EVROPSKA KOMISIJA

Bruselj, 28.3.2012
COM(2012) 140 final

SPOROČILO KOMISIJE SVETU IN EVROPSKEMU PARLAMENTU

Boj proti kriminalu v digitalni dobi: ustanovitev Evropskega centra za boj proti kibernetski kriminaliteti

SPOROČILO KOMISIJE SVETU IN EVROPSKEMU PARLAMENTU

Boj proti kriminalu v digitalni dobi: ustanovitev Evropskega centra za boj proti kibernetski kriminaliteti

1. UVOD: EVROPSKI ODZIV NA KRIMINAL, KI PRESEGA MEJE ENE DRŽAVE

Internet je postal sestavni in nepogrešljiv del naše družbe in gospodarstva. V spletne socialne mreže je vključenih 80 % mladih Evropejcev[1], spletno trgovanje na svetovni ravni pa letno ustvari približno 8 000 milijard USD[2]. Naše življenje in poslovne transakcije se vedno bolj selijo na splet, kar velja tudi za kriminalne dejavnosti – več milijonov ljudi po svetu postanejo žrtve kibernetske kriminalitete[3]. Med spletne kriminalne dejavnosti uvrščamo kazniva dejanja, kot so prodaja ukradenih kreditnih kartic za komaj en evro, kraja identitete in spolna zloraba otrok ter resni kibernetski napadi na institucije in infrastrukture.

Kibernetska kriminaliteta družbo veliko stane. Nedavno poročilo kaže, da žrtve kibernetske kriminalitete po svetu vsako leto izgubijo 388 milijard USD, po čemer je ta oblika kriminala bolj donosna od skupne svetovne trgovine z marihuano, kokainom in heroinom[4]. Čeprav je pri takih informacijah potrebna previdnost, saj se ocene stroškov lahko zaradi različnih opredelitev kibernetske kriminalitete razlikujejo, velja, da kibernetska kriminaliteta prinaša storilcem kaznivih dejanj velike dobičke ob nizkem tveganju. Poleg tega se njena pojavnost povečuje in povzroča vedno več škode. V času, ko je spodbujanje gospodarske rasti izjemnega pomena, bo okrepitev boja proti kibernetski kriminaliteti bistvena za ohranitev zaupanja državljanov in podjetij v varno spletno komuniciranje in trgovino. Tako se bo podprlo tudi doseganje ciljev glede rasti, ki so določeni v strategiji Evropa 2020[5] in sporočilu Evropska digitalna agenda[6].

Svoboda interneta je ključni dejavnik pri pojasnitvi digitalne revolucije v zadnjih letih. Naš odprti internet ne pozna nacionalnih meja ali enotne upravljavske strukture na svetovni ravni. Čeprav spodbujamo in varujemo svobodo spleta v skladu z Listino EU o temeljnih pravicah, si moramo prizadevati tudi za zaščito državljanov pred organiziranimi kriminalnimi združbami, ki to odprtost skušajo izkoristiti. Nobena oblika kriminala nima bolj mednarodnega značaja kot kibernetska kriminaliteta in od organov kazenskega pregona zahteva, da usklajeno sodelujejo prek nacionalnih meja z javnostjo in zainteresiranimi iz zasebnega sektorja. Prav k temu lahko EU pomembno prispeva tudi v prihodnje.

Evropska unija je oblikovala več pobud za boj proti kibernetski kriminaliteti. Mednje spada Direktiva o boju proti spolnemu izkoriščanju otrok na spletu in otroški pornografiji iz

---

1 Eurostat, novica o dostopu do interneta in njegovi uporabi z dne 14. decembra 2010.

2 McKinsey Global Institute, Internet Matters: the Net's sweeping impact on growth, jobs and prosperity. Poročilo iz maja 2011; zadnji dostop 8. februarja 2012.

3 Poročilo Norton Cybercrime Report 2011, Symantec, 7. september 2011, zadnji dostop 6. januarja 2012.

4 Glej prejšnjo opombo.

5 Evropa 2020 – Strategija za pametno, trajnostno in vključujočo rast, COM(2010) 2020 z dne 3. marca 2010.

6 Evropska digitalna agenda, COM(2010) 245 final z dne 26. avgusta 2010.

leta 2011 ter Direktiva o napadih na informacijske sisteme, ki se osredotoča na kaznovanje zlorabe orodij za izvajanje kibernetske kriminalitete, zlasti botnetov[7], ki naj bi bila sprejeta leta 2012. Europol je povečal obseg svojih dejavnosti v boju proti kibernetski kriminaliteti in je imel ključno vlogo v nedavni operaciji „Rescue“, med katero je bilo aretiranih 184 oseb, za katere obstaja sum, da so storilci kaznivih dejanj zoper spolno nedotakljivost otrok, in identificiranih več kot 200 otrok, ki so bili žrtve zlorabe. Navedena operacija je sledila eni največjih tovrstnih preiskav na svetu, ki so jo kdaj opravili organi kazenskega pregona. Podatki o identiteti in dejavnosti domnevnih storilcev kaznivih dejanj so bili razkriti s prizadevanji analitikov Europola in vdorom v ključni strežnik v središču omrežja mimo varnostnega sistema strežnika.

Boj proti kibernetski kriminaliteti, katerega glavna pravna podlaga je Konvencija Sveta Evrope o kibernetski kriminaliteti[8], je še naprej prednostna naloga EU. Vključen je tudi v cikel oblikovanja politik EU za boj proti organiziranemu kriminalu in hudim oblikam mednarodne kriminalitete[9] ter je sestavni del prizadevanj za razvoj celovite strategije EU, namenjene krepitvi kibernetske varnosti. EU tesno sodeluje tudi z mednarodnimi partnerji, na primer v okviru delovne skupine EU–ZDA za kibernetsko varnost in boj proti kibernetski kriminaliteti.

Kljub napredku še vedno obstaja več ovir za učinkovito preiskovanje kibernetske kriminalitete in sodni pregon storilcev na evropski ravni. Mednje spadajo: meje jurisdikcije, nezadostne zmogljivosti za izmenjavo obveščevalnih podatkov, tehnične težave pri izsleditvi izvora storilcev kibernetske kriminalitete, nesorazmerje med preiskovalnimi in forenzičnimi zmogljivostmi, premalo usposobljenega osebja in nedosledno sodelovanje z drugimi zainteresiranimi stranmi, ki so pristojne za kibernetsko varnost. EU tudi prek Instrumenta za stabilnost posveča pozornost hitremu razvoju nadnacionalnih groženj v zvezi s kibernetsko kriminaliteto v državah v razvoju in tranziciji, saj te navadno nimajo zadostnih zmogljivosti za boj proti tej obliki organiziranega kriminala.

V odgovor na te izzive je Komisija v strategiji notranje varnosti[10] nakazala, da je ustanovitev Evropskega centra za boj proti kibernetski kriminaliteti njena prednostna naloga. Komisija bo na podlagi študije izvedljivosti ustanovitve takega centra[11], ki jo je zahteval Svet[12], predlagala ustanovitev Evropskega centra za boj proti kibernetski kriminaliteti (v nadaljnjem besedilu:

---

7 Predlog Direktive Evropskega parlamenta in Sveta o napadih na informacijske sisteme, COM (2010)517 final z dne 30. septembra 2010. Botneti so omrežja računalnikov, okuženih s škodljivo programsko opremo, ki se lahko aktivirajo na daljavo za izvajanje posebnih nalog, tudi spletnih napadov.

8 Konvencija Sveta Evrope o kibernetski kriminaliteti, podpisana v Budimpešti, dne 23. novembra 2001. Znana tudi kot Konvencija iz Budimpešte. Konvencijo dopolnjuje *Dodatni protokol h Konvenciji o kibernetski kriminaliteti*, ki obravnava inkriminacijo rasističnih in ksenofobičnih dejanj, storjenih v informacijskih sistemih.

9 Cikel oblikovanja politik EU za boj proti organiziranemu kriminalu in hudim oblikam mednarodne kriminalitete, ki zajema obdobje 2011–2013, ima osem prednostnih nalog, med katere spada tudi „okrepitev boja proti kibernetski kriminaliteti in kriminalni zlorabi interneta s strani organiziranih kriminalnih združb“.

10 „EU bo do leta 2013 … ustanovila center za kibernetsko kriminaliteto, prek katerega bodo države članice in institucije EU lahko vzpostavile operativne in analitične zmogljivosti za preiskave ter sodelovanje z mednarodnimi partnerji“ iz sporočila „Izvajanje strategije notranje varnosti EU: pet korakov k varnejši Evropi“. COM(2010) 673 final z dne 22. novembra 2010.

11 Feasibility study for a European Cybercrime Centre, končno poročilo, februar 2012.

12 Sklepi Sveta v zvezi z akcijskim načrtom za izvajanje skupne strategije boja proti kaznivim dejanjem. 3010. seja Sveta za splošne zadeve, Luxembourg, 26. aprila 2010.

EC3), ki bo sestavni del Europola in bo deloval kot osrednja točka v boju proti kibernetski kriminaliteti v EU. V tem sporočilu so na podlagi študije izvedljivosti opisane predlagane temeljne naloge Evropskega centra za boj proti kibernetski kriminaliteti, pojasnjeni so razlogi za njegovo vključitev v Europol in način njegove ustanovitve. Potrebna sredstva bo treba dodatno oceniti in zagotoviti, preden začne EC3 popolnoma delovati. Ustanovitev tega centra se bo ustrezno upoštevala v prihodnji reviziji pravne podlage Europola.

2. PREDLOG ZA USTANOVITEV EVROPSKEGA CENTRA ZA BOJ PROTI KIBERNETSKI KRIMINALITETI

Da bi Evropski center za boj proti kibernetski kriminaliteti zagotavljal dodano vrednost in da bi se spoštovalo načelo subsidiarnosti, se predlaga, da se EC3 osredotoča na naslednje glavne pojavne oblike kibernetske kriminalitete:

(i) kibernetska kazniva dejanja, ki so jih zagrešile organizirane kriminalne združbe, zlasti tista, ki ustvarjajo ogromne nezakonite dobičke, kot so spletne goljufije;

(ii) kibernetska kazniva dejanja, ki žrtvam povzročajo resno škodo, kot so spolno izkoriščanje otrok na spletu; in

(iii) kibernetska kazniva dejanja (vključno s kibernetskimi napadi), ki vplivajo na ključno infrastrukturo in informacijske sisteme v Uniji[13].

Ker se kibernetska kriminaliteta nenehno spreminja, je treba predvideti tudi možnost ukrepanja zaradi zahtev držav članic in novih groženj kibernetskega kriminala, s katerimi bi se srečala Unija.

2.1. Ključne funkcije in naloge Evropskega centra za boj proti kibernetski kriminaliteti

EC3 mora imeti štiri temeljne naloge:

(a) Delovati mora kot osrednja evropska informacijska točka v boju proti kibernetski kriminaliteti

Z združevanjem informacij bi se zagotovilo zbiranje podatkov o kibernetski kriminaliteti iz številnih javnih, zasebnih in prosto dostopnih virov, s čimer bi se obogatili podatki, ki so na voljo policiji. Tako bi se postopoma premostile sedanje vrzeli v informacijah, ki so na voljo skupnostim, odgovornim za kibernetsko varnost in boj proti kibernetski kriminaliteti. Zbrane informacije bi se nanašale na dejavnosti in metode kibernetske kriminalitete ter osumljence. Služi za izboljšanje znanja o kibernetski kriminaliteti in njeno preprečevanje, odkrivanje in pregon ter za spodbujanje ustreznih stikov med organi kazenskega pregona, mrežo skupin za odzivanje na računalniške grožnje (CERT) ter strokovnjaki za varnost na področju informacijske in komunikacijske tehnologije (IKT) v zasebnem sektorju. Pri izmenjavi informacij je treba spoštovati sporazume o zaupnosti, sklenjene med različnimi stranmi, in med njimi dogovorjena pravila.

---

[13] Direktiva Sveta 2008/114/ES z dne 8. decembra 2008. Trenutno je v postopku revizije. EC3 bi morebitne spremembe upošteval.

Združevanje informacij bi bilo zelo koristno tudi za izboljšanje poročanja in izmenjavo informacij o kibernetski kriminaliteti. Komisija si želi, da bi države članice uvedle obveznost prijave hudih kibernetskih kaznivih dejanj nacionalnim organom kazenskega pregona[14]. To bi nacionalnim policijskim službam omogočilo, da Evropskemu centru za boj proti kibernetski kriminaliteti bolj dosledno zagotavljajo informacije o hudih kibernetskih kaznivih dejanjih, ta pa bi jih pošiljal kolegom iz drugih držav članic, ki bi lahko ugotovili, ali si prizadevajo za dosego istega cilja, in imeli korist od informacij, ki so jih drugi zbrali med preiskavami.

Cilj je postopno izboljšanje znanja o kibernetski kriminaliteti v Evropi, da bi se omogočila priprava kakovostnih strateških poročil o trendih in grožnjah, izboljšala obveščenost na podlagi celovitih številskih podatkov o kriminaliteti in nadgradili operativni obveščevalni podatki iz zbirke podatkov, ki temelji na različnih virih.

(b) Združevati mora strokovna znanja v Evropi o kibernetski kriminaliteti, da bi podprl države članice pri krepitvi zmogljivosti

EC3 bi moral državam članicam pomagati s strokovnim znanjem in usposabljanjem, da bi se kibernetska kriminaliteta omejila. Glavni poudarek je na pregonu, vendar bi bilo treba pravosodnim organom zagotoviti usposabljanje. Obstoječe pobude Europola, Cepola in držav članic bi se uskladile na podlagi temeljite analize potreb, da bi zagotovili boljšo usklajenost in dopolnjevanje. To usposabljanje bi segalo od izvajanja podrobnih tehničnih analiz do širšega izboljšanja usposobljenosti pripadnikov policije, tožilcev in sodnikov za obravnavanje primerov kibernetskih kaznivih dejanj.

Ustanoviti bi bilo treba službo za pomoč v boju proti kibernetski kriminaliteti, ki bi skrbela za izmenjavo najboljših praks in znanja, sodelovala z državami članicami, mednarodnimi organi kazenskega pregona, pravosodnimi organi, zasebnim sektorjem in organizacijami civilne družbe ter odgovarjala na njihove poizvedbe na primer ob kibernetskih napadih ali odkritju novih oblik spletnih goljufij.

Podpirati bi moral dejavnosti in zagotavljati svetovanje strokovnim skupinam na področju kibernetske kriminalitete, tudi projektni skupini Evropske unije za boj proti kibernetski kriminaliteti, in strokovnjakom v boju proti spolnemu izkoriščanju otrok na spletu. Vzpostaviti bi moral tudi sodelovanje z nastajajočo mrežo centrov odličnosti za boj proti kibernetski kriminaliteti, kot je 2Centre, in raziskovalno skupnostjo.

EC3 bi moral državam članicam pomagati tudi pri njihovih prizadevanjih za razvoj in uvedbo spletne aplikacije za poročanje o kibernetski kriminaliteti na podlagi dogovorjenih standardov, da bi se lahko poročila različnih akterjev (podjetij, nacionalnih/vladnih skupin za odzivanje na računalniške grožnje itn.) pošiljala nacionalnim organom kazenskega pregona, poročila slednjih pa Evropskemu centru za boj proti kibernetski kriminaliteti.

EC3 bi moral sodelovati z akterji na področju kazenskega pravosodja in pregona ter omogočati izmenjavo najboljših praks med njimi. Uspešno sodelovanje pravosodnih organov v boju proti kibernetski kriminaliteti je izrednega pomena za izboljšanje uspešnosti kazenskega pregona storilcev hudih kibernetskih kaznivih dejanj.

---

[14] Kot tistih iz členov 3 do 7 osnutka Direktive o napadih na informacijske sisteme, COM(2010) 517 final z dne 30. septembra 2010.

(c) Državam članicam mora zagotavljati podporo pri preiskovanju kibernetske kriminalitete

EC3 bi moral zagotoviti operativno podporo pri preiskovanju kibernetske kriminalitete, na primer s spodbujanjem ustanavljanja skupnih preiskovalnih skupin za boj proti kibernetski kriminaliteti in izmenjavo operativnih informacij o tekočih preiskavah.

Zagotavljati bi moral tudi zelo kakovostno forenzično pomoč (objekti, shranjevanje podatkov, orodja) in strokovna znanja s področja šifriranja pri preiskovanju kibernetske kriminalitete.

(d) Postati mora skupni glas evropskih preiskovalcev kibernetske kriminalitete iz vseh organov kazenskega pregona in pravosodnih organov

Postopoma bi lahko EC3 deloval kot stičišče evropskih preiskovalcev kibernetske kriminalitete in jim zagotovil, da kot en glas nastopijo v razpravah s podjetji IKT in drugimi podjetji iz zasebnega sektorja ter raziskovalno skupnostjo, združenji uporabnikov in organizacijami civilne družbe o najboljših načinih za preprečevanje kibernetske kriminalitete in usklajevanje ciljno usmerjenih raziskovalnih dejavnosti.

EC3 bi bil naravni vmesnik za sodelovanje z Interpolom in drugimi mednarodnimi policijskimi enotami na področju boja proti kibernetski kriminaliteti. Usklajeval bi lahko tudi prispevke k tekočim pobudam glede upravljanja interneta in delu odprte medvladne strokovne skupine ZN na področju kibernetske kriminalitete.

EC3 bi moral sodelovati z organizacijami, kot je INSAFE[15], in sicer pri izvajanju kampanj ozaveščanja javnosti, namenjenih spodbujanju previdnejše in varnejše uporabe interneta, in pri njihovem nadgrajevanju zaradi sprememb v kibernetskih kaznivih dejanjih, ki jih je Center odkril med svojimi analizami.

2.2. Sedež

Kot je razvidno iz študije izvedljivosti, bi moral biti Evropski center za boj proti kibernetski kriminaliteti sestavni del Europola in vključen v obstoječe strukture.

Ta pristop ima jasne prednosti. Europol uživa ugled med državami članicami in drugimi zainteresiranimi stranmi, vključno z Interpolom in mednarodnimi organi pregona, in je že pristojen za obravnavanje računalniškega kriminala[16]. Temeljna naloga Europola je pomoč pri izboljšanju varnosti v Evropi v korist vseh državljanov, tako da zagotavlja podporo organom kazenskega pregona v EU z izmenjavo in analizo obveščevalnih podatkov o kaznivih dejanjih.

2.3. Sredstva, potrebna za EC3

V študiji izvedljivosti so bili proučene različne možnosti v zvezi s sredstvi. Potrebna je dodatna ocena[17], zlasti na podlagi drugih nalog, ki jih bo morda moral opravljati Europol v prihodnosti, in širšega okvira v zvezi z osebjem agencij EU. Ta ocena se bo izvedla zlasti v

---

15 Evropska mreža centrov za ozaveščanje, ki spodbuja varno in odgovorno uporabo interneta in mobilnih naprav pri mladih ljudeh.

16 Sklep Sveta (2009/371/PNZ) z dne 6. aprila 2009 o ustanovitvi Evropskega policijskega urada (Europol), člen 4(1) v povezavi s prilogo.

17 Ocena mora biti v skladu s splošnimi kadrovskimi in proračunskimi zahtevami, ki veljajo za agencije na podlagi proračuna za leto 2013 in naslednjega večletnega finančnega okvira.

okviru revizije pravne podlage Europola in tekoče razprave o predlogu Komisije za ustanovitev Sklada za notranjo varnost. Vendar je že zdaj jasno, da bodo svoje strokovnjake morale napotiti države članice.

Komisija bo pri ocenjevanju potrebe po virih upoštevala tri vidike: prvič, domnevati je treba, da bo prišlo do zmernega in ne ogromnega povečanja skupnega števila obravnavanih primerov kibernetskih kaznivih dejanj; drugič, države članice bodo okrepile svoje zmogljivosti za boj proti kibernetski kriminaliteti; in tretjič, EC3 bo obravnaval le nekatere oblike kibernetskih kaznivih dejanj.

2.4. Upravljanje

Če bo EC3 sestavni del Europola, bi bilo pomembno zagotoviti sodelovanje drugih ključnih zainteresiranih strani pri strateškem usmerjanju dela Centra. Zato Komisija predlaga ustanovitev programskega odbora EC3 v okviru upravljavske strukture Europola, ki bi mu predsedoval vodja EC3. Ta instrument bi drugim zainteresiranim stranem, kot so Eurojust, Cepol, države članice, ki jih zastopa projektna skupina EU za boj proti kibernetski kriminaliteti, ENISA in Komisija, dal možnost, da prispevajo svoje znanje in izkušnje brez nepotrebnega dodatnega upravnega bremena. Odbor bi lahko skrbel, da EC3 odgovorno izvaja dejavnosti na področju boja proti kibernetski kriminaliteti, s čimer bi zagotovil njihovo izvajanje v partnerstvu z vsemi zainteresiranimi stranmi, in sicer ob priznavanju dodane vrednosti njihovega strokovnega znanja ter spoštovanju njihovih pristojnosti.

2.5. Sodelovanje s ključnimi akterji

EC3 bi moral zagotoviti usklajen odziv na kibernetsko kriminaliteto ter tako omogočiti skupno delo agencij EU in prevzeti vlogo enotne evropske točke za stike na tem področju.

(a) Države članice

Glavni cilj je pomoč državam članicam v boju proti kibernetski kriminaliteti. Služba za pomoč v boju proti kibernetski kriminaliteti v okviru EC3 ter izpolnjeni cilji EC3, kot sta bolj osredotočena analiza groženj in bolje obveščena operativna podpora, bodo prinesli koristi preiskovalcem kibernetske kriminalitete po vsej Evropi. Projektna skupina EU za boj proti kibernetski kriminaliteti bi zagotovila, da se v programskem odboru EC3 zastopajo tudi interesi držav članic. Poleg tega bodo morale države članice še naprej izvajati potrebne naložbe v nacionalne strukture za boj proti kibernetski kriminaliteti, da bi ustvarile ustrezne možnosti za sodelovanje z EC3.

(b) Evropske agencije in drugi akterji

Zadevne agencije, zlasti Eurojust, Cepol in ENISA ter CERT-EU, bi bile neposredno vključene v dejavnosti EC3 prek sodelovanja v programskem odboru ter operativnega sodelovanja, kadar je to primerno in ob spoštovanju njihovih pristojnosti.

(c) Mednarodni partnerji

EC3 bi si moral v svojih prizadevanjih, da postane osrednja evropska informacijska točka v boju proti kibernetski kriminaliteti, zagotoviti vlogo koristnega sogovornika z mednarodnimi partnerji na področju kibernetske kriminalitete. EC3 bi si moral v partnerstvu z Interpolom in našimi strateškimi partnerji po svetu prizadevati za izboljšanje usklajenih odzivov v boju proti

kibernetski kriminaliteti in zagotoviti, da se pri prihodnjem razvoju kibernetskega prostora upoštevajo pomisleki organov kazenskega pregona.

(d) Zasebni sektor, raziskovalne skupnosti in organizacije civilne družbe

Vzpostavitev zaupanja med zasebnim sektorjem in organi kazenskega pregona je zelo pomembna za boj proti kibernetski kriminaliteti. EC3 bi moral utrditi sodelovanje med Europolom ter njegovimi sedanjimi in novimi partnerji, vzpostaviti pa bi bilo treba tudi zanesljiva omrežja in platforme za izmenjavo informacij z industrijo in drugimi akterji, kot so raziskovalna skupnost in organizacije civilne družbe. Tako bi se v vsej skupnosti olajšala izmenjava informacij o različnih vprašanjih, vključno z zgodnjim opozarjanjem na kibernetske grožnje in odzivanjem na kibernetske napade in druge oblike kibernetske kriminalitete po vzoru na sodelovalni pristop projektnih skupin.

EC3 bi moral prispevati tudi k širitvi prizadevanj podjetij iz zasebnega sektorja z velikimi računalniškimi zmogljivostmi, kot so banke in spletne prodajalne, za boj proti kibernetski kriminaliteti in boljšo zaščito pred njo ter k zmanjšanju ranljivosti tehnologij v razvoju.

Jasnejši pregled kibernetske kriminalitete v realnem času in učinkovitejše razbijanje mrež storilcev kibernetskih kaznivih dejanj z okrepljenim razkrivanjem njihovih novih načinov delovanja ter hitro prijetje teh storilcev je v vzajemnem interesu organov kazenskega pregona in zasebnega sektorja.

3. NAČRT POTEKA USTANOVITVE EVROPSKEGA CENTRA ZA BOJ PROTI KIBERNETSKI KRIMINALITETI

3.1. Dejavnosti do konca leta 2013

Da se doseže začetna operativna zmogljivost, bo Komisija v tesnem sodelovanju z Europolom proučila, koliko človeških in finančnih virov bi bilo potrebnih, da se do izteka sedanjega finančnega okvira EU oblikuje skupina za ustanovitev EC3. Naloge te skupine bi bile na primer opredelitev mandata in organizacijske strukture EC3 ter razvoj kazalnikov za ocenjevanje njegove učinkovitosti. Vlogo in delovanje programskega odbora bodo opredelile povezane zainteresirane strani in se o tem tudi dogovorile.

Z namenom vzpostavitve celovitega združevanja informacij bi morala skupina za ustanovitev EC3 ustvariti povezave do pripravljalne skupine CERT-EU in po potrebi do agencije ENISA (ob upoštevanju njihovih omejenih virov). Zaradi izboljšanja poročanja o kibernetski kriminaliteti bo opravljen posnetek stanja, ki se bo uporabil za ugotavljanje interoperabilnosti obstoječih spletnih sistemov držav članic za poročanje o kibernetski kriminaliteti.

Ustanoviti bi bilo treba službo za pomoč v boju proti kibernetski kriminaliteti. Njeno delovanje bi lahko podpiralo posebno varno spletno okolje, namenjeno zadevni skupnosti. EC3 in njegov programski odbor bi lahko usklajevala ocenjevanje in racionalizacijo tekočih dejavnosti, ki jih na področju usposabljanja izvajajo Europol, Cepol ter Evropska skupina za usposabljanje in izobraževanje na področju kibernetske kriminalitete. Opraviti bi bilo treba analizo potreb na področju usposabljanja, ta pa bi morala upoštevati tudi zahteve sodnikov in tožilcev. Iz tega pregleda bi lahko nastalo osnovno usposabljanje za boj proti kibernetski kriminaliteti, ki bi bilo na voljo osebju sistema kazenskega pravosodja.

Poleg tega bo treba pripraviti natančnejšo oceno potrebnih človeških in finančnih virov in jo predvideti v sklepih o naslednjem večletnem finančnem okviru. Ta ocena bo vplivala na nadaljnji razvoj EC3.

4. SKLEPNA UGOTOVITEV

Ker organizirane kriminalne združbe širijo svoje dejavnosti na splet, jim morajo slediti tudi organi kazenskega pregona. EU lahko državam članicam in gospodarstvu zagotovi orodja za boj proti sodobni in stalno se razvijajoči grožnji kibernetske kriminalitete, ki ne pozna meja. Če se Evropskemu centru za boj proti kibernetski kriminaliteti zagotovijo potrebni človeški in finančni viri, lahko postane osrednja točka evropskega boja proti kibernetski kriminaliteti, ki bi z združevanjem strokovnega znanja zagotavljala podporo kazenskim preiskavam in spodbujala rešitve na ravni EU, pri tem pa dvigovala zavest o nevarnostih kibernetske kriminalitete po vsej Uniji. Tako bi Center prispeval k varovanju odprtega interneta in zakonitega digitalnega gospodarstva ter zaščiti evropskih državljanov in podjetij na spletu.

Svet se poziva, da podpre ta predlog, Evropski parlament in druge zadevne zainteresirane strani pa so vabljeni, da prispevajo k razvoju Centra.