EVROPSKÁ KOMISE

V Bruselu dne 28.3.2012
COM(2012) 140 final

SDĚLENÍ KOMISE RADĚ A EVROPSKÉMU PARLAMENTU

Řešení trestné činnosti v digitálním věku: zřízení Evropského centra pro boj proti kyberkriminalitě

SDĚLENÍ KOMISE RADĚ A EVROPSKÉMU PARLAMENTU

Řešení trestné činnosti v digitálním věku: zřízení Evropského centra pro boj proti kyberkriminalitě

1. ÚVOD: EVROPSKÁ ODPOVĚĎ NA TRESTNOU ČINNOST BEZ HRANIC

Internet se stal nedílnou a nepostradatelnou součástí naší společnosti a našeho hospodářství. Internetové sociální sítě využívá pro vzájemnou komunikaci mezi sebou i pro komunikaci se světem na 80 % mladých Evropanů[1] a prostřednictvím elektronického obchodu se každým rokem na celém světě uskuteční transakce ve výši 8 bilionů USD[2]. Na internetu se však v rostoucí míře neodehrávají jen náš každodenní život a obchod – internet je totiž zároveň stále častěji dějištěm trestné činnosti. Každý den se na celém světě stane obětí kybernetického trestného činu více než jeden milion lidí[3]. Trestná činnost na internetu má různé formy, které sahají od prodeje zcizených úvěrových karet za pouhé jedno euro přes krádeže totožnosti a pohlavní zneužívání dětí až po závažné kybernetické útoky na instituce a infrastrukturu.

Celková cena, kterou společnost za kyberkriminalitu platí, je významná. Z nedávno zveřejněné zprávy vyplývá, že celosvětově přicházejí oběti této trestné činnosti v jejím důsledku každým rokem o cca 388 miliard USD, a že kyberkriminalita je tak výnosnější než celosvětový obchod s marihuanou, kokainem a heroinem dohromady[4]. S těmito údaji je sice třeba nakládat opatrně, protože různé definice následků kyberkriminality mohou vést k rozdílným odhadům, avšak panuje shoda o tom, že kyberkriminalita je vysoce výnosnou a málo rizikovou formou trestné činnosti, která je stále častější a která způsobuje čím dál větší škody. V době, kdy má prvořadý význam podněcování hospodářského růstu, bude nanejvýš důležité zesílit boj proti kyberkriminalitě, aby se zachovala důvěra občanů a podniků v bezpečnou internetovou komunikaci a bezpečný internetový obchod. Podpora boje proti kyberkriminalitě bude rovněž přispívat k plnění růstových cílů vytyčených ve strategii Evropa 2020[5] a v Digitální agendě pro Evropu[6].

Svoboda internetu je klíčovým faktorem, jenž vysvětluje digitální revoluci posledních let. Otevřený internet totiž nezná nic, jako jsou hranice států nebo jediná celosvětová struktura řízení. Přestože tuto internetovou svobodu v souladu s Listinou základních práv EU podporujeme a ochraňujeme, musíme také usilovat o ochranu občanů před organizovanými zločineckými skupinami, které se snaží této otevřenosti využívat. Žádný druh trestné činnosti nezná hranic v takové míře jako kyberkriminalita a tato skutečnost si od donucovacích orgánů vyžaduje, aby přijaly koordinovaný přístup založený na spolupráci a přesahující hranice států,

---

1 *Eurostat, Internet Access and Use* (Přístup k internetu a jeho používání) ze dne 14. prosince 2010.

2 McKinsey Global Institute, *Internet Matters: the Net's sweeping impact on growth, jobs and prosperity*. (Internet a jeho komplexní dopad na růst, zaměstnanost a prosperitu). Zpráva z května 2011 nastudovaná dne 8. února 2012.

3 *Norton Cybercrime Report 2011*, Symantec. Zpráva společnosti Norton o kyberkriminalitě, vypracovaná 7. září 2011 a nastudovaná 6. ledna 2012

4 Ibid.

5 Evropa 2020 – Strategie pro inteligentní a udržitelný růst podporující začlenění, KOM(2010) 2020 ze dne 3. března 2010.

6 Digitální agenda pro Evropu, KOM(2010) 245 v konečném znění ze dne 26. srpna 2010.

do něhož by byly zapojeny i zúčastněné strany z veřejného a soukromého sektoru. Právě v této oblasti EU může být – a také je – výrazně přínosná.

Evropská unie vypracovává k řešení kyberkriminality různé iniciativy, mezi které patří například směrnice o boji proti pohlavnímu vykořisťování dětí na internetu a dětské pornografii z roku 2011 a směrnice o útocích proti informačním systémům, jež se zaměřuje na postihy za využívání nástrojů kyberkriminality, zejména tzv. botnetů[7], a jež by měla být přijata v roce 2012. Europol zintenzívnil svou činnost zaměřenou proti kyberkriminalitě a sehrál klíčovou úlohu v nedávné operaci „Rescue“, v rámci níž policie zatkla 184 osob podezřelých z pohlavního zneužívání dětí a identifikovala více než 200 obětí, a sice v návaznosti na nejrozsáhlejší vyšetřování svého druhu provedené donucovacími orgány z celého světa. Díky analytikům Europolu, kterým se podařilo prolomit zabezpečení klíčového počítačového serveru v ústředí sítě, byla odhalena totožnost a činnost podezřelých.

Boj proti kyberkriminalitě, jehož hlavním právním nástrojem je Úmluva Rady Evropy o kyberkriminalitě[8], zůstává i nadále klíčovou prioritou. Je zmíněn v politickém cyklu EU pro boj proti organizované a závažné mezinárodní trestné činnosti[9] a je nedílnou součástí snah o vypracování zastřešující unijní strategie ke zvýšení kybernetické bezpečnosti. Evropská unie rovněž úzce spolupracuje s mezinárodními partnery, například prostřednictvím aktuálně působící pracovní skupiny EU-USA pro problematiku kybernetické bezpečnosti a kyberkriminality.

Pomineme-li tento pokrok, na evropské úrovni brání účinnému vyšetřování kyberkriminality a stíhání pachatelů stále ještě několik překážek. Patří k nim kupříkladu hranice jurisdikcí, nedostatečné schopnosti sdílet zpravodajské informace, technické potíže při stopování původu pachatelů kybernetických trestných činů, nesourodost vyšetřovacích a forenzních kapacit, nedostatek vyškoleného personálu a nekonzistentní spolupráce s ostatními zúčastněnými stranami odpovědnými za kybernetickou bezpečnost. Prostřednictvím nástroje stability řeší EU také rychle se vyvíjející nadnárodní hrozby související s kyberkriminalitou v rozvojových zemích a v zemích procházejících transformací, v nichž potřebné kapacity pro boj proti této formě organizované trestné činnosti často chybí.

V reakci na tyto problémy Komise uvedla, že hodlá v rámci strategie vnitřní bezpečnosti zřídit Evropské centrum pro boj proti kyberkriminalitě[10]. V návaznosti na studii proveditelnosti[11]

---

7 Návrh směrnice Evropského parlamentu a Rady o útocích proti informačním systémům, KOM(2010) 517 v konečném znění ze dne 30. září 2010. Pojmem „botnet“ se rozumí síť počítačů napadených škodlivým softwarem, kterou lze dálkově aktivovat za účelem provedení konkrétních akcí, včetně kybernetických útoků.

8 Council of Europe Cybercrime Convention, Budapešť, 23. listopadu 2001, známá také pod názvem Budapešťská úmluva. Součástí úmluvy je dodatkový protokol týkající se stíhání činů rasistické a xenofobní povahy spáchaných prostřednictvím počítačových systémů.

9 Politický cyklus EU pro boj proti organizované a závažné mezinárodní trestné činnosti na roky 2011–2013 má osm priorit, z nichž jednou je „zesílit boj proti kyberkriminalitě a zneužívání internetu skupinami organizované trestné činnosti.“

10 „EU do roku 2013 vytvoří … centrum pro boj proti kyberkriminalitě, jehož prostřednictvím budou moci členské státy a evropské orgány budovat operační a analytické kapacity pro vyšetřování a spolupráci s mezinárodními partnery“ ve Strategii vnitřní bezpečnosti Evropské unie: pět kroku směrem k bezpečnější Evropě , KOM(2010) 673 v konečném znění ze dne 22. listopadu 2010.

11 *Feasibility study for a European Cybercrime Centre* (Studie proveditelnosti pro Evropské centrum pro boj proti kyberkriminalitě), závěrečná zpráva z února 2012.

zřízení takového centra a na žádost Rady[12] navrhuje Komise vytvoření Evropského centra pro boj proti kyberkriminalitě (EC3), jež bude součástí Europolu a jež bude základnou pro boj proti kyberkriminalitě v EU. Předmětné sdělení vychází ze studie proveditelnosti a pro Evropské centrum pro boj proti kyberkriminalitě vytyčuje navrhované hlavní funkce a vysvětluje, proč by toto centrum mělo být umístěno v Europolu a jaké jsou možnosti jeho zřízení. Před plným zprovozněním EC3 však bude potřeba dále posoudit a upravit záležitosti související se zdroji. Zřízení tohoto centra se odpovídajícím způsobem zohlední při nadcházející revizi právního základu pro Europol.

2. NÁVRH NA ZŘÍZENÍ EVROPSKÉHO CENTRA PRO BOJ PROTI KYBERKRIMINALITĚ

Aby bylo Evropské centrum pro boj proti kyberkriminalitě přínosné, Komise při zohlednění zásady subsidiarity navrhuje, aby se zaměřovalo na tyto hlavní druhy kyberkriminality:

i) kybernetické trestné činy páchané organizovanými zločineckými skupinami, zejména pak činy vytvářející vysoké nezákonné zisky, např. podvody na internetu;

ii) kybernetické trestné činy působící závažnou újmu jejich obětem, např. pohlavní vykořisťování dětí na internetu, a dále

iii) kybernetické trestné činy (včetně kybernetických útoků) poškozující kritickou infrastrukturu a informační systémy v Unii[13].

Jelikož se kyberkriminalita neustále vyvíjí, měl by se také vytvořit prostor pro přijímání opatření v reakci na požadavky členských států a pro opatření, jež by řešila nově vyvstávající kybernetická nebezpečí ohrožující Unii.

2.1. Hlavní funkce a očekávaný přínos Evropského centra pro boj proti kyberkriminalitě

Evropské centrum pro boj proti kyberkriminalitě by mělo mít čtyři hlavní funkce:

(a) sloužit jako evropská základna pro informace o kyberkriminalitě

Centrum by jako styčný informační orgán zajišťovalo shromažďování informací o kyberkriminalitě z celé řady veřejných, soukromých a otevřených zdrojů, a rozšiřovalo by tak dostupné policejní údaje. Centrum by mělo postupně vyplňovat stávající mezery v informacích, které poskytují subjekty odpovědné za kybernetickou bezpečnost a boj proti kyberkriminalitě. Shromažďované informace by se týkaly kybernetické trestné činnosti, metod a osob z této činnosti podezřelých. Centrum by přispívalo k rozšiřování znalostí o kyberkriminalitě a k jejímu předcházení, odhalování a stíhání a podporovalo by také odpovídající vazby mezi donucovacími orgány, skupinou pro reakci na počítačové hrozby (CERT) a odborníky na zabezpečení informačních a komunikačních technologií ze soukromého sektoru. Při sdílení informací by se musely dodržovat dohody a pravidla týkající se důvěrnosti, na kterých se různé strany dohodly.

---

[12] Závěry Rady o akčním plánu provádění jednotné strategie boje proti počítačové trestné činnosti, 3010. zasedání Rady pro obecné záležitosti, Lucemburk, 26. dubna 2010.

[13] Podle definic ve směrnici Rady 2008/114/ES ze dne 8. prosince 2008. Tato směrnice je v současné době revidována, EC3 by zohledňovalo další vývoj.

Funkce styčného informačního orgánu by byla rovněž užitečná pro snazší sdílení informací a lepší podávání zpráv. Komise by ráda, aby v členských státech platila povinnost ohlašovat závažné kybernetické trestné činy vnitrostátním donucovacím orgánům[14]. To by vnitrostátní policii umožňovalo konzistentněji poskytovat informace o závažných kybernetických trestných činech Evropskému centru pro boj proti kyberkriminalitě, jež by je pak zase dále šířilo, aby o nich věděli kolegové v ostatních členských státech pro případ, že by svou práci zaměřovali stejným směrem a informace získané jinde by pro ně byly při vyšetřování prospěšné.

Cílem je rozšířit postupem času obzory, pokud jde o kyberkriminalitu v Evropě, aby bylo možné vypracovávat vysoce kvalitní strategické zprávy o trendech a hrozbách, aby se na základě souhrnných údajů o trestné činnosti zvýšila informovanost a aby se díky informační základně postavené na různých zdrojích zlepšilo operační zpravodajství.

(b) shromažďovat Evropě dostupné odborné poznatky o kyberkriminalitě v zájmu podpory členských států při budování kapacit

Evropské centrum pro boj proti kyberkriminalitě by mělo členským státům pomáhat v potlačování kyberkriminality prostřednictvím poskytování odborných poznatků a školení. Na prvním místě stojí donucovací orgány, avšak školení by se mělo poskytovat i orgánům soudním. V zájmu zlepšení koordinace a komplementarity by se po důsledné analýze potřeb zefektivnily stávající iniciativy Europolu, Evropské policejní akademie (CEPOL) a členských států. Odborná příprava by měla sahat od hloubkových odborných poznatků až k širšímu budování kapacit, které by policii, státním zástupcům a soudcům pomáhaly řešit případy kyberkriminality.

Dále by se měl zřídit útvar pro boj proti kyberkriminalitě, jenž by umožňoval výměnu poznatků a osvědčených postupů, kontaktování členských států, donucovacích orgánů na mezinárodní úrovni, justice, soukromého sektoru a organizací občanské společnosti a zodpovídání jejich dotazů, například v případě kybernetických útoků nebo nových forem internetových podvodů.

Evropské centrum pro boj proti kyberkriminalitě by mělo být pracovní oporou a poradcem specializovaných odborných skupin, včetně pracovní skupiny EU pro boj proti kyberkriminalitě a odborníků zabývajících se bojem proti pohlavnímu vykořisťování dětí na internetu. Centrum by rovněž mělo navázat spolupráci se vznikající sítí středisek excelence pro problematiku kyberkriminality, např. se střediskem 2Centre, a s vědeckou obcí.

Evropské centrum pro boj proti kyberkriminalitě by mělo také vypomáhat členským státům v jejich snaze o vyvinutí a spuštění internetové aplikace pro hlášení případů kyberkriminality, která by se zakládala na sjednaných standardech a zajistila by napojení ohlašovacích kanálů pocházejících od různých aktérů (podniků, státních/vládních skupin pro reakci na počítačové hrozby, občanů atd.) na vnitrostátní donucovací orgány a následně prostřednictvím těchto orgánů na samotné EC3.

Plánované EC3 by mělo být v kontaktu s trestními soudy a donucovacími orgány a usnadňovat napříč těmito subjekty výměnu osvědčených postupů. Účinné zapojení soudnictví

[14] Například trestné činy uvedené v článcích 3 až 7 předloženého návrhu směrnice o útocích proti informačním systémům, KOM(2010) 517 v konečném znění ze dne 30. září 2010.

má mimořádný význam pro lepší stíhání nebezpečných pachatelů kybernetických trestných činů napříč členskými státy.

(c) poskytovat členským státům podporu při vyšetřování kyberkriminality

Evropské centrum pro boj proti kyberkriminalitě by mělo poskytovat operační podporu pro vyšetřování případů kyberkriminality, například podněcováním vzniku společných vyšetřovacích týmů a propagací výměny operačních informací při probíhajících vyšetřováních.

Centrum by při vyšetřování kyberkriminality mělo rovněž poskytovat forenzní pomoc na vysoké úrovni (zařízení, skladování, nástroje) a odborné poznatky o šifrování.

(d) vystupovat za evropský kolektiv odborníků, kteří se v donucovacích a soudních orgánech zabývají vyšetřováním kyberkriminality

Z EC3 by se mělo časem stát místo sdružující evropské vyšetřovatele zabývající se kyberkriminalitou, za které bude toto centrum mluvit v diskusích s odvětvím IKT a s podniky z jiných oblastí soukromého sektoru, s vědeckou obcí, se sdruženími uživatelů a organizacemi občanské společnosti o způsobech, jak lze kyberkriminalitě lépe předcházet a jak lze lépe koordinovat cílenou výzkumnou činnost.

Evropské centrum pro boj proti kyberkriminalitě by bylo přirozeným rozhraním pro specializované činnosti Interpolu a jiných mezinárodních policejních subjektů zabývajících se kyberkriminalitou. Mohlo by rovněž koordinovat vstupy do probíhajících iniciativ souvisejících se správou internetu a do otevřené mezivládní expertní skupiny OSN pro otázky kyberkriminality.

Centrum by mělo také spolupracovat s organizacemi, jako je INSAFE[15], na realizaci osvětových kampaní a na jejich aktualizaci v reakci na změny, které EC3 v kyberkriminalitě zaznamená, aby byla veřejnost vedena k opatrnému a bezpečnému chování na internetu.

2.2. Umístění

Jak bylo doloženo ve studii proveditelnosti, EC3 by mělo být součástí Europolu a mělo by být umístěno v rámci jeho stávajících struktur.

Tato možnost je spojena s řadou výhod. Europol je mezi členskými státy a dalšími zúčastněnými stranami (včetně Interpolu a donucovacích orgánů na mezinárodní úrovni) uznávaný a k řešení počítačové kriminality již má mandát[16]. Hlavním úkolem Europolu je podporovat donucovací orgány ve státech EU výměnami a rozbory kriminálního zpravodajství, a napomáhat tak větší bezpečnosti v Evropě ku prospěchu všech občanů.

---

15 Evropská síť center pro zvyšování povědomí mladých lidí o bezpečném a odpovědném užívání internetu a mobilních přístrojů.

16 Rozhodnutí Rady (2009/371/SVV) ze dne 6. dubna 2009 o zřízení Evropského policejního úřadu, ustanovení čl. 4 odst. 1 ve spojení s přílohou.

2.3. Dopady EC3 na zdroje

Studie proveditelnosti prozkoumala různé dopady na zdroje. Ty však bude potřeba dále posoudit [17], zejména ve světle dalších úkolů, jež bude možná muset Europol v budoucnu plnit, a s ohledem na obecnější okolnosti personálního obsazení agentur EU. Toto posouzení se provede konkrétně v rámci revize právního základu pro Europol a v rámci probíhající diskuse o návrhu Komise na Fond vnitřní bezpečnosti. Již v tuto chvíli je však zřejmé, že budou zapotřebí vyslaní odborníci z členských států.

Při posuzování odhadovaných požadavků na zdroje bude Komise vycházet ze tří předpokladů: 1) celkový počet řešených případů kybernetických trestných činů se mírně zvýší, ačkoli kyberkriminalita zaznamená masivní nárůst; 2) členské státy posílí své vlastní schopnosti bojovat s kyberkriminalitou a 3) Evropské centrum pro boj proti kyberkriminalitě se bude zabývat pouze určitou skupinou kybernetických trestných činů.

2.4. Správa

Bude-li EC3 umístěno v rámci Europolu, bude důležité do jeho strategického řízení zapojit i další klíčové zúčastněné strany. Komise proto navrhuje, aby se ve správní struktuře Europolu zřídila programová rada EC3, které by předsedal vedoucí EC3. Tento orgán by ostatním zúčastněným stranám, např. Eurojustu, Evropské policejní akademii, členským státům (zastoupeným pracovní skupinou EU pro otázky kyberkriminality), agentuře ENISA a Komisi umožnil přispívat svým *know-how*, aniž by tak zbytečně vznikala další administrativní zátěž. Programová rada by mohla podněcovat odpovědnost za plnění úkolů EC3 v oblasti kyberkriminality a zajišťovat tak, že úkoly se budou provádět v partnerství, přičemž by oceňovala přínosné odborné poznatky a respektovala mandáty všech zúčastněných stran.

2.5. Spolupráce s klíčovými aktéry

Evropské centrum pro boj proti kyberkriminalitě by mělo zajišťovat koordinované reakce na kyberkriminalitu, a to jednak tím, že by umožňovalo spolupráci mezi agenturami EU, jednak tím, že by v této oblasti sloužilo jako jedno evropské kontaktní místo.

(a) Členské státy

Hlavním účelem centra je napomáhat členským státům v boji proti kyberkriminalitě. Helpdesk a činnosti EC3, například cílenější analýzy nebezpečí a informovanější operační podpora, budou přínosné pro vyšetřovatele kybernetických trestných činů v celé Evropě. Zájmy členských států by v programové radě EC3 zastupovala pracovní skupina EU pro otázky kyberkriminality. Členské státy budou muset i nadále investovat potřebné prostředky do svých vnitrostátních struktur pro boj proti kyberkriminalitě, tak aby disponovaly odpovídajícím rozhraním pro interakci s EC3.

(b) Evropské agentury a ostatní aktéři

Do činností EC3 by byly přímo zapojeny příslušné agentury, konkrétně Eurojust, CEPOL a ENISA, a také CERT-EU, a to nejen svou účastí v programové radě, nýbrž i prostřednictvím případné operační spolupráce s přihlédnutím k jejich konkrétním mandátům.

---

[17] Posouzení musí být v souladu s celkovými požadavky na personál a rozpočet pro agentury v rozpočtu na rok 2013 a v příštím víceletém finančním rámci.

(c) Mezinárodní partneři

V rámci své snahy o postupné vyprofilování v evropskou základnu pro informace o kyberkriminalitě by se EC3 mělo stát v otázkách kyberkriminality cenným prostředníkem mezinárodních partnerů. Evropské centrum pro boj proti kyberkriminalitě by mělo v partnerství s Interpolem a strategickými partnery ve světě usilovat o zlepšování koordinovaných odpovědí v boji proti kyberkriminalitě a zajišťovat zohledňování problémů spojených s prosazováním práva při dalším vývoji kyberprostoru.

(d) Soukromý sektor, vědecká obec a organizace občanské společnosti

V boji proti kyberkriminalitě má mimořádný význam získávání vzájemné důvěry mezi soukromým sektorem a donucovacími orgány. Posilováním spolupráce Europolu se stávajícími a novými partnery by mělo EC3 budovat důvěryhodné sítě a platformy pro výměnu informací s průmyslem a dalšími aktéry, např. s vědeckou obcí a organizacemi občanské společnosti. Tyto sítě a platformy by mezi různými skupinami usnadnily sdílení informací o řadě otázek včetně včasného varování před kybernetickými hrozbami a umožnily by také reagovat na kybernetické útoky a jiné typy kyberkriminality způsobem, který by byl založený na spolupráci ve formě pracovních skupin.

Centrum by mělo rovněž přispívat k obecnějším snahám soukromých podniků se značným množstvím digitálních aktiv, např. bank a internetových prodejců, bojovat proti kyberkriminalitě, lépe se před ní chránit a minimalizovat zranitelnost vyvíjených technologií.

Lepší přehled o vývoji kyberkriminality v reálném čase je v zájmu donucovacích orgánů i soukromého sektoru a totéž platí o rozbíjení sítí této trestné činnosti, které lze zefektivnit lepším odhalováním nových způsobů, jakými tyto sítě své činnosti provozují, a rychlým zatýkáním pachatelů.

3. PLÁN PRO ZŘÍZENÍ EVROPSKÉHO CENTRA PRO BOJ PROTI KYBERKRIMINALITĚ

3.1. Činnosti do konce roku 2013

Aby bylo EC3 schopno zahájit počáteční provoz, Komise v úzké spolupráci s Europolem prozkoumá, jaké lidské a finanční zdroje by byly do konce stávajícího finančního rámce EU zapotřebí k ustavení zřizovacího týmu. Mezi úkoly zřizovacího týmu by například figurovalo navržení mandátu a organizační struktury EC3 a také vypracování ukazatelů k hodnocení práce tohoto centra. Úlohu a fungování programové rady by dále definovaly a dojednaly zapojené zúčastněné strany.

V zájmu zřízení centra s funkcí plnohodnotného styčného informačního orgánu by měl zřizovací tým navázat vazby s prekonfiguračním týmem CERT-EU a případně (s přihlédnutím k jejich omezeným zdrojům) s agenturou ENISA. V zájmu lepšího podávání zpráv o kyberkriminalitě proběhne mapování, jehož cílem bude vytvořit mapu interoperabilních internetových systémů pro hlášení kyberkriminality, které v současnosti fungují v členských státech.

Zřídit by se měl útvar pro kyberkriminalitu, který by mohl být podpořen vytvořením specializované bezpečné internetové platformy. V rámci koordinace EC3 a jeho programové rady by se mohly vyhodnotit a zefektivnit školení a vzdělávání poskytované v současné době

Europolem, CEPOLem a Evropskou skupinou pro odbornou přípravu a vzdělání v oblasti kyberkriminality. V oblasti vzdělávání by se měla provést analýza potřeb, jež by zvážila i potřeby soudců a státních zástupců. V návaznosti na tento přezkum by se mohl uspořádat základní vzdělávací kurz zaměřený na kyberkriminalitu, do kterého by se mohli hlásit odborníci pracující v oblasti trestního soudnictví.

Kromě výše uvedeného bude třeba přesněji vyhodnotit potřebné lidské a finanční zdroje a zajistit je v rozhodnutích v rámci příštího víceletého finančního rámce. Toto hodnocení je podkladem pro další rozvoj EC3.

4. ZÁVĚR

Vzhledem k tomu, že působnost organizované trestné činnosti se rozšiřuje o kyberprostor, musí se také rozšířit a posílit prosazování práva. Evropská unie může členským státům a průmyslu poskytnout nástroje k řešení novodobých, stále se vyvíjejících nebezpečí kyberkriminality, která svou povahou nezná hranic. Bude-li možné zajistit potřebné lidské a finanční zdroje, bude základnou evropského boje proti kyberkriminalitě Evropské centrum pro boj proti kyberkriminalitě. To by shromažďovalo odborné poznatky, podporovalo kriminální vyšetřování, podněcovalo řešení celounijního rozsahu a zvyšovalo v celé EU povědomí o problémech spojených s kyberkriminalitou, čímž by přispívalo k ochraně otevřeného internetu a zákonného digitálního hospodářství a k bezpečí evropských občanů a podniků na internetu.

Komise vyzývá Radu k přijetí tohoto návrhu a Evropský parlament a další příslušné zúčastněné strany pak vybízí k tomu, aby k vybudování centra přispěly.