EUROOPAN KOMISSIO

Bryssel 28.3.2012
COM(2012) 140 final

KOMISSION TIEDONANTO NEUVOSTOLLE JA EUROOPAN PARLAMENTILLE

Rikostentorjunta digitaaliaikana: Euroopan verkkorikostorjuntakeskuksen perustaminen

KOMISSION TIEDONANTO NEUVOSTOLLE JA EUROOPAN PARLAMENTILLE

Rikostentorjunta digitaaliaikana: Euroopan verkkorikostorjuntakeskuksen perustaminen

1. JOHDANTO: RAJATYLITTÄVÄN RIKOLLISUUDEN TORJUNTA EU:SSA

Internetistä on tullut olennainen osa yhteiskuntaa ja taloutta. Nuorista eurooppalaisista 80 prosenttia on yhteydessä toisiinsa ja koko maailmaan internetin sosiaalisten verkostojen välityksellä[1], ja verkkokaupassa liikkuu rahaa maailmanlaajuisesti vuosittain noin 8 biljoonaa Yhdysvaltain dollaria[2]. Mutta sitä mukaa kuin yhä suurempi osa jokapäiväistä elämäämme ja liiketoimintaa siirtyy verkkoon, myös verkkorikollisuus yleistyy – koko maailmassa yli miljoona ihmistä joutuu verkkorikollisuuden uhriksi päivittäin[3]. Verkossa tehdään monenlaisia rikoksia: varastettuja luottokortteja kaupitellaan yhdellä eurolla, henkilötietoja varastetaan, lapsia käytetään seksuaalisesti hyväksi ja instituutioiden ja infrastruktuurin toiminta pyritään lamauttamaan vakavien verkkohyökkäysten avulla.

Verkkorikollisuus aiheuttaa yhteiskunnalle huomattavat kustannukset. Tuoreen raportin mukaan verkkorikollisuuden uhrit menettävät vuosittain noin 388 miljardia Yhdysvaltain dollaria maailmanlaajuisesti. Tällä perusteella verkkorikollisuus tuottaisi enemmän kuin maailmanlaajuinen marihuanan, kokaiinin ja heroiinin kauppa yhteensä[4]. Tällaisiin tietoihin on toki suhtauduttava varoen, koska verkkorikollisuuden erilaisten määritelmien perusteella voidaan päätyä hyvin erilaisiin kustannusarvioihin. Yleisesti ollaan kuitenkin yhtä mieltä siitä, että verkkorikollisuus on erittäin tuottoisaa ja vähäriskistä rikollista toimintaa, joka yleistyy jatkuvasti ja muuttuu yhä haitallisemmaksi. Aikana, jolloin talouskasvun edistäminen on välttämätöntä, on myös äärimmäisen tärkeää tehostaa verkkorikollisuuden torjuntaa, jotta voidaan säilyttää kansalaisten ja yritysten luottamus verkossa tapahtuvaan viestintään ja kaupankäyntiin. Näin voidaan myös tukea Eurooppa 2020 -strategiassa[5] ja Euroopan digitaalistrategiassa[6] vahvistettuja kasvutavoitteita.

Internetin vapaus on viime vuosina tapahtuneen digitaalisen vallankumouksen keskeinen taustatekijä. Avoin internet ei tunne valtioiden rajoja eikä sillä ole yhtä ainoaa maailmanlaajuista hallintojärjestelmää. Samalla kun edistämme ja suojaamme tätä verkkotoiminnan vapautta EU:n perusoikeuskirjan mukaisesti, meidän on myös suojeltava kansalaisia järjestäytyneiltä rikollisryhmiltä, jotka pyrkivät käyttämään tätä avoimuutta omiin tarkoituksiinsa. Verkkorikollisuus on rikollisuuden lajeista rajattomin, minkä vuoksi sen torjunta edellyttää lainvalvontaviranomaisilta koordinoituja toimia ja yhteistyötä yli valtioiden rajojen sekä julkisten että yksityisten sidosryhmien kanssa. Tässä EU voi tuoda toimintaan huomattavaa lisäarvoa.

---

1 Eurostat, *Internet Access and Use*, 14.12.2010.

2 McKinsey Global Institute: *Internet matters: The Net's sweeping impact on growth, jobs, and prosperity*. Raportti toukokuulta 2011, konsultoitu 8.2.2012.

3 *Norton Cybercrime Report 2011*, Symantec, 7.9.2011, konsultoitu 6.1.2012.

4 Ks. edellä.

5 *Eurooppa 2020: Älykkään, kestävän ja osallistavan kasvun strategia*, KOM(2010) 2020, 3.3.2010.

6 Euroopan digitaalistrategia, KOM(2010) 245 lopullinen, 26.8.2010.

Euroopan unioni on jo toteuttanut erilaisia aloitteita verkkorikollisuuden torjumiseksi. Näitä ovat vuonna 2011 hyväksytty direktiivi lasten seksuaalisen hyväksikäytön ja seksuaalisen riiston sekä lapsipornografian torjumisesta ja direktiiviehdotus tietojärjestelmiin kohdistuvista hyökkäyksistä, jonka painopisteenä on verkkorikollisuuden välineiden ja erityisesti bottiverkkojen[7] käytön rankaiseminen; ehdotus on määrä hyväksyä vuonna 2012. Europol on jo tehostanut toimintaansa verkkorikollisuuden torjumiseksi. Sillä oli keskeinen asema muun muassa hiljattain toteutetussa ”Operation Rescue” -operaatiossa, jonka yhteydessä poliisi pidätti 184 henkilöä epäiltynä lapsiin kohdistuvista seksuaalirikoksista ja totesi yli 200 lapsen joutuneen hyväksikäytön uhriksi. Kyseessä oli yksi laajimmista tämäntyyppisistä lainvalvontaviranomaisten tutkimuksista koko maailmassa. Europolin tutkijat onnistuivat murtamaan verkoston yhteyspisteenä toimineen palvelimen turvasuojauksen ja siten paljastamaan epäiltyjen rikoksentekijöiden henkilöllisyyden ja toiminnan.

Verkkorikollisuuden torjunta on EU:n toiminnassa tärkeä painopisteala, ja tärkein siihen liittyvä oikeudellinen väline on tietoverkkorikollisuutta koskeva Euroopan neuvoston yleissopimus[8]. Tietoverkkorikollisuuden torjunta mainitaan myös järjestäytynyttä ja vakavaa kansainvälistä rikollisuutta koskevassa EU:n toimintapoliittisessa syklissä[9], minkä lisäksi se on olennainen osa pyrkimyksiä kehittää kokonaisvaltainen EU:n strategia verkkoturvallisuuden lujittamiseksi. EU on myös tehnyt tiivistä yhteistyötä kansainvälisten kumppaneiden kanssa esimerkiksi verkkoturvallisuutta ja verkkorikollisuutta käsittelevässä EU:n ja Yhdysvaltojen työryhmässä.

Näistä edistysaskelista huolimatta verkkorikollisuuden tehokkaan tutkinnan ja rikoksentekijöiden syytteeseenpanon tiellä on Euroopassa vielä monia esteitä, kuten oikeudenkäyttöalueiden rajat, riittämätön valmius tiedustelutietojen jakamiseen, verkkorikosten tekijöiden jäljittämiseen liittyvät tekniset vaikeudet, vaihtelevat valmiudet suorittaa rikostutkintaa ja rikosteknisiä tutkimuksia, koulutetun henkilöstön riittämättömyys ja muiden verkkoturvallisuudesta vastaavien sidosryhmien kanssa tehtävän yhteistyön hajanaisuus. Vakautusvälineen avulla EU voi puuttua myös nopeasti kehittyviin valtioiden rajat ylittäviin uhkiin, jotka liittyvät tietoverkkorikollisuuteen kehitysmaissa ja siirtymävaiheen maissa, missä valmiudet torjua tällaista järjestäytynyttä rikollisuutta ovat usein puutteelliset.

Vastauksena näihin haasteisiin komissio ilmoitti perustavansa Euroopan verkkorikostorjuntakeskuksen, joka on yksi sisäisen turvallisuuden strategian painopisteitä[10].

---

7 Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi tietojärjestelmiin kohdistuvista hyökkäyksistä, KOM(2010) 517 lopullinen, 30.9.2010. Bottiverkot ovat haittaohjelmien saastuttamien tietokoneiden muodostamia verkkoja, jotka voidaan aktivoida etäältä toteuttamaan esimerkiksi verkkohyökkäyksiä.

8 Tietoverkkorikollisuutta koskeva Euroopan neuvoston yleissopimus, tehty Budapestissa 23. marraskuuta 2001, nk. Budapestin yleissopimus. Yleissopimukseen on liitetty *lisäpöytäkirja*, joka koskee tietojärjestelmien välityksellä tehtyjen luonteeltaan rasististen ja muukalaisvihamielisten tekojen kriminalisointia.

9 Järjestäytynyttä ja vakavaa kansainvälistä rikollisuutta koskeva EU:n toimintapoliittinen sykli kattaa vuodet 2011–2013. Se käsittää kahdeksan ensisijaista tavoitetta, joista yksi on ”tehostetaan tietoverkkorikollisuuden torjuntaa ja torjutaan tehokkaammin internetin rikollista väärinkäyttöä järjestäytyneissä rikollisryhmissä”.

10 ”EU:hun perustetaan vuoteen 2013 mennessä ... tietoverkkorikollisuutta käsittelevä keskus, jonka avulla jäsenvaltiot ja EU:n toimielimet voivat kehittää tietoverkkorikollisuuden tutkintaan liittyvää operatiivista ja analyysivalmiuttaan ja tehdä yhteistyötä kansainvälisten kumppanien kanssa”, EU:n sisäisen turvallisuuden strategian toteuttamissuunnitelma: viisi askelta kohti turvallisempaa Eurooppaa. KOM(2010) 673 lopullinen, 22.11.2010.

Laadittuaan keskuksen perustamista koskevan toteutettavuustutkimuksen[11] komissio ehdottaa neuvoston pyynnön perusteella[12], että Europolin yhteyteen perustetaan Euroopan verkkorikostorjuntakeskus, joka toimii yhteyspisteenä verkkorikollisuuden torjumisessa EU:ssa. Tässä toteutettavuustutkimukseen perustuvassa tiedonannossa hahmotellaan ehdotetun Euroopan verkkorikostorjuntakeskuksen keskeisiä toimintoja ja perustellaan, miksi se olisi sijoitettava Europolin yhteyteen sekä tarkastellaan keskuksen perustamista yleensä. Ennen kuin keskus voi aloittaa toimintansa, on kuitenkin arvioitava yksityiskohtaisemmin sen resurssitarpeita ja säädettävä niistä erikseen. Keskuksen perustamista tarkastellaan asianmukaisella tavalla Europolin oikeusperustan tulevan tarkistuksen yhteydessä.

2. EHDOTUS EUROOPAN VERKKORIKOSTORJUNTAKESKUKSEN PERUSTAMISESTA

Jotta Euroopan verkkorikostorjuntakeskus voisi tarjota todellista lisäarvoa toissijaisuusperiaatetta kunnioittaen, sen olisi keskityttävä seuraaviin verkkorikollisuuden keskeisiin ilmenemismuotoihin:

i) järjestäytyneiden rikollisryhmien tekemät verkkorikokset ja etenkin teot, jotka tuottavat merkittävää rikoshyötyä, kuten verkkopetokset;

ii) verkkorikokset, jotka aiheuttavat uhreille vakavaa haittaa, kuten verkossa tapahtuva lasten seksuaalinen hyväksikäyttö; ja

iii) verkkorikokset (verkkohyökkäykset mukaan lukien), jotka kohdistuvat unionin elintärkeisiin infrastruktuureihin ja tietojärjestelmiin[13].

Koska verkkorikollisuus muuttaa jatkuvasti muotoaan, olisi myös oltava mahdollista toteuttaa toimia sekä jäsenvaltioiden vaatimusten perusteella että unioniin kohdistuvien uusien verkkorikollisuuden muotojen torjumiseksi.

2.1. Euroopan verkkorikostorjuntakeskuksen keskeiset tehtävät ja tavoitteet

Euroopan verkkorikostorjuntakeskuksella olisi oltava neljä ydintehtävää:

a) Euroopan verkkorikollisuutta koskevan tiedon yhteyspiste

Tietojen yhdistämistoiminnan avulla voitaisiin varmistaa, että käytettävissä olevia verkkorikollisuutta koskevia poliisitietoja voidaan täydentää mahdollisimman laajalti erilaisista julkisista, yksityisistä ja avoimen koodin lähteistä kerätyillä tiedoilla. Näin voitaisiin vähitellen paikata aukkoja, joita verkkoturvallisuudesta ja verkkorikollisuuteen puuttumisesta vastaavilla yhteisöillä vielä on käytettävissä olevissa tiedoissaan. Tietoja kerättäisiin verkkorikollisuudesta, sen toimintatavoista ja epäillyistä rikoksentekijöistä. Tämä parantaisi tietämystä sekä verkkorikollisuudesta että sen ehkäisemisestä, paljastamisesta ja syytteeseenpanosta ja edistäisi yhteyksien muodostamista lainvalvontaviranomaisten,

---

11 Feasibility study for a European Cybercrime Centre, loppuraportti, helmikuu 2012.

12 Neuvoston päätelmät tietoverkkorikollisuuden vastaisen yhteisen strategian täytäntöönpanoa koskevasta toimintasuunnitelmasta, yleisten asioiden neuvoston 3010. kokous Luxemburgissa 26. huhtikuuta 2010.

13 Siten kuin ne määritellään 8 päivänä joulukuuta 2008 annetussa neuvoston direktiivissä 2008/114/EY. Tämä direktiivi on parhaillaan tarkistettavana, joten siihen tehtävät muutokset olisi otettava huomioon verkkorikostorjuntakeskusta perustettaessa.

tietotekniikan kriisiryhmien (CERT) ja yksityisen sektorin tieto- ja viestintätekniikka-alan turvallisuusasiantuntijoiden välillä. Tietoja jaettaessa on noudatettava eri osapuolten välisiä luottamuksellisuutta koskevia sopimuksia ja sääntöjä.

Tietojen yhdistäminen edistäisi myös verkkorikollisuutta koskevaa raportointia ja tietojen jakamista. Komissio haluaisi jäsenvaltioiden vaativan, että vakavista tietoverkkorikoksista on ilmoitettava kansallisille lainvalvontaviranomaisille[14]. Näin kansalliset poliisivoimat voisivat toimittaa verkkorikostorjuntakeskukselle tietoja vakavista verkkorikoksista nykyistä johdonmukaisemmin. Keskus puolestaan voisi jakaa näitä tietoja muiden jäsenvaltioiden kollegoille, jotta nämä voisivat hyödyntää niitä omissa tutkintatoimissaan ja tietäisivät, pyrkivätkö he samaan tavoitteeseen.

Tavoitteena on laajentaa tietämystä verkkorikollisuudesta Euroopassa, jotta voidaan laatia korkealaatuisia strategisia selvityksiä rikollisuuden suuntauksista ja siihen liittyvistä uhkista, koota kattavat tiedot rikosten määrästä ja parantaa eri lähteistä saatavaa operatiivista tiedustelutietoa.

b) Euroopan verkkorikollisuutta koskevan asiantuntemuksen keskittäminen tueksi jäsenvaltioiden valmiuksien kehittämiselle

Verkkorikostorjuntakeskuksen olisi avustettava jäsenvaltioita antamalla niille asiantuntemusta ja koulutusta verkkorikollisuuden torjumiseksi. Ensisijainen painopiste on lainvalvonta, mutta lisäksi olisi tarjottava koulutusta myös lainkäyttöviranomaisille. Europolin, CEPOLin ja jäsenvaltioiden olemassa olevia aloitteita olisi virtaviivaistettava perusteellisen tarveanalyysin pohjalta, jotta voidaan parantaa toimien koordinointia ja niiden keskinäistä täydentävyyttä. Koulutuksen pitäisi kattaa sekä perusteellinen tekninen asiantuntemus että poliisin, syyttäjien ja tuomareiden valmiuksien laajempi kehittäminen, jotta voidaan tukea verkkorikoksiin liittyvää tapaustutkintaa.

Olisi perustettava verkkorikollisuutta käsittelevä yhteyspiste, joka olisi vastuussa parhaiden käytänteiden ja tietämyksen vaihdosta ja yhteydenpidosta jäsenvaltioiden ja kansainvälisten lainvalvontaviranomaisten, oikeuslaitoksen, yksityisen sektorin ja kansalaisyhteiskunnan järjestöjen kanssa ja vastaisi niiden kyselyihin esimerkiksi silloin kun tulee ilmi verkkohyökkäyksiä tai uudenlaisia verkkohuijauksia.

Yhteyspisteen olisi tuettava verkkorikollisuuden asiantuntijaryhmien toimia ja annettava niille neuvoja. Tällaisia ryhmiä ovat esimerkiksi tietoverkkorikollisuutta käsittelevä Euroopan unionin erityisryhmä (European Union Cybercrime Task Force, EUCTF) ja verkossa tapahtuvan lasten seksuaalisen hyväksikäytön torjunnan asiantuntijat. Yhteyspiste voisi myös rakentaa yhteistyötä perusteilla olevan verkkorikollisuutta käsittelevien osaamiskeskusten (esim. 2Centre) verkoston ja tutkijoiden kanssa.

Verkkorikostorjuntakeskuksen olisi myös autettava jäsenvaltioita niiden pyrkimyksissä kehittää verkkorikosten ilmoittamista varten yhteisiin standardeihin perustuva verkkosovellus, jonka kautta kansalliset lainvalvontaviranomaiset ja Euroopan verkkorikostorjuntakeskus saavat tietoonsa eri toimijoiden (esim. yritysten, kansallisten/valtiollisten tietotekniikan kriisiryhmien ja kansalaisten) tekemät verkkorikoksia koskevat ilmoitukset.

---

[14] Tässä tarkoitetaan esimerkiksi parhaillaan käsiteltävänä olevan, tietojärjestelmiin kohdistuvista hyökkäyksistä annetun direktiiviehdotuksen 3–7 artiklassa lueteltuja rikoksia, KOM(2010) 517 lopullinen, 30.9.2010.

Verkkorikostorjuntakeskuksen olisi helpotettava parhaiden käytänteiden vaihtoa rikosoikeudellisen yhteisön ja lainvalvontaviranomaisten kesken. Oikeuslaitoksen tehokas osallistuminen verkkorikollisuuden torjuntaan on ensiarvoisen tärkeää, jotta verkkorikoksiin perustuvaa syyteharkintaa voidaan tehostaa kaikissa jäsenvaltioissa.

c) Jäsenvaltioiden verkkorikostutkimusten tukeminen

Verkkorikostorjuntakeskuksen olisi annettava operatiivista tukea verkkorikollisuutta koskevissa tutkimuksissa esimerkiksi edistämällä verkkorikollisuutta käsittelevien yhteisten tutkimusryhmien perustamista ja operatiivisten tietojen vaihtoa meneillään olevissa tutkimuksissa.

Sen olisi myös tuettava verkkorikollisuutta koskevia tutkimuksia tarjoamalla korkean tason rikosteknistä apua (laitteistoja, tallennustilaa, välineitä) ja salausasiantuntemusta.

d) Euroopan verkkorikostutkijoiden edustaminen lainvalvontaviranomaisten ja oikeuslaitoksen parissa

Ajan mittaan verkkorikostorjuntakeskuksesta voisi tulla eurooppalaisten verkkorikostutkijoiden yhteyspiste, joka edustaa heitä keskusteltaessa tieto- ja viestintätekniikka-alan ja muiden yksityissektorin yritysten sekä tutkijoiden, käyttäjäjärjestöjen ja kansalaisyhteiskunnan järjestöjen kanssa siitä, miten verkkorikollisuutta voidaan parhaiten torjua ja sitä koskevia tutkimustoimia koordinoida.

Verkkorikostorjuntakeskus olisi luonteva taho yhteydenpitoon Interpolin verkkorikollisuutta käsittelevien yksiköiden ja muiden poliisiviranomaisten kansainvälisten verkkorikollisuutta käsittelevien yksiköiden kanssa. Se voisi myös koordinoida osallistumista käynnissä oleviin internetin hallintoa koskeviin aloitteisiin ja YK:n tietoverkkorikollisuutta käsittelevään avoimeen hallitustenväliseen asiantuntijaryhmään (UNODC).

Verkkorikostorjuntakeskuksen olisi myös tehtävä yhteistyötä esimerkiksi INSAFEn[15] kaltaisten julkisia tiedotuskampanjoita toteuttavien järjestöjen kanssa pitämällä ne ajan tasalla havaitsemiensa verkkorikollisuuden uusien ilmiöiden suhteen, niin että voidaan edistää varovaista ja turvallista verkkokäyttäytymistä.

2.2. Sijainti

Kuten toteutettavuustutkimuksesta käy ilmi, Euroopan verkkorikostorjuntakeskus olisi perustettava osaksi Europolin nykyistä rakennetta ja sijoitettava sen yhteyteen.

Tähän liittyy selviä etuja. Europolin asema tunnustetaan jäsenvaltioiden ja muiden sidosryhmien, kuten Interpolin ja kansainvälisten lainvalvontaviranomaisten keskuudessa, ja sillä on jo valtuudet käsitellä tietokonerikoksia[16]. Europolin keskeisenä tehtävänä on edistää turvallisemman Euroopan luomista kansalaisten hyväksi tukemalla EU:n lainvalvontaviranomaisia rikoksia koskevien tiedustelutietojen vaihtamisessa ja analysoimisessa.

---

[15] Valistuskeskusten eurooppalainen verkosto, joka edistää internetin ja matkaviestintälaitteiden turvallista ja vastuullista käyttöä nuorten keskuudessa.

[16] Neuvoston päätös (2009/371/YOS), tehty 6 päivänä huhtikuuta 2009, Euroopan poliisiviraston perustamisesta, 4 artiklan 1 kohta yhdessä liitteen kanssa.

2.3. Verkkorikostorjuntakeskuksen resurssitarpeet

Toteutettavuustutkimuksessa selvitettiin keskuksen resurssitarpeita. Niitä on arvioitava tarkemmin[17] muun muassa ottaen huomioon Europolin mahdolliset muut tulevat tehtävät ja EU:n erillisvirastojen henkilöstömäärä yleensä. Resurssitarpeiden arvioinnissa on otettava huomioon erityisesti Europolin oikeusperustan tarkistaminen ja käynnissä oleva keskustelu sisäisen turvallisuuden rahastoa koskevasta komission ehdotuksesta. Jo tässä vaiheessa näyttäisi kuitenkin selvältä, että keskukseen tarvitaan jäsenvaltioiden lähettämiä asiantuntijoita.

Komissio käyttää resurssitarpeiden arvioinnissa ohjenuorana kolmea oletusta: ensinnäkin verkkorikostapausten kokonaismäärä todennäköisesti lisääntyy jonkin verran, mutta ei jyrkästi; toiseksi jäsenvaltioiden omat valmiudet torjua verkkorikollisuutta paranevat; ja kolmanneksi verkkorikostorjuntakeskus käsittelee vain tietyntyyppisiä verkkorikoksia.

2.4. Hallinto

Kun verkkorikostorjuntakeskus sijoitetaan Europolin yhteyteen, on tärkeää varmistaa, että myös muut keskeiset sidosryhmät osallistuvat sen strategiseen ohjaukseen. Tämän vuoksi komissio ehdottaa, että Europolin hallintorakenteen yhteyteen perustetaan verkkorikostorjuntakeskuksen johtoryhmä, jonka puheenjohtajana toimii verkkorikostorjuntakeskuksen johtaja. Johtoryhmän välityksellä muut sidosryhmät, kuten Eurojust, Euroopan poliisiakatemia (CEPOL), jäsenvaltiot tietoverkkorikollisuutta käsittelevään EU:n erityisryhmään osallistuvien edustajiensa välityksellä, Euroopan verkko- ja tietoturvavirasto (ENISA) ja komissio voisivat tuoda osaamisensa keskuksen käyttöön aiheuttamatta kohtuutonta ylimääräistä hallinnollista rasitusta. Johtoryhmän tehtävänä olisi kantaa vastuu verkkorikollisuutta koskevasta toiminnasta ja siten varmistaa, että se toteutetaan yhteistyössä, kaikkien sidosryhmien asiantuntemuksen pohjalta ja niiden toimivaltaa kunnioittaen.

2.5. Yhteistyö keskeisten toimijoiden kanssa

Verkkorikostorjuntakeskuksen olisi varmistettava, että verkkorikollisuutta pyritään torjumaan koordinoidusti, paitsi luomalla edellytykset EU:n virastojen väliselle yhteistyölle, myös toimimalla tämän alan yhteyspisteenä Euroopassa.

a) Jäsenvaltiot

Keskeisenä tavoitteena on auttaa jäsenvaltioita torjumaan verkkorikollisuutta. Verkkorikollisuuteen erikoistunut keskuksen neuvontapiste ja sen muut palvelut kuten kohdennetummat uhka-analyysit ja laajempiin tietoihin perustuva operatiivinen tuki tuovat hyötyä verkkorikollisuuden tutkijoille eri puolilla Eurooppaa. Tietoverkkorikollisuutta käsittelevä EU:n erityisryhmä takaisi, että jäsenvaltioiden huolenaiheet tulisivat kuulluiksi keskuksen johtoryhmässä. Lisäksi jäsenvaltioiden on jatkossakin tehtävä kansallisiin rakenteisiinsa tarvittavat investoinnit verkkorikollisuuden torjumiseksi, koska niillä on oltava asianmukaiset kumppanit verkkorikostorjuntakeskuksen kanssa tehtävää yhteistyötä varten.

b) EU:n erillisvirastot ja muut toimijat

[17] Arviointi on sovitettava yhteen vuoden 2013 talousarviossa esitettävän erillisvirastojen henkilöstö- ja budjettitarpeiden kokonaistilanteen ja seuraavan monivuotisen rahoituskehyksen kanssa.

Alalla toimivat virastot, erityisesti Eurojust, CEPOL ja ENISA, sekä tietotekniikan kriisiryhmät (CERT-EU) osallistuisivat suoraan keskuksen toimintaan paitsi sen johtoryhmän, tarvittaessa myös operatiivisen yhteistyön välityksellä, omien toimivaltuuksiensa puitteissa.

c) Kansainväliset kumppanit

Sen lisäksi, että verkkorikostorjuntakeskuksesta olisi tultava verkkorikollisuuden torjunnan tietokeskus Euroopassa, siitä olisi kehitettävä arvokas yhteistyötaho verkkorikollisuuden torjunnasta vastaaville kansainvälisille kumppaneille. Keskuksen olisi yhdessä Interpolin ja muiden eri puolilla maailmaa toimivien EU:n strategisten kumppaneiden kanssa pyrittävä parantamaan koordinoituja ratkaisuja verkkorikollisuuden torjuntaan ja varmistettava, että lainvalvontaviranomaisten näkemykset otetaan huomioon tietoverkkojen kehittämisessä.

d) Yksityinen sektori, tutkimusyhteisöt ja kansalaisyhteiskunnan järjestöt

Verkkorikollisuuden torjunnassa on olennaisen tärkeää kehittää luottamusta yksityisen sektorin ja lainvalvontaviranomaisten välillä. Vahvistamalla Europolin toimintaa nykyisten ja uusien kumppanien kanssa verkkorikostorjuntakeskus voi luoda luotettavia verkostoja ja tiedonvaihtofoorumeja teollisuuden ja muiden toimijoiden, kuten tutkimusyhteisön ja kansalaisyhteiskunnan järjestöjen, kanssa. Nämä helpottaisivat tietojen jakamista eri yhteisöjen kesken eri aiheista, kuten verkkouhkiin varautumisesta. Lisäksi verkkohyökkäyksiin ja muihin verkkorikoksiin olisi helpompi reagoida yhteistyöhön perustuvien erityisryhmien avulla.

Verkkorikostorjuntakeskuksen olisi myös tuettava sellaisia yksityisen sektorin yrityksiä, kuten pankkeja ja verkossa toimivia vähittäiskauppiaita, jotka hallinnoivat merkittävää digitaalista omaisuutta ja pyrkivät siksi laajemmin torjumaan verkkorikollisuutta ja suojautumaan siltä sekä kehittämään teknologiaa, joka olisi mahdollisimman vähän altis tällaiselle rikollisuudelle.

On sekä lainvalvontaviranomaisten että yksityisen sektorin edun mukaista, että verkkorikollisuutta pystytään luotaamaan nykyistä paremmin reaaliajassa ja että verkkorikollisten verkostot pyritään purkamaan tehokkaammin kehittämällä parempia keinoja paljastaa uusia toimintatapoja ja ottaa verkkorikolliset nopeasti kiinni.

3. ETENEMISSUUNNITELMA KOHTI EUROOPAN VERKKORIKOSTORJUNTAKESKUKSEN PERUSTAMISTA

3.1. Toimet vuoden 2013 loppuun saakka

Alustavan toimintavalmiuden saavuttamiseksi komissio tutkii tiiviissä yhteistyössä Europolin kanssa, minkä verran talous- ja henkilöstöresursseja tarvittaisiin verkkorikostorjuntakeskuksen toteuttamisryhmän toimintaa varten voimassa olevan rahoituskehyksen loppuun saakka. Ryhmän tehtävänä olisi esimerkiksi laatia keskuksen toimintapuitteet ja organisaatiorakenne sekä määrittää indikaattorit sen suorituskyvyn arviointia varten. Keskuksen johtoryhmän asema ja tehtävät määritellään aikanaan yhdessä sidosryhmien kanssa.

Jotta verkkorikostorjuntakeskuksessa voitaisiin ottaa käyttöön kattava tietojen yhdistämistoiminto, toteuttamisryhmän olisi luotava yhteyksiä tietotekniikan kriisiryhmän kokoonpanon vahvistamista edeltävään ryhmään ja tarvittaessa myös ENISAan (niiden

rajalliset resurssit huomioon ottaen). Verkkorikosten ilmoittamisen kehittämistä varten kartoitetaan jäsenvaltioissa jo perustettujen verkossa toimivien ilmoitusjärjestelmien yhteentoimivuus.

Olisi perustettava verkkorikollisuutta käsittelevä yhteyspiste. Sen tukena voisi olla erityinen suojattu verkkoyhteisöfoorumi. Europolin, CEPOLin ja verkkorikollisuutta koskevaa koulutusta käsittelevän ryhmän (European Cybercrime Training and Education Group, ECTEG) nykyistä koulutustoimintaa voitaisiin arvioida ja virtaviivaistaa verkkorikostorjuntakeskuksen ja sen johtoryhmän johdolla. Olisi myös analysoitava koulutustarpeita ja otettava tätä varten huomioon tuomarien ja syyttäjien vaatimukset. Tämän tarkastelun pohjalta voitaisiin toteuttaa verkkorikollisuutta käsittelevää koulutusta rikosoikeusjärjestelmän eri toimijoille.

Lisäksi on laadittava täsmällisempi arvio tarvittavista talous- ja henkilöresursseista ja säädettävä tarvittavista määrärahoista seuraavan monivuotisen rahoituskehyksen nojalla tehtävissä päätöksissä. Arviointi tarjoaa pohjan verkkorikostorjuntakeskuksen jatkokehittämiselle.

4. PÄÄTELMÄT

Kun järjestäytynyt rikollisuus laajentaa toimintaansa verkkoympäristöön, lainvalvontaviranomaisten on pysyteltävä tilanteen tasalla. EU voi tarjota jäsenvaltioille ja teollisuudelle keinot tarttua verkkorikollisuuden muodostamaan uuteen ja jatkuvasti kehittyvään uhkaan, jolle on luonteenomaista se, ettei se tunne maantieteellisiä rajoja. Jos Euroopan verkkorikostorjuntakeskus saa tarvittavat talous- ja henkilöresurssit, se voi toimia yhteyspisteenä verkkorikollisuuden torjunnassa Euroopassa kokoamalla yhteen asiantuntemusta, tukemalla rikosten tutkintaa ja edistämällä EU:n laajuisia ratkaisuja. Samalla se voi lisätä tietoisuutta verkkorikollisuuteen liittyvistä kysymyksistä kaikkialla unionissa. Näin keskus edistäisi internetin avoimuutta ja digitaalitaloutta sekä Euroopan kansalaisten ja yritysten turvallista toimintaympäristöä verkossa.

Neuvostoa ja Euroopan parlamenttia pyydetään hyväksymään tämä ehdotus, ja muita sidosryhmiä kannustetaan myötävaikuttamaan keskuksen kehittämiseen.