



EUROPOS KOMISIJA

Briuselis, 2012 03 28
COM(2012) 140 final

KOMISIJOS KOMUNIKATAS TARYBAI IR EUROPOS PARLAMENTUI

Kova su nusikalstamumu skaitmeniniame amžiuje. Europos kovos su elektroniniu nusikalstamumu centro kūrimas

KOMISIJOS KOMUNIKATAS TARYBAI IR EUROPOS PARLAMENTUI

Kova su nusikalstamumu skaitmeniniame amžiuje. Europos kovos su elektroniniu nusikalstamumu centro kūrimas

1. ĮVADAS. EUROPOS KOVA SU NUSIKALTIMAIS, KURIEMS NĖRA SIENŲ

Internetas tapo neatskiriama ir būtina mūsų visuomenės ir ekonomikos dalis. 80 proc. jaunų europiečių kasdien palaiko tarpusavio ryšius naudodamiesi socialiniais tinklais internete¹, o metinė pasaulinės elektroninės prekybos apimtis yra apie 8 trilijonai USD². Tačiau kadangi vis didesnė kasdienio bendravimo ir verslo sandorių dalis vyksta internete, nusikalstama veikla taip pat plinta: visame pasaulyje elektroninių nusikaltimų aukomis kasdien tampa daugiau kaip 1 milijonas žmonių³. Su elektroninėmis ryšio priemonėmis susijusi nusikalstama veikla gali būti labai įvairi: vogtos kreditinės kortelės parduodamos vos už vieną eurą, vykdomos tapatybės vagystės ir seksualinė prievarta prieš vaikus, rengiamos rimtos kibernetinės atakos prieš institucijas ir infrastruktūros objektus.

Bendra elektroninių nusikaltimų žala visuomenei yra didelė. Neseniai paskelbtoje ataskaitoje teigiama, kad kasmet visame pasaulyje elektroninių nusikaltimų aukos patiria apie 388 mlrd. USD nuostolių – ši suma viršija bendrą metinį pelną, gaunamą iš pasaulinės prekybos marihuana, kokainu ir heroinu⁴. Nors tokią informaciją reikėtų vertinti atsargiai, nes pasitelkus skirtingus būdus elektroninių nusikaltimų pasekmėms vertinti nuostolių įverčiai būtų nevienodi, vis dėlto sutariama, kad elektroniniai nusikaltimai yra nelabai rizikinga didelį pelną duodanti nusikalstama veikla, kuri tampa vis labiau įprasta ir žalinga. Šiuo metu, kai itin svarbu skatinti ekonomikos augimą, nuožmesnė kova su elektroniniais nusikaltimais bus pagrindinis būdas piliečių ir įmonių pasitikėjimui saugiu interneto ryšiu ir prekyba internetu užtikrinti. Drauge taip pat bus siekiama strategijoje „Europa 2020“⁵ ir „Europos skaitmeninėje darbotvarkėje“⁶ nustatytų augimo tikslų.

Interneto laisvė yra svarbiausias veiksnys, lėmęs pastarųjų metų skaitmeninę revoliuciją. Mūsų atviram internetui negalioja nei nacionalinės sienos, nei bendra pasaulinė valdymo struktūra. Nors interneto laisvės skatinimas ir apsauga atitinka ES Pagrindinių teisių chartijos principus, taip pat turime siekti apsaugoti piliečius nuo organizuotų nusikalstamų grupuočių, siekiančių pasinaudoti šiuo atvirumu. Elektroniniai nusikaltimai, palyginti su kita nusikalstama veikla, visiškai nepaiso nacionalinių sienų, todėl teisėsaugos institucijos turi laikytis tarpvalstybinio požiūrio, vadovaujantis kuriuo bendradarbiaujama su viešaisiais ir privačiais suinteresuotaisiais subjektais ir tarpusavyje derinami veiksmai. Būtent šioje srityje ES gali užtikrinti ir iš tiesų užtikrina didelę papildomą naudą.

¹ 2010 m. gruodžio 14 d. Eurostato apklausa apie interneto prieigą ir naudojimąsi.

² *McKinsey Global Institute* 2011 m. gegužės mėn. paskelbta ataskaita *Internet matters: The Net's sweeping impact on growth, jobs, and prosperity*; prisijungimo prie ataskaitos internete data – 2012 m. vasario 8 d.

³ 2011 m. rugsėjo 7 d. *Symantec* paskelbta ataskaita *Norton Cybercrime Report 2011*; prisijungimo prie ataskaitos internete data – 2012 m. sausio 6 d.

⁴ *ibid.*

⁵ Strategija „Europa 2020“. Pažangaus, tvaraus ir integracinio augimo strategija“, COM(2010) 2020, 2010 m. kovo 3 d.

⁶ „Europos skaitmeninė darbotvarkė“, COM(2010) 245 galutinis, 2010 rugpjūčio 26 d.

Europos Sąjunga parengė įvairių kovos su elektroniniais nusikaltimais iniciatyvų. Tokių iniciatyvų pavyzdžiai – 2011 m. direktyva dėl kovos su seksualine prievarta prieš vaikus, jų seksualiniu išnaudojimu ir vaikų pornografija ir direktyva dėl atakų prieš informacines sistemas, daugiausia dėmesio skiriant baudmėms už elektroninių nusikaltimų priemonių, visų pirma botnetų, naudojimą⁷, kuri turėtų būti priimta 2012 m. Europolas išplėtė veiklą kovodamas su elektroniniais nusikaltimais ir po vieno itin nuodugnaus tyrimo, kuriame dalyvavo teisėsaugos institucijos iš viso pasaulio, atliko svarbiausią vaidmenį neseniai surengtoje *Gelbėjimo operacijoje* (angl. *Operation Rescue*), per kurią policija sulaukė 184 asmenis, įtariamus seksualiniais nusikaltimais prieš vaikus, ir nustatė daugiau kaip 200 prievartą patyrusių vaikų tapatybę. Europolo analitikai sėkmingai įveikė svarbiausio tinklo kompiuterinio serverio apsaugines priemones ir nustatė įtariamų nusikaltėlių tapatybes ir veiklą.

Kova su elektroniniais nusikaltimais, kurios pagrindinė priemonė yra Europos Tarybos Konvencija dėl elektroninių nusikaltimų⁸, tebėra svarbiausias prioritetas. Tai pripažinta Kovos su organizuotu ir sunkių formų tarptautiniu nusikalstamumu ES politikos ciklo dokumentuose⁹ ir ši kova yra neatskiriama pastangų formuoti visa apimančią ES strategiją kibernetiniam saugumui stiprinti dalis. ES taip pat aktyviai bendradarbiauja su tarptautiniais partneriais, pvz., dalyvauja ES ir JAV darbo grupės kibernetinio saugumo ir elektroninio nusikalstamumo klausimais veikloje.

Nors padaryta pažanga, vis dar iškyla tam tikrų kliūčių siekiant Europos lygmeniu veiksmingai tirti elektroninius nusikaltimus ir traukti pažeidėjus baudžiamojon atsakomybėn. Tokių kliūčių pavyzdžiai: jurisdikcijos ribos, nepakankami dalijimosi žvalgybos informacija pajėgumai, techniniai sunkumai nustatant elektroninius nusikaltimus darančių asmenų tapatybę, skirtingi tyrimo ir teismo ekspertizės gebėjimai, kvalifikuotų darbuotojų trūkumas ir nenuoseklus bendradarbiavimas su suinteresuotaisiais subjektais, atsakingais už kibernetinį saugumą. Taikydama Stabilumo priemonę ES taip pat sprendžia sparčiai didėjančių su elektroniniais nusikaltimais susijusių tarpvalstybinių grėsmių problemą besivystančiose ir pereinamojo laikotarpio šalyse, kuriose paprastai trūksta pajėgumų, reikalingų kovoti su šios formos organizuotu nusikalstamumu.

Siekdama spręsti šias problemas, Komisija, laikydamosi vidaus saugumo strategijoje¹⁰ nurodyto prioriteto, pareiškė ketinanti sukurti Europos kovos su elektroniniu nusikalstamumu centrą. Atlikusi tokio centro kūrimo galimybių studiją¹¹, Tarybos prašymu¹² Komisija siūlo

⁷ Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos dėl atakų prieš informacines sistemas, [COM\(2010\) 517 galutinis](#), 2010 m. rugsėjo 30 d. Botnetai yra kompiuterių, kuriuose įdiegta kenkimo programinė įranga, tinklai. Toks „užkrėstų“ kompiuterių tinklas gali būti naudojamas nuotoliniu būdu konkrečioms veiksmams atlikti, įskaitant kibernetinėms atakoms rengti.

⁸ 2001 m. lapkričio 23 d. Budapešte priimta [Europos Tarybos Konvencija dėl elektroninių nusikaltimų](#), taip pat žinoma kaip Budapešto konvencija. Prie jos pridėtas *Konvencijos dėl elektroninių nusikaltimų papildomas protokolai* dėl rasistinio ir ksenofobinio pobūdžio veikų, padarytų naudojantis kompiuterinėmis sistemomis, kriminalizavimo.

⁹ Per kovos su organizuotu ir sunkių formų tarptautiniu nusikalstamumu ES politikos ciklą, apimančią 2011–2013 m., įgyvendinami aštuoni prioritetai, vienas iš jų – „suintensyvinanti kovą su elektroniniais nusikaltimais ir organizuotų nusikalstamų grupuočių nusikalstamu internetu naudojimu“.

¹⁰ „ES [...] iki 2013 m. sukurs kovos su elektroniniu nusikalstamumu centrą, per kurį valstybės narės ir ES institucijos turės galimybę plėtoti operatyvinius ir analitinius tyrimų ir bendradarbiavimo su tarptautiniais partneriais gebėjimus“. [ES vidaus saugumo strategijos įgyvendinimas. Penki žingsniai kuriant saugesnę Europą](#). COM(2010) 673 galutinis, 2010 m. lapkričio 22 d.

¹¹ [Europos kovos su elektroniniu nusikalstamumu centro galimybių studija](#), 2012 m. vasario mėn.

sukurti Europos kovos su elektroniniu nusikalstamumu centrą (EC3), kuris bus Europolo dalis ir kuris vadovaus kovai su elektroniniu nusikalstamumu ES. Šiame galimybių studija pagrįstame komunikate nurodomos siūlomos pagrindinės Europos kovos su elektroniniu nusikalstamumu centro funkcijos, paaiškinama, kodėl jis turėtų būti Europolo dalis, ir kaip centras galėtų būti įkurtas. Tačiau iki kol centras pradės visiškai veikti, reikės toliau įvertinti ir nustatyti poveikį ištekliams. *Į šio centro kūrimą bus tinkamai atsižvelgta artimoje ateityje atliekant Europolo teisinio pagrindo peržiūrą.*

2. PASIŪLYMAS SUKURTI EUROPOS KOVOS SU ELEKTRONINIU NUSIKALSTAMUMU CENTRĄ

Kad Europos kovos su elektroniniu nusikalstamumu centras (EC3) duotų papildomos naudos ir būtų laikomasi subsidiarumo principo, siūloma daugiausia dėmesio skirti šių pagrindinių kategorijų elektroniniams nusikaltimams:

- (i) organizuotų nusikalstamų grupuočių daromi elektroniniai nusikaltimai, iš kurių gaunamas didelis neteisėtas pelnas, pvz., sukčiavimas internete;
- (ii) elektroniniai nusikaltimai, kurių aukos patiria didelę žalą, pvz., seksualinis vaikų išnaudojimas internete ir
- (iii) elektroniniai nusikaltimai (įskaitant kibernetines atakas), dėl kurių Sąjungoje nukenčia ypatingos svarbos infrastruktūros objektai ir informacinės sistemos¹³.

Atsižvelgiant į nuolat kintantį elektroninių nusikaltimų pobūdį, EC3 taip pat turėtų turėti galimybę imtis veiksmų tiek tenkinant valstybių narių prašymus, tiek šalinant naujas elektroninių nusikaltimų grėsmes Sąjungoje.

2.1. Europos kovos su elektroniniu nusikalstamumu centro pagrindinės funkcijos ir tikėtini veiklos rezultatai

EC3 turėtų atlikti keturias pagrindines funkcijas:

- (a) *Būti pagrindiniu Europos kovos su elektroniniu nusikalstamumu informacijos centru*

Informacijos sugretinimo funkcija leistų užtikrinti, kad iš įvairiausių viešųjų, privačiųjų ir atvirų šaltinių būtų renkama informacija apie elektroninius nusikaltimus, papildanti turimus policijos duomenis. Centras turėtų laipsniškai užpildyti informacijos, gaunamos iš suinteresuotųjų subjektų, atsakingų už kibernetinį saugumą, ir subjektų, kovojančių su elektroniniais nusikaltimais, spragas. Renkama informacija būtų susijusi su elektroniniais nusikaltimais, tokios veikos metodais ir įtariamaisiais. Tai padėtų geriau suprasti elektroninius nusikaltimus, užkirsti jiems kelią, juos nustatyti ir traukti baudžiamojon atsakomybėn nusikaltėlius, taip pat skatinti teisėsaugos institucijų, kompiuterinių incidentų tyrimo tarnybos (CERT) bendruomenės ir privačiojo sektoriaus informacinių ir ryšių technologijų (IRT)

¹² 2010 m. balandžio 26 d. Liuksemburge vykusiame 3010-ame Bendrųjų reikalų tarybos posėdyje priimtos Tarybos išvados dėl veiksmų plano, skirto Kovos su elektroniniais nusikaltimais suderintai strategijai įgyvendinti.

¹³ Kaip nustatyta 2008 m. gruodžio 8 d. Tarybos direktyvoje 2008/114/EB. Direktyva šiuo metu peržiūrima ir į tolesnius pakeičius būtų atsižvelgta vykdant EC3 veiklą.

saugumo specialistų tinkamus ryšius. Dalijantis informacija svarbu laikytis skirtingų šalių sudarytų konfidencialumo susitarimų ir tarpusavyje nustatytų taisyklių.

Informacijos sugretinimo funkcija taip pat būtų naudinga tobulinant ataskaitas apie elektroninius nusikaltimus ir dalijantis tokia informacija. Komisija pageidauja, kad valstybės narės įtvirtintų reikalavimą apie sunkius elektroninius nusikaltimus pranešti nacionalinėms teisėsaugos institucijoms¹⁴. Taip nacionalinės policijos tarnybos galėtų nuosekliau teikti informaciją apie sunkius elektroninius nusikaltimus EC3, kuris savo ruožtu skleistų tą informaciją, kad kolegose kitose valstybėse narėse žinotų, ar laikomasi tinkamos krypties, ir atlikdami tyrimus pasinaudotų vieni kitų turima informacija.

Tikslas – ilgainiui susidaryti aiškesnį vaizdą apie elektroninius nusikaltimus Europoje, kad būtų rengiamos kokybiškos strateginės ataskaitos dėl tendencijų ir grėsmių, būtų įgyta daugiau žinių remiantis išsamiais duomenimis apie nusikaltimus ir būtų tobulinama operatyvinė žvalgybinė informacija, gaunama iš bazės, kurioje renkami duomenys iš įvairių šaltinių.

(b) Sutelkti Europos kovos su elektroniniais nusikaltimais srities žinias siekiant padėti valstybėms narėms stiprinti gebėjimus

EC3 turėtų suteikti valstybėms narėms reikalingų praktinių žinių ir padėti rengti mokymus, kad būtų sumažintas elektroninis nusikalstamumas. Daugiausia dėmesio skiriama teisėsaugai, tačiau mokymai taip pat turėtų būti rengiami ir teisminėms institucijoms. Atlikus nuodugnų poreikių vertinimą, dabartinės Europolo, CEPOL ir valstybių narių iniciatyvos būtų racionalizuotos, kad būtų užtikrintas geresnis koordinavimas ir papildomumas. Toks mokymas turėtų apimti įvairias temas: nuo specialiųjų techninių žinių iki platesnio pobūdžio policijos pareigūnų, prokurorų ir teisėjų gebėjimų nagrinėti elektroninių nusikaltimų bylas stiprinimo.

Turėtų būti sukurta kovos su elektroniniais nusikaltimais tarnyba, kad būtų keičiamasi geriausia patirtimi ir žiniomis, palaikomi ryšiai su valstybėmis narėmis, tarptautinėmis teisėsaugos institucijomis, teisminėmis institucijomis, privačiuoju sektoriumi ir pilietinės visuomenės organizacijomis ir reaguojama į jų užklausas, pvz., tais atvejais, kai susiduriama su kibernetinėmis atakomis arba naujų formų apgavystėmis internete.

Ši tarnyba turėtų remti elektroninių nusikaltimų specialistų grupių, įskaitant Europos Sąjungos kovos su elektroniniais nusikaltimais darbo grupę ir ekspertų, kovojančių su seksualiniu vaikų išnaudojimu internete, veiklą ir juos konsultuoti. Taip pat turėtų būti bendradarbiaujama su rengiamu elektroninių nusikaltimų kompetencijos centrų tinklu, pvz., *2Centre*, ir mokslinių tyrimų bendruomene.

EC3 taip pat turėtų padėti valstybėms narėms rengti pranešimų apie elektroninius nusikaltimus teikimo internetu programą, pagrįstą sutartais standartais, kad įvairių veikėjų (įmonių, nacionalinių ir (arba) vyriausybinių kompiuterinių incidentų tyrimo tarnybų (CERT), piliečių ir t. t.) pranešimai būtų teikiami nacionalinėms teisėsaugos institucijoms, o jos savo ruožtu pranešimus perduotų EC3, taip pat padėti naudotis šia programa.

¹⁴ Pavyzdžiui, apie nusikaltimus, išvardytus siūlomos direktyvos dėl atakų prieš informacines sistemas 3–7 straipsniuose, COM(2010) 517 galutinis, 2010 m. rugsėjo 30 d.

EC3 turėtų užmegzti ryšius su baudžiamosios teisenos bendruomene ir teisėsaugos srities subjektais, taip pat sudaryti palankias sąlygas keistis geriausia patirtimi. Veiksmingas teisminių institucijų dalyvavimas kovojant su elektroniniais nusikaltimais itin svarbus siekiant visose valstybėse narėse veiksmingiau traukti baudžiamojon atsakomybėn sunkius elektroninius nusikaltimus darančius asmenis.

(c) *Padėti valstybėms narėms tirti elektroninius nusikaltimus*

EC3 turėtų teikti operatyvinę paramą tiriant elektroninius nusikaltimus, pvz., skatinti kurti jungtines elektroninių nusikaltimų tyrimų grupes ir per vykdomus tyrimus keistis operatyvine informacija.

Tiriant elektroninius nusikaltimus EC3 taip pat turėtų teikti aukšto lygmens pagalbą, susijusią su teismo ekspertize (įrenginiai, laikymo patalpos, priemonės), ir su šifravimu susijusias praktines žinias.

(d) *Tapti bendrą Europos elektroninių nusikaltimų tyrėjų, dirbančių teisėsaugos ir teisminėse institucijose, poziciją atstovaujančiu centru*

Ilgainiui EC3 galėtų tapti Europos elektroninių nusikaltimų tyrėjų vienijančiu centru ir užtikrinti, kad diskusijose su IRT pramone, kitomis privačiojo sektoriaus įmonėmis, mokslinių tyrimų bendruomene, naudotojų asociacijomis ir pilietinės visuomenės organizacijomis tyrėjai laikytųsi vienodos pozicijos siekdami nustatyti veiksmingesnes elektroninių nusikaltimų prevencijos priemones ir derinti tikslingą mokslinių tyrimų veiklą.

EC3 būtų sąsaja, jungianti su elektroniniais nusikaltimais susijusius Interpolo padalinius ir kitus tarptautinės policijos pajėgų skyrius, atsakingus už elektroninius nusikaltimus. EC3 taip pat galėtų koordinuoti veiksmus, kuriais prisidedama prie vykdomų iniciatyvų interneto valdymo klausimais, ir dalyvavimą JT atviros sudėtis tarpvyriausybinių elektroninių nusikaltimų ekspertų grupės veikloje.

Vykdydamas visuomenės informavimo kampanijas ir atnaujindamas jų turinį pagal centro išanalizuotus elektroninių nusikaltimų pokyčius, EC3 taip pat turėtų bendradarbiauti su tokiomis organizacijomis kaip INSAFE¹⁵, kad būtų skatinamas atsargus ir saugus elgesys internete.

2.2. Buvimo vieta

Kaip patvirtinta galimybių studijoje, Europos kovos su elektroniniu nusikalstamumu centras turėtų būti Europolo dalis ir veikti jo patalpose.

Tai duotų aiškios naudos. Valstybės narės ir kiti suinteresuotieji subjektai, įskaitant Interpolą ir tarptautines teisėsaugos institucijas, pripažįsta Europolo funkciją ir jam jau suteikti įgaliojimai tirti elektroninius nusikaltimus¹⁶. Svarbiausia Europolo funkcija – padėti užtikrinti didesnę visų Europos piliečių saugumą remiant ES teisėsaugos institucijų keitimąsi kriminalinės žvalgybos informacija ir jos analizę.

¹⁵ Europos informuotumo didinimo centrų tinklas, skatinantis jaunimą saugiai ir atsakingai naudotis internetu ir mobiliais prietaisais.

¹⁶ 2009 m. balandžio 6 d. Tarybos sprendimo ([2009/371/TVR](#)) dėl Europos policijos biuro (Europolo) įsteigimo 4 straipsnio 1 dalis kartu su priedu.

2.3. EC3 poveikis ištekliams

Galimybių studijoje išnagrinėti skirtingi atvejai, darantys poveikį ištekliams. Jie turės būti nuodugniai įvertinti¹⁷, visų pirma atsižvelgiant į kitas užduotis, kurias ateityje gali tekti atlikti Europolui, ir į bendras sąlygas, susijusias su darbuotojų įdarbinimu ES agentūrose. Atliekant vertinimą visų pirma turės būti atsižvelgiama į peržiūrimą Europolo teisinį pagrindą ir vykstančias diskusijas dėl Komisijos pasiūlymo kurti Vidaus saugumo fondą. Tačiau jau dabar beveik aišku, kad valstybės narės turės komandiruoti darbuotojus.

Vertindama numatomus išteklių poreikius, Komisija remsis šiomis trimis prielaidomis: pirma, prielaida, kad bendras nagrinėtinų elektroninių nusikaltimų bylų skaičius nežymiai padidės, o elektroninių nusikaltimų skaičius smarkiai išaugs; antra, valstybės narės sustiprins savo pajėgumus kovoti su elektroniniais nusikaltimais ir trečia, EC3 tirs tik tam tikrų kategorijų elektroninius nusikaltimus.

2.4. Valdymas

Į Europolo sudėtį įtraukus EC3 būtų svarbu užtikrinti, kad strateginiame centro valdyme dalyvautų ir kiti pagrindiniai suinteresuotieji subjektai. Todėl Komisija siūlo Europolo valdymo struktūroje įsteigti EC3 programos valdybą, kuriai pirmininkautų EC3 vadovas. Tokiu būdu kiti suinteresuotieji subjektai, pvz., Eurojustas, CEPOL, valstybės narės, atstovaujamos ES kovos su nusikaltimais darbo grupės, Europos tinklų ir informacijos apsaugos agentūra (ENISA) ir Komisija, be nereikalingos papildomos administracinės naštos turėtų galimybę perteikti savo praktinę patirtį. Valdyba skatintų EC3 atskaitingumą kovojant su elektroniniais nusikaltimais ir taip užtikrintų, kad veikla būtų vykdoma laikantis partnerystės principų, pripažįstant papildomą visų suinteresuotųjų subjektų praktinių žinių naudą ir atsižvelgiant į jų įgaliojimus.

2.5. Bendradarbiavimas su pagrindiniais dalyviais

EC3 turėtų užtikrinti koordinuotą kovą su elektroniniais nusikaltimais ne tik sudarydamas galimybę ES agentūroms bendradarbiauti, bet ir būdamas bendru Europos informaciniu centru šioje srityje.

(a) Valstybės narės

Svarbiausias tikslas – padėti valstybėms narėms kovoti su elektroniniais nusikaltimais. EC3 kovos su elektroniniais nusikaltimais pagalbos tarnyba ir siektini rezultatai, pvz., tikslingesnė grėsmių analizė ir tikslesnė informacija pagrįsta operatyvinė parama, bus naudingi elektroninių nusikaltimų tyrėjams Europoje. ES kovos su elektroniniais nusikaltimais darbo grupė užtikrintų, kad EC3 programos valdyboje būtų atsižvelgiama į valstybėms narėms susirūpinimą keliančius klausimus. Be to, valstybės narės turės toliau investuoti stiprindamos nacionalines kovos su elektroniniais nusikaltimais struktūras, kad turėtų tinkamą sąsają ryšiams su EC3 palaikyti.

(b) Europos agentūros ir kiti veikėjai

¹⁷ Vertinimas turi atitikti bendrus agentūroms taikomus su darbuotojų skaičiumi ir biudžetu susijusius reikalavimus, nustatytus 2013 m. biudžete ir kitoje daugiametėje finansinėje programoje.

Susijusios agentūros, visų pirma Eurojustas, CEPOL, ENISA ir CERT-ES, būtų tiesiogiai įtrauktos į EC3 veiklą ne tik dalyvaudamos programos valdyboje, bet prireikus palaikydamos operatyvinį bendradarbiavimą ir atsižvelgdamos į savo įgaliojimus.

(c) Tarptautiniai partneriai

Siekdamas tapti pagrindiniu Europos kovos su elektroniniu nusikalstamumu informaciniu centru, EC3 turėtų būti svarbus tarptautinis partneris kovos su elektroniniais nusikaltimais srityje. Palaikydamas partnerystės ryšius su Interpolu ir mūsų strateginiais partneriais visame pasaulyje, EC3 turėtų siekti, kad kova su elektroniniais nusikaltimais būtų kuo geriau koordinuojama, ir užtikrinti, kad plėtojant elektroninę erdvę būtų atsižvelgta į susirūpinimą keliančius klausimus, susijusius su teisės aktų vykdymu.

(d) Privatusis sektorius, mokslinių tyrimų bendruomenės ir pilietinės visuomenės organizacijos

Kovojant su elektroniniais nusikaltimais svarbiausia kurti privačiojo sektoriaus ir teisėsaugos institucijų tarpusavio pasitikėjimą. Siekdamas įtvirtinti Europolo darbą su dabartiniais ir naujais partneriais, EC3, bendradarbiaudamas su pramonės atstovais ir kitas veikėjais, pvz., mokslinių tyrimų bendruomene ir pilietinės visuomenės organizacijomis, turėtų plėtoti patikimus tinklus ir keitimosi informacija platformas. Jie turėtų sudaryti palankesnes sąlygas skirtingoms bendruomenėms keistis įvairaus pobūdžio informacija, įskaitant išankstinį įspėjimą apie kibernetinius pavojus, ir imtis bendrų „darbo grupės“ pobūdžio atsakomųjų priemonių kibernetinių atakų ir kitų kategorijų elektroninių nusikaltimų atvejais.

EC3 taip pat turėtų padėti didelį elektroninį turtą turinčioms privačiojo sektoriaus įmonėms, pvz., bankams ir internete prekiaujantiems mažmenininkams, kovoti su elektroniniais nusikaltimais ir geriau nuo jų apsaugoti, taip pat plėtojant technologijas mažinti jų pažeidžiamumą.

Teisėsaugos institucijas ir privatųjį sektorių sieja abipusis interesas realiu laiku tiksliau įvertinti elektroninių nusikaltimų padėtį, taip pat siekti veiksmingiau ardyti elektroninių nusikaltėlių tinklus sparčiau nustatant naujus veikimo būdus ir nedelsiant sulaikant kibernetinius nusikaltėlius.

3. EUROPOS KOVOS SU ELEKTRONINIU NUSIKALSTAMUMU CENTRO VEIKLOS VYKDYMO PLANAS

3.1. Veikla iki 2013 m. pabaigos

Kad būtų užtikrinti pradiniai veiklos pajėgumai, Komisija, glaudžiai bendradarbiaudama su Europolu, nagrinės, kokių žmogiškųjų ir finansinių išteklių reikėtų buriant EC3 įgyvendinimo komandą iki dabartinės ES finansinės programos pabaigos. Įgyvendinimo komandos užduotys būtų, pavyzdžiui, parengti EC3 įgaliojimus ir organizacijos struktūrą, taip pat rodiklius veiklos rezultatams vertinti. Programos valdybos funkcija ir veikla bus išsamiau apibrėžta ir suderinta su susijusiais suinteresuotaisiais subjektais.

Siekiant užtikrinti visapusišką duomenų sugretinimo funkciją, EC3 įgyvendinimo komanda prireikus turėtų užmegzti ryšius su CERT išankstinės veiklos grupe ir su ENISA, atsižvelgdama į jų ribotus išteklius. Siekiant tobulinti pranešimų apie elektroninius nusikaltimus teikimo tvarką, bus atlikta padėties analizė, kad būtų parengtas esamų pranešimų

apie elektroninius nusikaltimus teikimo internetu sistemų valstybėse narėse suderinamumo planas.

Turėtų būti sukurta kovos su elektroniniais nusikaltimais tarnyba. Šiai tarnybai vykdyti veiklą turėtų padėti speciali saugi interneto bendruomenės platforma. Dabartinę Europolo, CEPOL ir Europos mokymo ir švietimo elektroninių nusikaltimų srityje grupės mokymo veiklą EC3 kartu su programos valdyba galėtų koordinuotai įvertinti ir racionalizuoti. Turėtų būti atlikta mokymo poreikių, taip pat atsižvelgiant į teisėjų ir prokurorų reikalavimus, analizė. Atlikus tokio pobūdžio peržiūrą galėtų būti surengtas bendras mokymo kursas kovos su elektroniniais nusikaltimais tema; jame galėtų dalyvauti baudžiamosios teisenos sistemos nariai.

Be to, reikės tiksliau įvertinti, kokių būtinų žmogiškųjų ir finansinių išteklių reikėtų, ir tai turėtų būti numatyta sprendimuose, kurie bus priimami pagal kitą daugiametę finansinę programą. Į šio vertinimo išvadas bus atsižvelgta toliau plėtojant EC3.

4. IŠVADA

Teisėsaugos institucijos negali likti nuošalyje ir leisti organizuotų nusikaltėlių grupuotėmis toliau plėsti veiklą elektroninėje erdvėje. Valstybėms narėms ir pramonės atstovams ES gali suteikti priemonių kovoti su šiuolaikine ir plintančia elektroninių nusikaltimų, kuriems negalioja sienos, grėsme. Jeigu bus užtikrinti būtini žmogiškieji ir finansiniai ištekliai, Europos kovos su elektroniniu nusikalstamumu centras taps pagrindiniu Europos kovos su elektroniniu nusikalstamumu informaciniu centru; bus sutelktos praktinės žinios, teikiama parama atliekant baudžiamuosius tyrimus ir skatinant ieškoti visai ES bendrų sprendimų, kartu didinant informuotumą apie elektroninius nusikaltimus visoje Sąjungoje. Centras padėtų užtikrinti interneto saugumą ir teisėtą skaitmeninę ekonomiką ir apsaugoti internetu besinaudojančius Europos piliečius ir įmones.

Taryba raginama pritarti šiam pasiūlymui, o Europos Parlamentas ir kiti susiję suinteresuotieji subjektai skatinami prisidėti kuriant centrą.