CONSIGLIO DELL'UNIONE EUROPEA

Bruxelles, 4 aprile 2012 (10.04)
(OR. en)

8543/12

ENFOPOL 94
TELECOM 72

NOTA DI TRASMISSIONE

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	30 marzo 2012
Destinatario:	Uwe CORSEPIUS, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2012) 140 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL CONSIGLIO E AL PARLAMENTO EUROPEO Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica

Si trasmette in allegato, per le delegazioni, il documento della Commissione COM(2012) 140 final.

All.: COM(2012) 140 final

COMMISSIONE EUROPEA

Bruxelles, 28.3.2012
COM(2012) 140 final

COMUNICAZIONE DELLA COMMISSIONE AL CONSIGLIO E AL PARLAMENTO EUROPEO

Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica

COMUNICAZIONE DELLA COMMISSIONE AL CONSIGLIO E AL PARLAMENTO EUROPEO

Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica

1. INTRODUZIONE: LA RISPOSTA EUROPEA ALLA CRIMINALITÀ SENZA FRONTIERE

Internet è ormai parte integrante e indispensabile della nostra società e della nostra economia. L'80% dei giovani europei si collegano tra loro e con il mondo tramite le reti sociali online[1] e ogni anno nel settore del commercio elettronico si effettuano scambi per un valore complessivo pari a circa 8 000 miliardi di dollari[2]. Tuttavia, proprio perché la nostra vita quotidiana e le transazioni commerciali passano sempre di più per Internet, aumentano anche le attività criminali online (ogni giorno le vittime della criminalità informatica nel mondo sono oltre un milione[3]). I crimini perpetrati in rete sono svariati: vanno dalla vendita per cifre irrisorie di carte di credito rubate, al furto di identità, all'abuso sessuale su minori e a gravi attacchi informatici contro istituzioni e infrastrutture.

Il costo totale della criminalità informatica per la società è alto. Da una recente relazione risulta che la criminalità informatica causa alle sue vittime perdite per un valore complessivo pari a 388 miliardi di dollari, risultando più vantaggiosa del traffico mondiale combinato di marijuana, cocaina ed eroina[4]. Sebbene tali informazioni vadano prese con cautela, poiché le stime dei costi variano a seconda di cosa si intende per criminalità informatica, c'è accordo sul fatto che la criminalità informatica è una forma di attività criminale ad alto profitto e a basso rischio che sta diventando sempre più diffusa e dannosa. In un periodo in cui è quanto mai importante sostenere la crescita economica, è fondamentale potenziare la lotta alla criminalità informatica per mantenere la fiducia dei cittadini e delle imprese nella sicurezza delle comunicazioni e del commercio online. In tal modo si sosterranno anche gli obiettivi di sviluppo fissati nella strategia Europa 2020[5] e nell'agenda digitale europea[6].

Il principale fattore che spiega la rivoluzione digitale degli ultimi anni è la libertà di Internet: un Internet aperto che non conosce né frontiere nazionali né una struttura unica di governance globale. Tuttavia, se da un lato occorre promuovere e proteggere questa libertà online conformemente alla Carta dei diritti fondamentali dell'Unione europea, dall'altro è necessario tutelare i cittadini dalle bande criminali organizzate che cercano di sfruttare questa apertura. Nessun tipo di criminalità è così sganciato dalle frontiere come la criminalità informatica, il che rende necessario un approccio coordinato e collaborativo al di là delle frontiere da parte

---

1 Eurostat, Accesso e uso di Internet, 14 dicembre 2010.

2 *McKinsey Global Institute, Internet Matters*: *the Net's sweeping impact on growth, jobs and prosperity*. Relazione maggio 2011, consultata l'8 febbraio 2012.

3 *Norton Cybercrime Report 2011*, *Symantec*, 7 settembre 2011, consultata il 6 gennaio 2012.

4 Idem.

5 Europa 2020 - Una strategia per una crescita intelligente, sostenibile e inclusiva (COM(2010) 2020 del 3 marzo 2010).

6 Un'agenda digitale europea (COM(2010) 245 definitivo del 26 agosto 2010).

delle autorità di contrasto, anche nei confronti degli interlocutori sia pubblici che privati. È a questo livello che l'Unione europea può apportare, e apporta, un valore aggiunto significativo.

L'Unione europea ha elaborato varie iniziative per combattere la criminalità informatica, tra cui la direttiva del 2011 relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile, e una direttiva – che dovrebbe essere adottata nel 2012 - relativa agli attacchi contro i sistemi di informazione, che si concentra sulla perseguibilità penale dello sfruttamento degli strumenti della criminalità informatica, in particolare le *botnet*[7]. . Europol ha incrementato le sue attività contro la criminalità informatica, svolgendo un ruolo fondamentale nella recente operazione "Rescue" durante la quale la polizia ha arrestato 184 indagati per reati di pedofilia e identificato oltre 200 vittime di abusi minorili grazie a una delle più grandi indagini di questo tipo svolta dalle autorità di contrasto di tutto il mondo. Il lavoro degli analisti di Europol, che sono riusciti a neutralizzare i dispositivi di sicurezza di un server essenziale al centro della rete, ha permesso di scoprire l'identità e le attività dei presunti autori dei reati.

La lotta alla criminalità informatica, il cui strumento giuridico principale è la convenzione del Consiglio d'Europa sulla criminalità informatica[8], continua ad essere una priorità principale. È parte integrante del ciclo programmatico dell'UE per contrastare la criminalità organizzata e le forme gravi di criminalità internazionale[9] e rientra tra gli sforzi intesi a sviluppare una strategia generale dell'UE per rafforzare la sicurezza informatica. L'Unione europea si è inoltre impegnata attivamente con partner internazionali, ad esempio attraverso l'attuale gruppo di lavoro UE-USA sulla sicurezza informatica e la criminalità informatica.

Nonostante tali progressi, persistono vari ostacoli allo svolgimento efficace delle indagini sui reati informatici e all'azione penale nei confronti dei loro autori a livello europeo, tra cui i confini delle giurisdizioni nazionali, insufficienti capacità di condivisione dell'intelligence, difficoltà tecniche nel risalire agli autori dei reati informatici, disparità delle capacità investigative e delle capacità di analisi tecnica forense, scarsezza di personale formato e insufficiente sinergia con altre entità preposte alla sicurezza informatica. Tramite lo strumento per la stabilità l'Unione europea affronta il problema della rapida evoluzione delle minacce transnazionali collegate alla criminalità informatica nei paesi in via di sviluppo e in fase di transizione, in cui spesso mancano le capacità necessarie per combattere questo tipo di criminalità organizzata.

In risposta a tali sfide, la Commissione ha comunicato la propria intenzione di istituire un Centro europeo per la lotta alla criminalità informatica quale priorità della strategia di sicurezza interna[10]. Dopo aver condotto uno studio di fattibilità sull'istituzione di un siffatto

---

7 Proposta di direttiva del Parlamento europeo e del Consiglio relativa agli attacchi contro i sistemi di informazione (COM (2010)517 definitivo del 30 settembre 2010). Le botnet sono reti di computer infettati da software maligni che possono essere attivate a distanza per eseguire azioni specifiche, ad esempio attacchi informatici.

8 Convenzione del Consiglio d'Europa sulla criminalità informatica firmata a Budapest il 23 novembre 2001, denominata anche convenzione di Budapest. La convenzione è accompagnata da un *protocollo aggiuntivo alla convenzione sulla criminalità informatica* relativo alla criminalizzazione degli atti di natura razzista e xenofoba commessi attraverso l'uso di sistemi informatici.

9 Il ciclo programmatico dell'UE per contrastare la criminalità organizzata e le forme gravi di criminalità internazionale relativo al periodo 2011-2013 fissa otto priorità, tra cui "intensificare la lotta contro la criminalità informatica e l'utilizzo a fini criminosi di Internet da parte delle organizzazioni criminali".

10 "Entro il 2013 l'UE creerà […] un centro per la criminalità informatica che permetterà agli Stati membri e alle istituzioni dell'UE di sviluppare capacità operative ed analitiche ai fini delle indagini e della

centro[11], su richiesta del Consiglio[12] la Commissione propone di istituire un Centro europeo per la lotta alla criminalità informatica (EC3) che farà parte di Europol e fungerà da punto di riferimento nella lotta alla criminalità informatica nell'Unione europea. La presente comunicazione, che attinge allo studio di fattibilità, illustra le funzioni fondamentali proposte del centro, spiega il motivo per cui questo dovrebbe essere situato negli edifici di Europol e il modo in cui può essere istituito. Prima che l'EC3 diventi pienamente operativo si dovranno tuttavia valutare ulteriormente le implicazioni in termini di risorse e provvedere al riguardo. Dell'istituzione del centro si terrà opportunamente conto nell'imminente revisione della base giuridica di Europol.

2. PROPOSTA DI ISTITUZIONE DI UN CENTRO EUROPEO PER LA LOTTA ALLA CRIMINALITÀ INFORMATICA

Affinché il Centro europeo per la lotta alla criminalità informatica (EC3) apporti valore aggiunto e sia rispettato il principio di sussidiarietà, si propone che l'EC3 si concentri sui seguenti reati informatici principali:

i) reati informatici commessi da gruppi di criminalità organizzata, in particolare i reati informatici che permettono di realizzare ingenti profitti illegali quali la frode informatica;

ii) reati informatici che recano gravi danni alle vittime, quali lo sfruttamento sessuale dei minori online, e

iii) reati informatici (compresi gli attacchi informatici) contro sistemi di informazione e infrastrutture critiche dell'Unione[13].

Considerato che una caratteristica della criminalità informatica è la sua continua evoluzione, è necessario che il centro possa intervenire sia in risposta alle esigenze degli Stati membri sia per far fronte all'emergere di nuove minacce di criminalità informatica nei confronti dell'Unione.

2.1. Funzioni fondamentali e compiti del Centro europeo per la lotta alla criminalità informatica

L'EC3 dovrebbe avere quattro funzioni fondamentali:

(a) Fungere da punto di riferimento europeo per le informazioni sulla criminalità informatica

La funzione di fusione delle informazioni garantirà che siano raccolte informazioni sulla criminalità organizzata dal maggior numero possibile di fonti pubbliche, private o accessibili al pubblico, arricchendo i dati di polizia disponibili, e permetterà di colmare progressivamente

---

cooperazione con i partner internazionali", La strategia di sicurezza interna dell'UE in azione: cinque tappe verso un'Europa più sicura (COM(2010) 673 definitivo del 22 novembre 2010).

11 *Feasibility study for a European Cybercrime Centre*, relazione finale, febbraio 2012.

12 Conclusioni del Consiglio su un piano d'azione per l'attuazione della strategia concertata di lotta alla criminalità informatica, 3010ª sessione del Consiglio "Affari generali", Lussemburgo, 26 aprile 2010.

13 Quali definiti nella direttiva 2008/114/CE del Consiglio dell'8 dicembre 2008. Tale direttiva è attualmente oggetto di revisione; l'EC3 terrà conto degli ulteriori sviluppi.

le lacune delle informazioni fornite dagli organismi preposti alla sicurezza informatica e alla lotta alla criminalità informatica. Le informazioni raccolte riguarderanno le attività di criminalità informatica, i metodi con cui tali attività vengono svolte e i loro presunti autori. Tale funzione permetterà di conoscere meglio il fenomeno della criminalità informatica, migliorare la prevenzione, l'accertamento e la repressione dei reati informatici e favorire lo sviluppo di legami tra autorità di contrasto, la rete delle squadre di pronto intervento informatico (CERT) e gli specialisti del settore privato in materia di sicurezza delle tecnologie dell'informazione e della comunicazione (TIC). Lo scambio di informazioni dovrà avvenire nel rispetto degli accordi e delle norme sulla riservatezza vigenti tra le varie parti.

La funzione di fusione delle informazioni sarà inoltre utile per migliorare la segnalazione dei reati informatici e lo scambio di informazioni. Secondo la Commissione è opportuno che gli Stati membri prevedano l'obbligo di segnalare alle autorità di contrasto nazionali i reati informatici gravi[14]. I servizi di polizia nazionali saranno così in grado di fornire in modo più sistematico informazioni sui reati informatici gravi all'EC3, che, a sua volta, le divulgherà ai colleghi degli altri Stati membri affinché sappiano se stanno lavorando agli stessi obiettivi e beneficino delle reciproche informazioni sulle indagini.

L'obiettivo è ampliare progressivamente il quadro delle informazioni sulla criminalità informatica in Europa in modo da poter elaborare relazioni strategiche di alta qualità sulle tendenze e sulle minacce, avere una conoscenza approfondita del fenomeno grazie a dati esaustivi sulla criminalità e migliorare l'intelligence operativa basandosi su informazioni provenienti da varie fonti.

(b) Mettere in comune le competenze europee in materia di criminalità informatica per aiutare gli Stati membri a rafforzare le loro capacità

L'EC3 dovrebbe aiutare gli Stati membri a contrastare la criminalità informatica mettendo a disposizione le sue competenze e organizzando attività di formazione. Primi destinatari dovrebbero essere le autorità di contrasto, ma è opportuno che la formazione sia rivolta anche alle autorità giudiziarie. Le iniziative esistenti di Europol, CEPOL e degli Stati membri dovrebbero essere razionalizzate sulla base di un'analisi approfondita delle esigenze, al fine di migliorare il coordinamento e la complementarità. Le attività di formazione dovrebbero andare dall'acquisizione di competenze tecniche approfondite al rafforzamento delle capacità degli ufficiali e degli agenti di polizia, dei pubblici ministeri e dei giudici di trattare i casi di criminalità informatica.

È opportuno creare un servizio "criminalità informatica" per scambiare le migliori pratiche e le conoscenze in questo settore, instaurare contatti con gli Stati membri, le autorità di contrasto internazionali, le autorità giudiziarie, il settore privato e le organizzazioni della società civile e rispondere alle loro domande, ad esempio, in caso di attacchi informatici o nuove forme di truffe online.

Esso dovrebbe fornire sostegno alle attività dei gruppi di esperti sulla criminalità informatica, compresi la task force dell'Unione europea sulla criminalità informatica e gli esperti in materia di lotta allo sfruttamento sessuale dei minori online, e prestare loro consulenza. Dovrebbe inoltre favorire la cooperazione con la rete in via di sviluppo dei centri di eccellenza contro la criminalità informatica, quale il "2Centre", e la comunità dei ricercatori.

---

[14] Quali quelli elencati negli articoli da 3 a 7 della proposta di direttiva relativa agli attacchi contro i sistemi di informazione (COM(2010) 517 definitivo del 30 settembre 2010).

L'EC3 dovrebbe altresì aiutare gli Stati membri a sviluppare e introdurre un'applicazione online per le segnalazioni relative alla criminalità informatica, basata su standard concordati, affinché i flussi di segnalazioni provenienti da vari operatori (società, squadre di pronto intervento informatico nazionali/governative, cittadini, ecc.) siano convogliati verso le autorità di contrasto nazionali e da queste ultime verso l'EC3.

L'EC3 dovrebbe collaborare con la comunità della giustizia penale e le autorità di contrasto e facilitare lo scambio delle migliori pratiche. L'effettiva partecipazione delle autorità giudiziarie alla lotta contro la criminalità informatica è fondamentale per perseguire più efficacemente i criminali informatici pericolosi nei diversi Stati membri.

(c) *Fornire sostegno agli Stati membri nelle indagini sulla criminalità informatica*

L'EC3 dovrebbe fornire sostegno operativo alle indagini sulla criminalità informatica, ad esempio incoraggiando l'istituzione di squadre investigative comuni sulla criminalità informatica e lo scambio di informazioni operative nelle indagini in corso.

Dovrebbe inoltre fornire un'assistenza di alta qualità nell'analisi tecnica forense (strutture, archivi, strumenti) e competenze di criptazione per le indagini sulla criminalità informatica.

(d) *Diventare il portavoce degli investigatori europei sulla criminalità informatica a livello di autorità di contrasto e giudiziarie*

L'EC3 potrebbe progressivamente diventare un punto di incontro per gli investigatori europei sulla criminalità informatica, facendosi loro portavoce nelle discussioni con l'industria delle TIC e le altre società del settore privato nonché con la comunità dei ricercatori, le associazioni degli utenti e le organizzazioni della società civile riguardo alle modalità per migliorare la prevenzione della criminalità informatica e coordinare le attività di ricerca mirate.

Il centro sarebbe l'interfaccia naturale con le attività di Interpol sulla criminalità informatica e le altre unità internazionali di polizia preposte alla lotta contro la criminalità informatica. Potrebbe inoltre coordinare i contributi alle iniziative esistenti sulla governance di Internet e al gruppo intergovernativo aperto di esperti sulla criminalità organizzata delle Nazioni Unite.

L'EC3 dovrebbe inoltre collaborare con organizzazioni quali la rete INSAFE[15] alla realizzazione di campagne di sensibilizzazione, aggiornandole in risposta alle evoluzioni della criminalità informatica da esso individuate attraverso l'analisi, al fine di promuovere un comportamento online prudente e sicuro.

2.2. Ubicazione

Come indicato nello studio di fattibilità, il Centro europeo per la lotta alla criminalità informatica dovrebbe far parte di Europol ed essere situato presso le sue attuali strutture.

I vantaggi di tale scelta sono chiari: Europol gode di un ruolo riconosciuto tra gli Stati membri e altri partner istituzionali, compresi Interpol e le autorità di contrasto internazionali, e il suo mandato comprende già la criminalità informatica[16]. La funzione fondamentale di Europol è

---

15 INSAFE è una rete europea di centri di sensibilizzazione che promuove tra i giovani un uso sicuro e responsabile di Internet e dei dispositivi mobili.

16 Decisione 2009/371/GAI del Consiglio, del 6 aprile 2009, che istituisce l'Ufficio europeo di polizia (Europol), articolo 4, paragrafo 1, in combinato disposto con l'allegato.

contribuire a rendere l'Europa più sicura per tutti i cittadini, fornendo sostegno alle autorità di contrasto dell'Unione attraverso lo scambio e l'analisi di intelligence sulle attività criminali.

2.3. Implicazioni dell'EC3 in termini di risorse

Lo studio di fattibilità ha esaminato varie implicazioni in termini di risorse, che dovranno essere ulteriormente valutate[17], in particolare alla luce di altri compiti che potrebbero essere assegnati in futuro a Europol e nel contesto più generale della dotazione di personale delle agenzie dell'Unione europea. La valutazione sarà svolta nell'ambito della revisione della base giuridica di Europol e delle discussioni in corso sulla proposta della Commissione relativa all'istituzione di un fondo per la sicurezza interna. Risulta tuttavia già chiara la necessità di personale distaccato dagli Stati membri.

Nel valutare la stima del fabbisogno di risorse, la Commissione sarà guidata da tre considerazioni: primo, si ipotizza un aumento moderato del numero complessivo dei casi da esaminare in materia di criminalità informatica, anziché un aumento massiccio dei reati di criminalità informatica; secondo, gli Stati membri aumenteranno le loro capacità di lotta alla criminalità organizzata; terzo, l'EC3 si occuperà solo di alcuni tipi di reati informatici.

2.4. Governance

Data la collocazione dell'EC3 all'interno di Europol, è importante garantire che altre principali parti interessate partecipino alla direzione strategica del centro. La Commissione propone pertanto di istituire nella struttura amministrativa di Europol un consiglio di direzione dell'EC3, presieduto dal direttore dell'EC3. Questo strumento offrirebbe ai partner quali Europol, CEPOL, gli Stati membri (rappresentati dalla task force dell'Unione europea sulla criminalità informatica), l'ENISA e la Commissione, di apportare le rispettive conoscenze senza generare inutili oneri amministrativi aggiuntivi. Il consiglio di direzione potrebbe garantire che l'EC3 svolga le attività relative alla criminalità informatica in modo responsabile e assicurare così che queste siano condotte in partenariato, riconoscendo le competenze aggiuntive di tutte le parti interessate e rispettandone il mandato.

2.5. Cooperazione con i principali operatori

L'EC3 dovrebbe garantire una risposta coordinata alla criminalità informatica, non solo permettendo la collaborazione tra le agenzie dell'Unione europea, ma anche fungendo da punto di contatto europeo unico in questo campo.

(a) Stati membri

L'obiettivo principale è aiutare gli Stati membri a combattere la criminalità informatica. Il servizio "criminalità informatica" e i servizi che l'EC3 fornirà, quali un'analisi più mirata delle minacce e un miglior supporto operativo, saranno di utilità per gli investigatori sulla criminalità informatica in Europa. La task force dell'Unione europea sulla criminalità informatica rappresenterà al consiglio di direzione dell'EC3 le esigenze degli Stati membri. Inoltre, gli Stati membri dovranno continuare ad investire nelle necessarie strutture nazionali di lotta alla criminalità informatica in modo da disporre di interfacce adeguate ad interagire con l'EC3.

---

[17] La valutazione deve essere coerente con il fabbisogno complessivo di risorse umane e finanziarie delle agenzie indicato nel bilancio 2013 e nel prossimo quadro finanziario pluriennale.

(b) Agenzie europee e altri attori

Le agenzie pertinenti (Eurojust, CEPOL e ENISA) e le squadre di pronto intervento informatico dell'UE saranno direttamente coinvolte nelle attività dell'EC3, non solo tramite la partecipazione al consiglio di direzione ma anche tramite la cooperazione operativa, se del caso e tenuto conto dei rispettivi mandati.

(c) Partner internazionali

Per diventare il punto di riferimento europeo per le informazioni sulla criminalità informatica, l'EC3 dovrà dimostrarsi un valido interlocutore per i partner internazionali in tema di criminalità informatica. In partenariato con Interpol e i nostri partner strategici nel mondo, l'EC3 dovrebbe sforzarsi di migliorare il coordinamento delle risposte nel quadro della lotta alla criminalità informatica e garantire che nello sviluppo del cyberspazio si tenga conto delle esigenze in materia di applicazione della legge.

(d) Settore privato, comunità dei ricercatori e organizzazioni della società civile

Nel quadro della lotta alla criminalità informatica è di estrema importanza instaurare un clima di fiducia e sicurezza tra il settore privato e le autorità di contrasto. Consolidando il lavoro di Europol con i partner attuali e futuri, l'EC3 dovrebbe creare reti di fiducia e piattaforme per lo scambio di informazioni con l'industria e altri partner quali la comunità dei ricercatori e le organizzazioni della società civile. Si dovrebbero così favorire lo scambio di informazioni tra le comunità su vari temi, tra cui le segnalazioni tempestive di minacce informatiche, e risposte collaborative di tipo "task force" agli attacchi informatici e ad altri tipi di reati informatici.

L'EC3 dovrebbe inoltre contribuire a iniziative più ampie avviate dalle imprese del settore privato che dispongono di consistenti patrimoni digitali, quali le banche e i rivenditori online, e volte a combattere la criminalità informatica, a migliorare la protezione e a ridurre al minimo i punti vulnerabili delle tecnologie in fase di sviluppo.

È nel reciproco interesse delle autorità di contrasto e del settore privato avere un quadro più preciso del fenomeno della criminalità informatica in tempo reale e adoperarsi per smantellare in modo più efficace le reti di criminalità informatica attraverso una miglior individuazione dei nuovi modi di operare e il rapido arresto dei criminali informatici.

3. TABELLA DI MARCIA PER LA REALIZZAZIONE DEL CENTRO EUROPEO PER LA LOTTA ALLA CRIMINALITÀ INFORMATICA

3.1. Attività fino alla fine del 2013

Al fine di raggiungere la capacità operativa iniziale, la Commissione, in stretta collaborazione con Europol, studierà le esigenze in termini di risorse umane e finanziarie necessarie per istituire una squadra preposta alla realizzazione dell'EC3 fino alla fine dell'attuale quadro finanziario dell'Unione europea. Tale squadra sarà incaricata, ad esempio, di elaborare il mandato del centro e la sua struttura organizzativa, e sviluppare indicatori per valutarne le prestazioni. Il ruolo e il funzionamento del consiglio di direzione saranno stabiliti e concordati dalle parti interessate associate.

In vista della creazione di una funzione di fusione completa delle informazioni, la squadra incaricata della realizzazione dell'EC3 dovrebbe creare collegamenti con la squadra di preconfigurazione del CERT-UE e con l'ENISA, ove pertinente (tenuto conto delle loro

risorse limitate). Per migliorare la segnalazione dei reati informatici, sarà effettuato un inventario dei sistemi online di segnalazione dei reati informatici esistenti negli Stati membri per creare una "mappa delle interoperabilità" di tali sistemi.

Dovrebbe essere istituito un servizio "criminalità informatica", che potrebbe avvalersi dell'appoggio di una piattaforma online comune, dedicata e sicura. Le attuali attività di formazione di Europol, CEPOL e del Gruppo europeo di formazione e istruzione in materia di criminalità informatica (ECTEG) potrebbero essere valutate e rese più efficienti sotto il coordinamento dell'EC3 e del suo consiglio di direzione. Dovrebbe essere effettuata un'analisi delle esigenze di formazione, che tenga conto anche delle richieste dei giudici e dei pubblici ministeri. Sulla base di tali analisi potrebbe essere organizzato un corso di formazione di base sulla criminalità informatica aperto agli operatori della giustizia penale.

Si dovrà inoltre procedere a una valutazione più precisa delle risorse umane e finanziarie necessarie, di cui si dovrà tenere conto nelle decisioni nell'ambito del prossimo quadro finanziario pluriennale. Tale valutazione servirà per stabilire l'ulteriore sviluppo dell'EC3.

4. CONCLUSIONI

Le autorità di contrasto devono stare al passo con le evoluzioni del mondo della criminalità organizzata, che sta espandendo le sue attività nel cyberspazio. L'Unione europea può fornire agli Stati membri e all'industria gli strumenti necessari per far fronte alla moderna minaccia della criminalità informatica, che evolve in continuazione e che, per definizione, non conosce frontiere. A condizione che siano stanziate le risorse umane e finanziarie necessarie, un Centro europeo per la lotta alla criminalità informatica fungerà da punto di riferimento per la lotta alla criminalità informatica in Europa, mettendo in comune le competenze, sostenendo le indagini penali e promuovendo soluzioni a livello di Unione, sensibilizzando nel contempo il pubblico europeo al problema della criminalità informatica. In quanto tale, il centro contribuirà alla salvaguardia di un Internet aperto e dell'economia digitale legittima, nonché alla protezione delle attività online dei cittadini e delle imprese europee.

Si invita il Consiglio ad approvare la presente proposta e si incoraggiano il Parlamento europeo e le altre parti interessate a contribuire allo sviluppo del centro.