COMISIA EUROPEANĂ

Bruxelles, 28.3.2012
COM(2012) 140 final

# COMUNICARE A COMISIEI CĂTRE CONSILIU ŞI PARLAMENTUL EUROPEAN

## Combaterea criminalității în era digitală actuală: instituirea unui Centru european de combatere a criminalității informatice

**COMUNICARE A COMISIEI CĂTRE CONSILIU ŞI PARLAMENTUL EUROPEAN**

**Combaterea criminalităţii în era digitală actuală: instituirea unui Centru european de combatere a criminalităţii informatice**

## 1. INTRODUCERE: RĂSPUNSUL EUROPEAN LA CRIMINALITATEA FĂRĂ FRONTIERE

Internetul a devenit o parte integrantă şi indispensabilă a societăţii şi a economiei noastre. 80 % din tinerii europeni se conectează unii cu alţii şi cu lumea prin intermediul unor reţele de socializare online[1], iar valoarea schimburilor comerciale mondiale efectuate anual prin comerţ electronic atinge aproximativ 8 trilioane USD[2]. Însă, dat fiind că din ce în ce mai multe aspecte din viaţa noastră cotidiană şi din ce în ce mai multe tranzacţii comerciale se realizează online, infracţiunile devin, la rândul lor, din ce în ce mai frecvente. În fiecare zi, peste un milion de persoane din lumea întreagă sunt victime ale criminalităţii informatice[3]. Activităţile infracţionale online variază de la vânzarea unor cărţi de credit furate pentru suma modică de un euro, la furtul de identitate şi la abuzuri sexuale asupra copiilor, mergând până la atacuri informatice grave împotriva instituţiilor şi a infrastructurilor.

Costul total al criminalităţii informatice pe care îl suportă societatea este semnificativ. Un raport recent arată că victimele înregistrează anual pierderi de aproximativ 388 de miliarde USD, la nivel mondial, din cauza criminalităţii informatice, ceea ce face ca această activitate să fie mai rentabilă decât comerţul mondial cu marijuana, cocaină şi heroină, luate împreună[4]. Deşi astfel de informaţii ar trebui nuanţate, deoarece diferitele definiţii ale conceptului de criminalitate informatică ar putea duce la diferenţe în estimarea costurilor, este totuşi un fapt general acceptat că aceasta reprezintă o activitate infracţională cu risc redus şi cu profit ridicat, care devine din ce în ce mai frecventă şi mai dăunătoare. Într-o perioadă în care este extrem de important să se încurajeze creşterea economică, intensificarea luptei împotriva criminalităţii informatice va fi esenţială pentru a păstra încrederea pe care cetăţenii şi întreprinderile şi-o pun în comunicarea şi în comerţul online securizate. Aceasta va sprijini, de asemenea, obiectivele de creştere stabilite în cadrul Strategiei Europa 2020[5] şi al Agendei digitale pentru Europa[6].

Libertatea de utilizare a internetului reprezintă factorul determinant care explică revoluţia digitală din ultimii ani. Internetul nostru deschis nu este îngrădit nici de frontiere naţionale şi nici de o structură unică de guvernanţă globală. Însă, pe lângă promovarea şi protejarea acestei libertăţi online, în conformitate cu Carta drepturilor fundamentale a UE, trebuie, de asemenea, să depunem eforturi pentru a proteja cetăţenii de bandele de criminalitate

---

1 Eurostat, Accesul la internet şi utilizarea acestuia, 14 decembrie 2010.

2 McKinsey Global Institute, *Internet Matters*: *the Net's sweeping impact on growth, jobs and prosperity* (Aspecte legate de internet: vastul impact al reţelei asupra creşterii, ocupării forţei de muncă şi prosperităţii). Raportul din mai 2011, consultat la data de 8 februarie 2012.

3 *Norton Cybercrime Report 2011* (Raportul Norton asupra criminalităţii informatice 2011), Symantec, 7 septembrie 2011, consultat la data de 6 ianuarie 2012.

4 Ibidem.

5 Europa 2020 – O strategie europeană pentru o creştere inteligentă, durabilă şi favorabilă incluziunii, COM(2010) 2020 final, 3 martie 2010.

6 O Agendă digitală pentru Europa, COM(2010) 245 final, 26 august 2010.

organizată care caută să exploateze o astfel de deschidere. Niciun tip de infracțiune nu este atât de neîngrădit ca și criminalitatea informatică, ceea ce determină autoritățile de aplicare a legii să adopte o abordare transfrontalieră coordonată și bazată pe colaborare, împreună cu părțile interesate din sectorul public și privat. În acest domeniu, UE poate contribui cu o valoare adăugată semnificativă și chiar face acest lucru.

Uniunea Europeană a elaborat mai multe inițiative pentru combaterea criminalității informatice. Printre acestea se numără Directiva privind combaterea exploatării sexuale a copiilor și a pornografiei infantile online, adoptată în 2011, precum și o directivă privind atacurile împotriva sistemelor informatice, care vizează penalizarea exploatării instrumentelor criminalității informatice, în special a botneturilor[7] și care ar trebui să fie adoptată în 2012. Europol și-a mărit numărul activităților de combatere a criminalității informatice, jucând un rol-cheie în recenta operațiune „*Rescue*", în cadrul căreia poliția a arestat 184 de persoane suspectate de săvârșirea unor infracțiuni în materie de abuzuri sexuale asupra copiilor și a identificat peste 200 de victime ale abuzurilor asupra copiilor, ca urmare a uneia dintre cele mai mari investigații de acest gen realizate de către autoritățile de aplicare a legii din întreaga lume. Grație activităților întreprinse de analiștii Europol care au reușit să neutralizeze dispozitivele de securitate ale unui server-cheie din centrul rețelei, au putut fi dezvăluite identitatea și activitățile persoanelor suspectate de săvârșirea infracțiunilor.

Lupta împotriva criminalității informatice, al cărei instrument juridic principal este Convenția privind criminalitatea informatică a Consiliului Europei[8], rămâne, în continuare, o prioritate absolută. Aceasta este identificată în cadrul ciclului de politici ale UE privind combaterea criminalității organizate și a formelor grave de criminalitate internațională[9] și face parte integrantă din eforturile care vizează dezvoltarea unei strategii europene globale pentru a consolida securitatea informatică. UE a inițiat, de asemenea, un dialog strâns cu partenerii internaționali, de exemplu prin intermediul actualului grup de lucru UE-SUA privind securitatea informatică și criminalitatea informatică.

Lăsând deoparte progresele realizate, există în continuare o serie de obstacole în calea efectuării, cu eficiență, a investigațiilor în materie de criminalitate informatică și a urmăririi penale, la nivel european, a autorilor infracțiunilor. Printre obstacole se numără: granițele jurisdicționale, capacitățile insuficiente privind schimbul de informații, dificultățile tehnice cu privire la localizarea originii autorilor actelor de criminalitate informatică, diferențele existente în capacitățile de investigare și de expertiză legală, lipsa de personal calificat, precum și lipsa cooperării cu alte părți interesate, responsabile de securitatea informatică. În cadrul Instrumentului de stabilitate, UE abordează, de asemenea, chestiunea legată de evoluția rapidă a amenințărilor transnaționale în materie de criminalitate informatică în țările în curs de

---

7 Propunere de directivă a Parlamentului European și a Consiliului privind atacurile împotriva sistemelor informatice, COM (2010)517 final, 30 septembrie 2010. Botneturile sunt rețele de calculatoare virusate, infectate cu programe informatice ostile care pot fi activate de la distanță pentru a efectua acțiuni specifice, inclusiv atacuri informatice.

8 Convenția privind criminalitatea informatică a Consiliului Europei, Budapesta, 23 noiembrie 2001, cunoscută, de asemenea, sub denumirea de Convenția de la Budapesta. Convenția este însoțită de un *Protocol adițional la Convenția privind criminalitatea informatică*, referitor la incriminarea actelor de natură rasistă și xenofobă comise prin intermediul sistemelor informatice.

9 Ciclul de politici ale UE privind criminalitatea organizată și formele grave de criminalitate internațională, referitor la perioada 2011-2013, are opt priorități, dintre care una este reprezentată de „intensificarea luptei împotriva criminalității informatice și a utilizării necorespunzătoare a internetului de către grupările de criminalitate organizată".

dezvoltare și în cele aflate în tranziție, acolo unde lipsesc adesea capacitățile necesare pentru combaterea acestei forme de criminalitate organizată.

Ca răspuns la aceste provocări, Comisia și-a exprimat intenția de a institui un Centru european de combatere a criminalității informatice ca o prioritate a Strategiei de securitate internă[10]. Ca urmare a studiului de fezabilitate privind crearea unui astfel de centru[11], la cererea Consiliului[12], Comisia propune instituirea unui Centru european de combatere a criminalității informatice (EC3), care va face parte din Europol și va reprezenta punctul de convergență în lupta împotriva criminalității informatice la nivelul UE. Prezenta comunicare, bazată pe studiul de fezabilitate, descrie funcțiile esențiale preconizate pentru Centrul european de combatere a criminalității informatice și explică de ce acesta ar trebui să fie înființat în cadrul Europol, precum și modul în care acesta poate fi instituit. Va fi totuși necesar ca implicațiile în materie de utilizare a resurselor să fie evaluate mai aprofundat și să fie furnizate înainte ca EC3 să devină pe deplin operațional. Instituirea acestui centru va fi luată în considerare, după caz, în cadrul viitoarei revizuiri a temeiului juridic al Europol.

## 2. PROPUNERE DE INSTITUIRE A UNUI CENTRU EUROPEAN DE COMBATERE A CRIMINALITĂȚII INFORMATICE

Pentru ca Centrul european de combatere a criminalității informatice (EC3) să poată aduce o valoare adăugată, respectând în același timp principiul subsidiarității, se propune ca EC3 să se concentreze asupra următoarelor aspecte majore ale criminalității informatice:

(i) acte de criminalitate informatică comise de către grupurile de criminalitate organizată, în special acele acte care generează profituri considerabile obținute din săvârșirea de infracțiuni, cum ar fi frauda online;

(ii) acte de criminalitate informatică ce aduc prejudicii grave victimelor lor, cum ar fi exploatarea sexuală a copiilor pe internet; precum și

(iii) acte de criminalitate informatică (inclusiv atacuri informatice) îndreptate împotriva infrastructurii critice și a sistemelor informatice ale Uniunii[13].

Având în vedere evoluția continuă a criminalității informatice, ar trebui să existe și posibilitatea de a lua măsuri, atât pentru a răspunde cerințelor statelor membre, cât și pentru a face față apariției unor noi amenințări în domeniul criminalității informatice cu care se va confrunta Uniunea.

---

10 „Până în 2013, UE va înființa … un centru de combatere a criminalității cibernetice, care va permite statelor membre și instituțiilor UE să dezvolte capacități operaționale și analitice pentru efectuarea de anchete și cooperarea cu parteneri internaționali” din Strategia de securitate internă a UE în acțiune: cinci pași către o Europă mai sigură. COM(2010)673 final, 22 noiembrie 2010.

11 Feasibility study for a European Cybercrime Centre, Final Report, February 2012. (Studiu de fezabilitate privind un Centru european de combatere a criminalității informatice, raport final, februarie 2012).

12 Concluziile Consiliului privind un plan de acțiune pentru punerea în aplicare a strategiei comune de combatere a criminalității informatice, cea de a 3010-a reuniune a Consiliului Afaceri Generale, Luxemburg, 26 aprilie 2010.

13 Astfel cum sunt definite în Directiva 2008/114/CE a Consiliului din 8 decembrie 2008. Această directivă este în curs de revizuire; EC3 va ține seama de evoluțiile ulterioare.

## 2.1. Funcțiile de bază și misiunile pe care ar trebui să le îndeplinească Centrul european de combatere a criminalității informatice

EC3 ar trebui să aibă patru funcții de bază:

*(a) Să fie punctul de convergență, la nivel european, al informațiilor privind criminalitatea informatică*

O funcție de integrare a informației ar garanta faptul că datele privind criminalitatea informatică sunt colectate dintr-un număr foarte mare de surse publice, private și deschise, îmbogățind astfel datele de care dispune poliția. Aceasta ar trebui să acopere treptat actualele lacune existente la nivelul informațiilor furnizate de comunitățile responsabile de securitatea informatică și de combaterea criminalității informatice. Informațiile colectate ar viza activitățile, metodele și persoanele suspectate de criminalitate informatică. Această funcție are ca scop îmbunătățirea cunoștințelor privind criminalitatea informatică și totodată prevenirea acesteia, detectarea și urmărirea penală a infractorilor, vizând încurajarea legăturilor adecvate între autoritățile de aplicare a legii, comunitatea echipelor de intervenție în caz de urgență informatică (CERT) și specialiștii din sectorul privat în materie de securitate în domeniul tehnologiei informației și comunicațiilor (TIC). Schimbul de informații trebuie să respecte acordurile și normele de confidențialitate existente între diferitele părți.

Funcția de integrare a informației ar permite, de asemenea, îmbunătățirea raportării actelor de criminalitate informatică și a schimbului de informații. Comisia ar dori ca statele membre să impună ca infracțiunile grave în materie de criminalitate informatică să fie semnalate autorităților naționale de aplicare a legii[14]. Acest lucru ar permite serviciilor de poliție naționale să furnizeze, într-un mod mai sistematic, informații privind infracțiunile informatice grave centrului EC3, care, la rândul său, ar difuza aceste informații, astfel încât colegii din alte state membre să știe dacă urmăresc același obiectiv și să beneficieze de informații reciproce în cadrul investigațiilor lor.

Scopul avut în vedere este acela de a oferi, în timp, o perspectivă mai vastă asupra criminalității informatice în Europa, astfel încât să poată fi elaborate rapoarte strategice de înaltă calitate cu privire la tendințe și amenințări, să se dobândească, pe baza cifrelor exhaustive privind criminalitatea, cunoștințe solide asupra fenomenului și să se îmbunătățească informațiile operaționale folosind o bază de date alimentată dintr-o varietate de surse.

*(b) Să pună în comun expertiza europeană în materie de combatere a criminalității informatice pentru a sprijini statele membre în consolidarea propriilor capacități*

Prin expertiza sa și prin organizarea unor cursuri de formare, EC3 ar trebui să sprijine statele membre să reprime criminalitatea informatică. Aplicarea legii reprezintă obiectivul principal, însă este oportun ca și membrilor magistraturii să li se propună cursuri de formare. Pe baza unei analize riguroase a necesităților ar trebui ca inițiativele existente la nivelul Europol, CEPOL și al statelor membre să fie raționalizate pentru a se asigura o mai bună coordonare și complementaritate. Această formare ar trebui să includă o expertiză tehnică aprofundată, o consolidare mai largă a capacităților pentru a permite ofițerilor de poliție, procurorilor și judecătorilor să abordeze activitățile care țin de criminalitatea informatică.

---

[14] Cazuri precum cele menționate la articolele 3 - 7 din proiectul de directivă privind atacurile împotriva sistemelor informatice, COM (2010)517 final, 30 septembrie 2010.

Ar trebui să se înființeze un serviciu de combatere a criminalității informatice care să permită schimbul de bune practici și de cunoștințe, precum și relaționarea cu statele membre, cu autoritățile de aplicare a legii, cu sistemul judiciar, cu sectorul privat și cu organizațiile societății civile și care să răspundă întrebărilor acestora, de exemplu, în cazul unor atacuri informatice sau al apariției unor noi forme de înșelăciune online.

Acesta ar trebui să sprijine activitățile și să ofere consultanță grupurilor de experți în domeniul criminalității informatice, inclusiv grupului operativ al UE în materie de combatere a criminalității informatice și experților în lupta lor împotriva exploatării sexuale online a copiilor. De asemenea, acesta ar trebui să stabilească o cooperare cu rețeaua în plină expansiune a centrelor de excelență în materie de criminalitate informatică, cum ar fi 2Centre, și cu comunitatea cercetătorilor.

De asemenea, EC3 ar trebui să sprijine statele membre în eforturile lor vizând elaborarea și desfășurarea unei aplicații online de raportare a infracțiunilor informatice, bazată pe standarde convenite, astfel încât fluxurile de raportare care provin de la diverși actori (societăți, CERT naționale/guvernamentale, cetățeni etc.) să fie canalizate spre organismele naționale de aplicare a legii, iar cele care provin de la aceste organisme să fie direcționate spre centrul EC3.

EC3 ar trebui să faciliteze schimbul de bune practici în materie de justiție penală și de aplicare a legii. Participarea efectivă a sistemului judiciar la lupta împotriva criminalității informatice este fundamentală pentru a realiza o mai bună urmărire penală, în toate statele membre, a infractorilor informatici periculoși.

*(c) Să ofere sprijin statelor membre în cadrul investigațiilor privind criminalitatea informatică*

EC3 ar trebui să acorde sprijin operațional investigațiilor privind criminalitatea informatică, de exemplu încurajând crearea unor echipe comune de anchetă privind criminalitatea informatică și schimbul de informații operaționale în cadrul investigațiilor în curs.

Acesta ar trebui să ofere, de asemenea, asistență de mare calitate în domeniul expertizei criminalistice (infrastructuri, depozitare, instrumente), precum și competențe în materie de criptare pentru investigațiile privind criminalitatea informatică.

*(d) Să devină purtătorul de cuvânt al investigatorilor europeni privind criminalitatea informatică la nivelul autorităților de aplicare a legii și al sistemului judiciar*

În timp, EC3 ar putea deveni un punct de convergență pentru investigatorii europeni în materie de criminalitate informatică, permițându-le acestora să se exprime cu o singură voce în cadrul discuțiilor cu sectorul TIC, cu alte societăți din sectorul privat, precum și cu comunitatea cercetătorilor, cu asociații ale utilizatorilor și cu organizațiile societății civile asupra modalității de a îmbunătăți prevenirea criminalității informatice și coordonarea activităților de cercetare cu obiective precise.

EC3 ar fi interfața naturală între activitățile Interpolului în materie de criminalitate informatică și alte unități internaționale de poliție responsabile de combaterea criminalității informatice. Acesta ar putea coordona, de asemenea, contribuțiile la inițiativele existente privind guvernanța internetului, precum și contribuțiile grupului interguvernamental deschis de experți al ONU privind criminalitatea informatică.

EC3, ar trebui, de asemenea, să colaboreze cu organizații precum rețeaua INSAFE[15], în vederea realizării unor campanii publice de sensibilizare, actualizându-le în funcție de evoluțiile în materie de criminalitate informatică, identificate cu ajutorul analizei furnizate de EC3 cu scopul de a încuraja un comportament online prudent și sigur.

### 2.2. Amplasare

Astfel cum s-a evidențiat în studiul de fezabilitate, Centrul european de combatere a criminalității informatice ar trebui să facă parte din Europol și să fie situat în cadrul structurilor existente ale acestuia.

Această situație prezintă avantaje considerabile. Rolul Europol este recunoscut de statele membre și de alte părți interesate, inclusiv de către Interpol și de autoritățile internaționale de aplicare a legii; acesta dispune deja de un mandat care îi permite să ia măsuri cu privire la criminalitatea informatică[16]. Principala misiune a Europol este aceea de a promova o Europă mai sigură pentru toți cetățenii săi, furnizând sprijin autorităților de aplicare a legii ale UE prin intermediul analizei și al schimbului de informații în materie penală.

### 2.3. Implicațiile pe care le presupune EC3 în termeni de resurse

Studiul de fezabilitate a examinat diversele implicații în termeni de resurse. Este necesar ca acestea să fie evaluate în continuare[17], în special având în vedere alte sarcini care ar putea fi desfășurate de către Europol în viitor, precum și în contextul mai general al personalului alocat agențiilor UE. Această evaluare va fi realizată, în special, în contextul revizuirii temeiului juridic al Europol și al discuțiilor în curs privind propunerea Comisiei referitoare la instituirea unui fond pentru securitatea internă. Cu toate acestea, este deja clar că va fi necesară detașarea experților din statele membre.

Atunci când va evalua necesitățile estimate în termeni de resurse, Comisia se va baza pe trei considerente: în primul rând, se presupune că va exista o creștere moderată a numărului total de cazuri în materie de criminalitate informatică ce urmează să fie examinate, și nu o creștere masivă; în al doilea rând, statele membre își vor îmbunătăți capacitatea de a lupta împotriva criminalității informatice; și, în al treilea rând, EC3 va trata numai anumite tipuri de infracțiuni informatice.

### 2.4. Guvernanță

Instituirea EC3 în cadrul Europol ar fi importantă pentru a garanta participarea altor actori-cheie la conducerea strategică a centrului. Prin urmare, Comisia sugerează înființarea, în cadrul structurii de guvernanță a Europol, a unui comitet de gestionare a programului EC3, care ar fi prezidat de directorul EC3. Acest instrument ar oferi altor părți interesate, precum Eurojust, CEPOL, statele membre, reprezentate de către grupul operativ al UE de combatere a criminalității informatice, ENISA și Comisia, posibilitatea ca fiecare să contribuie cu know-how-ul respectiv, fără a crea sarcini administrative suplimentare inutile. Comitetul ar putea lua măsuri menite să garanteze faptul că centrul EC3 își desfășoară activitățile în materie de

---

15 INSAFE este o rețea europeană de centre de sensibilizare care promovează o utilizare sigură și responsabilă a internetului și a dispozitivelor mobile de către tineri.

16 Decizia Consiliului (2009/371/JAI) din 6 aprilie 2009 privind înființarea Oficiului European de Poliție, articolul 4 alineatul (1) în coroborare cu anexa.

17 Evaluarea trebuie să fie coerentă cu cerințele globale în materie de personal și de buget pentru agenții, specificate în cadrul Bugetului 2013 și în următorul cadru financiar multianual.

criminalitate informatică în mod responsabil, asigurând astfel îndeplinirea acestor activități în parteneriat, recunoscând expertiza suplimentară și respectând mandatul tuturor părților interesate.

## 2.5. Cooperarea cu actorii-cheie

EC3 ar trebui să asigure un răspuns coordonat la criminalitatea informatică, care să permită nu numai colaborarea dintre diferitele agenții ale UE, ci care să și joace rolul unui punct de contact european unic în acest domeniu.

*(a) Statele membre*

Obiectivul principal este acela de a sprijini statele membre în lupta împotriva criminalității informatice. Serviciul de asistență („*helpdesk*”), precum și serviciile în materie de criminalitate informatică prestate de EC3, cum ar fi o analiză mai precisă a amenințărilor și un sprijin operațional mai bine informat, vor fi utile investigatorilor din domeniul criminalității informatice din întreaga Europă. Grupul operativ al UE de combatere a criminalității informatice ar garanta faptul că preocupările statelor membre ar fi luate în considerare în cadrul comitetului de gestionare a programului EC3. În plus, statele membre vor trebui să realizeze în continuare investițiile necesare în structurile naționale de combatere a criminalității informatice, astfel încât să dispună de interfețe adecvate pentru a interacționa cu EC3.

*(b) Agențiile europene și alți actori*

Agențiile relevante, în special Eurojust, CEPOL și ENISA, precum și CERT-UE, ar fi direct implicate în activitățile EC3, nu numai datorită participării lor la comitetul de gestionare a programului, ci și datorită cooperării operaționale, acolo unde este cazul și ținând seama de mandatele lor respective.

*(c) Partenerii internaționali*

Pentru a-și atinge obiectivul de a deveni punctul de convergență european al informațiilor privind criminalitatea informatică, EC3 ar trebui să devină un interlocutor prețios pentru partenerii internaționali în chestiuni privind combaterea criminalității informatice. Ar trebui ca EC3, în cooperare cu Interpol și cu partenerii noștri strategici la nivel mondial, să se străduiască să amelioreze coordonarea răspunsurilor în materie de combatere a criminalității informatice și să se asigure că, în cadrul elaborării ulterioare a spațiului virtual, preocupările privind aplicarea legii sunt luate în considerare.

*(d) Sectorul privat, comunitățile de cercetători și organizațiile societății civile*

În contextul luptei împotriva criminalității informatice este extrem de important să se instaureze un climat de încredere între sectorul privat și autoritățile de aplicare a legii. Consolidând activitatea Europol cu partenerii actuali și viitori, ar trebui ca EC3 să creeze rețele de încredere și platforme fiabile pentru schimbul de informații cu sectorul industrial și cu alți actori, cum ar fi comunitatea de cercetători și organizațiile societății civile. Acestea ar trebui să faciliteze atât schimbul de informații între comunități, pe diverse teme, printre care alerta timpurie privind amenințările informatice, cât și reacțiile comune, de tip „*task force*”, la atacurile informatice și la alte tipuri de criminalitate informatică.

EC3 ar trebui să contribuie, de asemenea, la promovarea unor inițiative mai ample din partea societăților din sectorul privat care au active digitale substanțiale, cum ar fi băncile și comercianții cu amănuntul online, pentru a combate criminalitatea informatică, pentru a se proteja mai eficient de aceasta și pentru a reduce cât mai mult prezența unor puncte vulnerabile în tehnologiile în curs de dezvoltare.

Este în interesul reciproc al autorităților de aplicare a legii și al sectorului privat să obțină, în timp real, o perspectivă mai clară asupra fenomenului criminalității informatice și să depună eforturi pentru dezmembrarea mai eficientă a rețelelor criminalității informatice cu ajutorul unor mijloace mai bune de detectare a noilor moduri de operare și al arestării rapide a infractorilor din domeniul informatic.

## 3. O FOAIE DE PARCURS PENTRU INSTITUIREA CENTRULUI EUROPEAN DE COMBATERE A CRIMINALITĂȚII INFORMATICE

### 3.1. Activități până la sfârșitul anului 2013

Pentru a atinge capacitatea operațională inițială, Comisia va analiza, în strânsă cooperare cu Europol, necesitățile în materie de resurse umane și financiare în vederea alcătuirii unei echipe responsabile de instituirea EC3 până la sfârșitul cadrului financiar actual al UE. Sarcinile acestei echipe ar include, printre altele, elaborarea mandatului și a structurii organizaționale a EC3, precum și dezvoltarea unor indicatori care să permită evaluarea performanței acestuia. Modul de funcționare și rolul comitetului de gestionare a programului vor fi definite și adoptate de comun acord de către părțile interesate asociate.

În vederea stabilirii unei funcții de integrare completă a informației, echipa responsabilă cu instituirea centrului ar trebui să creeze legături cu echipa de preconfigurare a CERT-UE, precum și cu ENISA, dacă este cazul (ținând seama de resursele lor limitate). Pentru a îmbunătăți raportarea actelor în materie de criminalitate informatică, se va realiza un demers de identificare a situației pentru a crea un inventar interoperabil al sistemelor de raportare a criminalității informatice online din statele membre.

Ar trebui să se înființeze un serviciu de luptă împotriva criminalității informatice. Acest serviciu ar putea fi sprijinit cu ajutorul unei platforme securizate online, special create și destinate comunității de specialiști în domeniul criminalității organizate. Activitățile actuale de formare ale Europol, ale CEPOL și ale grupului european de formare și educație în materie de combatere a criminalității informatice ar putea fi evaluate și reorganizate sub îndrumarea EC3 și a comitetului său de gestionare a programului. Ar trebui să se efectueze o analiză a necesităților în materie de formare, care să țină seama, de asemenea, de cerințele judecătorilor și ale procurorilor. Pe baza acestei analize, s-ar putea organiza un curs de formare de bază privind criminalitatea informatică, deschis membrilor sistemului justiției penale.

În plus, în deciziile care se vor lua în contextul următorului cadru financiar multianual va trebui să se efectueze și să se prevadă o evaluare mai precisă a resurselor umane și financiare necesare. Această evaluare va permite definirea dezvoltării viitoare a EC3.

## 4. CONCLUZII

Dat fiind că universul criminalității organizate își extinde activitățile asupra spațiului virtual, autoritățile de aplicare a legii trebuie să țină pasul cu aceste evoluții. UE poate oferi statelor membre și industriei instrumentele necesare de combatere a criminalității informatice, care reprezintă o amenințare modernă, în continuă evoluție și care, prin definiție, nu are frontiere. Cu condiția ca resursele umane și financiare necesare să poată fi obținute, Centrul european de combatere a criminalității informatice va deveni punctul focal al luptei Europei împotriva criminalității informatice prin punerea în comun a competențelor, sprijinirea anchetelor penale și promovarea unor soluții la nivelul UE, sensibilizând în același timp cetățenii europeni cu privire la aspectele legate de criminalitatea informatică. Ca atare, centrul ar contribui la garantarea unui internet deschis și a unei economii digitale legitime, precum și la protecția activităților online desfășurate de cetățenii și de întreprinderile din Europa.

Consiliul este invitat să aprobe prezenta propunere, iar Parlamentul European și celelalte părți interesate sunt încurajate să contribuie la dezvoltarea centrului.