Sisäasiainministeriö E-KIRJE SM2012-00227

PO Seesmaa Anne-Maria(SM) 15.05.2012

Eduskunta
Suuri valiokunta

Viite

Asia
Komission tiedonanto neuvostolle ja Euroopan parlamentille; Rikostentorjunta digitaaliaikana: Euroopan verkkorikostorjuntakeskuksen perustaminen

U/E-tunnus: **EUTORI-numero:**

Ohessa lähetetään perustuslain 97§:n mukaisesti selvitys komission tiedonannosta koskien Euroopan verkkorikostorjuntakeskuksen perustamista.

Ylitarkastaja Anne-Maria Seesmaa

LIITTEET Muistio SM2012-00226; COM (2012) 140 final FI; COM (2012) 140 final SE

Asiasanat	oikeus- ja sisäasiat
Hoitaa	**OM, SM, UM**
Tiedoksi	EUE, STM, TEM, TH, VM, VNEUS

Sisäasiainministeriö PERUSMUISTIO SM2012-00226

PO Seesmaa Anne-Maria(SM) 15.05.2012

Asia

Komission tiedonanto neuvostolle ja Euroopan parlamentille; Rikostentorjunta digitaaliaikana: Euroopan verkkorikostorjuntakeskuksen perustaminen

Kokous

Liitteet Viite

EUTORI/Eurodoc nro:

[VN:n ja EK:n asiankäsittelyjärjestelmän EURODOC:n/EUTORI:n tunnus]

U-tunnus / E-tunnus:

Käsittelyn tarkoitus ja käsittelyvaihe:

Komissio esittelee tiedonannossa ehdotustaan Euroopan verkkorikostorjuntakeskuksen perustamisesta.

Asiakirjat:

Komission tiedonanto neuvostolle ja Euroopan parlamentille; Rikostentorjunta digitaaliaikana: Euroopan verkkorikostorjuntakeskuksen perustaminen, COM (2012) 140 final.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely:

Asiassa ei tehdä päätöksiä.

Käsittelijä(t):

Anne-Maria Seesmaa/ Sisäasiainministeriö, puh. 071 878 8590

Suomen kanta/ohje:

Tietoverkkorikollisuuden torjunta edellyttää lainvalvontaviranomaisilta koordinoituja toimia ja yhteistyötä yli valtioiden rajojen. Suomi pitää tärkeänä tietoverkkoturvallisuuden edistämistä. Suomi pitää ehdotusta verkkorikostorjuntakeskuksen perustamisesta turvallisuutta edistävänä ja lisäarvoa tuovana toimena ja täten tukee ehdotusta keskuksen perustamisesta.

Kuten komissio, myös Suomi katsoo, että verkkorikostorjuntakeskus olisi perustettava osaksi Euroopan poliisiviraston (Europol) nykyistä rakennetta ja sijoitettava sen yhteyteen. Tietoverkkorikollisuuden torjuminen kuuluu jo nyt Europolin toimivaltaan, joten keskuksen perustamisella virastoon ei sinänsä olisi vaikutusta sen toimivaltuuksiin. Keskuksen perustamista Europoliin puoltaa myös se, että Europolin asema tunnustetaan jäsenvaltioiden ja muiden sidosryhmien keskuudessa.

Keskuksen perustamista on tarkasteltava huolellisesti Europolin oikeusperustan tulevan tarkistuksen yhteydessä. Europolin oikeusperustaan tulee ottaa asianmukaiset määräykset keskuksen toiminnasta. Verkkorikostorjuntakeskuksen ydintehtävänä on toimia Euroopan tietoverkkorikollisuutta koskevan tiedon yhteyspisteenä. Komission tiedonannon mukaan, tietojen yhdistämistoiminnalla voitaisiin vähitellen paikata aukkoja, joita tietoverkkoturvallisuudesta ja tietoverkkorikollisuuteen puuttumisesta vastaavilla yhteisöillä vielä on käytettävissä olevissa tiedoissaan. Tietoja kerättäisiin tietoverkkorikollisuudesta, sen toimintatavoista ja epäillyistä rikoksentekijöistä. Tietojen yhdistäminen edistäisi tietoverkkorikollisuutta koskevaa raportointia ja tietojen jakamista. Tähän liittyen, komissio haluaisi jäsenvaltioiden vaativan, että vakavista tietoverkkorikoksista on ilmoitettava kansallisille lainvalvontaviranomaisille. Tiedonannosta ei käy selväksi, kehen tai mihin tahoihin ilmoitusvelvollisuus tarkalleen kohdistuisi. Tällaisen ilmoitusvelvollisuuden asettamisesta pitäisi säätää laissa. Määrittelemätön ja laaja ilmoitusvelvollisuus, joka saattaisi koskea esimerkiksi yksityisiä henkilöitä, olisi ongelmallinen. Ilmoitusvelvollisuuskysymys tulee huomioida asianmukaisesti Europolin oikeusperustan tarkistamisen yhteydessä.

Suomi pitää tärkeänä, että jatkotyössä arvioidaan täsmällisemmin myös keskuksen resurssitarpeet. Myös resurssitarpeiden arvioinnissa on otettava huomioon Europolin oikeusperustan tarkistaminen.

Pääasiallinen sisältö:

Euroopan unioni on jo toteuttanut erilaisia aloitteita tietoverkkorikollisuuden torjumiseksi. Näitä ovat vuonna 2011 hyväksytty direktiivi lasten seksuaalisen hyväksikäytön ja seksuaalisen riiston sekä lapsipornografian torjumisesta ja parhaillaan käsiteltävänä oleva direktiiviehdotus tietojärjestelmiin kohdistuvista hyökkäyksistä. Tietoverkkorikollisuuden torjunta on EU:n toiminnassa tärkeä painopisteala, ja tärkein siihen liittyvä oikeudellinen väline on tietoverkkorikollisuutta koskeva Euroopan neuvoston yleissopimus. Tietoverkkorikollisuuden torjunta sisältyy myös järjestäytynyttä ja vakavaa kansainvälistä rikollisuutta koskevaan EU:n toimintapoliittiseen sykliin ollen yksi kahdeksasta painopisteestä vuosille 2012-14, minkä lisäksi se on olennainen osa pyrkimyksiä kehittää kokonaisvaltainen EU:n strategia tietoverkkoturvallisuuden lujittamiseksi. EU on myös tehnyt tiivistä yhteistyötä kansainvälisten kumppaneiden kanssa esimerkiksi tietoverkkoturvallisuutta ja tietoverkkorikollisuutta käsittelevässä EU:n ja Yhdysvaltojen työryhmässä. Näistä edistysaskelista huolimatta tietoverkkorikollisuuden tehokkaan tutkinnan ja rikoksentekijöiden syytteeseenpanon tiellä on Euroopassa vielä monia esteitä, kuten oikeudenkäyttöalueiden rajat, riittämätön valmius tiedustelutietojen jakamiseen, tietoverkkorikosten tekijöiden jäljittämiseen liittyvät tekniset vaikeudet, vaihtelevat valmiudet suorittaa rikostutkintaa ja rikosteknisiä tutkimuksia, koulutetun henkilöstön riittämättömyys ja muiden tietoverkkoturvallisuudesta vastaavien sidosryhmien kanssa tehtävän yhteistyön hajanaisuus.

Vastauksena näihin haasteisiin komissio ilmoitti perustavansa Euroopan verkkorikostorjuntakeskuksen, joka liittyy yhteen neuvoston alkuvuodesta 2010

hyväksymän sisäisen turvallisuuden strategian painopisteeseen: Strategiassa on keskeisiksi uhkiksi ja haasteiksi nostettu muun muassa tietoverkkorikollisuus. Lisäksi, komissio laati loppuvuodesta 2010 toimintasuunnitelman strategian täytäntöönpanemiseksi. Yksi toimintasuunnitelman strategisista tavoitteista on kansalaisten ja yritysten turvallisuuden parantaminen verkkoympäristössä.

Komissio laati keskuksen perustamista koskevan toteutettavuustutkimuksen, jonka loppuraportti valmistui helmikuussa 2012. Toteutettavuustutkimuksen sekä neuvoston pyynnön perusteella komissio ehdottaa, että Europolin yhteyteen perustetaan Euroopan verkkorikostorjuntakeskus, joka toimii yhteyspisteenä verkkorikollisuuden torjumisessa EU:ssa. Tiedonannossaan komissio hahmottelee ehdotetun Euroopan verkkorikostorjuntakeskuksen keskeisiä toimintoja ja perustelee, miksi se olisi sijoitettava Europolin yhteyteen.

Komission ehdotuksen mukaisesti, keskuksen tulisi keskittyä tietoverkkorikollisuuden keskeisiin ilmenemismuotoihin; i) järjestäytyneiden rikollisryhmien tekemät tietoverkkorikokset ja etenkin teot, jotka tuottavat merkittävää rikoshyötyä, ii) tietoverkkorikokset, jotka aiheuttavat uhreille vakavaa haittaa, ja iii) tietoverkkorikokset (ml. verkkohyökkäykset), jotka kohdistuvat unionin elintärkeisiin infrastruktuureihin ja tietojärjestelmiin.

Verkkorikostorjuntakeskuksen keskeiset ydintehtävät olisivat a) toimia Euroopan tietoverkkorikollisuutta koskevan tiedon yhteyspisteenä, b) keskittää Euroopan tietoverkkorikollisuutta koskeva asiantuntemus tueksi jäsenvaltioiden valmiuksien kehittämiselle, c) tukea jäsenvaltioiden tietoverkkorikostutkimuksia ja d) edustaa Euroopan tietoverkkorikostutkijoita lainvalvontaviranomaisten ja oikeuslaitoksen parissa.

Ehdotuksen mukaisesti, keskuksen perustamiseen osaksi Europolin nykyistä rakennetta liittyy monia etuja. Europolin asema tunnustetaan jäsenvaltioiden ja muiden sidosryhmien, kuten Interpolin ja kansainvälisten lainvalvontaviranomaisten keskuudessa, ja sillä on jo valtuudet käsitellä tietokonerikoksia. Europolin keskeisenä tehtävänä on edistää turvallisemman Euroopan luomista kansalaisten hyväksi tukemalla EU:n lainvalvontaviranomaisia rikoksia koskevien tiedustelutietojen vaihtamisessa ja analysoimisessa.

Keskuksen hallinnolliseksi rakenteeksi 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.

Ennen kuin keskus voi aloittaa toimintansa, on kuitenkin mm. arvioitava yksityiskohtaisemmin sen resurssitarpeita ja säädettävä niistä erikseen sekä laadittava keskuksen toimintapuitteet ja organisaatiorakenne.

Keskuksen perustamista tarkastellaan asianmukaisella tavalla Europolin oikeusperustan tulevan tarkistuksen yhteydessä.

Kansallinen käsittely:

Jaosto 7 kirjallinen menettely 8.-14.5.2012

Eduskuntakäsittely:

Käsittely Euroopan parlamentissa:

Komissio on toimittanut tiedonannon Euroopan parlamentille 2.4.2012.

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema:

Tiedonannolla ei ole lainsäädännöllisiä vaikutuksia.

Taloudelliset vaikutukset:

Tiedonannolla ei ole taloudellisia vaikutuksia. Euroopan verkkorikostorjuntakeskuksen perustamisesta mahdollisesti aiheutuvista taloudellisista vaikutuksista ei tässä vaiheessa vielä ole tarkempaa tietoa.

Muut mahdolliset asiaan vaikuttavat tekijät:

Asiasanat	oikeus- ja sisäasiat
Hoitaa	**OM, SM, UM**
Tiedoksi	EUE, STM, TEM, TH, VM, VNEUS

EUROOPAN UNIONIN NEUVOSTO

Bryssel, 4. huhtikuuta 2012 (10.04)
(OR. en)

8543/12

ENFOPOL 94
TELECOM 72

SAATE

Lähettäjä:	Euroopan komission pääsihteerin puolesta Jordi AYET PUIGARNAU, johtaja
Saapunut:	30. maaliskuuta 2012
Vastaanottaja:	Uwe CORSEPIUS, Euroopan unionin neuvoston pääsihteeri
Kom:n asiak. nro:	COM(2012) 140 final
Asia:	KOMISSION TIEDONANTO NEUVOSTOLLE JA EUROOPAN PARLAMENTILLE Rikostentorjunta digitaaliaikana: Euroopan verkkorikostorjuntakeskuksen perustaminen

Valtuuskunnille toimitetaan oheisena komission asiakirja – COM(2012) 140 final

Liite: COM(2012) 140 final

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.

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

---

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.

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]. 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

---

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.

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.

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, 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

---

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.

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

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.
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.

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-

---

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.

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

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

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.

EUROPEISKA UNIONENS RÅD

Bryssel den 4 april 2012 (10.4)
(OR. en)

8543/12

ENFOPOL 94
TELECOM 72

FÖLJENOT

från:	Jordi AYET PUIGARNAU, direktör, för Europeiska kommissionens generalsekreterare
mottagen den:	30 mars 2012
till:	Uwe CORSEPIUS, generalsekreterare för Europeiska unionens råd
Komm. dok. nr:	COM(2012) 140 final
Ärende:	Meddelande från kommissionen till rådet och Europaparlamentet Brottsbekämpning i vår digitala tidsålder: inrättande av ett Europeiskt centrum mot it-brottslighet

För delegationerna bifogas kommissionens dokument – COM(2012) 140 final.

Bilaga: COM(2012) 140 final

EUROPEISKA KOMMISSIONEN

Bryssel den 28.3.2012
COM(2012) 140 final

MEDDELANDE FRÅN KOMMISSIONEN TILL RÅDET OCH EUROPAPARLAMENTET

Brottsbekämpning i vår digitala tidsålder: inrättande av ett Europeiskt centrum mot it-brottslighet

MEDDELANDE FRÅN KOMMISSIONEN TILL RÅDET OCH EUROPAPARLAMENTET

Brottsbekämpning i vår digitala tidsålder: inrättande av ett Europeiskt centrum mot it-brottslighet

1. INLEDNING: EUROPAS SVAR PÅ GRÄNSÖVERSKRIDANDE BROTT

Internet (nedan också kallat nätet eller online) har blivit en integrerad och oumbärlig del av vårt samhälle och vår ekonomi. Åttio procent av alla unga européer är uppkopplade på nätet och har därigenom kontakt med omvärlden via sociala nätverk online[18], och e-handeln omsätter ungefär 8 biljoner US-dollar varje år[19].Men eftersom mer och mer av vår vardag och våra affärstransaktioner utspelas online, ökar också den brottsliga verksamheten - mer än en miljon människor i hela världen faller varje dag offer för it-brottslighet[20]. Brottslig verksamhet på nätet varierar från att sälja stulna kreditkort för så lite som en euro, identitetsstöld och sexuella övergrepp mot barn, till omfattande it-attacker mot institutioner och infrastruktur. För samhället är den totala kostnaden för it-brott stor. En färsk rapport tyder på att offren förlorar cirka 388 miljarder US-dollar varje år över hela världen till följd av it-brottslighet, vilket gör den mer lönsam än den globala handeln med marijuana, kokain och heroin tillsammans[21]. Även om dessa uppgifter bör behandlas med försiktighet, eftersom olika sätt att definiera vad it-brottslighet innebär kan leda till en variation av kostnadsberäkningar, finns det emellertid enighet om att it-brott är en mycket lönsam form av kriminell lågriskverksamhet som blir allt vanligare och gör allt större skada. I en tid då främjandet av ekonomisk tillväxt är av största vikt, kommer en upptrappning av bekämpningen av it-brottsligheten att vara nödvändig för att behålla medborgarnas och näringslivets förtroende för säker elektronisk kommunikation och handel. Den kommer också att stödja målen för tillväxt i Europa 2020-strategin[22] och den digitala agendan för Europa[23].

Friheten på internet är den viktigaste faktorn för att förklara den digitala revolutionen under senare år. Vårt öppna internet har varken några nationella gränser eller en global styrningsstruktur. Men samtidigt som främjandet och skyddet av denna frihet online överensstämmer med stadgan om grundläggande rättigheter i EU, måste vi också sträva efter att skydda medborgarna från organiserade kriminella ligor som försöker utnyttja denna öppenhet. Ingen brottslighet är så gränslös som it-brottslighet, vilket kräver att de brottsbekämpande myndigheterna, tillsammans med aktörer inom den offentliga och privata sektorn, antar ett samordnat och samarbetsinriktat tillvägagångssätt över de nationella gränserna. Det är på detta område som EU kan göra stor nytta, vilket redan sker.

Europeiska unionen har utvecklat olika initiativ för att hantera it-brott. Dessa inbegriper 2011 års direktiv om bekämpande av sexuellt utnyttjande av barn och barnpornografi på internet, och ett direktiv om angrepp mot informationssystem, med inriktning på att straffbelägga

18 Eurostat, tillgång till och användning av internet, 14 december 2010.
19 McKinsey Global Institute, Internet Matters: the Net's sweeping impact on growth, jobs and prosperity. Report May 2011 accessed on 8 February 2012.
20 Norton Cybercrime Report 2011, Symantec, 7 September 2011, accessed on 6 January 2012.
21 Ibid.
22 Europa 2020 – En strategi för smart och hållbar tillväxt för alla (KOM(2010) 2020 slutlig, 3.3.2010).
23 En digital agenda för Europa, KOM(2010) 245 slutlig, 26.8.2010.

användningen av verktyg för it-brottslighet, framför allt botnät[24], vilka bör antas under 2012. Europol har utökat sin verksamhet mot it-brottslighet och spelar en central roll i den senaste undsättningsinsatsen ”Operation Rescue”, där polisen arresterade 184 misstänkta barnsexförbrytare och identifierade mer än 200 offer för övergrepp efter en av de brottsbekämpande myndigheternas största utredningar i sitt slag över hela världen. De misstänkta brottslingarnas identitet och verksamhet kunde avslöjas tack vare det arbete Europols analytiker lagt ned för att spräcka säkerhetslösningarna i en av nätverkets centrala servrar.

Bekämpningen av it-brottslighet, där det viktigaste rättsliga instrumentet är Europarådets konvention om it-brottslighet[25], fortsätter att vara en av de främsta prioriteringarna. Den fastställs i EU:s policycykel för organiserad och grov internationell brottslighet[26], och utgör en integrerad del av EU:s insatser för att utarbeta en övergripande strategi i syfte att stärka säkerheten på internet. EU har också ingått ett nära samarbete med internationella partner, t.ex. den befintliga EU–USA-arbetsgruppen om it-säkerhet och it-brottslighet.

Bortsett från dessa framsteg finns det fortfarande flera hinder för en effektiv utredning av it-brottslighet och åtal av brottslingar på europeisk nivå. Dessa hinder är bland annat: gränserna för domstolarnas behörighet, otillräckligt underrättelsesamarbete, tekniska svårigheter med att spåra de gärningsmän som är upphov till it-brotten, olikartat utredande och kriminalteknisk kapacitet, brist på utbildad personal och inkonsekvent samarbete med andra aktörer med ansvar för säkerheten på internet. Genom stabilitetsinstrumentet hanterar EU den snabba utvecklingen av gränsöverskridande hot avseende it-brotten i utvecklings- och övergångsländer där den kapacitet som krävs för att bekämpa denna form av organiserad brottslighet ofta saknas.

Som svar på dessa utmaningar framhöll kommissionen sin avsikt att skapa ett europeiskt centrum för frågor mot it-brottslighet EC3 (nedan också kallat *centrumet*) som en prioritet i strategin för den inre säkerheten[27]. Efter att ha utfört en genomförbarhetsstudie om inrättandet av ett sådant centrum[28] har kommissionen, på rådets begäran[29], föreslagit ett europeiskt centrum mot it-brottslighet som kommer att ingå i Europol och fungera som kontaktpunkt vid bekämpningen av it-brott inom EU. I detta meddelande, som utarbetats mot bakgrund av genomförbarhetsstudien, skisseras de föreslagna huvudfunktionerna i Europeiska centrumet mot it-brottslighet, förklaras varför centrumet bör lokaliseras inom Europol, och hur det kan inrättas. Innan centrumet kan bli till fullo operativt kommer man emellertid att behöva

---

24 Förslag till Europaparlamentets och rådets direktiv om angrepp mot informationssystem KOM (2010)517 slutlig, 30.9.2010. Botnät är nätverk av datorer som har infekterats av sabotageprogram som på avstånd kan aktiveras för att utföra särskilda uppgifter, inklusive it-angrepp.

25 Council of Europe Cybercrime Convention, Budapest, 23 November 2001, kallas också Budapestkonventionen. Konventionen fogas ett *tilläggsprotokoll till konventionen om it-brottslighet* beträffande kriminaliseringen av rasistiska eller främlingsfientliga handlingar som begåtts via datorsystem.

26 EU:s politiska planering avseende organiserad och grov internationell brottslighet som omfattar åren 2011–2013 har åtta prioriteringar, varav en är att trappa upp kampen mot it-brottslighet och organiserade kriminella gruppers missbruk av internet.

27 ”Under 2013 kommer EU att inrätta ett centrum för frågor om it-brottslighet inom ramen för befintliga strukturer. Detta kommer att ge medlemsstaterna och EU-institutionerna möjlighet att bygga upp en operativ och analytisk kapacitet för utredningar och samarbete med internationella partner” i EU:s strategi för den inre säkerheten i praktiken: Fem steg mot ett säkrare Europa (The EU Internal Security Strategy in action: five steps towards a more secure Europe) KOM(2010) 673 slutlig, 22.11.2010.

28 Feasibility study for a European Cybercrime Centre, Final Report, February 2012.

29 Rådets slutsatser om en handlingsplan för att genomföra den samordnade strategin för att bekämpa it-brottslighet, 3010:e mötet i rådet (allmänna frågor), Luxemburg den 26 april 2010.

utvärdera resursbehovet och ställa anslag till dess förfogande. Inrättandet av centrumet kommer också, om det är lämpligt, att avspeglas i den kommande revisionen av Europols rättsliga grund.

2. FÖRSLAG TILL INRÄTTANDE AV ETT EUROPEISKT CENTRUM MOT IT-BROTTSLIGHET

För att Europeiska centrumet mot it-brottslighet (nedan kallat *centrumet*) ska ge mervärde, samtidigt som hänsyn tas till subsidiaritetsprincipen föreslås det att centrumet inriktas på följande grupper av it-brott:

i) It-brott som begåtts av organiserade kriminella grupper, särskilt de som genererar stor kriminell vinning genom bedrägerier på internet.

ii) It-brott som ger uppov till allvarlig skada för offren, till exempel sexuell exploatering av barn på internet.

iii) It-brott (inklusive it-angrepp) som drabbar kritisk infrastruktur och informationssystem inom EU[30].

Med beaktande av att it-brottsligheten ständigt förändras bör det också finnas utrymme för att vidta åtgärder både för att tillgodose medlemsstaternas krav och för att hantera uppkomsten av de nya hot som EU utsätts för i samband med it-brotten.

2.1. Centrala funktioner och vilka funktioner som bör finnas i ett Europeiskt centrum mot it-brottslighet

Centrumet bör ha fyra huvudfunktioner:

(a) Fungera som kontaktpunkt för information som rör europeisk it-brottslighet

En samordnande funktion skulle säkerställa insamling av uppgifter om it-brottslighet från bredast möjliga lager av offentliga, privata och öppna källor, och berika den polisiära underrättelseverksamheten. Den bör gradvis överbrygga nuvarande luckor i de uppgifter som finns tillgängliga från de enheter som ansvarar för säkerheten på internet och för att hantera it-brottslighet. De uppgifter som samlas in skulle beröra it-brottslighetens verksamheter och metoder samt misstänkta it-brottslingar. Dessa skulle användas både för att förbättra kunskapen om it-brott och dess förebyggande, upptäckt och straffbeläggg, samt uppmuntra lämpliga kopplingar mellan de brottsbekämpande myndigheterna, organisationen för incidenthantering (Cert) och säkerhetsspecialister för informations- och kommunikationsteknik (IKT) från den privata sektorn. Vid utbytet av uppgifter måste man respektera sekretessavtalen och reglerna om tystnadsplikt mellan olika parter.

Den samordnande funktionen är också värdefull för att förbättra den polisiära underrättelseverksamheten i samband med it-brott. Kommissionen skulle önska att medlemsstaterna gör det till ett krav att grova it-brott rapporteras till de nationella brottsbekämpande myndigheterna[31]. Detta skulle göra det möjligt för de nationella polismyndigheterna att mer konsekvent lämna uppgifter om grova it-brott till centrumet,

[30] Enligt definitionen i rådets direktiv 2008/114/EG av den 8 december 2008. Detta direktiv är för närvarande föremål för översyn, den ytterligare utvecklingen kommer att beaktas av centrumet.

[31] Såsom dem som anges i artiklarna 3-7 i förslaget till direktiv om angrepp mot informationssystem, KOM (2010) 517 slutlig, 30.9.2010.

vilket i sin tur kunde sprida dessa uppgifter så att kollegor i andra medlemsstater får veta om de strävar mot samma mål och kan dra nytta av varandras uppgifter vid utredningar.

Syftet är att bredda lägesbilden av it-brottsligheten i Europa under en längre tid för att framställa högkvalitativa strategiska rapporter om trender och hot, att öka sakkunnigheten på grundval av omfattande uppgifter om brott och att förbättra den operativa underrättelseverksamheten från en uppgiftsbas som bygger på olika uppgiftskällor.

(b) Sammanslagning av sakkunskaper om den europeiska it-brottsligheten för att stödja medlemsstaternas kapacitetsuppbyggnad

Centrumet bör bistå medlemsstaterna med sakkunskap och utbildning för att förebygga och bekämpa it-brottslighet. Det inriktas främst på brottsbekämpning, men utbildning bör också erbjudas rättsväsendet. De befintliga initiativen från Europol, Cepol och medlemsstaterna kommer att rationaliseras efter en djupgående behovsanalys för att se till att verksamheten samordnas och kompletteras på ett bättre sätt. Utbildningen bör omfatta allt från djupgående teknisk sakkunskap till en bredare kapacitetsuppbyggnad för polistjänstemäns, åklagares och domares förmåga att hantera enskilda it-brott.
En kontaktpunkt för it-brott bör inrättas för utbyte av bästa praxis och kunskap, och för att samarbeta med och besvara frågor från medlemsstaterna och internationella brottsbekämpande myndigheter, rättsväsendet, den privata sektorn och det civila samhällets organisationer, t.ex. när det gäller it-angrepp eller nya former av bedrägerier på inernet.
Den bör stödja verksamhet i, och ge råd till, expertgrupper på it-brott, inbegripet EU:s arbetsgrupp om it-brottslighet och experter på bekämpning av sexuell exploatering av barn på internet. Den bör även inleda samarbete med det nätverk av kompetenscentrum som håller på att utvecklas vad gäller it-brott, t.ex. 2Centre, och med forskarsamhället.
Centrumet bör också hjälpa medlemsstaterna i deras insatser att utveckla en onlineapplikation för rapportering av it-brott, som baseras på gemensamma standarder, för att länka rapporteringsflöden från en rad olika aktörer (företag, nationella/statliga organisationer för incidenthantering, medborgare osv.) med de nationella brottsbekämpande organen och från de nationella brottsbekämpande organen till centrumet.
Centrumet bör samarbeta och underlätta utbytet av bästa praxis på hela det straffrättsliga och brottsbekämpande området. Effektivt deltagande av rättsväsendet i bekämningen av it-brottslighet är av största betydelse för att förbättra lagföringen av brottslingar som bedriver grova it-brott mellan medlemsstaterna.

(c) Ge stöd till medlemsstaternas utredningar av it-brott

Centrumet bör ge operativt stöd till utredningar av it-brott, t.ex. för att uppmuntra inrättandet av gemensamma arbetsgrupper för utredning av it-brott och utbyte av operativa uppgifter i pågående utredningar.
Det bör också ge högkvalitativt kriminalteknisk stöd (anläggningar, lagring och verktyg) och tillhandahålla krypteringsexperter för utredningar av it-brott.

(d) Bli de europeiska it-brottsutredarnas gemensamma röst på brottsbekämpningsområdet och inom rättsväsendet

Med tiden kan centrumet komma att fungera som en samlingspunkt för europeiska utredare av it-brott, förse dem med en gemensam röst vid diskussionerna med IKT-branschen och andra privata företag och med forskarsamhället, intresseorganisationerna för användare och organisationer i det civila samhället om hur man bättre förhindrar it-brott och samordnar riktad forskningsverksamhet.
Centrumet skulle vara den naturliga plattformen för Interpols it-brottsutredningar och andra internationella polisenheter som utreder it-brott. Det skulle också kunna samordna bidrag till

pågående initiativ för internetförvaltning samt FN:s öppna mellanstatliga expertgrupp om it-brottslighet.
Centrumet bör också samarbeta med organisationer såsom Insafe[32] i samband med informationskampanjer som riktar sig till allmänheten och uppdatera dem när centrumet genom analys identifierat förändringar i it-brotten i syfte att främja en försiktig och säker internetanvändning.

2.2. Lokalisering

Vilket framgår av genomförbarhetsstudien bör Europeiska centrumet mot it-brottslighet ingå som en del av Europol, och lokaliseras inom dess befintliga strukturer.

Detta medför tydliga fördelar. Europol har en erkänd roll bland medlemsstaterna och andra berörda parter, inklusive med Interpol och andra internationella brottsbekämpande myndigheter, och har redan till uppgift att ta itu med it-brottslighet[33]. Europols huvudfunktion är att bidra till ett säkrare Europa till nytta för alla medborgare, genom att stödja EU:s brottsbekämpande myndigheter genom utbyte och analys av kriminalunderrättelsesystem.

2.3. Centrumets konsekvenser vad gäller resurser

Genomförbarhetsstudien har granskat olika konsekvenser i resurshänseende. Dessa måste undersökas närmare[34], särskilt mot bakgrund av andra uppgifter som Europol i framtiden kan komma att behöva utföra och mer allmänt när det gäller bemanningen av EU:s organ. Denna bedömning kommer framför allt att ske inom ramen för översynen av Europols rättsliga grund och den pågående diskussionen om kommissionens förslag om en fond för den inre säkerheten. Det förefaller emellertid i detta skede redan uppenbart att utstationering av personal från medlemsstaterna kommer att behövas.

Vid bedömningen av beräknade anslagsbehov kommer kommissionen att vägledas av tre överväganden: för det första kan man anta att det kommer att förekomma en måttlig ökning av den totala mängden it-brott i motsats till en kraftig ökning av it-brott. För det andra kommer medlemsstaterna att öka sin egen kapacitet för att bekämpa it-brott. För det tredje kommer centrumet bara att hantera en viss grupp av it-brott.

2.4. Styrelseformer

Att placera centrumet inom Europol gör det viktigt att säkerställa att andra viktiga intressenter deltar i den strategiska ledningen av centrumet. Därför föreslår kommissionen att ett programråd för centrumet inrättas inom Europols ledningsstruktur, där ordförandeposten för programrådet innehas av chefen för centrumet. Detta instrument skulle ge andra berörda parter, t.ex. Eurojust, Cepol, medlemsstaterna, företrädda av EU:s arbetsgrupp mot it-brottslighet, Europeiska byrån för nät- och informationssäkerhet (Enisa) och kommissionen, möjlighet att dela med sig av sina respektive sakkunskaper, utan att förorsaka onödiga extra administrativa bördor. Detta programråd skulle kunna ta på sig ansvaret för centrumets verksamhet, vilket skulle säkerställa att verksamheten genomförs i partnerskap, med

---

32 Europeiskt nätverk av informationscentrum för att främja en säker och ansvarsfull användning av internet och mobila anordningar för ungdomar.

33 Rådets beslut (**2009/371/RIF)** av den 6 april 2009 om inrättande av Europeiska polisbyrån, artikel 4.1 jämförd med bilagan.

34 Bedömningen måste vara förenlig med de övergripande personal- och budgetmässiga kraven för organ i 2013 års budget och nästa fleråriga budgetram.

erkännande av alla berörda parters tillförda sakkunskaper och med iakttagande av samtliga intressenters uppdrag.

2.5. Samarbete med viktiga aktörer

Centrumet bör säkerställa ett samordnat agerande mot it-brottslighet, som inte bara möjliggör gemensamt arbete mellan EU:s organ, utan också fungerar som en enda europeisk kontaktpunkt på detta område.

(a) Medlemsstater

Det främsta syftet är att bistå medlemsstaterna vid deras bekämpning av it-brottslighet. Centrumets helpdesk för it-brott och förväntade resultat, t.ex. mer fokuserade hotbildsanalyser samt mer välinformerat operativt stöd kommer att gynna it-brottsutredare i hela Europa. EU:s arbetsgrupp mot it-brottslighet ska säkerställa att medlemsstaternas betänkligheter representeras i centrumets programråd. Medlemsstaternas måste fortsätta att göra nödvändiga investeringar i sina nationella strukturer för att bekämpa it-brottslighet, så att de har lämpliga plattformar för sin samverkan med centrumet.

(b) Europeiska organ och andra aktörer

Relevanta organ, bl.a. Eurojust, Cepol, Enisa och Cert-EU, skulle vara direkt involverade i centrumets verksamheter inte bara genom deras deltagande i programrådet, utan när det är lämpligt, också genom det operativa samarbetet med hänsyn till deras respektive uppdrag.

(c) Internationella partner

I dess strävan att utvecklas till ett informationsnav för Europeisk it-brottslighet, bör centrumet bli en värdefull samtalspartner för internationella partner om frågor om it-brottslighet. Centrumet bör, i samarbete med Interpol och våra strategiska partner runt om i världen, sträva efter att förbättra de samordnade insatserna i bekämpningen av it-brottslighet och säkerställa att brottsbekämpande intressen beaktas vid den framtida utvecklingen av internet.

(d) Privata sektorn, forskarsamhället och civila samhällsorganisationer

Uppbyggnaden av tilltron till och förtroendet mellan den privata sektorn och de brottsbekämpande myndigheterna är av största betydelse vid bekämpningen av it-brottslighet. För att konsolidera Europols arbete med befintliga och nya partner, bör centrumet bygga pålitliga nätverk och plattformar för informationsutbyte med industrin och andra berörda aktörer såsom forskarsamhället och civila samhällsorganisationer. Dessa bör underlätta informationsutbytet mellan de olika grupperna på en rad områden, t.ex. tidig varning för it-hot och insatser av typen samarbetsinriktade arbetsgrupper mot it-angrepp och andra typer av it-brottslighet.

Centrumet bör också bidra till mer omfattande insatser som görs av privata företag med betydande digitala informationsflöden, såsom banker och onlineåterförsäljare, för att bekämpa och ge bättre skydd mot it-brott och för att minimera sårbarheter vid utvecklingen av teknik.

Det är av ömsesidigt intresse för de brottsbekämpande myndigheterna och den privata sektorn att bättre kunna mäta it-brottsligheten i realtid samt att sträva efter en mer effektiv avveckling av nätverk som bedriver it-brott genom bättre upptäckt av nya tillvägagångssätt och snabb arrestering av it-brottslingar.

3. EN FÄRDPLAN MOT GENOMFÖRANDET AV ETT EUROPEISKT CENTRUM MOT IT-BROTTSLIGHET

3.1. Verksamhet fram till slutet av 2013

För att i inledningen få fram en operativ kapacitet kommer kommissionen att, i nära samarbete med Europol, undersöka vilka personalresurser och ekonomiska resurser som behövs för att inrätta en genomförandegrupp för centrumet fram till slutet av EU:s nuvarande budgetram. Genomförandegruppens uppgifter skulle t.ex. omfatta utarbetande av centrumets uppdrag och organisatoriska uppbyggnad, men också utvecklingen av indikatorer för att utvärdera dess resultat. De associerade intressenterna kommer att fastställa och komma överens om vilken roll och funktion programrådet ska ha.

I syfte att införa en fullständig samordnande funktion för information, bör genomförandegruppen för centrumet skapa länkar till Cert-EU:s förkonfigurationsgrupp och, när det är lämpligt, med Enisa (med hänsyn tagen till organets begränsade resurser). För att förbättra rapporteringen av it-brottsligheten ska en kartläggning genomföras för att skapa en karta över driftskompatibiliteten mellan de befintliga rapporteringssystemen om it-brott online i medlemsstaterna.
En kontaktpunkt för it-brott bör inrättas. Denna kontaktpunkt skulle kunna stödjas genom en därför avsedd, säker gemenskapsplattform online. Genom samordning av centrumet och dess programråd skulle man kunna bedöma och effektivisera den nuvarande utbildningsverksamheten som utförs av Europol, Cepol och Europeiska utbildningsgruppen när det gäller it-brottslighet (Ecteg). En bedömning av utbildningsbehovet, där också hänsyn tas till kraven på domare och åklagare, bör genomföras. Utifrån denna översyn skulle en grundläggande kurs mot it-brottslighet, som är öppen för aktörer, kunna utvecklas.

Dessutom kommer man att behöva göra en mer exakt bedömning av nödvändiga personalresurser och finansiella resurser, vilka ska tas upp i besluten om nästa fleråriga budgetram. Denna bedömning ska ge vägledning om centrumets eventuella utveckling i framtiden.

4. SLUTSATS

När den organiserade brottsligheten utökar sin verksamhet i cyberrymden måste de brottsbekämpande myndigheterna hålla jämna steg. EU kan förse medlemsstaterna och näringslivet med nya verktyg för att ta itu med det ständiga hotet från it-brottsligheten som, per definition, sträcker sig över alla gränser. Förutsatt att de nödvändiga personalresurserna och ekonomiska resurserna kan tryggas kommer ett Europeiskt centrum mot it-brottslighet att inrättas och fungera som en kontaktpunkt i Europas bekämpning av it-brottslighet genom att samla sakkunskaper, ge stöd till straffrättsliga utredningar och främja lösningar på EU-nivå, samtidigt som centrumet ska öka kunskaperna om frågor som rör it-brottsligheten i hela EU. Därmed skulle centrumet bidra till att trygga ett öppet internet och en laglig digital ekonomi och skydda EU:s medborgare och företag online.

Rådet uppmanas att godkänna detta förslag och Europaparlamentet och andra berörda parter uppmuntras att bidra till utvecklingen av centrumet.