion virastoihin ja pankkeihin;
- haittaohjelmat kuten Jsocket ja Dridex, joiden kohteena olivat yksityiset yritykset ja yksityishenkilöt. Useimmissa tapauksissa hyökkäys kohdistui mobiililaitteisiin tai yksityishenkilöihin;
- kiristysohjelmat: Cryptolocker, Cryptowall, Locky ja mobiililaitteisiin kohdistetut haittaohjelmat;
- yksityisiin yrityksiin kohdistuvat tietokoneisiin tunkeutumiset, joihin liittyy myös kiristys;
- "kortittomiin" maksutapahtumiin liittyvät petokset (Card Not Present): yksityishenkilöiden ja yksityisten yritysten varastettujen luottokorttitietojen käyttäminen;
- kyberpetokset, kuten datan peukaloiminen tietojenkäsittelyn tuloksen vääristämiseksi tai verkkosivujen haavoittuvuuksien hyödyntäminen taloudellisen hyödyn toivossa;
- verkkourkintakampanjat: kohteena ovat yksityishenkilöt ja tavoitteena on kerätä henkilötietoja, verkkopankkitunnuksia tai luottokorttitietoja;
- yksityisiin yrityksiin kohdistuvat CEO fraud -tapaukset (tekeytyminen yrityksen johtohenkilöksi), joissa käytetään joskus sähköpostitilejä, joihin on murtauduttu.

Hyökkäyksiä ovat tehneet sekä ulkomaiset että kotimaiset yksityishenkilöt ja järjestäytyneet rikollisryhmät. Useimmissa tapauksissa tutkintaan liittyi yhteistyö Europolin ja/tai FBI:n kanssa.

6.1.2. Mekanismi kyberhyökkäyksiin vastaamiseksi

Suomessa ei ole vahvistettua monialaista mekanismia, johon kuuluisi useita valtion virastoja ja/tai yksityisiä toimijoita. Kaikki asiaankuuluvat toimijat ovat kuitenkin osallistuneet moniin kyberharjoituksiin ja näistä kysymyksistä keskustellaan useissa työryhmissä. Vakavien kyberhyökkäysten (rikosten) käsittelystä vastaavat pääasiassa kaksi toimijaa: poliisi ja kyberturvallisuuskeskus. Suomen viranomaisten mukaan niiden välinen yhteistyö toimii erittäin hyvin.

Tietoyhteiskuntakaaren (275 §) mukaan teleyrityksen on ilmoitettava Viestintävirastolle, jos sen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus. Teleyrityksen on ilmoitettava Viestintävirastolle myös häiriön tai sen uhan arvioitu kesto ja vaikutukset, korjaustoimenpiteet sekä ne toimenpiteet, joilla häiriön toistuminen pyritään estämään.

Henkilötietojen tietoturvaloukkausten ilmoittamiseen sovellettavista toimenpiteistä säädetään 24. kesäkuuta 2013 annetussa Euroopan komission asetuksessa 611/2013 henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY mukaisten henkilötietojen tietoturvaloukkausten ilmoittamiseen sovellettavista toimenpiteistä. Asetuksella on yhdenmukaistettu menettelyjä, joilla ilmoitetaan Viestintävirastolle ja käyttäjille henkilötietojen tietoturvaloukkauksista, ja näiden ilmoitusten sisältöä. Asetus on suoraan sovellettavaa lainsäädäntöä, joten se koskee kaikkia teleyrityksiä sellaisenaan. Muista tietoturvaloukkauksista ilmoittamisesta on säädetty Viestintäviraston määräyksessä 66 teletoiminnan häiriötilanteista.

Käytännössä kaikki ilmoitukset turvallisuushäiriöistä tehdään määräyksen 66 liitteessä 2 (teleyrityksen ilmoitus tietoturvahäiriöstä) olevaa lomaketta käyttäen. Ilmoitus voidaan tehdä myös sähköpostitse. Teksti voi olla vapaamuotoinen, kunhan siinä esitetään samat tiedot kuin ilmoituslomakkeessa. Jos on syytä epäillä, että ilmoituksen toimittamiseen käytetyn viestintäpalvelun tietoturvallisuutta on loukattu, tai jos tilanne edellyttää Viestintävirastolta välittömiä toimia, ensi-ilmoitus on tehtävä välittömästi puhelimitse siihen mennessä saatujen tietojen pohjalta. Pitkäkestoisissa tapauksissa teleyrityksen on pidettävä Viestintävirasto ajan tasalla tilanteen kehittymisestä. Sähköisesti toimitettu ilmoitus, joka voidaan tulostaa kirjallisessa ja luettavassa muodossa, katsotaan kirjalliseksi ilmoitukseksi.

Tunnistuspalvelun tarjoajien ja yleisölle laatuvarmenteita tarjoavien varmentajien ilmoitusvelvollisuudesta Viestintävirastolle annetussa määräyksessä 7 velvoitetaan nämä toimijat tekemään ilmoituksia. Määräyksen mukaan toimijoiden on ennen toimintansa aloittamista tehtävä Viestintävirastolle ilmoitus ja toimitettava tiedot, joiden perusteella virasto arvioi toiminnan luotettavuuden ja tietoturvallisuuden.

Toimijoiden on ilmoitettava Viestintävirastolle myös toiminnan merkittävistä muutoksista ja toimintansa lopettamisesta. Lisäksi toimijoiden on toimitettava Viestintävirastolle vuosittain selvitys toimintansa laajuudesta ja palvelun tietoturvaan kohdistuvista uhkista.

Tunnistuspalvelun tarjoajien ja laatuvarmenteita tarjoavien varmentajien on ilmoitettava Viestintävirastolle palveluidensa tietoturvaan kohdistuvista merkittävistä uhkista tai häiriöistä sekä näiden korjaamiseksi tehdyistä toimenpiteistä. Viestintävirasto voi tarvittaessa pyytää palveluntarjoajalta lisätietoja muutoksista ja häiriöistä. Viestintävirasto voi myös määrätä palveluntarjoajan korjaamaan todetut puutteet.

Viestintävirasto on antanut määräyksellä ja siihen liittyvällä selitysmuistiolla lisäohjeita toiminnan muutoksia koskevien ilmoitusten, vuosittaisten selvitysten ja häiriöilmoitusten sisällöstä ja toimittamisesta. Viestintävirasto tuottaa huoltovarmuuden kannalta kriittisille toimijoille tietoturvallisuuden tilannekuvatietoa ja tarjoaa toimijoille yhteisen tietojenvaihtokanavan.

Viestintävirasto pitää yllä huoltovarmuuskriittisten palvelujen tarjoajille suunnattuja kaksisuuntaisia postituslistoja. Postituslistoilla toimijat voivat keskustella luottamuksellisesti tietoturvallisuuteen liittyvistä asioista. Myös Viestintäviraston Kyberturvallisuuskeskus lähettää listoille turvatiedotteita ajankohtaisista aiheista. Tiedotteet kiinnostavat sekä kaikkia huoltovarmuuskriittisiä yrityksiä että erityisesti kyseisellä listalla olevaa yritysjoukkoa.

Suomessa käytetään laajalti mobiililaajakaistapalveluja ja tietojen säilyttämistä koskevat tiedot säilytetään vain muutaman kuukauden ajan. Epäiltyä ei pystytä tavoittamaan ilman mobiililaajakaistaan kirjautumisessa käytetyn portin numeroa, koska sadoilla käyttäjillä voi olla sama IP-osoite.

6.2. Verkossa esiintyvän lapsipornografian ja seksuaalisen hyväksikäytön vastaiset toimenpiteet

6.2.1. Ohjelmistot uhrien tunnistamiseksi ja toimenpiteet uudelleen uhriksi joutumisen estämiseksi

Suomessa aloitettiin vuonna 2015 hanke kansallisen tietokannan perustamiseksi lasten hyväksikäyttöön liittyvälle aineistolle. Tätä tietokantaa käytetään myös uhrien tunnistamisessa.

Suomen viranomaiset ilmoittivat, etteivät ne ole ottaneet käyttöön minkäänlaisia erityistoimenpiteitä sen välttämiseksi, että lapsi joutuu uudelleen uhriksi, jos kuvia/videoita ei tuhota.

6.2.2. Toimenpiteet verkossa tapahtuvan seksuaalisen hyväksikäytön/riiston, nk. sekstareiden ja verkkokiusaamisen torjumiseksi

Kyberrikoskeskus ylläpitää ja päivittää säännöllisesti lapsipornografiasivustojen estolistaa. Estolista toimitetaan internetpalveluntarjoajille, jotta ne voivat estää asiakkailtaan pääsyn näille sivustoille. Viranomaiset ilmoittivat, että yksikään internetpalveluntarjoaja ei käytä listaa.

6.2.3. Toimenpiteet lapsiseksiturismin, lasta hyväksikäyttävien pornografisten esitysten jne. torjumiseksi

Suomen matkatoimistoalan liitto (SMAL) on ollut aktiivinen tällä alalla 1990-luvulta saakka. Se on laatinut esitteen "Matkailun pimeä puoli" ja päivittänyt esitettä. SMAL:iin kuuluvat suurimmat matkanjärjestäjät ovat omaksuneet ECPATin, kansainvälisten matkajärjestäjien ja Unicefin luoman käyttäytymisohjeistuksen. Tämän käyttäytymisohjeistuksen omaksunut matkanjärjestäjä kouluttaa henkilöstönsä ja tiedottaa asiasta asiakkaitaan tämänkaltaisen matkailun estämiseksi. Käyttäytymisohjeistuksen omaksuneet matkanjärjestäjät vastaavat lähes 85 prosentista ulkomaille suuntautuvista lentomatkapaketeista.

Poliisilla on Nettivinkki-järjestelmä.

Suomi on osallistunut kansainvälisiin (Euroopan komission osittain rahoittamiin) Safer Internet -ohjelmiin jo yli kymmenen vuoden ajan. Kansallisen audiovisuaalisen instituutin mediakasvatus- ja kuvaohjelmayksikkö on vuodesta 2012 saakka koordinoinut Suomen Safer Internet Centren (FISIC) toimintaa läheisessä yhteistyössä Mannerheimin lastensuojeluliiton ja Pelastakaa lapset ry:n kanssa. Suomen Safer Internet Centre kuuluu kansainväliseen Insafe-verkostoon.

FISICin tarkoituksena on edistää internetin ja mobiiliteknologioiden turvallisempaa ja parempaa käyttöä lasten ja nuorten parissa. FISIC koostuu tietoisuutta lisäävistä toiminnoista, auttavista puhelin- ja nettipalveluista sekä vihjepalvelutyöstä. Tietoisuutta lisäävillä toiminnoilla pyritään lisäämään kansalaisten tietoisuutta ja taitoja paremman ja turvallisemman internetin ja muun digitaalisen toimintaympäristön luomiseksi. Tässä yhteydessä järjestetään tiedotuskampanjoita ja kehitetään levitykseen tarkoitettua aineistoa ja välineistöä. Tärkein levityskanava lasten ja nuorten kanssa työskenteleville ammattilaisille on Mediataitokoulu-sivusto (www.mediataitokoulu.fi), joka sisältää tietoa, harjoituksia sekä medialukutaitoon, mediakasvatukseen ja internetin turvallisuuteen liittyvän viitetietokannan. Vuosittain järjestettävä Mediataitoviikko on osa FISICin tietoisuutta lisäävää työtä medialukutaidon ja mediakasvatuksen kansallisten tavoitteiden edistämiseksi.

Auttavan puhelimen ja nettipalvelujen tarkoituksena on vastata lasten verkkoteknologioiden käyttöön liittyviin lasten ja vanhempien kysymyksiin verkossa ja puhelimessa. Vanhemmat ja lapset saavat neuvoja, miten käsitellä vahingollisia yhteydenottoja (ns. grooming), vahingollista toimintaa (verkkokiusaaminen) ja vahingollista sisältöä sekä epämiellyttäviä tai pelottavia kokemuksia verkkoteknologian käytössä.

Pelastakaa lapset ry ylläpitää Nettivihje-vihjepalvelua, johon yleisö voi ilmoittaa mahdollisesti laittomasta, erityisesti lasten seksuaaliseen hyväksikäyttöön liittyvästä sisällöstä Suomessa. Nettivihje on osa INHOPE-verkostoa (International Association of Internet Hotlines).

Pelastakaa lapset ry työskentelee myös seksuaalirikollisten auttamiseksi. Sen kampanjassa seksuaalirikollisia kehotetaan ottamaan vastuu teoistaan.

6.2.4. Lapsipornografiaa sisältävien tai levittävien sivustojen vastaiset toimijat ja toimenpiteet

Kyberrikoskeskuksen lapsipornografiaan erikoitunut ryhmä työskentelee kansallisesti ja kansainvälisesti. Ryhmässä on kolme poliisia. Heidän roolinsa on toimia kansallisen ja kansainvälisen tason yhteyspisteenä. He tekevät yhteistyötä kansainvälisten kumppaneiden kanssa sekä analysoivat tapauksia ja ehdotettuja kansainvälisiä hankkeita. He suorittavat alustavaa tutkintaa lisätietojen saamiseksi mahdollisista suomalaisista rikollisista sekä sen selvittämiseksi, mikä poliisilaitos sopisi parhaiten käsittelemään tapausta.

Kaikkien poliisilaitosten väkivalta- ja seksuaalirikosyksiköt käsittelevät lasten seksuaaliseen hyväksikäyttöön liittyviä tapauksia. Lasten kanssa työskenteleville tutkijoille annetaan erityiskoulutusta.

Lapsipornografian levittämisen estotoimista annetun Suomen lain mukaan teleyrityksellä on oikeus tarjota palvelujaan niin, että niiden avulla ei ole pääsyä lapsipornosivustoihin. Poliisi ylläpitää luetteloa lapsipornosivustoista. Luettelo toimitetaan internetpalveluntarjoajille, jotta ne voivat estää käyttäjiensä pääsyn näille sivustoille. Yksityinen sektori saa valita mahdollisen suodatuksen / pääsyn estämisen menetelmät. Internetpalveluntarjoajat ovat velvollisia poistamaan kaiken niiden ylläpitämiltä sivustoilta löytyvän lapsipornografisen aineiston (tietoyhteiskunnan palvelujen tarjoamisesta annetun lain (458/2002) 15 §).

Tietoyhteiskuntakaaren (917/2014) mukaan:

185 §

Tiedon saannin estoa koskeva määräys

Käräjäoikeus voi syyttäjän tai tutkinnanjohtajan hakemuksesta taikka sen hakemuksesta, jonka oikeutta asia koskee, määrätä 184 §:ssä tarkoitetun tietoyhteiskunnan palvelun tarjoajan sakon uhalla estämään tallentamansa tiedon saannin, jos tieto on ilmeisesti sellainen, että sen sisällön pitäminen yleisön saatavilla tai sen välittäminen on säädetty rangaistavaksi tai korvausvastuun perusteeksi. Hakemus on käsiteltävä kiireellisesti. Hakemusta ei voida hyväksyä varaamatta palvelun tarjoajalle ja sisällön tuottajalle tilaisuutta tulla kuulluksi, paitsi jos kuulemista ei voida toimittaa niin nopeasti kuin asian kiireellisyys välttämättä vaatii. Käräjäoikeuden määräys on annettava tiedoksi myös sisällön tuottajalle. Jos sisällöntuottaja on tuntematon, käräjäoikeus voi määrätä tietoyhteiskunnan palvelun tarjoajan huolehtimaan tiedoksiannosta. Määräys raukeaa, jollei sen kohteena olevan tiedon sisältöön tai välittämiseen perustuvasta rikoksesta nosteta syytettä tai, milloin kysymys on korvausvastuusta, panna vireille kannetta kolmen kuukauden kuluessa määräyksen antamisesta. Käräjäoikeus voi syyttäjän, asianomistajan tai asianosaisen edellä tarkoitettuna määräaikana esittämästä vaatimuksesta pidentää tätä määräaikaa enintään kolmella kuukaudella.

Tietoyhteiskunnan palvelun tarjoajalla ja sisällön tuottajalla on oikeus hakea määräyksen kumoamista siinä käräjäoikeudessa, jossa määräys on annettu. Määräyksen kumoamista koskevan asian käsittelyssä noudatetaan oikeudenkäymiskaaren 8 luvun säännöksiä. Tuomioistuin huolehtii kuitenkin tarpeellisista toimenpiteistä syyttäjän kuulemiseksi. Kumoamista on haettava 14 päivän kuluessa siitä, kun hakija on saanut tiedon määräyksestä. Tietoa ei saa saattaa uudelleen saataville kumoamista koskevan asian käsittelyn ollessa vireillä, ellei asiaa käsittelevä tuomioistuin toisin määrää. Myös syyttäjällä on oikeus hakea muutosta päätökseen, jolla määräys on kumottu.

Jos palvelin sijaitsee Suomen ulkopuolella, tieto toimitetaan toimivaltaiselle viranomaiselle kansainvälisiä kanavia pitkin, yleensä SIENA-viestillä.

6.3. Korttipetokset verkossa

6.3.1. Raportointi verkossa

Jos kansalainen huomaa luottokorttilaskussaan väärinkäytöksen, hän ottaa ensimmäiseksi yhteyttä kortin myöntäneeseen pankkiin. Pankki saattaa tapauksesta riippuen vaatia kortinhaltijaa ilmoittamaan tapauksesta poliisille. Jos pankki toteaa, että kortinhaltijalla ei selvästikään ollut minkäänlaista yhteyttä maksutapahtumaan, se palauttaa rahat kortinhaltijalle ja kattaa tappiot. Jos tapaus on epäselvä, useimmat pankit vaativat yleensä asiakasta ilmoittamaan tapauksesta poliisille kahdesta syystä: ensinnäkin siksi, että poliisi voi tutkia asiaa, ja toiseksi siksi, että monet pankit eivät tiedä, puhuuko asiakas totta, ja varmistuakseen asiasta ne haluavat poliisin olevan osallisena tapauksen käsittelyssä.

Suomen poliisi ilmoitti, että sen yhteistyö suomalaisten pankkien kanssa toimii hyvin. Säännöllisissä kokouksissa keskustellaan siitä, millaisista tapauksista pankkien olisi ilmoitettava poliisille. Vallitseva käsitys on, että "kortittomiin" maksutapahtumiin liittyvät tapaukset (Card Not Present) ja verkossa tapahtuvat väärinkäytökset ovat niin tavallisia ja yleisiä, että jos ne kaikki ilmoitettaisiin poliisille tutkintaa varten, poliisin tutkintayksikön resurssit eivät riittäisi alkuunkaan. Näillä tapauksilla ei yleensä ole kortinhaltijan lisäksi mitään yhteyksiä Suomeen ja väärinkäytöksiin liittyvät rahamäärät ovat niin pieniä, että useimmat maat eivät vastaisi keskinäistä oikeusapua koskevaan pyyntöön, jos sellainen lähetettäisiin. Näin ollen taktiikkana on kerätä merkittävämpiä tapauksia ja ehkäistä rikollisia ilmiöitä tiedonvaihdon avulla, jotta laajempialaiset rikosyritykset voidaan pysäyttää alkuvaiheessa. Tämän vuoksi kaikkia tapauksia ei ilmoiteta poliisille. Pankit ilmoittaisivat kuitenkin pyydettäessä mielellään kaikki petostapaukset poliisille, mutta asiasta keskustellaan jatkuvasti vastavuoroisen yhteistyön ja rajallisten resurssien hengessä.

Kansalaiset itse ilmoittavat kuitenkin usein tapauksista poliisille. Tämän voi tehdä helposti verkossa olevalla lomakkeella. Valitettavasti useimmista ilmoituksista puuttuu tietoa, jolloin tapauksia on mahdotonta tutkia.

6.3.2. Yksityisen sektorin rooli

Suomen poliisi ja kaikki suomalaiset kortteja myöntävät pankit ovat muodostaneet korttimaksujen riskienhallintaa käsittelevän ryhmän, joka kokoontuu kuusi kertaa vuodessa ja jonka puitteissa jaetaan asiaankuuluvaa tietoa. Kiireellisissä tapauksissa tämän luottamuksellisen verkoston puitteissa voidaan aloittaa sähköpostikeskustelu tai soittaa toiselle.

Suositukset kehittyneiden geoblokkaus- tai varoitusjärjestelmien käyttämiseksi ovat tavallisia. Poliisi ja pankkisektori vaihtavat keskenään tietoja rikosten tekotavoista mukauttaakseen maksuinfrastruktuuria ja tehdäkseen siitä turvallisemman.

Verkkomaksujen todentaminen edellyttää myös vähittäiskauppasektorin yhteistyötä. Jotkut myyjät edellyttävät kolmiovaiheista todentamista (pankkitunnuksilla), kun tehdään ostoksia luottokortilla. Tämä on kuitenkin aina vähittäismyyntiyrityksen päätös. Pankit suosittelevat omia tuotteitaan Verified By Visa ja MasterCard Secure Code, mutta vähittäismyyntiyritys päättää, käyttääkö se niitä. Poliisi ei erityisesti mainosta näitä palveluita.

Keskusrikospoliisissa ei ole tähän vastuualueeseen erikoistunutta henkilöstöä. Kaikkien poliisien on katsottu olevan yhdessä vastuussa näistä kysymyksistä omilla aloillaan. Näitä kysymyksiä pidetään hyvin tärkeinä ja etenkin johtotason henkilöt ovat investoineet paljon vaivaa ja aikaa hyvien yhteistyösuhteiden luomiseen yksityisen sektorin toimijoiden kanssa.

6.4. Päätelmät

- Suomessa ei ole monialaista kyberrikostorjunnan mekanismia, johon kuuluisi valtion virastoja ja yksityisiä toimijoita. Viranomaiset kuitenkin ilmoittivat, että kaikki asiaankuuluvat toimijat ovat osallistuneet moniin kyberharjoituksiin ja näistä kysymyksistä keskustellaan useissa työryhmissä. Vakavien kyberhyökkäysten (rikosten) käsittelystä vastaavat pääasiassa poliisi ja kyberturvallisuuskeskus/Viestintävirasto.

- Arviointiryhmä katsoo, että kyberrikoksiin liittyvä raportointimekanismi on rajallinen, eikä se ole pakollinen. Näin ollen poliisi ei saa tietoa kyberhyökkäyksistä, ellei se totea niitä itse. Kun kyberturvallisuuskeskuksen tietoon tulee tapauksia, jotka saattavat olla rikos, se kehottaa kansalaista tekemään ilmoituksen poliisille. Näin ollen suositellaan, että harkittaisiin aktiivisesti pakottavamman ilmoitusjärjestelmän käyttöönottoa erityisesti vakavien rikosten osalta (esim. kriittiset infrastruktuurit, pankkeihin kohdistuvat hyökkäykset).

- Kyberturvallisuuskeskus/Viestintävirasto lähettää varoituksia asiaankuuluville sidosryhmille. Kun arviointivierailu tehtiin, poliisin kanssa tehtävä yhteisymmärrysmuistio oli viimeistelyvaiheessa. Vierailun jälkeen arviointiryhmälle on ilmoitettu, että Viestintäviraston ja poliisin yhteistyötä koskeva yhteisymmärrysmuistio on allekirjoitettu lokakuussa 2016.[9]

- Suomen viranomaiset ilmoittivat, että Suomi on menestynyt hyvin Microsoftin verkkoluottamusarvioinneissa, minkä katsotaan johtuvan kahdesta syystä: (1) Viestintävirasto käyttää onnistuneesti automatisoituja ilmoitustyökaluja ja (2) maan koko, minkä vuoksi keskeisten toimijoiden välinen yhteydenpito on helppoa. Arviointiryhmä katsoo, että laatimalla viralliset puitteet varmistetaan nykyisten hyvien suhteiden kestävyys.

[9] Arviointiryhmä ei tutustunut muistion sisältöön.

- Lapsipornografian vastaisen työn osalta poliisi ilmoitti, että sillä on vaikeuksia pysyä ajan tasalla ulkomailta vastaanotettujen, lasten seksuaaliseen hyväksikäyttöön liittyvien tapausten kanssa. Näin ollen se aloittaa harvoin omia tutkintoja. Lapsipornografiatietokannan perustaminen on vielä kesken. Suomen keskusrikospoliisi on yhteydessä Tanskaan tietokannan perustamiseksi.

- Arviointiryhmä pani merkille, että kyberrikoskeskus ylläpitää ja päivittää listaa lapsipornografiaa sisältävistä sivustoista. Lista toimitetaan internetpalveluntarjoajille niiden asiakkaiden estämiseksi pääsemästä tällaisille sivustoille. Lapsipornografian levittämisen estotoimista annetun Suomen lain mukaan teleyrityksellä on oikeus tarjota palvelujaan niin, että niiden avulla ei ole pääsyä lapsipornosivustoihin. Viranomaiset kuitenkin ilmoittivat, että yksikään internetpalveluntarjoaja ei käytä listaa. Arviointiryhmä katsookin, että Suomen viranomaisten olisi neuvoteltava internetpalveluntarjoajien kanssa ja kannustettava niitä hyödyntämään tätä listaa.

- Arviointiryhmä on tyytyväinen suunnitelmiin perustaa tunnistetietokanta lapsipornografiamateriaalia varten. Ryhmä suosittelee, että tämän aloitteen pitkän tähtäimen kestävyyden varmistamiseksi tarvittavat resurssit määritellään ja niiden saatavuus taataan. Tämä on tarpeen etenkin siksi, että asianomaisia valokuvia tulevat usein tutkimaan sellaiset poliisin tutkijat, jotka eivät ole saaneet erityistä koulutusta. Yksityisen sektorin kanssa tehtävästä yhteistyöstä todettakoon, että maan koko ja keskeisten sidosryhmien väliset suhteet ovat edesauttaneet hyvän yhteistyöpohjan luomista myös paikallistasolla. eCIP-verkoston perustaminen on vain yksi esimerkki, jonka arviointiryhmä pani merkille paikan päälle tehdyn vierailun aikana.

- Arviointiryhmä pani merkille, että verkkopetosten torjuminen tuntuu olevan jakautunut pieniin yksittäisiin tapauksiin. Tämäntyyppisten tapausten yleiskuvasta ei tunnu olevan selkeää käsitystä. Joidenkin rikosten kohdalla tutkinnan avaaminen riippuu uhrin päätöksestä tehdä valitus. Tällainen toiminta saattaa antaa varsin tehottoman kuvan.

- Kyberrikollisuuden lisäksi mahdollinen erikoistumisen lisääminen saattaisi johtaa myös petoksiin keskittyvän yksikön perustamiseen syyttäjäviranomaisten puitteissa. Arviointiin osallistuneet oikeuslaitoksen edustajat toivat esille tällaisen toiveen.

7. KANSAINVÄLINEN YHTEISTYÖ

7.1. Yhteistyön EU:n virastojen kanssa

7.1.1. Muodolliset vaatimukset yhteistyön tekemiseksi Europolin/EC3:n, Eurojustin, ENISAn kanssa

Kansallisten viranomaisten ja Eurojustin väliselle yhteistyölle ei ole asetettu muodollisia vaatimuksia.

7.1.2. Europolin/EC3:n, Eurojustin, ENISAn kanssa tehdyn yhteistyön arviointi

Suomi pitää Europolin/EC3:n ja Eurojustin työtä erittäin arvokkaana kyberrikollisuuden torjunnan kannalta rikosten rajattoman luonteen vuoksi. Eurooppalaisilla virastoilla on tärkeä rooli tuoda jäsenvaltioita ja myös kolmansia maita yhteen helpottamalla strategisia ja operatiivisia tapaamisia ja tarjoamalla muita arvokkaita palvelujaan kyberrikollisuuden torjunnassa.

Europol on analysoinut valtavan määrän IP-osoitteita, chattipalstoja ja lokitiedostoja. EC3 on löytänyt yhteyksiä tekijöiden sekä tunnettujen rikollisryhmien ja -verkostojen välillä. Eurojust on koordinoinut yhteisten tutkintaryhmien työskentelyä, koordinoinut ja toiminut tukena toimintapäivien järjestämisessä sekä myöntänyt rahoitusta sähköisen todistusaineiston hyväksyttävyyden takaamiseksi kautta koko rikosprosessin. Europolin ja Eurojustin kokoukset lisäävät tutkinta- ja syyttäjäviranomaisten välistä keskinäistä luottamusta yli rajojen. Keskinäinen luottamus on tärkeää tiedustelutiedon vaihtamisen kannalta ja välttämätöntä tehokkaan oikeudellisen yhteistyön kannalta. Eurojustin tuella kasvokkain järjestetyt koordinointikokoukset ovat osoittautuneet luottamuksen rakentamisen kannalta tärkeiksi.

Rinnakkaiset tutkinnat ovat usein eri vaiheissa: esim. yhteisen tutkintaryhmän "Mozart" yhteydessä Suomen ja Alankomaiden oli odotettava syytteiden nostamisen kanssa ja vältettävä lehdistötiedotteiden antamista, ettei häirittäisi tutkintaa muissa jäsenvaltioissa. Toimien lykkääminen oli vaikea päätös, koska rikos jatkui ja uusia uhreja ilmaantui joka päivä, mutta lykkääminen onnistui Eurojustin koordinointikokousten ansiosta.

Kyberrikoskeskus toimii läheisessä yhteistyössä Europolin/EC3:n ja Eurojustin kanssa. ENISAn kanssa yhteistyötä on vain vähän. Myös poliisilaitokset tekevät jonkin verran yhteistyötä EC3:n kanssa. Suomessa uskotaan, että yhteistyötä voitaisiin parantaa lähettämällä kaikista kyberrikostapauksista automaattisesti enemmän tietoa EC3:lle. Näin parannettaisiin EC3:n tietopohjaa ja vastineeksi Suomeen saataisiin tietoa kotimaisista tapauksista, joilla on yhteyksiä muihin tapauksiin Euroopassa.

On perustettu kyberrikollisuuden alan pohjoismainen yhteistyöfoorumi, jonka puitteissa kyberrikoskeskusten johtajat tapaavat kaksi kertaa vuodessa ja keskustelevat yhteisistä päämääristä ja EMPACT-toimista, laativat yhteisiä kantoja, jakavat parhaita käytäntöjä sekä vaihtavat asiantuntemusta.

Suomen viranomaiset katsovat, että EC3:n olisi lisättävä analyysivoimavaroihin panostamista tai ainakin ylläpidettävä nykyinen taso. Sekä Suomen lainvalvontaviranomaiset että Suomen syyttäjäviranomaiset hyötyisivät siitä, jos Suomen poliisilla olisi oma yhteyshenkilö verkkorikollisuutta torjuvan yhteisen toiminnan työryhmässä (J-CAT). USA:n ja Yhdistyneen kuningaskunnan viranomaiset hyödyntävät EC3:a omien tapaustensa tutkinnassa. J-CATin johtokunta, jossa EU:n jäsenvaltiot eivät ole hyvin edustettuina, asettaa USA:n ja Yhdistyneen kuningaskunnan tapausten tutkinnan etusijalle. Vaarana on, että pienempien jäsenvaltioiden tutkimat tapaukset saavat tukea epätasaisesti. Suomalainen J-CAT -yhteyshenkilö parantaisi tiedonvaihtoa EC3:n suuntaan ja Suomen viranomaisiin päin sekä EC3:n ja Eurojustin kansallisen toimiston välillä.

Suomen oikeuslaitos hyötyisi "kybersihteeristöstä", joka ylläpitäisi kyberrikollisuudelle omistettua verkostoa. Sihteeristö toimisi laaja-alaisesti monien erilaisten rikostyyppien parissa ja syyttäjien tukena välittämällä ajantasaista tietoa ja asiantuntemusta. Kybersihteeristö/yksikkö merkitsisi sitä, että Eurojustilla olisi pysyvä talon sisäinen kyberasiantuntemus. Tällä hetkellä asiantuntemus riippuu liiaksi kansallisissa toimistoissa työskentelevistä henkilöistä, jotka ovat kiinnostuneita kyberkysymyksistä, ja heitä on myös liian vähän.

Yhteisen tutkintaryhmän rahoituksen hakumenettelyjen yksinkertaistaminen edelleen sekä lisäresurssien osoittaminen Eurojustin koordinointiroolia varten on ensisijaisen tärkeää kybertutkinnan/syytteeseenpanon kannalta, koska tämä tutkinta/syytteeseenpano on luonteeltaan usein monenvälistä ja jopa mannertenvälistä, johon osallistuu toimijoita julkiselta ja yksityiseltä sektorilta.

Suomi on osallistunut kolmeen kyberrikollisuuteen liittyvään yhteiseen tutkintaryhmään. Yhteisen tutkintaryhmän "Mozart" (Itävallan vetämä pankkien haittaohjelmiin liittyvä tutkinta) ja yhteisen tutkintaryhmän "Eurymus" (Suomen vetämä hakkerointiin, "swatting"-ilmiöön jne. liittyvä tutkinta) koordinointikokoukset järjestettiin Eurojustin tuella. Yksi yhteinen tukintaryhmä ei pyytänyt Eurojustilta tukea. Näissä kahdessa monenvälisessä tutkinnassa yhdeksi parhaaksi käytännöksi osoittautui kaksipäiväisten kokousten pitäminen Haagissa: aluksi operatiivisen tiedon vaihtaminen ja analysointi Europolissa ja sitten oikeudellisen tason koordinointi Eurojustissa.

Operaatio Blackshades oli monikansallinen Eurojustin koordinoima operaatio, johon osallistui yli 10 maata ja myös EU:n ulkopuolisia maita. Operaatiossa lainvalvontaviranomaiset ottivat tähtäimeen Blackshades- ohjelmiston ostajat. Yhteisten toimintapäivien aikana tehtiin satoja kotietsintöjä ja tusinoittain pidätyksiä kyseisen haittaohjelman ostajien tiloissa.

Maksukorttipetosten alalla Suomi on ollut osallisena monissa onnistuneesti ratkaistuissa Europolin/Eurojustin koordinoimissa tapauksissa. Esimerkkinä mainittakoon Suomessa vuonna 2011 pidätetty skimmaukseen syyllistynyt ryhmä, jolloin Saksa ja Romania aloittivat Suomessa kerätyn ja Europolille toimitetun tiedon pohjalta operaation Pandora-Storm koko järjestäytyneen rikollisryhmän hajottamiseksi. Prosessi kesti kaksi vuotta ja edellytti monien EU:n jäsenvaltioiden yhteistyötä, mutta tuloksena myös järjestön ylempiä johtajia saatiin pidätettyä.

7.1.3. Yhteisten tutkintaryhmien ja kyberpartioiden operatiivinen toiminta

Suomen viranomaisten mielestä yhteiset tutkintaryhmät ovat tehokas ja hyödyllinen yhteistyön väline, kun osallistuvilla mailla on yhteisiä etuja ja yhteistyön tavoite on riittävän selkeä. On kuitenkin hyvin valitettavaa, että USA:n viranomaiset eivät voi toimia yhteisen tutkintaryhmän jäsenenä, koska USA:n viranomaiset ovat hyvin tärkeänä vastapuolena lähes jokaisessa merkittävässä tutkinnassa.

Viranomaiset antoivat joitakin esimerkkejä yhteisiin tutkintaryhmiin perustuvasta hyvästä yhteistyöstä. Suomi oli kaikkiaan kuuden maan edustajista koostuneen yhteisen tutkintaryhmän "Mozart" jäsen. Yhteinen tutkintaryhmä "Mozart" perustettiin vuonna 2013 tutkimaan verkkopankkipetoksia. Yhteisen tutkintaryhmän kolmivuotisen tutkinnan tuloksena useita petoksentekijöitä, muulien houkuttelijoita ja rahamuuleja pidätettiin useissa maissa - sekä EU-maissa että EU:n ulkopuolisissa maissa. Tässä nimenomaisessa tutkinnassa EC3 osoittautui erinomaiseksi organisaatioksi analysoinnin ja koordinoinnin kannalta. EC3:n ansiosta kansallinen tutkintaryhmä saattoi keskittyä kansalliseen tutkintaan, samalla kun EC3 keräsi tietoa kokonaiskuvan muodostamiseksi, tunnisti kohteita ja paljasti tiedustelutiedon aukkoja. Yhteisen tutkintaryhmän perustamisen ansiosta tehtäviä voitiin jakaa ja resursseja pystyttiin käyttämään tehokkaammin. Suomen viranomaiset pystyivät hyödyntävään olemassa olevia yhteyksiä erittäin tehokkaasti koko yhteisen tutkintaryhmän eduksi. Tietoa ja todistusaineistoa kerättiin massiiviset määrät, mutta yhteisen tutkintaryhmän ansiosta niiden jakaminen oli helppoa. Yhteisen tutkintaryhmän "Mozart" toiminta päättyi maaliskuussa 2016, kun pääasialliset kohteet saatiin kiinni ja tutkintaryhmä ei enää ollut tarpeen.

Yhteinen tutkintaryhmä "Eurymus", jonka kohteena oli Euroopasta käsin toimiva hakkeriryhmä, oli arviointivierailun aikana edelleen toiminnassa, mutta sen toiminta päättyi syyskuussa 2016. EC3 on osallistunut myös tämän yhteisen tutkintaryhmän työhön ja avustanut analysointi- ja koordinointityössä.

Eurojust myönsi yhteisen tutkintaryhmän "Mozart" yhteistyölle erityistä rahoitusta. Yhteinen tutkintaryhmä "Eurymus" ei ole tarvinnut erityistä rahoitusta.

Monet poliisilaitokset ovat visuaalisesti läsnä kybertoimintaympäristössä. Helsingin poliisilaitos on erityisen taitava tässä. Sillä on ryhmä poliiseja, joka vastaa kokopäiväisesti näistä tehtävistä. Nettipoliisitoiminta on osaltaan poliisin ennalta estävää toimintaa. Nettipoliisit osallistuvat myös rikosten selvittelyyn ja tiedottavat tärkeistä ja ajankohtaisista asioista. Nettipoliisit voivat tuoda tärkeitä asioita esiin huumorilla höystettynä. Nettipoliisitoiminnalla halutaan myös madaltaa kynnystä ottaa yhteyttä poliisiin. Nettipoliisit eivät voi kuitenkaan käsitellä luottamuksellisia tai yksityisyyden suojan piiriin kuuluvia tietoja.

7.2. Suomen viranomaisten ja Interpolin välinen yhteistyö

Interpolin kanavia käytettiin yhteyshenkilön löytämiseen sellaisista EU:n ulkopuolisista maista, joihin Suomella ei ole yhteyksiä. Tämän jälkeen Interpolilta pyydettiin apua operatiivisen kokouksen järjestämisessä EU:n ulkopuolista maiden kanssa.

7.3. Yhteistyö kolmansien valtioiden kanssa

Suomella ei ole mitään erityistä kolmansiin maihin liittyvää toimintapolitiikkaa. Suomi on aktiivisesti pyrkinyt yhteistyöhön erityisesti naapurimaiden sekä Kiinan ja USA:n kanssa. Kolmansien maiden yhteystoimistot Europolissa ovat olleet hyödyllisiä yhteyksien luomisessa tiettyihin kolmansiin maihin, joihin Suomella ei ole vakiintuneita yhteyksiä, kuten Kolumbia ja Australia. Joissakin tapauksissa, kuten Blackshades-operaation yhteydessä kaksi vuotta sitten, Eurojustilla oli merkittävä rooli oikeudellisessa yhteistyössä USA:n ja Kanadan kaltaisten kolmansien maiden välisessä oikeudellisessa yhteistyössä. Suomen näkökulmasta Europolin/Eurojustin tärkein lisäarvo on niiden kyky löytää yhteyshenkilöitä ja luoda yhteyksiä.

Monenvälisissä tapauksissa yksi jäsenvaltio on voinut toimittaa keskinäistä oikeusapua koskevan pyynnön kolmannelle valtiolle ja jakaa sitten saamansa tiedot yhteisen tutkintaryhmän muiden jäsenten kanssa.

7.4. Yhteistyö yksityisen sektorin kanssa

Keskeiset taktiikat rajat ylittävän yhteistyön esteiden kiertämiseksi erityisesti verkossa tehtävien korttipetosten kohdalla ovat seuraavat:

1. Aktiivinen osallistuminen Europolin EMPACT-hankkeisiin ja -kokouksiin;
2. Rajat ylittävän tutkinnan aloittaminen mahdollisuuksien mukaan;
3. Käsiteltävänä olevia tapauksia koskevien tietojen lähettäminen Europolille, jotta eurooppalaisten järjestäytyneiden rikollisryhmien toimintaa voidaan analysoida tehokkaasti.

Suomen viranomaiset totesivat, että rajat ylittävää yhteistyötä on tehostettava. Syyttäjien käytössä olevia työkaluja ovat keskinäisen oikeusavun välineet, Euroopan oikeudellinen verkosto ja Eurojust. Epävirallisten kanavien, kuten sähköposti tai puhelin, kautta tehtävä nopea yhteistyö on osoittautunut toimivaksi joidenkin todettujen haasteiden selvittämiseksi ja sen avulla on voitu valmistella virallisia pyyntöjä.

Yksityisten yritysten rekistereiden toimittaminen suoraan lainvalvontayhteisölle tapahtuu vapaaehtoispohjalta ja ottaen suvereniteetin asianmukaisesti huomioon. Osa tarjoaa palvelunsa suoraan päätoimipaikastaan ja osa alueellisten edustajiensa kautta. Tämä yhteistyö aloitettiin vuonna 2006 ja Suomen viranomaiset eivät ole törmänneet mihinkään merkittäviin esteisiin. Jos yksityinen yritys ei tarjoa näitä palveluja, sovelletaan keskinäistä oikeusapumenettelyä.

7.5. Kansainvälisen yhteistyön välineet

7.5.1. Keskinäinen oikeusapu

Kyberrikollisuuden alalla keskinäistä oikeusapua annetaan Budapestin yleissopimuksen perusteella. Oikeusapua koskevia säännöksiä on myös kansainvälisestä oikeusavusta rikosasioissa annetussa laissa, joka muodostaa yleiset oikeuspuitteet, joiden nojalla Suomi voi toimeenpanna ja tehdä oikeusapupyyntöjä esimerkiksi ilman vastavuoroisuusvaatimusta. Lisäksi Suomi on allekirjoittanut tärkeimmät keskinäistä oikeusapua koskevat yleissopimukset, kuten keskinäistä oikeusapua rikosasioissa koskevan eurooppalaisen yleissopimuksen ja sen kaksi pöytäkirjaa.

Keskinäisen oikeusapupyynnön toimeenpano Suomessa ei edellytä kaksoisrangaistavuutta, paitsi jos on tarkoitus käyttää pakkokeinoja. Kaksoisrangaistavuuden periaate ei myöskään koske tapauksia, joissa pyydetään soveltamaan datan säilyttämismääräystä (kansainvälisestä oikeusavusta rikosasioissa annetun lain 15 §). Jos kaksoisrangaistavuutta kuitenkin edellytetään, sitä sovelletaan *in abstracto*.

Suomi on parhaillaan panemassa täytäntöön 3. huhtikuuta 2014 annettua direktiiviä 2014/41/EU rikosasioita koskevasta eurooppalaisesta tutkintamääräyksestä, jolla muutetaan EU:n jäsenvaltioiden välistä keskinäisen oikeusavun järjestelmää. Kun täytäntöönpaneva lainsäädäntö tulee voimaan, poliisiviranomaiset eivät enää voi antaa eurooppalaista tutkintamääräystä ilman oikeusviranomaisen vahvistusta. Syyttäjät on tarkoitus nimetä vahvistaviksi viranomaisiksi. Toimittamisen osalta on tarkoitus noudattaa joustavaa järjestelmää, jotta on mahdollista ottaa yhteyttä sekä määräyksen antaviin että määräyksen vahvistaviin viranomaisiin.

Muiden EU:n jäsenvaltioiden Suomelle esittämien esitutkintavaiheen keskinäistä oikeusapua koskevien pyyntöjen keskitettynä yhteyspisteenä toimii Keskusrikospoliisi (ks. Euroopan oikeudellinen kartasto). Keskusrikospoliisin kansainvälisten asioiden yksikkö päättää pyynnön täytäntöönpanosta ja välittää pyynnön tutkivalle yksikölle, ellei kansainvälisten asioiden yksikkö voi hoitaa asiaa itse.

EU:n ulkopuolisten maiden Suomelle esittämät keskinäistä oikeusapua koskevat pyynnöt lähetetään keskusviranomaisena toimivalle oikeusministeriölle (kansainvälisen oikeudenhoidon yksikkö). Interpolin välityksellä toimitettavat kiireelliset pyynnöt hyväksytään keskinäistä oikeusapua rikosasioissa koskevan eurooppalaisen yleissopimuksen mukaisesti (15 artiklan 5 kohta).

Lainvalvontaviranomaiset ja syyttäjät ovat velvollisia toimimaan läheisessä yhteistyössä ja lainvalvontaviranomaisten on noudatettava syyttäjän määräyksiä ja ohjeita esitutkintalain 5 luvussa säädetyn mukaisesti.

Suomen muille EU:n jäsenvaltioille esittämät keskinäistä oikeusapua koskevat pyynnöt lähetetään suoraan. Keskusrikospoliisi on tutkintaviranomaisten keskitetty kansallinen yhteyspiste. Keskusrikospoliisin kansainvälisten asioiden yksikkö tarkistaa pyynnöt ennen kuin ne käännetään ja lähetetään asianomaiselle maalle. Vaikka Euroopan oikeudellisessa kartastossa onkin ilmoitettu sähköpostiosoitteet ja faksinumerot, ongelmana on se, että Suomen kansalliset tietosuojasäännökset ovat tiukemmat kuin käytettävissä olevat tekniset mahdollisuudet nopeaa viestintää varten (lukuun ottamatta Interpolin I 24/7 -järjestelmää ja Europolin SIENA-sovellusta).

Syyttäjäviranomaiset ottavat suoraan yhteyttä muiden EU:n jäsenvaltioiden oikeusviranomaisiin. Euroopan oikeudelliseen verkostoon ja Eurojustiin ollaan yhteydessä vain silloin, kun tarvitaan niiden apua. Teknisesti ottaen myös tuomioistuimet ovat toimivaltaisia viranomaisia, mutta ne käyttävät hyvin harvoin oikeutta pyytää apua.

Pyynnöt koskevat usein Facebookin, Microsoftin, Googlen ja Skypen sekä Kikin palveluita. Muiden yritysten palveluja esiintyy vain harvoin. Näin ollen suurin osa keskinäistä oikeusapua koskevista pyynnöistä osoitetaan Yhdysvalloille ja Kanadalle. Suomen pyynnöt lähetetään siis keskusviranomaisen eli oikeusministeriön kautta. Sitä vastoin Suomessa on vain muutamia tässä yhteydessä kansainvälisesti merkittäviä yrityksiä, joiden palveluista muut valtiot esittävät keskinäistä oikeusapua koskevia pyyntöjä. Pyyntöjen lukumäärä on vielä vaatimaton.

Kyberrikoksiin liittyvistä keskinäistä oikeusapua koskevista pyynnöistä ei ole tilastoja. Kumpaankin suuntaan oikeusministeriön kautta toimitettavia pyyntöjä ei luetteloida rikostyypin mukaan, joten tästä ei voida antaa tietoa.

Keskinäistä oikeusapua koskevan pyynnön lähettämiseen ei sovelleta mitään erityisiä oikeudellisia ehtoja. Koska kyberrikollisuus on hyvin teknistä, yksikön on kuitenkin oltava selkeästi tunnistettavissa ja jäljitettävissä. Tietyissä tilanteissa tämä saattaa edellyttää teknisten yksityiskohtien toimittamista kokonaiskontekstista. Pyynnön esittävänä maana Suomi voi periaatteessa pyytää samoja tutkintatoimia kuin kotimaisissa tilanteissa.

Kun Suomi on pyynnön esittävä maa, se noudattaa oikeusapua koskevia EU:n/kansainvälisiä välineitä ja pyynnön täytäntöönpanevan valtion asettamia edellytyksiä. Suomi esimerkiksi noudattaa USA:n oikeusministeriön käytäntöjä ja suosituksia, jolloin USA:ssa sijaitsevaan palveluntarjoajaan voidaan ottaa yhteyttää suoraan, jos tarvitaan vain tilaajatietoja. Kun Suomi on täytäntöönpaneva valtio, pyynnöt olisi lähetettävä vain toimivaltaisten viranomaisten kautta (kun pyydetään muita kuin julkisesti saatavilla olevia sähköisessä muodossa olevia tietoja). Kun pyyntö tarkoittaa pakkokeinojen käyttämistä (kuten liikenne- tai sisältötietojen osalta), sovelletaan periaatteessa samaa menettelyä kuin kotimaisissa tapauksissa. On siis saatava tuomioistuimen päätös, mikäli sitä edellytetään vastaavassa kotimaisessa asiassa. Yleisesti ottaen Suomi kannattaa ajatusta siitä, että tutkitaan mahdollisuuksia soveltaa yksinkertaisempia menettelyjä, kun pyyntö koskee vain tilaajatietoja.

Koska Yhdysvallat on maa, jolle Suomi esittää eniten oikeusapupyyntöjä, FBI:n oikeusasiamiehen toimisto on hyvin tärkeä neuvonnasta vastaava yhteyspiste. Joskus otetaan suoraan yhteyttä USA:n oikeusministeriön virkailijaan, esimerkiksi sen selvittämiseksi, onko saatavilla olevaa tietoa riittävästi tarvittavan tiedon toimittamiseksi.

Syyttäjät hyödyntävät jo ennen keskinäistä oikeusapua koskevan pyynnön toimittamista suoritettavaa kuulemista. Jotkin maat kuten USA ovat pyytäneet saada keskinäistä oikeusapua koskevan pyynnön luonnoksen voidakseen ilmoittaa, onko pyyntöön tehtävä muutoksia/lisäyksiä, ennen kuin se toimitetaan virallisesti. Syyttäjien useimmiten käyttämä kanava on Eurojustin kansallinen toimisto. Euroopan oikeudellisen verkoston yhteyspisteverkko on myös käytettävissä.

Suomella on useiden maiden kanssa kahdenvälisiä sopimuksia rikosten torjunnasta.
Eniten käytetty sopimus on Suomen tasavallan hallituksen ja Viron tasavallan sopimus yhteistyöstä rikosten torjunnassa. Saatavilla ei ole tilastoja siitä, kuinka usein sopimusta on sovellettu kyberrikollisuuteen. Myös Liettuan, Latvian ja Ruotsin kanssa tehtävä yhteistyö toimii mutkattomasti.

Keskinäistä oikeusapua koskeva pyyntö on ainoa väline, jota käytetään todistusaineiston keräämisessä tapauksissa, joihin liittyy EU:n ulkopuolisia maita. Jos kyseiseen maahan ei ole ennestään yhteyksiä, Suomi pyrkii nopeuttamaan menettelyä lähettämällä keskinäistä oikeusapua koskevan pyynnön tai ennakkovaroituksen etukäteen.

7.5.2. Vastavuoroisen tunnustamisen välineet

Ei ole olemassa tilastoja siitä, missä määrin vastavuoroisen tunnustamisenvälineitä on käytetty kyberrikollisuuden alalla.

Keskusrikospoliisi on viimeisten seitsemän vuoden aikana käyttänyt eurooppalaista pidätysmääräystä kahdessa eri tapauksessa. Kaikkiaan kolme henkilöä on pidätetty ja luovutettu rikoksen johdosta Suomeen tutkintaa, syytteeseenpanoa ja oikeudenkäyntiä varten.
Vastavuoroista oikeusapua koskevia pyyntöjä käytetään kyberrikostutkinnassa usein, ja Keskusrikospoliisi on osallistunut moniin kyberrikostutkinnan yhteisiin tutkintaryhmiin.

7.5.3. Luovuttaminen / Rikoksen johdosta tapahtuva luovuttaminen

Kaikkiin rikoksiin, joista määrättävä enimmäisrangaistus on vähintään vuosi vankeutta, voidaan Suomessa soveltaa rikoksen johdosta tapahtuvaa luovuttamista ja luovuttamista.

Oikeusministeriö on toimivaltainen viranomainen, joka lähettää kolmansille maille osoitettavat rikoksen johdosta tapahtuvaa luovuttamista koskevat pyynnöt ja vastaanottaa niiden lähettämät pyynnöt. Rikoksen johdosta tapahtuvaa luovuttamista koskeva pyyntö lähetetään ainoastaan asiaa käsittelevän syyttäjän aloitteesta. Rikoksen johdosta tapahtuvaa luovuttamista pyytää ja siitä päättää aina oikeusministeriö. Kaikki lähetysmuodot sallitaan: pyynnöt voidaan toimittaa suoraan, diplomaattikanavien kautta tai Interpolin kautta.

Toimivaltainen viranomainen, joka antaa eurooppalaisen pidätysmääräyksen, on asiaa käsittelevä syyttäjä. Eurooppalaista pidätysmääräystä koskevat pyynnöt olisi lähetettävä Helsingin syyttäjänviraston syyttäjille. Eurooppalaisen ja pohjoismaisen pidätysmääräyksen menettely on kyberrikosten kohdalla tarkalleen sama eli sama kuin kaikkien muidenkin luovutuskelpoisten rikosten. Sama koskee rikoksen johdosta tapahtuvaa luovuttamista. Väliaikainen säilöönotto on mahdollista.

Suomessa rikoksen johdosta tapahtuvan luovuttamisen ja luovuttamisen menettelyt vaihtelevat pyynnön esittävästä maasta riippuen. Rikoksen johdosta tapahtuvan luovuttamisen / luovuttamisen oikeuskehys riippuu siitä, onko pyynnön esittävä maa joku EU:n jäsenvaltioista tai assosioituneista maista, jotka ovat panneet täytäntöön eurooppalaisesta pidätysmääräyksestä tehdyn puitepäätöksen, tai toinen Pohjoismaa. Näissä tapauksissa toimivaltainen viranomainen on Helsingin käräjäoikeus ja kaikissa muissa rikoksen johdosta tapahtuvan luovuttamisen tapauksissa oikeusministeriö. Tämän jaottelun vuoksi tapauksiin sovelletaan eri menettelyjä, mikä vaikuttaa sovellettavaan lainsäädäntöön ja voi myös vaikuttaa rikoksenjohdosta tapahtuvan luovuttamisen / luovuttamisen kestoon ja lopputulokseen.

Rikoksen johdosta tapahtuvaa luovuttamista tai luovuttamista koskevan pyynnön kiireellisyys ei vaikuta menettelyyn mitenkään, sillä Suomen lainsäädännössä ei ole erityistä "kiireellistä luovuttamismenettelyä". Pyynnön kohteena olevan henkilön etsintä ja kiinniottaminen hoidetaan kuitenkin tapauskohtaisesti ja siihen voidaan osoittaa sellaiset resurssit ja hoitaa asia siten, että menettely sujuu mahdollisimman nopeasti.

Saatavilla ei ole tilastoja keskimääräisistä vastausajoista rikoksen johdosta tapahtuvaa luovuttamista koskevaan pyyntöön.
Eurooppalaiseen tai pohjoismaiseen pidätysmääräykseen perustuva luovuttaminen tapahtuu suhteellisen nopeasti. Menettely kestää keskimäärin noin 20 päivää, kun luovutettava henkilö hyväksyy luovuttamisen, ja noin 30 päivää, kun hän ei hyväksy sitä.

Mitä vastausaikaan tulee, poliisi voi ryhtyä toimiin välittömästi, kun pyyntö toimitetaan Schengenin tietojärjestelmässä tehtävän kuulutuksen tai Interpolin tietokannassa julkaistavan kansainvälisen etsintäkuulutuksen muodossa. Jos rikoksen johdosta tapahtuvaa luovuttamista koskeva pyyntö toimitetaan oikeusministeriöön tai soveltuvissa tapauksissa syyttäjälle, ne pyytävät poliisia ryhtymään asianmukaisiin toimenpiteisiin ilman merkittävää viivettä.
Tässä yhteydessä sovelletaan samoja sääntöjä kuin kaikkiin muihinkin rikoksen johdosta tapahtuviin luovuttamisiin, ja näin ollen keskimääräinen vastausaika on sama eli enintään kaksi kuukautta.

Vain kolmessa tapauksessa henkilö on luovutettu kyberrikoksen johdosta: kaikki kolme luovutettiin Yhdysvaltoihin rikoksen johdosta tapahtuvaa luovuttamista koskevan kahdenvälisen sopimuksen perusteella. Kahdessa tapauksessa oli kyse internetissä harjoitetusta salakuljetettujen savukkeiden laittomasta kaupasta ja yhdessä oli kyse salahankkeesta tietokonepetoksia ja - väärinkäytöksiä koskevan Yhdysvaltojen lain rikkomiseksi (identiteettivarkaus).

Pohjoismaiden osalta on pohjoismainen pidätysmääräysjärjestely, jota käytetään myös luovuttamistarkoituksiin.

7.6. Päätelmät

- Suomen syyttäjälaitoksen koon, valtakunnansyyttäjän viraston operatiivisen roolin ja epämuodollisen sisäisen yhteistyömenetelmän ansiosta vaikuttaa siltä, että Eurojustin käyttäminen ja yhteistyö Eurojustin kanssa toimii tyydyttävällä tavalla apua tarvitsevien syyttäjien kannalta.

- Kyberrikostorjuntakeskus tekee läheistä yhteistyötä Europolin/EC3:n kanssa, mutta ENISAn kanssa yhteistyö oli hyvin vähäistä.

- Suomi pitää Europolin/EC3:n ja Eurojustin työtä erittäin arvokkaana kyberrikollisuuden torjunnan kannalta rikosten rajattoman luonteen vuoksi. Eurooppalaisilla virastoilla on tärkeä rooli tuoda jäsenvaltioita ja myös kolmansia maita yhteen helpottamalla strategisia ja operatiivisia tapaamisia ja tarjoamalla muita arvokkaita palvelujaan kyberrikollisuuden torjunnassa.

- Suomen viranomaiset hyödyntävät usein yhteisiä tutkintaryhmiä. Suomen kokemukset yhteisten tutkintaryhmien puitteissa tehtävästä yhteistyöstä vaikuttavat hyvin myönteisiltä ja sen avulla on saatu hyviä operatiivisia tuloksia monissa tutkinnoissa. Tämän välineen nauttima luottamus perustuu yhteisistä tutkintaryhmistä aikaisemmin saatuihin myönteisiin kokemuksiin ja siihen, että ryhmän perustaminen on hallinnollisesti kohtalaisen yksinkertaista. Arviointiryhmä katsoo, että tämä käytäntö voi toimia hyvänä esimerkkinä muille jäsenvaltioille.

- Keskusrikospoliisin jatkuva työskentely suhteiden parantamiseksi ja hyvien suhteiden ylläpitämiseksi kolmansiin maihin nähden on vaikuttavaa. Hyvin epämuodollinen tapa tehdä yhteistyötä on todennäköisesti erittäin tehokas perusta onnistuneelle kansainväliselle yhteistyölle.

- Lisäksi arviointiryhmä antaa kiitosta Suomen tavalle käsitellä ulkomaisia ja erityisesti yhdysvaltalaisia internetpalveluntarjoajia. Viestinnästä palveluntarjoajien edustajien kanssa vastaa yksi tietty yhteyspiste. Yhteyspistettä hoitava pätevä henkilö on myös ylläpitänyt hyviä suhteita palveluntarjoajien asiaankuuluvaan henkilöstöön, mikä auttaa luomaan vastavuoroisen luottamuksen henkeä ja mahdollistaa vapaaehtoisen yhteistyön.

- Palveluntarjoajia voidaan tällä hetkellä pyytää säilyttämään dataa 90 päivän ajan keskinäistä oikeusapua koskevaa pyyntöä odotettaessa, mutta Suomen viranomaisten mukaan ajanjaksoa olisi pidennettävä 180 päivään. Lisäksi voitaisiin luoda järjestelmä, jonka avulla datan saatavuus todettaisiin ennen keskinäistä oikeusapua koskevan pyynnön laatimista. Näin vältettäisiin tilanne, jossa keskinäistä oikeusapua koskevan pyynnön kohteena olevia tietoja ei ole olemassakaan. Vakiolomakkeet pyyntöjä varten helpottaisivat myös työtä.

- Arviointiryhmä totesi, että Pohjoismaiden välinen kansainvälinen yhteistyö rikosasioissa on erittäin hyvä esimerkki muille. Esimerkkejä yhteistyöstä ovat pohjoismainen pidätysmääräys, yhteyshenkilöiden jakaminen ja pohjoismainen koulutusfoorumi.

- Myös yhteistyö Itämeren alueen maiden, kuten Viron, Latvian, Liettuan ja Ruotsin kanssa on esimerkillistä. Tämän ryhmän edustajien ensimmäinen kokous pidettiin syyskuussa 2016. Arviointiryhmän mielestä naapurimaiden kanssa tehtävä yhteistyö on esimerkki parhaista käytännöistä.

8. KOULUTUS, TIETOISUUDEN LISÄÄMINEN JA ENNALTAEHKÄISY

8.1. Erikoistunut koulutus

Tuomarit

Oikeusministeriö tarjoaa tuomareille kyberrikollisuutta käsittelevää koulutusta. Muutaman viime vuoden aikana noin 150 tuomaria on saanut koulutusta tästä aiheesta. Tuomareiden ja oikeuslaitoksen henkilökunnan kouluttamisesta on tarkoitus tehdä systemaattisempaa. Koulutusta suunnittelemaan perustetaan uusi riippumaton elin, tuomarinkoulutuslautakunta. Koulutus järjestetään vaiheittain. Ensin on yksivuotinen peruskoulutusohjelma ja sitä seuraa työssäoppimisen avulla toteutettava koulutusohjelma. Ohjelman osallistujat valitaan koko maasta. Lakimiehet, joilla on vähintään kolmivuotinen työkokemus soveltuvista tehtävistä, voivat tulevaisuudessa hakea kolmivuotista asessorin virkaa. Asessori nimitetään määräajaksi, ja työ sisältää merkittävän määrän koulutusta.

Syyttäjät

Syyttäjien koulutus perustuu Suomessa uusille syyttäjille järjestettäviin startti-koulutusohjelmiin. Ohjelma kestää kuusi kuukautta ja koostuu pääosin verkkokursseista ja kahdesta koulutuspäivästä Syyttäjäakatemiassa. Tavoitteena on tarjota perustiedot syyttäjän työstä.

Syyttäjille, joilla on 1–3 vuotta työkokemusta, järjestetään kursseja, jotka koostuvat osittain verkkokursseista ja kaikkiaan 15 koulutuspäivästä (5 x 3 päivää) Syyttäjäakatemiassa. Kurssien tavoitteena on vahvistaa ja syventää syyttäjien yleistä ammattitaitoa, eivätkä ne sisällä yksittäisiin rikoksiin liittyvää koulutusta.

Kansainvälinen syyttäjäyhdistys (IAP) tarjoaa jäsenilleen kyberrikoksiin liittyviä verkkokursseja. Valtakunnansyyttäjän virasto, Suomen syyttäjäyhdistys ja jotkut yksittäiset syyttäjät ovat IAP:n jäseniä. IAP:n puitteissa toimii kyberrikosverkosto GPEN, joka muun toimintansa lisäksi järjestää kyberrikoksia käsitteleviä kursseja, esitelmiä ja verkkoseminaareja. Jotkut suomalaiset syyttäjät ovat osallistuneet näihin verkkoseminaareihin.

Vuosina 2010–2016 järjestettiin seuraavat kyberrikollisuuteen liittyvät kurssit:

- Tieto- ja viestintätekniikan ABC - perustiedot, kolme kaksipäiväistä kurssia (2010, 2011, 2012)
    - Kouluttajina keskusrikospoliisi ja valtakunnansyyttäjänvirasto
    - Rikostekninen tutkinta, todisteiden kerääminen, lapsipornografiaan liittyvät perusongelmat, verkkopetokset, luottokorttipetokset
- Sananvapauteen liittyvät rikokset verkossa - kaksipäiväinen kurssi (2011)
    - Kouluttajina keskusrikospoliisi, valtakunnansyyttäjänvirasto ja kihlakunnansyyttäjät
    - Kunnianloukkaus, lähdesuoja, uhkaukset verkossa, virtuaalipoliisi, pakkokeinot
- Tekijänoikeusrikokset - yksipäiväinen kurssi (2013)
    - Kouluttajina keskusrikospoliisi, kihlakunnansyyttäjä, käräjäoikeuden tuomari, tekijänoikeuden tiedotus- ja valvontakeskus ja puolustusasianajaja
    - Rikostekninen tutkinta, uhrien vaatimukset, Pirate Bay, vertaisverkot
- Luottokorttipetokset, puolipäiväinen kurssi (2014)
    - Kouluttajina keskusrikospoliisi, asiantuntijoita Nets Oy:stä
- Lapsipornografinen materiaali, kaksi kolmipäiväistä kurssia (2014, 2015)
    - Kouluttajina keskusrikospoliisi, paikallispoliisi, kihlakunnansyyttäjä ja poliisiammattikorkeakoulu
    - Rikokset, kuvien luokittelu, lapsipornografinen materiaali, verkostojen ominaispiirteet, esitutkintavaiheen yhteistyö, valtakunnansyyttäjän yksinomaiseen toimivaltaan kuuluvat tapaukset, sisällön levitysmenetelmät, sisällön tutkinta, tunnistenumerot, yhteyskäytännön teknisen osan laatu, poliisi todistajana, rikoksentekovälineen menetetyksi tuomitseminen

- Väestörekisterilain rikkomukset - kaksipäiväinen kurssi (2015)
    - Kouluttajina syyttäjälaitos, poliisi, tietosuojavaltuutetun toimisto, Tampereen kaupunki
    - Rikosten sisältö, rekisterinpitäjän toiminta ja vastuu, tietosuojavaltuutetun rooli
- Säännöllinen koulutus kihlakunnansyyttäjien toimipaikoissa (haluttaessa) - kolmituntinen peruskoulutus

Vuonna 2017 on tarkoitus järjestää kaikille syyttäjille kyberalan peruskurssi ja tapauspohjainen edistyneempi kurssi.

Poliisi

Suomen poliisiammattikorkeakoulun opetussuunnitelmaan on kuulunut kyberrikollisuuden liittyviä kursseja 2000-luvun alusta saakka. Näillä kursseilla on käsitelty monia kyberrikostorjuntaan liittyviä aiheita, kuten digitaaliforensiikkaa (eli tietokone-, verkko- ja mobiiliforensiikkaa), internetin käyttämistä rikostorjunnan ja kyberrikosten tutkinnan tukena sekä lasten seksuaaliseen hyväksikäyttöön liittyvät rikokset (mukaan lukien näitä rikoksia kuvaava materiaali). Kouluttajina on ollut pääasiassa keskusrikospoliisin ja muiden yksiköiden asiantuntijoita. Tämän lisäksi on järjestetty useita koulutustapahtumia erityisesti edistyneen digitaaliforensiikan alalla, joista ovat vastanneet kyberrikosyksiköiden asiantuntijat. Nämä koulutustapahtumat ovat useimmiten olleet digitaaliforensiikan alan yritysten tarjoamia kaupallisia kursseja. Kurssit ovat yleensä käsittäneet joko koulutusta kouluttavan yrityksen valmistamien yksittäisten välineiden käytössä tai näitä välineitä hyödyntävää yleisempää koulutusta. Koulutus on suurelta osin ollut kertaluontoista, ilman systemaattisia pitkän tähtäimen suuntaviivoja tai tavoitteita, ja koostunut erillisistä kursseista kokonaisen koulutusohjelman sijasta.

Poliisiammattikorkeakoulu tekee parhaillaan merkittäviä uudistuksia tarjoamaansa kyberrikostorjunnan alan koulutukseen. Muun muassa koulutusohjelmaa ollaan laatimassa, ulkoistettuja koulutuspalveluita harkitaan uudelleen, esimerkiksi ottamalla eri lainvalvontaviranomaisten vaihtelevat tarpeet huolellisemmin huomioon, kansainvälistä yhteistyötä kyberrikollisuuden alan koulutuksessa on lisätty ja kyberrikollisuuden alan koulutukseen ja tutkimukseen on osoitettu lisää henkilöstöresursseja.

Poliisiammattikoulussa on kerran vuosina 2009 - 2011 järjestetty rikostutkijoille tieto- ja viestintätekniikan erikoistumiskoulutus. Vastaavia opintoja ollaan kehittämässä ja ne on tarkoitus toteuttaa myöhemmin uudistetun opinto-ohjelman puitteissa. Suomesta tulee myös Nordic Computer Forensic Investigators -ohjelman jäsen; ohjelma koostuu koulutuskokonaisuuksista eri tasoilla.

Suomen poliisiammattikorkeakoulu vastaa poliisin tutkinto- ja jatkokoulutuksesta, koulutuskeskuksessa annettavasta täydennyskoulutuksesta sekä poliisialan tutkimus- ja kehittämistoiminnasta, kyberrikoksiin liittyvä koulutus ja tutkimus mukaan lukien. Kansallisten poliisilaitosten asiantuntijat tukevat poliisiammattikorkeakoulua seuraamalla kurssien vaatimuserittelyä ja laadunvarmistusta sekä osallistumalla opetukseen.

Poliisiammattikorkeakoulun koulutuskustannukset olivat vuonna 2015 noin 270 000 euroa. Poliisilaitosten itsensä kattamat koulutuskustannukset ovat oletettavasti ylittäneet 50 000 euroa maanlaajuisesti.

Kyberrikollisuuden alan peruskurssit kiinnostavat pääasiassa lainvalvontaviranomaisia ja kursseja tarjoavat näin ollen ensi sijassa niiden omat koulutusorganisaatiot, vaikka tämänkaltaisen koulutuksen kysyntä on viime aikoina lisääntynyt myös lainvalvontasektorin ulkopuolella.

Poliisiammattikorkeakoulu on viime aikoina lisännyt korkea-asteen koulutuslaitosten koulutusyhteistyön painotusta kyberrikollisuuden alan koulutuksessa. Tavoitteena on hyödyntää kunkin osapuolen vahvuuksia ja keskeistä tietotaitoa ja yhdistää ne toisiinsa sellaisten uusien kurssien kehittämiseksi, joista olisi hyötyä kaikille yhteistyön osapuolille.

Akateeminen maailma

Suomen poliisiammattikorkeakoulu tekee yhteistyötä yliopistojen ja korkeakoulujen kanssa sekä koulutuksessa että tutkimuksessa. Korkea-asteen koulutuksessa on tarjolla paljon kyberturvallisuuteen liittyviä kursseja, mutta niissä ei yleensä keskitytä pääasiassa kyberrikollisuuteen, vaikka aiheet voivatkin usein liittyä siihen. Kyberturvallisuus on myös tutkimuskohteena joissakin yliopistoissa.

EU:n virastot

CEPOL ja EC3 varaavat omilla kursseillaan paikkoja suomalaisille opiskelijoille käytäntöjensä mukaisesti. Suomalaisten opiskelijoiden lukumäärä on vuositasolla suhteellisen pieni. Suomen poliisilla on oma edustajansa Euroopan kyberrikollisuuden tutkinnan koulutusryhmässä (ECTEG). ECTEG:n kehittämiä kursseja ei ole vielä toteutettu Suomessa, mutta ne ovat keskeisessä asemassa Poliisiammattikorkeakoulun opetussuunnitelman uudistussuunnitelmassa.

Suomen viranomaisten näkemys

Olisi yksinkertaistettava oikeuslaitoksen mahdollisuuksia hyödyntää ENISAn ja CEPOLin koulutusta ja koulutusmateriaalia. Kaikkea kyberalan koulutusta ja EU:n rahoittamia akateemisia hankkeita olisi koordinoitava paremmin. Europolin, ENISAn, Eurojustin tai komission olisi ryhdyttävä johtamaan tätä työtä. On ilmeistä, että kyberalan koulutus on hajanaista ja tehotonta.

Ei ole olemassa minkäänlaista koulutuskokonaisuutta tai koulutusvastuuta. Oikeusministeriö on vastuussa tuomareista, valtakunnansyyttäjän virasto syyttäjistä ja lainvalvontaviranomaiset omasta henkilöstöstään. Yhteinen koulutus olisi toivottavaa erillisen koulutuksen lisäksi.

8.2. Tiedotustoimet

Viestintävirasto ylläpitää kansallista kyberturvallisuuden tilannekuvaa. Yksi viestintäviraston tavoitteista on lisätä kansalaisten ja yritysten tietoturvaosaamista muun muassa ohjeistuksen avulla. Viestintäviraston Kyberturvallisuuskeskus julkaisee myös varoituksia, "Tietoturva nyt!"-artikkeleja ja ilmoituksia haavoittuvuuksista.

Tämän lisäksi kyberturvallisuus ja kyberrikollisuuteen liittyvät uhat on huomioitu suomalaisessa perusasteen koulutuksessa. Perusasteen koulutuksen opetussuunnitelmassa kyberturvallisuus ja tietoturva on mainittu oppilaiden tietotekniikan taitojen parantamisen yhteydessä. Tavoitteena on laaja tietoisuus kyberrikollisuuteen liittyvistä uhkista. Tietotekniikan opetus alkaa ensimmäisellä luokalla. Oppilaita opetetaan toimimaan vastuullisesti ja turvallisesti. Heitä opetetaan ymmärtämään tieto- ja viestintäteknologioiden periaatteita ja alan tärkeimpiä käsitteitä. Oppilaita opastetaan käyttämään tietotekniikkaa vastuullisella, turvallisella ja ergonomisella tavalla. Oppilaat saavat perusasteen koulutuksen aikana kokemusta tietotekniikan käytöstä myös globaalissa kanssakäymisessä. He oppivat tietoisiksi sen merkityksestä, mahdollisuuksista ja riskeistä globaalissa toiminnassa. Kouluissa opetetaan myös, miten suojata itseään kyberrikollisuuden riskeiltä.

8.3. Ennaltaehkäisy

8.3.1. Kansallinen lainsäädäntö/toimintapolitiikka ja muut toimenpiteet

Poliisilain mukaisesti poliisin tehtävänä on rikosten ennalta estäminen, paljastaminen ja selvittäminen. Poliisin ennalta estävän toiminnan strategia hyväksyttiin vuonna 2014. Strategiassa korostetaan viranomaisten ja muiden sidosryhmien välisen yhteistyön merkitystä. Rikosten ennaltaehkäisy perustuu tietojohtoiseen poliisitoimintaan. Strategian kaksi avainseikkaa ovat parempi tilannetietoisuus ja painopisteiden valinta.

Sosiaalisen median leviäminen on vaikuttanut Suomen poliisin työhön. Poliisit toimivat sosiaalisessa mediassa. Viestinnällään he pyrkivät palvelemaan kansalaisia joka päivä, jopa virka-ajan jälkeen, lisäämään poliisin näkyvyyttä, tarjoamaan kanssakäymisen mahdollisuuksia ja näin ehkäisemään rikoksia sekä tietenkin jakamaan yleisluontoista tietoa ja neuvontaa sekä edistämään kansalaisten yhteiskunnallista osallistumista.

Huhtikuussa 2016 hyväksyttiin uusi ja ajantasainen kansallinen väkivaltaisen radikalisoitumisen ja ekstremismin ennaltaehkäisyn toimenpideohjelma.

Keskusrikospoliisi on viestinyt suurelle yleisölle tiedostusvälineiden ja Kyberrikoskeskuksen sekä keskuksen päällikön Twitter-tilien kautta parantaakseen yleisön tietoisuutta ja varoittaakseen ajankohtaisista ilmiöistä. Useille intressiryhmille (yksityisen sektorin yritykset, rahoitussektori ja yliopisto-opiskelijat) on lisäksi pidetty monia esityksiä.

Tähän saakka ennaltaehkäisevä toiminta on ollut tapauskohtaista, eikä sitä ole suunniteltu etukäteen. Tällä alueella on tunnustettua parantamisen tarvetta ja tulevaisuudessa ennaltaehkäisevää työtä painotetaan enemmän ja sitä tehdään suunnitellusti yhteistyössä Kyberturvallisuuskeskuksen kanssa.

Kyberturvallisuuskeskus on julkaissut varoituksia, "Tietoturva nyt!"-artikkeleja ja ilmoituksia haavoittuvuuksista. Lisäksi se työskentelee useiden sidosryhmien kanssa tietoturvaloukkausten ehkäisemiseksi ja ratkaisemiseksi.

8.3.2. Julkisen ja yksityisen sektorin kumppanuus

Sisäministeriöllä on yksityisen sektorin kanssa toimiva työryhmä, jonka tavoitteena on ehkäistä yrityksiin kohdistuvia rikoksia kyberrikollisuus mukaan lukien.

Suomessa katsotaan, että yhteistyö yksityisen sektorin kanssa on tärkeää kyberrikollisuuden ehkäisyssä. Yksityisen sektorin kanssa ei kuitenkaan ole minkäänlaisia kiinteitä rakenteita, yhteisymmärrysmuistioita tai muita sopimuksia, paitsi jos käytetään yksityisen sektorin palveluja ja/tai tuotteita. Operatiivinen yhteistyö perustuu keskinäiseen luottamukseen ja toteutetaan tapauskohtaisesti.

8.4. Päätelmät

- Oikeusministeriö vastaa tuomareiden koulutuksesta. Vaikka Suomen viranomaiset ilmoittivat, että 150 tuomaria on saanut koulutusta tästä aiheesta, kyseiset aloitteet vaikuttavat sattumanvaraisilta ja vain perustiedot antavilta. Maassa ei ole jäsenneltyä ja tulevaisuuteen suuntautuvaa koulutusohjelmaa, jolla pyrittäisiin parantamaan tuomareiden tietoja ja taitoja kyberrikollisuuden alalla. Arviointiryhmä katsoo, että tarvittaisiin enemmän erikoistumista sen varmistamiseksi, että kaikilla tuomareilla olisi tietyt tiedot kyberrikollisuudesta.

- Syyttäjien osalta arviointiryhmä totesi, että erikoistuminen oli rajallista. Lisäksi on tehty suunnitelmia syyttäjien kouluttamiseksi perustietojen osalta. Arviointiryhmän tapaamien syyttäjien mielestä on selvää, että kaikki syyttäjät ja tuomarit tarvitsevat lisää koulutusta kyberrikollisuuteen liittyvissä kysymyksissä.

- Poliisin osalta erikoistuneiden tutkijoiden tiedot ovat erinomaisella tasolla. Ei kuitenkaan pitäisi aliarvioida alueellisten poliisilaitosten kykyä ratkaista kyberrikoksia. Suurin haaste on ollut, että tähän mennessä tarjottu koulutus on osoitettu ainoastaan asiantuntijoille, ja arviointiryhmän mielestä koulutusmahdollisuuksien tulisi kattaa myös alueelliset poliisilaitokset.

- Poliisin koulutus on järjestetty tapauskohtaisesti. Poliisiammattikorkeakoululla ei ole vielä järjestelmällistä lähestymistapaa poliisin tutkijoiden kouluttamiseen. Poliisiammattikorkeakoulussa järjestettävillä kursseilla opettavat luennoitsijat tulevat pääasiassa Keskusrikospoliisista. Sisäisen turvallisuuden rahaston rahoittamaan hankkeeseen kuului koulutustarpeita ja koulutuksen täytäntöönpanoa koskenut kyselytutkimus. Asiantuntijatiedot ja työkalujen saatavuus riippuvat pääasiassa yksittäisten poliisilaitosten aloitteellisuudesta. Näin ollen Poliisiammattikorkeakoulu voisi harkita järjestelmällisen koulutuksen tarjoamista erikoistuneille poliiseille hyödyntämällä ulkoisten lähteiden, kuten ECTEG ja CEPOL, kautta jo olemassa olevia koulutusmahdollisuuksia.

- Merkittävä Suomessa todettu ongelma on puuttuva pitkän tähtäimen suunnitelma, jolla varmistettaisiin poliisille, syyttäjille ja tuomareille annettavan kyberalan koulutuksen jatkuvuus. Keskusrikospoliisissa tapahtuvan erikoistumisen lisäksi on parannettava yleistä tietotasoa kyberrikollisuudesta oikeuslaitoksessa ja poliisien keskuudessa. Arviointiryhmä pani merkille yritykset sisällyttää syyttäjien koulutukseen kyberrikollisuutta käsitteleviä kursseja, mutta kaikkien edellä mainittujen ammattiryhmien osalta suositellaan kuitenkin järjestelmällisempää lähestymistapaa.

- Ennaltaehkäisyn osalta Viestintävirastolla ei ole omia, suurelle yleisölle suunnattuja ehkäisykampanjoita. Itse asiassa vaikuttaa siltä, että suurelle yleisölle suunnattujen ehkäisykampanjoiden osalta puuttuu keskitetty lähestymistapa tai yksi koordinoiva elin. Vaikuttaa siltä, että suurelle yleisölle on suunnattu hyvin rajallisia ja satunnaisia ehkäisykampanjoita ja muita toimia lasten hyväksikäytöstä ja yleisemmin internetin turvallisuudesta. Arviointiryhmä katsoo, että Kyberrikoskeskuksella, Kyberturvallisuuskeskuksella, kyberturvallisuusyrityksillä ja kansalaisjärjestöillä olisi mahdollisuus täyttää tämä aukko yhdistämällä resurssejaan ja toteuttaa näkyviä ja kestäviä kampanjoita, joilla pyrittäisiin lisäämään suuren yleisön tietoisuutta tästä ilmiöstä.

- Yleisön vähäinen tietoisuus ja puutteelliset tiedot kyberuhkista sekä alan oikeudelliset säännökset ovat tärkeimmät syyt harkita vastuun siirtämistä uudelleen niille tietotekniikka-alan yhteisöille, jotka tekevät yhteistyötä suoraan poliisin kanssa. Lisäksi olisi harkittava nuorille suunnattujen erityisesti lapsipornografiaan liittyvien ehkäisykampanjoiden järjestämistä, jotta voidaan estää heitä joutumasta kyberrikosten uhreiksi.

9. LOPPUSANAT JA SUOSITUKSET

9.1. Suomen viranomaisten ehdotukset

Suomen viranomaiset katsovat, että niiden resurssien olisi oltava oikeasuhteisia riskeihin ja haasteisiin nähden. Vaikka Suomi ei olekaan kyberrikollisuuden keskeisiä kohdemaita, sillä on samat haasteet kuin suuremman riskin mailla, iskujen tiheys ja lukumäärä vain on pienempi.

Kyberrikoskeskus arvioi, että mitä valmiuksiin tulee (ennaltaehkäisy, tilannetietoisuus), kyberrikollisuuden torjuntaan on osoitettu enemmän asiantuntemusta ja ammattitaitoisia resursseja kaikkialla Suomessa.

Kansallisessa kyberturvallisuusstrategiassa, aivan kuin EU:n strategiassakin painotetaan vain lyhyesti syyttäjien ja tuomareiden kouluttamisen tärkeyttä. Suomen toimeenpano-ohjelma ei sisällä toimia, jotka liittyisivät koulutukseen oikeuslaitoksen sisällä taikka valmiuksien kehittämiseen. Rikosoikeudellisen vastuun pitäisi olla yksi kyberturvallisuusstrategian perusteista. Nykyinen strategia käsittelee tiedustelutiedon keräämistä ja rikosten ennaltaehkäisyä sekä julkisen ja yksityisen sektorin yhteistyötä ja poliisin resursseja. Nämä eivät yksin riitä saattamaan rikollisia oikeuden eteen.

Toisaalta poliisin läsnäolo sosiaalisessa mediassa on uusi ja kehittyvä ilmiö. Se on osa kaikkea poliisitoimintaa, ennaltaehkäisevä toiminta mukaan lukien. Viestinnällään he pyrkivät palvelemaan kansalaisia joka päivä, jopa virka-ajan jälkeen, lisäämään poliisin näkyvyyttä, tarjoamaan kanssakäymisen mahdollisuuksia ja näin ehkäisemään rikoksia sekä tietenkin jakamaan yleisluontoista tietoa ja neuvontaa sekä edistämään kansalaisten yhteiskunnallista osallistumista.

9.2. Suositukset

Suomen arviointiin osallistunut asiantuntijaryhmä pystyi onnistuneesti arvioimaan Suomen järjestelmän puitepäätöksen ja direktiivien käytännön täytäntöönpanon ja toiminnan osalta.

Suomen viranomaisten olisi ryhdyttävä jatkotoimiin tässä raportissa annettujen suositusten pohjalta 18 kuukauden kuluessa arvioinnista ja raportoitava edistymisestä yleisten kysymysten, ml. arvioinnin työryhmälle (GENVAL).

Arviointiryhmä katsoi tarpeelliseksi esittää joitakin ehdotuksia Suomen viranomaisille. Erilaisten hyvien käytäntöjen pohjalta esitetään myös niihin liittyviä suosituksia EU:lle, sen toimielimille ja virastoille, erityisesti Europolille.

9.2.1. Suositukset Suomen viranomaisille

1. Suomen kyberturvallisuusstrategiaa olisi tarpeen tarkastella uudelleen, jotta se vastaisi nykyisiä tarpeita; strategiaan olisi esimerkiksi sisällytettävä oikeuslaitoksen tarpeet ja puututtava alan toimijoiden ilmi tuomaan vaikutelmaan arvostuksen puuttumisesta strategisella tasolla. (vrt. 3.1, 3.2 ja 3.5)

2. Olisi saatava luotettavia ja kattavia tilastotietoja kyberrikostorjuntaan osallistuvilta eri sidosryhmiltä (kuten CERT-FI, Viestintävirasto, poliisi ja oikeuslaitos) kyberrikollisuuden keskeisten suuntausten määrittelemiseksi ja selkeämmän kuvan muodostamiseksi kyberrikollisuuden kehityksestä Suomessa. (vrt. 3.3 ja 3.5)

3. Suomen viranomaisia olisi kannustettava lisäämään kyberrikostorjuntaan erikoistuneiden syyttäjien lukumäärää. (vrt. 4.1.1 ja 4.5)

4. Suomen viranomaisia olisi kannustettava lisäämään tietoa ja parantamaan osaamista alue- ja paikallistasolla, erityisesti määräämällä kaikkien poliisilaitosten yleisen, ei-teknisen henkilöstön kouluttamisesta yhtenäisen ja johdonmukaisen näkökannan varmistamiseksi kyberrikollisuuteen liittyvissä kysymyksissä. (vrt. 4.2 ja 4.5)

5. Suomen viranomaisia kannustetaan tarkastelemaan uudelleen pakkokeinojen voimassa olevaa valikoimaa, jota voidaan soveltaa kyberrikostapauksissa; valikoimaa olisi pyrittävä laajentamaan kyberrikostutkinnan erityisluonteen huomioon ottaen. (vrt. 5.2.1 ja 5.5)

6. Olisi harkittava poliisi-ilmoitusta koskevan velvollisuuden tehostamista, esimerkiksi ottamalla käyttöön pakottavampi ilmoitusjärjestelmä erityisesti keskeisiin infrastruktuureihin tai pankkeihin kohdistuviin hyökkäyksiin liittyvien vakavien rikosten osalta. (vrt. 6.1.2, 6.3.1 ja 6.4)

7. Suomen viranomaisia olisi kannustettava saattamaan päätökseen lapsipornografiamateriaalin tiivistetyn tietokannan perustaminen. (vrt. 6.2.1 ja 6.4)

8. Olisi keskusteltava internetpalveluntarjoajien kanssa ja kannustettava niitä hyödyntämään luetteloa lapsipornografiaa sisältävistä sivustoista. (vrt. 6.2.2 ja 6.4)

9. Oikeuslaitoksen yleistietoja kyberrikoksista olisi parannettava lisäämällä tuomareiden ja syyttäjien koulutusmahdollisuuksia ja järjestämällä enemmän kyberrikollisuutta käsitteleviä tapahtumia tai koulutuskokonaisuuksia. (vrt. 8.1 ja 8.4)

10. Olisi tehostettava ehkäisy- ja tiedotuskampanjoita sekä muita yleisölle suunnattuja toimia verkossa tapahtuvan lasten hyväksikäytön ja internetin turvallisuuden aloilla. (vrt. 8.2, 8.3.1 ja 8.4)

9.2.2. Suositukset Euroopan unionille, sen toimielimille tai virastoille ja muille jäsenvaltioille

1. Jäsenvaltioiden olisi harkittava Suomen keskusrikospoliisin hallinnoimaa budjettia vastaavan erillisen budjetin perustamista kyberrikollisuuden alan koulutusta ja poliisilaitosten laitteistoja varten sekä kansallisella että aluetasolla. (vrt. 3.4 ja 3.5)

2. Jäsenvaltioiden olisi harkittava järjestelmää, jossa paikallisia poliisilaitoksia avustetaan lievempien kyberrikosten tukinnassa sen sijaan, että tutkinta siirretään kokonaan keskustasolle, tiedon jakamisen ja valmiuksien kehittämisen helpottamiseksi paikallistasolla Suomen keskusrikospoliisin käytäntöjä vastaavasti. (vrt. 4.2 ja 4.5)

3. Jäsenvaltioille suositellaan hyvien yhteistyöfoorumien perustamista yksityisen sektorin kanssa Suomen eCIP-verkoston tapaan. (vrt. 6.2.4 ja 6.4)

4. Jäsenvaltioille suositellaan yhteisten tutkintaryhmien käyttämistä kyberrikosten rajatylittävässä tutkinnassa, koska Suomen esimerkki osoittaa tämän kehyksen tarjoavan monia mahdollisuuksia. (vrt. 7.1.2 ja 7.6)

5. Jäsenvaltioille suositellaan yhden yhteyspisteen perustamista poliisille kansainvälisiä palveluntarjoajia varten, jotta voidaan varmistaa kansallisten viranomaisten ja yksityisten yritysten välinen luottamukseen ja keskinäiseen kunnioitukseen perustuva sujuva viestintä Suomen poliisin esimerkin mukaisesti. (vrt. 7.5.1 ja 7.6)

6. Jäsenvaltioille suositellaan yhteistyön tehostamista naapurimaiden kanssa kyberrikostorjunnan toimintapolitiikan vahvistamiseksi samaan tapaan kuin Suomi toimii Pohjoismaiden ja Baltian maiden kanssa. (vrt. 7.5.3 ja 7.6)

7. EU:n toimielimiä olisi kannustettava etsimään ratkaisuja oikeudellisiin ongelmiin, jotka liittyvät lainkäyttövaltaan ja sähköisen todistusaineiston keräämiseen pilvipalveluista. (vrt. 5.5)

8. EU:n toimielinten ja virastojen olisi tutkittava tapoja ottaa kolmansia maita mukaan yhteisissä tutkintaryhmissä tehtävään yhteistyöhön. (vrt. 7.3)

ANNEX A: PROGRAMME FOR THE ON-SITE VISIT AND PERSONS INTERVIEWED/MET

6 - 9 September 2016

Monday, 5 September 2016

Arrival of GENVAL experts, Helsinki - Vantaa airport

Tuesday, 6 September 2016

National Bureau of Investigation, Jokiniemenkuja 4, Vantaa.

Participants:
Ministry of the Interior, National Police Board, National Bureau of Investigation Ministry of Justice and Office of the Prosecutor General.

9.30.	**Welcoming of the Evaluation Team**
9.45.	**National structures. General matters**
11.00.	**Coffee break**
11.15.	**Cyber attacks**
12.30.	**Lunch**
13.30.	**Online card fraud**
14.30.	**Prevention of cybercrime**
16.30.	**End of the meeting**

Transfer to hotel

Wednesday, 7 September 2016

Office of the Prosecutor General, Albertinkatu 25 A, Helsinki

Participants:
Office of the Prosecutor General, Ministry of Justice, Ministry of the Interior, National Bureau of Investigation.

Representative of the Save the Children takes part in session "Offences related to child sexual abuse online Child pornography".

9.00. **Finnish prosecution service**

9.30. **Mutual recognition**

10.15. **Coffee break**

10.30. **Offences related to child sexual abuse online and child pornography**

11.30. **Training and awareness raising activities**
Investigation and prosecution

12.30. **Lunch**

Ministry of Justice, Eteläesplanadi 10, Helsinki

Participants:

Ministry of Justice, Office of the Prosecutor General, Ministry of the Interior

13.30. **Criminalisation. Procedural issues**

14.30. **Coffee break**

14.45. **Jurisdiction**

Mutual legal assistance. Surrender / Extradition

16.30. **End of the meeting**

Thursday, 8 September 2016

Ministry of Transport and Communications, Eteläesplanadi 16, Helsinki

Participants:

Ministry of Transport and Communications, Finnish Communications Regulatory Authority (National Cyber Security Centre Finland (NCSC-FI)), Ministry of the Interior, Ministry of Justice, National Bureau of Investigation.

9.30. - 10.00. **Prevention of cybercrime in the field of the Ministry of Transport and Communications**

10.00. - 10.45. **National Cyber Security Centre Finland, tasks and role**

10.45. - 11.00. **Coffee break**

11.00. - 11.30. **Cooperation with private sector**

11.30. - 12.30. **Discussion**

12.30. - 14.00. **Lunch**

Ministry of the Interior, Erottajankatu 2, Helsinki

Room: 238

14.00. - 15.00. **Cyber Security in Finland**

End of the meeting

Friday, 9 September 2016

Ministry of the Interior, Erottajankatu 2, Helsinki

Room: 238

Participants:

Ministry of the Interior, National Police Board, National Bureau of Investigation Ministry of Justice and Office of the Prosecutor General.

9.00. **Wrap-up-session**

12.00. **Close of the meeting**

ANNEX B: PERSONS INTERVIEWED/MET

Meetings on 6 September 2016

Venue: National Bureau of Investigation,

Person interviewed/met	**Organisation represented**
Mika Junninen	Senior planning officer Ministry of Justice
Tuuli Eerolainen	Legal Counsellor Office of the Prosecutor General
Hannele Taavila	Counsellor for Legislative Affairs Ministry of the Interior
Tiina Ferm	Counsellor for Legislative Affairs Ministry of the Interior
Jenni Juslen	Senior Adviser National Police Board
Timo Laine	Chief Superintendent National Police Board
Timo Piiroinen	Head of Cybercrime Center, National Bureau of Investigation
Tero Muurman	Detective Chief Inspector ,National Bureau of Investigation
Ville Elenius,	Senior Detective Constable, National Bureau of Investigation
Lars Henriksson	Detective Superintendent National Bureau of Investigation

Meetings on 7 September 2016

Venue: Office of the Prosecutor General

Person interviewed/met	Organisation represented
Tuuli Eerolainen	Legal Counsellor Office of the Prosecutor General
Harri Tiesmaa	Legal Counsellor Office of the Prosecutor General
Pia Mäenpää	District prosecutor , Prosecutor's Office of Eastern Finland
Juho Lehtimäki	District prosecutor, Prosecutor's office of Itä-Uusimaa
Tero Toiviainen	Senior Specialist Police University College
Sari Sarani	Detective Chief Inspector, National Bureau of Investigation
Veera Uusoksa	Manager, Children and Digital Media Save the Children Finland

Venue: Ministry of Justice

Person interviewed/met	Organisation represented
Mika Junninen	Senior planning officer, Ministry of Justice
Merja Norros	Ministerial Counsellor, Ministry of Justice
Janne Kanerva	Counsellor of Legislation, Ministry of Justice
Anu Juho	Judge, Helsinki District Court
Tuuli Eerolainen	Legal Counsellor Office of the Prosecutor General

Person interviewed/met	Organisation represented
Lars Henriksson	Detective Superintendent National Bureau of Investigation

Meetings on 8 September 2016

Venue: Ministry of Transport and Communication

Person interviewed/met	Organisation represented
Timo Kievari	Director of Safety and Security unit, Ministry of Transport and Communication
Jarna Hartikainen	Head of Cooperation and Situation Awareness, National Cyber Security Centre Finland
Jyrki Pennanen	Private Sector - Fingrid Plc
Tomi Pitkänen	Private Sector - Neste Plc
Tiina Ferm	Counsellor for Legislative Affairs Ministry of the Interior

Venue: Ministry of Interior

Person interviewed/met	Organisation represented
Yrjö Benson	Special Adviser, Ministry of Finance
Tuuli Eerolainen	Legal Counsellor Office of the Prosecutor General
Hannele Taavila	Counsellor for Legislative Affairs Ministry of the Interior

Meetings on 9 September 2016

Venue: Ministry of Interior

Person interviewed/met	**Organisation represented**
Hannele Taavila	Counsellor for Legislative Affairs Ministry of the Interior
Juhani Korhonen	Ministerial Counsellor , Ministry of Justice
Mika Junninen	Senior planning officer Ministry of Justice
Timo Piiroinen	Head of Cybercrime Center, National Bureau of Investigation
Tuuli Eerolainen	Legal Counsellor Office of the Prosecutor General

ANNEX C: LIST OF ABBREVIATIONS/GLOSSARY OF TERMS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	FINNISH OR ACRONYM IN ORIGINAL LANGUAGE	FINNISH OR ACRONYM IN ORIGINAL LANGUAGE	ENGLISH
AFTA	*AFTA*		Association of Finnish Travel Agents
CAM	*CAM*		child abuse material
CRM	*CRM*		Card Risk Management
CC	*CC*		the Finnish Criminal Code
FICORA	*FICORA*		The Finnish Communications Regulatory Authority
FISIC	*FISIC*		the Finnish Safer Internet Centre
MoU	*MoU*		Memorandum of Understanding
NBI	*NBI*		The National Bureau of Investigations
NCSA-FI	*NCSA-FI*		The National Communications Security Authority
NCSC-FI	*NCSC-FI*		The National Cyber Security Centre Finland
OCG	*OCG*		organised crime groups
SAKARI	*SAKARI*		Case management system
SMAL	*SMAL*		The Association of Finnish Travel Agents

Annex D: Finnish Legislation

Illegal access to information system

Offences in question are *computer break-in* and *aggravated computer break-in* (Chapter 38, Section 8 and Section 8(a) of the Criminal Code). Regardless of the English language names of these offences it's not necessary that the offence is committed by using a computer or is directed to a computer (see definitions below).

Chapter 38, Section 8 - Computer break-in

(1) A person who by using an access code that does not belong to him or her or by otherwise breaking a protection unlawfully hacks into an information system where information or data is processed, stored or transmitted electronically or in a corresponding technical manner, or into a separately protected part of such a system, shall be sentenced for a *computer break-in* to a fine or to imprisonment for at most two years.

(2) Also a person who, without hacking into the information system or a part thereof,

(1) by using a special technical device or

(2) otherwise by by-passing the system of protection in a technical manner, by using a vulnerability in the information system or otherwise by evidently fraudulent means

unlawfully obtains information or data contained in an information system referred to in subsection 1, shall be sentenced for a computer break-in.

Chapter 38, Section 8(a) - Aggravated computer break-in

(1) If the computer break-in is committed

(1) as part of an organised criminal group referred to in Chapter 6, section 5, paragraph 2 or

(2) in a particularly methodical manner

and the computer break-in is aggravated also when assessed as a whole, the offender shall be sentenced for *an aggravated computer break-in* to a fine or to imprisonment for at most three years.

Chapter 6, Section 5 - Grounds increasing the punishment

(1) The following are grounds for increasing the punishment:

(1) the methodical nature of the criminal activity,

(2) commission of the offence as part of the activity of an organised criminal group,

(3) commission of the offence for remuneration,

(4) commission of the offence for a motive based on race, skin colour, birth status, national or ethnic origin, religion or belief, sexual orientation or disability or another corresponding grounds, and

(5) the criminal history of the offender, if the relation between it and the new offence, due to the similarity between the offences or otherwise, shows that the offender is apparently heedless of the prohibitions and commands of the law.

(2) "Organized criminal group" refers to a structured association of three or more persons, existing for a period of time and acting in concert with the aim of committing offences that are punishable by a maximum sentence of imprisonment for at least four years, or offences referred to in Chapter 11, section 10 or Chapter 15, section 9.

Chapter 6, Section 6 – Grounds reducing the punishment

The following are grounds for reducing the punishment:

(1) significant pressure, threat or a similar influence that has affected the commission of the offence,

(2) strong empathy or an exceptional and sudden temptation that has led to the offence, the exceptionally great contribution of the injured party or a corresponding circumstance that has been conducive to decreasing the capability of the offender to conform to the law,

(3) reconciliation between the offender and the injured person, other attempts of the offender to prevent or remove the effects of the offence or his or her attempt to further the clearing up of the offence, and

(4) the grounds mentioned in section 8(1) and (3).

Chapter 6, Section 7 – Grounds mitigating the punishment

In addition to what is provided above in section 6, grounds mitigating the punishment that are also to be taken into consideration are

(1) another consequence to the offender of the offence or of the sentence**,**

(2) the advanced age, poor health or other personal circumstances of the offender, and

(3) a considerably long period that has passed since the commission of the offence, if the punishment that accords with established practice would for these reason lead to an unreasonable or exceptionally detrimental result.

Chapter 6, Section 8 – Mitigation of the penal latitude

(1) The sentence is determined in accordance with a mitigated penal latitude if

  (1) the offender has committed the offence below the age of 18 years,

  (2) the offence has remained an attempt,

  (3) the offender is convicted as an abettor in an offence, through application of the provisions of Chapter 5, section 6, or his or her complicity in the offence is otherwise clearly less than that of other accomplices,

  (4) the offence has been committed in circumstances that closely resemble those that lead to the application of grounds for exemption from liability, or

  (5) there are special reasons for this pursuant to section 6 or 7 or on other exceptional grounds, mentioned in the sentence.

(2) In determining the punishment pursuant to subsection 1, at most three fourths of the maximum sentence of imprisonment or fine and at least the minimum sentence provided for the offence may be imposed on the offender. If the offence is punishable by life imprisonment, the maximum punishment is instead twelve years of imprisonment and the minimum punishment is two years of imprisonment.

(3) What is provided in subsection 2 also applies in determining the sentence for a person who committed an offence in a state of diminished responsibility. However, diminished responsibility does not affect the applicable maximum punishment.

(4) If the maximum punishment for the offence is imprisonment for a fixed period, the court may in cases referred to in this section impose a fine as the punishment instead of imprisonment, if there are especially weighty reasons for this.

Chapter 6, Section 8(a) – Mitigation of the penal latitude on the basis of confession

(1) The sentence is determined in accordance with a mitigated penal latitude if the offender has contributed to the clarification of his or her offence as provided in Chapter 1, sections 10 and 10(a) and Chapter 5(b) of the Criminal Procedure Act (689/1997) and in Chapter 3, section 10(a) of the Criminal Investigation Act (805/2011).

(2) In determining the punishment on the basis of subsection 1, at the most two thirds of the maximum length of imprisonment or of the maximum amount of the fine may be imposed, and at the least the minimum amount that is provided for the type of punishment. If the maximum punishment that is provided for the offence is imprisonment for a determinate period, the court may impose a fine instead of imprisonment, if there are special reasons for this.

(3) The judgment shall note not only the punishment imposed but also what punishment the court would have imposed without the benefit of what is provided above.

The penalty scale of computer break-in runs from a fine to imprisonment for at most two years and the penalty scale of aggravated computer break-in runs from a fine to imprisonment for at most three years. The minimum and maximum level of fine is defined in Chapter 2(a), Section 1(1) of the Criminal Code. A fine shall be passed as day fines, the minimum number of which is one and the maximum number is 120. The minimum level of imprisonment is defined in Chapter 2(c), Section 2(2) of the Criminal Code. A sentence of fixed-term imprisonment is imposed for at least fourteen days.

Chapter 6, Section 9 of the Criminal Code contains provisions on the choice between conditional and unconditional imprisonment:

Illegal system interference

Chapter 38, Section 5 – Interference with communications

(1) A person who by tampering with the operation of a device used in postal, telecommunications or radio traffic, by maliciously transmitting interfering messages over radio or telecommunications channels or in another comparable manner unlawfully prevents or interferes with postal, telecommunications or radio traffic, shall be sentenced for *interference with communications* to a fine or to imprisonment for at most two years.

Chapter 38, Section 6 - Aggravated interference with communications

(1) If in the interference with communications

(1) the offender commits the offence by making use of his or her position in the service of an institution referred to in the Telecommunications Act, a cable operator referred to in the Cable Transmission Act (307/1987) or a public broadcasting institution, or his or her other special position of trust,

(2) the offence prevents or interferes with the radio transmission of distress signals or such other telecommunications or radio transmissions that are made in order to protect human life,

(3) the offence is committed as part of activity that has to a significant degree affected information systems through the use of a device, computer program or set of programming instructions referred to in Chapter 34, section 9(a), paragraph 1, subparagraph (a) or a password, access code or other corresponding information referred to in subparagraph (b),

(4) the offence is committed as part of an organised criminal group referred to in Chapter 6, section 5, paragraph 2,

(5) the offence causes particularly serious impediment or economic loss, or

(6) the offence is directed at a device, information system or communications, the damaging of which could endanger the energy supply, general health care, national defence, the administration of justice or another function that is important to society and that is comparable to these,

and the interference with communications is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated interference with communications* to imprisonment for at least four months and at most five years.

Chapter 38, Section 7 - Petty interference with communications

(1) If the interference with communications, in view of its nature or extent or the other circumstances of the offence, is of minor significance when assessed as a whole, the offender shall be sentenced for *petty interference with communications* to a fine.

Chapter 38, Section 7(a) – Interference in an information system

(1) A person who in order to cause detriment or economic loss to another, by entering, transferring, damaging, altering or deleting data or in another comparable manner unlawfully prevents the operation of an information system or causes serious interference in it shall be sentenced for *interference in an information system* to a fine or to imprisonment for at most two years.

Chapter 38, Section 7(b) – Aggravated interference in an information system

(1) If in the interference in an information system

(1) particularly significant detriment or economic loss is caused,

(2) the offence is committed in a particularly methodical manner,

(3) the offence is committed as part of activity that has to a significant degree affected information systems through the use of a device, computer program or set of programming instructions referred to in Chapter 34, section 9(a), paragraph 1, subparagraph (a) or a password, access code or other corresponding information referred to in subparagraph (b),

(4) the offence is committed as part of an organised criminal group referred to in Chapter 6, section 5, paragraph 2,

(5) the offence is directed at an information system, the damaging of which could endanger the energy supply, general health care, national defence, the administration of justice or another function that is important to society and that is comparable to these,

and the interference in an information system is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated interference in an information system* to imprisonment for at least four months and at most five years.

Illegal data interference

Offences in question are *Damage to data, aggravated damage to data and petty damage to data* (Chapter 35, Sections 3(a) to 3(c) of the Criminal Code).

Chapter 35, Section 3(a) – Damage to data

(1) A person who, in order to cause damage to another, unlawfully destroys, demolishes, hides, damages, alters, renders unusable or conceals data recorded on an information device or another recording or data in an information system, shall be sentenced for *damage to data* to a fine or to imprisonment for at most two years.

Chapter 35, Section 3(b) – Aggravated damage to data

(1) If the damage to data

(1) causes particularly serious harm or economic loss,

(2) is committed as part of the activity of an organised criminal group referred to in Chapter 6, section 5, subsection 2,

(3) is committed as part of activity that has affected a significant amount of information systems through the use of a device, computer program or set of programming instructions referred to in Chapter 34, section 9(a), paragraph 1, subparagraph (a) or a password, access code or other corresponding information referred to in subparagraph (b), or

(4) is directed at an information system, the damaging of which could endanger the energy supply, general health care, national defence, the administration of justice or another function that is important to society and that is comparable to these,

and the damage to data is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated damage to data* to imprisonment for at least four months and at most five years.

Chapter 35, Section 3(c) - Petty damage to data

If the damage to data, when assessed as a whole, with due consideration to the minor significance of the damage or the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for *petty damage to data* to a fine.

Illegal interception of computer data

Offences in question are *message interception* and *aggravated message interception* (Chapter 38, Sections 3 and 4 of the Criminal Code).

Relevant are also Chapter 38, Section 8(2) of the Criminal Code concerning computer break-in and Section 8(a) concerning aggravated computer break-in related to offences defined in Section 8(2). These offences are already covered by answers connected with illegal access to information system, see above.

Chapter 38, Section 3 - Message interception

(1) A person who unlawfully

(1) opens a letter or another closed communication addressed to another or by hacking obtains information on the contents of an electronic or other technically recorded message which is protected from outsiders, or

(2) obtains information on the contents of a telephone call, telegram, transmission of text, images or data, or another comparable telemessage transmitted by telecommunications or an information system or on the transmission or reception of such a message

shall be sentenced for *message interception* to a fine or to imprisonment for at most two years.

Chapter 38, Section 4 - Aggravated message interception

(1) If in the message interception

(1) the offender commits the offence by making use of his or her position in the service of a telecommunications company, as referred in the Act on the Protection of Electronic Messages (516/2004) or his or her other special position of trust,

(2) the offender commits the offence by making use of a computer program or special technical device designed or altered for such purpose, or otherwise especially methodically, or

(3) the message that is the object of the offence has an especially confidential content or the act constitutes a grave violation of the protection of privacy and the message interception is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated message interception* to imprisonment for at most three years.

Misuse of devices

The offences in question are *endangerment of data processing* and *an offence involving a system for accessing protected services* (Chapter 34, Section 9(a) and Chapter 38, Section 8 (b) of the Criminal Code.

Chapter 34, Section 9(a) – Endangerment of data processing

A person who, in order to impede or damage data processing or the functioning or security of an information system or telecommunications system,

(1) imports, obtains for use, manufactures, sells or otherwise disseminates or makes available
   (a) a device or computer program or set of programming instructions designed or altered to endanger or damage data processing or the functioning of an information system or telecommunications system or to break or disable the technical security of electronic communications or the security of an information system, or
   (b) an information system password, access code or other corresponding information belonging to another, or

(2) disseminates or makes available instructions for the production of a computer program or set of programming instructions referred to in paragraph (1), shall be sentenced, unless an equally severe or more severe penalty for the act is provided elsewhere in the law, for *endangerment of data processing* to a fine or to imprisonment for at most two years.

Chapter 38, Section 8(b) — Offence involving a system for accessing protected services

A person who, in violation of the prohibition laid down in section 269, subsection 2 of the Information Society Code (917/2014), for commercial purposes or so that the act is conducive to causing considerable detriment or loss to a provider of protected services, produces, imports, offers for sale, rents out or distributes a system for accessing protected services, or advertises, installs or maintains the same, shall, unless a more severe or equally severe penalty is provided elsewhere in law for the act, be sentenced for an *offence involving a system for accessing protected services* to a fine or to imprisonment for at most one year.

Computer-related child pornography offences

Offences in question are *distribution of a sexually offensive picture, aggravated distribution of a sexually offensive picture depicting a child* and *possession of a sexually offensive picture depicting a child* (Chapter 17, Sections 18, 18(a) and 19 of the Criminal Code). These provisions are general, covering all kind of ways to commit these offences.

Chapter 17, Section 18 - Distribution of a sexually offensive picture

(1) A person who manufactures, offers for sale or for rent or otherwise offers or makes available, keeps available, exports, imports to or transports through Finland to another country, or otherwise distributes pictures or visual recordings that factually or realistically depict

(1) a child,

(2) violence or

(3) bestiality

shall be sentenced for *distribution of a sexually offensive picture* to a fine or imprisonment for at most two years.

---

(4) A child is defined as a person below the age of eighteen years and a person whose age cannot be determined but whom there is justifiable reason to assume is below the age of eighteen years. The picture or visual recording is deemed factual in the manner referred to in subsection 1, paragraph 1, if it has been produced in a situation in which a child has actually been the object of sexually offensive conduct and realistic, if it resembles in a misleading manner a picture or a visual recording produced through photography or in another corresponding manner of a situation in which a child is the object of sexually offensive conduct.

The definitions of the terms factual and realistic apply correspondingly in the cases referred to in subsection 1, paragraphs 2 and 3.

Chapter 17, Section 18(a) - Aggravated distribution of a sexually offensive picture depicting a child

(1) If, in the distribution of a sexually offensive picture depicting a child

(1) the child is particularly young,

(2) the picture also depicts severe violence or particularly humiliating treatment of the child,

(3) the offence is committed in a particularly methodical manner or

(4) the offence has been committed within the framework of an organized criminal group referred to in Chapter 6, section 5, subsection 2 and the offence is aggravated also when assessed as whole, the offender shall be sentenced for *aggravated distribution of a sexually offensive picture depicting a child* to imprisonment for at least four months and at most six years.

Chapter 17, Section 19 - Possession of a sexually offensive picture depicting a child

(1) A person who unlawfully has in his or her possession a picture or visual recording which depicts a child in the sexually offensive manner referred to in section 18, shall be sentenced for *possession of a sexually offensive picture depicting a child* to a fine or to imprisonment for at most one year.

(2) A person who in return for payment or otherwise by agreement has obtained access to a picture or visual recording referred to in subsection 1 so that it is available to him or her on a computer or another technical device without being recorded on the device shall also be sentenced for possession of a sexually offensive picture depicting a child.

Computer-related solicitation of children

The offence in question is *Solicitation of a child for sexual purposes* (Chapter 20, Section 8(b) of the Criminal Code). Provisions are general, covering all kind of ways to commit these offences.

Chapter 20, Section 8(b) – Solicitation of a child for sexual purposes

(1) A person who suggests a meeting or other contact with a child so that it is apparent from the contents of the suggestion or otherwise from the circumstances that the intent of the person is to prepare sexually offensive pictures or visual recordings of the child in the manner referred to in Chapter 17, section 18, subsection 1, or to subject the child to the offence referred to in section 6 or 7 of this Chapter, shall be sentenced for *solicitation of a child for sexual purposes* to a fine or to imprisonment for at most one year.

(2) Unless a more severe sentence is provided in law for the act, also a person who solicits a person below the age of eighteen years to engage in sexual intercourse or in another sexual act in the manner referred to in section 8(a) or to perform in a sexually offensive organized performance shall be sentenced for solicitation of a child for sexual purposes.

Computer-related fraud

Offences in question are *fraud, aggravated fraud, petty fraud, means of payment fraud, aggravated means of payment fraud* and *petty means of payment fraud* (Chapter 36, Sections 1 to 3 of the Criminal Code and Chapter 37, Sections 8 to 10 of the Criminal Code).

Chapter 36, Section 1 - Fraud

(1) A person who, in order to obtain unlawful financial benefit for himself or herself or another or in order to harm another, deceives another or takes advantage of an error of another so as to have this person do something or refrain from doing something and in this way causes economic loss to the deceived person or to the person over whose benefits this person is able to dispose, shall be sentenced for *fraud* to a fine or to imprisonment for at most two years.

(2) Also a person who, with the intention referred to in subsection 1, by entering, altering, destroying or deleting data or by otherwise interfering with the operation of a data system, falsifies the end result of data processing and in this way causes another person economic loss, shall be sentenced for fraud.

Chapter 36, Section 2 - Aggravated fraud

(1) If the fraud

(1) involves the seeking of considerable benefit,

(2) causes considerable or particularly significant loss,

(3) is committed by taking advantage of special confidence based on a position of trust or

(4) is committed by taking advantage of a special weakness or other insecure position of another and the fraud is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated fraud* to imprisonment for at least four months and at most four years.

Chapter 36, Section 3 - Petty fraud

If the fraud, when assessed as a whole, with due consideration to the benefit sought or the amount of loss caused or to the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for *petty fraud* to a fine.

Chapter 37, Section 8 - Means of payment fraud

(1) A person who, in order to obtain unlawful economic benefit for himself or herself or another

(1) uses a means of payment without the permission of the lawful holder, in excess of his or her right based on such permission, or otherwise without lawful right, or

(2) transfers a means of payment or means of payment form to another in order to have it used without lawful right shall be sentenced for *means of payment fraud* to a fine or to imprisonment for at most two years.

(2) Also a person who, by overdrawing his or her account or exceeding the agreed maximum credit limit, misuses a means of payment referred to in subsection 1 and in this way causes economic loss to another shall be sentenced for means of payment fraud, unless when using the means of payment he or she intended to compensate the loss without delay.

Chapter 37, Section 9 - Aggravated means of payment fraud

If in the means of payment fraud

(1) considerable or particularly significant loss is caused or

(2) the offender has, for the commission of the offence, made or had made means of payment forms from which the means of payment used in the offence was prepared, or if the offence is otherwise committed in a particularly methodical manner and the means of payment fraud is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated means of payment fraud* to imprisonment for at least four months and at most four years.

Chapter 37, Section 10 - Petty means of payment fraud

If the means of payment fraud, when assessed as a whole, with due consideration to the amount of benefit sought or the amount of loss caused or to the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for *petty means of payment fraud* to a fine.

Computer-related forgery

Offences in question are *forgery, aggravated forgery* and *petty forgery* (Chapter 33, Sections 1 to 3 of the Criminal Code). These provisions are general, covering all kind of ways to commit these offences.

Chapter 33, Section 1 - Forgery

(1) A person who prepares a false document or other item or falsifies such a document or item in order for it to be used as misleading evidence or uses a false or falsified item as misleading evidence shall be sentenced for *forgery* to a fine or imprisonment for at most two years.

Chapter 33, Section 2 - Aggravated forgery

If in the forgery

(1) the item that is the object of the offence is an archival document stored by an authority or a general register kept by an authority and such a document or register is important from a general point of view, or the item otherwise has a particularly significant probative value, or

(2) the offender uses technical equipment procured for the commission of forgery offences or otherwise acts in a particularly methodical manner and the forgery is aggravated also when assessed as a whole, the offender shall be sentenced for *aggravated forgery* to imprisonment for at least four months and at most four years.

Chapter 33, Section 3 - Petty forgery

If the forgery, when assessed as a whole, with due consideration to the nature of the item or to the other circumstances connected with the offence, is to be deemed petty, the offender shall be sentenced for *petty forgery* to a fine.