CONSIGLIO DELL'UNIONE EUROPEA

Bruxelles, 30 maggio 2007 (02.07)
(OR. en)

10089/07

CRIMORG 102

NOTA DI TRASMISSIONE

Origine:	Signor Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	24 maggio 2007
Destinatario:	Signor Javier SOLANA, Segretario Generale/Alto Rappresentante
Oggetto:	Comunicazione della Commissione al Parlamento europeo, al Consiglio e al Comitato delle regioni - Verso una politica generale di lotta contro la cibercriminalità

Si trasmette in allegato, per le delegazioni, il documento della Commissione COM(2007) 267 definitivo.

All.: COM(2007) 267 definitivo

COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 22.5.2007
COM(2007) 267 definitivo

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO E AL COMITATO DELLE REGIONI

Verso una politica generale di lotta contro la cibercriminalità

{SEC(2007) 641}
{SEC(2007) 642}

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO E AL COMITATO DELLE REGIONI

Verso una politica generale di lotta contro la cibercriminalità

1. INTRODUZIONE

1.1. Cos'è la cibercriminalità?

La sicurezza dei sistemi di informazione, che sono strumenti sempre più importanti nelle nostre società, riguarda vari aspetti; un elemento centrale è la lotta contro la cibercriminalità. Non esiste una definizione concordata di cibercriminalità; i termini "cibercriminalità", "reato informatico", "reato connesso ai sistemi informatici" e "reato ad alta tecnologia" sono spesso usati come sinonimi. Ai fini della presente comunicazione, con "cibercriminalità" si intendono "gli atti criminali commessi contro reti di comunicazioni elettroniche e sistemi di informazione o avvalendosi di tali reti e sistemi".

Nella pratica, la "cibercriminalità" indica tre categorie di attività criminali: la prima comprende i **reati tradizionali** come la frode o la falsificazione, anche se con riferimento specifico ai reati commessi servendosi di reti di comunicazioni elettroniche e sistemi di informazione (in seguito "reti elettroniche"); la seconda concerne la pubblicazione sul web di **contenuti illegali** (materiale pedopornografico o incitamento all'odio razziale), e la terza i **reati propri alle reti elettroniche**, ossia gli attacchi contro i sistemi di informazione, il *denial of service* e la pirateria. Attacchi di questo tipo possono anche colpire le infrastrutture critiche fondamentali in Europa e i sistemi di allarme rapido esistenti in vari settori, con conseguenze potenzialmente disastrose per l'intera società. Denominatore comune di questi reati è che possono essere commessi su larga scala e produrre effetti a grande distanza. Di conseguenza, i metodi investigativi usati nei loro confronti presentano aspetti tecnici spesso identici. La presente comunicazione si concentrerà per l'appunto su questi aspetti comuni.

1.2. Ultimi sviluppi in materia di cibercriminalità

1.2.1. Quadro generale

L'evoluzione costante delle attività criminali, combinata a una mancanza di informazioni affidabili, permette difficilmente di farsi un'idea precisa della situazione. Si possono tuttavia individuare alcune tendenze generali:

- il numero di reati informatici è in aumento e le attività criminali sono sempre più sofisticate e internazionali[1];
- vi sono chiari indizi della crescente partecipazione di gruppi di criminalità organizzata alla cibercriminalità;

[1] La maggior parte delle osservazioni sulle tendenze attuali contenute nella presente comunicazione è tratta dallo studio d'impatto di una comunicazione sulla cibercriminalità commissionato dalla Commissione nel 2006 (contratto n. JLS/2006/A1/003).

- eppure, resta stazionario il numero di procedimenti penali in Europa nel quadro della cooperazione transnazionale fra autorità di contrasto.

1.2.2. Reati tradizionali su reti elettroniche

Sulle reti elettroniche si possono commettere moltissimi reati: particolarmente comuni e in aumento sono le frodi o i tentativi di frode di vario tipo, mentre il furto di identità, il *phishing*[2], lo spam e i codici maligni sono strumenti che permettono frodi su larga scala. Un problema dilagante è anche il commercio illecito su Internet, a livello nazionale e internazionale, di stupefacenti, specie in via di estinzione e armi.

1.2.3. Contenuti illegali

In Europa cresce il numero di siti Internet a contenuto illegale che diffondono materiale pedopornografico, incitano ad atti terroristici ed esaltano la violenza, il terrorismo, il razzismo e la xenofobia. Contrastare tali siti è estremamente difficile, poiché spesso i proprietari e i gestori si trovano in paesi diversi da quello considerato, in molti casi al di fuori dell'Unione europea. I siti possono essere spostati molto velocemente, anche all'esterno dell'UE, e la definizione di illegalità varia notevolmente da uno Stato all'altro.

1.2.4. Reati propri alle reti elettroniche

Gli attacchi su larga scala contro sistemi di informazione, organizzazioni o singoli individui (spesso attraverso le cosiddette *botnets*[3]) sarebbero sempre più frequenti. Di recente sono stati addirittura rilevati attacchi diretti sistematici, coordinati e su larga scala contro le infrastrutture critiche di informazione di uno Stato. Hanno aggravato il fenomeno la fusione di tecnologie e l'interconnessione accelerata dei sistemi di informazione, rendendoli ancora più vulnerabili. Gli attacchi sono spesso organizzati a dovere e perpetrati al fine di estorsione. Probabilmente il numero degli attacchi denunciati è ridotto al minimo dal timore, in parte, dei danni commerciali che comporterebbe la cattiva pubblicità causata dai problemi di sicurezza.

1.3. Obiettivi

A fronte di un contesto in continua evoluzione, urge intervenire a livello nazionale ed europeo contro tutte le forme di reato informatico, che sono una minaccia sempre più grave per le infrastrutture critiche, la società, le imprese e i cittadini. La protezione del singolo dalla cibercriminalità si scontra spesso con problemi connessi alla determinazione della giurisdizione competente, del diritto applicabile, all'attività di contrasto transnazionale o al riconoscimento e all'uso di prove elettroniche. La dimensione essenzialmente transnazionale della cibercriminalità accentua tali difficoltà. Per affrontare queste minacce, la Commissione vara un'iniziativa di politica generale intesa a migliorare il coordinamento europeo e internazionale della lotta alla cibercriminalità.

---

[2] Il *phishing* designa il tentativo di acquisizione fraudolenta di informazioni sensibili, come password o estremi di carte di credito, fingendosi una persona di fiducia in una comunicazione elettronica.

[3] Con il termine "botnet" si indica un insieme di sistemi compromessi che eseguono programmi sotto un comando comune.

L'obiettivo è rafforzare la lotta contro la cibercriminalità a livello nazionale, europeo e internazionale. Già da tempo gli Stati membri e la Commissione ritengono prioritario sviluppare una specifica politica dell'UE al riguardo. L'iniziativa si concentrerà sugli aspetti repressivi e penali della lotta e integrerà altre azioni dell'UE volte a migliorare la sicurezza nel ciberspazio in generale. La politica verterà sui seguenti aspetti: una maggiore cooperazione operativa fra autorità di contrasto; una cooperazione politica e un coordinamento migliori fra gli Stati membri; la cooperazione politica e giuridica con i paesi terzi; la sensibilizzazione; la formazione; la ricerca; il rafforzamento del dialogo con l'industria e un'eventuale azione legislativa.

Tale politica volta a combattere e perseguire la cibercriminalità sarà definita e attuata nel pieno rispetto dei diritti fondamentali, in particolare della libertà di espressione, del rispetto della vita privata e familiare e della protezione dei dati personali. Le azioni legislative che saranno promosse nel quadro di questa politica saranno sottoposte anzitutto a un esame della compatibilità con quei diritti, in particolare con la Carta dei diritti fondamentali dell'Unione europea. Tutte queste iniziative saranno inoltre portate avanti nel pieno rispetto degli articoli da 12 a 15 della direttiva sul commercio elettronico[4], se applicabile.

L'obiettivo della presente comunicazione è scindibile in tre grandi filoni operativi:

- migliorare e facilitare il coordinamento e la cooperazione fra unità che si occupano di cibercriminalità, altre autorità competenti e altri esperti nell'Unione europea;

- elaborare un quadro politico coerente dell'UE di lotta alla cibercriminalità, in coordinamento con gli Stati membri, le organizzazioni e altri attori competenti a livello UE e internazionale;

- fare opera di sensibilizzazione sui costi e sui pericoli della cibercriminalità.

2. STRUMENTI GIURIDICI ESISTENTI DI LOTTA CONTRO LA CIBERCRIMINALITÀ

2.1. Strumenti e azioni a livello dell'UE

La presente comunicazione consolida e sviluppa la comunicazione del 2001 "Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica"[5] (in seguito "comunicazione del 2001"), che proponeva l'adozione di disposizioni di diritto penale sostanziali e procedurali adeguate per contrastare le attività criminali transnazionali e nazionali. A tale comunicazione hanno fatto seguito varie proposte importanti, in particolare quella che ha portato alla decisione quadro 2005/222/GAI relativa agli attacchi contro i sistemi di informazione[6]. In questo contesto sono stati adottati anche altri strumenti legislativi, più generali, riguardanti aspetti della lotta alla

---

4 Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (GU L 178 del 17.7.2000, pag. 1).

5 COM(2000) 890, 26.1.2001.

6 GU L 69, del 16.3.2005, pag. 67.

cibercriminalità, come la decisione quadro 2001/413/GAI relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti[7].

La decisione quadro 2004/68/GAI relativa alla lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile[8] è un esempio emblematico della particolare attenzione che la Commissione rivolge alla **tutela dei bambini**, specie in relazione alla lotta contro tutte le forme di diffusione di materiale pedopornografico sui sistemi di informazione, una priorità orizzontale che manterrà anche nel futuro.

Per affrontare le sfide alla sicurezza della società dell'informazione, la Comunità europea ha elaborato una strategia per la sicurezza delle reti e dell'informazione articolata in tre punti: misure specifiche per la sicurezza delle reti e dell'informazione; quadro normativo per le comunicazioni elettroniche; lotta contro la cibercriminalità. Benché, in una certa misura, questi tre aspetti possano essere sviluppati separatamente, le numerose interdipendenze giustificano uno stretto coordinamento. Nel settore connesso della sicurezza delle reti e dell'informazione, nel 2001 la Commissione ha adottato una comunicazione, parallelamente a quella sulla cibercriminalità, dal titolo "Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo"[9]. La direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche (e-Privacy) contempla l'obbligo per i fornitori di servizi di comunicazione elettronica accessibili al pubblico di salvaguardare la sicurezza dei loro servizi, e prevede disposizioni contro lo spam e i programmi spia. Da allora, la politica di sicurezza delle reti e dell'informazione è stata sviluppata con varie misure, tra cui, di recente, una prima comunicazione "Una strategia per una società dell'informazione sicura"[10] che rivitalizza la strategia in corso e fissa il quadro per portare avanti e perfezionare un approccio coerente per la sicurezza delle reti e dell'informazione, una seconda comunicazione sulla lotta contro le comunicazioni commerciali indesiderate (spam), i programmi spia (spyware) e i software maligni[11], e la creazione nel 2004 dell'Agenzia europea per la sicurezza delle reti e dell'informazione[12]. L'obiettivo principale di questa agenzia è sviluppare conoscenze specializzate per promuovere la cooperazione tra i settori pubblico e privato e fornire assistenza alla Commissione e agli Stati membri. Nella lotta alla cibercriminalità avranno un ruolo importante anche i **risultati delle ricerche** tecnologiche tese a rendere sicuri i sistemi di informazione. Di conseguenza, le tecnologie dell'informazione e delle comunicazioni e la sicurezza figurano tra gli obiettivi del Settimo programma quadro di ricerca dell'UE, operativo dal 2007 al 2013[13]. La revisione del quadro normativo per le comunicazioni elettroniche potrebbe comportare modifiche per rendere più efficaci le disposizioni di sicurezza della direttiva e-Privacy e della direttiva 2002/22/CE sul servizio universale[14].

---

7 GU L 149 del 2.6.2001, pag. 1.

8 GU L 13 del 20.1.2004, pag. 44.

9 COM(2001) 298.

10 COM(2006) 251.

11 COM(2006) 688.

12 Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio, del 10 marzo 2004, che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione (GU L 77 del 13.3.2004, pag. 1).

13 Nel quadro del Sesto programma quadro di ricerca e sviluppo tecnologico l'Unione europea ha già sostenuto vari progetti di ricerca con buoni risultati.

14 COM(2006) 334, SEC(2006) 816, SEC(2006) 817.

2.2. Strumenti a livello internazionale

Le reti di informazione sono reti globali: la politica di lotta alla cibercriminalità non sarà quindi efficace se gli sforzi sono circoscritti al territorio dell'UE. Chiunque può attaccare i sistemi di informazione e commettere illeciti di vario tipo da uno Stato membro all'altro, ma anche, senza difficoltà, dall'esterno della giurisdizione dell'UE. Per questo, la Commissione partecipa attivamente a dibattiti e strutture di cooperazione internazionali, tra cui il G8 Gruppo Roma-Lione sulla lotta alla criminalità ad alta tecnologia e i progetti gestiti da Interpol. Con particolare attenzione segue poi i lavori della rete di punti di contatto attivi ventiquattro ore su ventiquattro nel settore della criminalità ad alta tecnologia internazionale (la cosiddetta rete 24/7)[15], cui aderiscono molti Stati in tutto il mondo, tra i quali la maggior parte degli Stati membri dell'UE. La rete del G8 è un meccanismo che permette di accelerare i contatti tra gli Stati partecipanti, grazie a punti di contatto consultabili giorno e notte per casi implicanti la produzione di prove elettroniche o richiedenti l'assistenza urgente di autorità di contrasto straniere.

Il principale strumento europeo e internazionale in questo settore è senza dubbio la convenzione del Consiglio d'Europa del 2001 sulla cibercriminalità[16], adottata ed entrata in vigore nel 2004, che contiene definizioni comuni di vari tipi di reato informatico e pone le basi per una cooperazione giudiziaria operativa tra gli Stati che ne sono parte. L'hanno firmata molti Stati, tra cui gli Stati Uniti d'America e altri Stati non europei, e tutti gli Stati membri, alcuni dei quali però non l'hanno ancora ratificata oppure non hanno ratificato il protocollo addizionale sugli atti di natura razzista o xenofoba commessi attraverso i sistemi informatici. Considerata l'importanza comunemente accordata alla convenzione, la Commissione incoraggerà gli Stati membri e i paesi terzi interessati a ratificarla ed esaminerà la possibilità per la Comunità europea di divenirne parte.

3. ULTERIORE SVILUPPO DI STRUMENTI SPECIFICI DI LOTTA CONTRO LA CIBERCRIMINALITÀ

3.1. Rafforzare la cooperazione operativa fra autorità di contrasto e gli sforzi di formazione a livello dell'UE

La mancanza o il sottoutilizzo di strutture immediate per la **cooperazione operativa transnazionale** rimane un punto debole dello spazio di giustizia, libertà e sicurezza. In casi urgenti di cibercriminalità, l'assistenza giudiziaria tradizionale si è dimostrata lenta e inefficace, e le nuove strutture di cooperazione non sono ancora abbastanza sviluppate. Sebbene in Europa le autorità giudiziarie e di contrasto nazionali collaborino strettamente tramite Europol, Eurojust e altre strutture, rimane l'evidente necessità di rafforzare e chiarire le responsabilità di ciascuno. Dalle consultazioni condotte dalla Commissione emerge che l'uso di questi canali fondamentali non è ottimale. Un approccio europeo più coordinato deve essere tanto operativo quanto strategico e riguardare anche lo scambio di informazioni e migliori pratiche.

---

15 Si veda l'articolo 35 della convenzione del Consiglio d'Europa sulla cibercriminalità.

16 http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Nel prossimo futuro la Commissione insisterà particolarmente sulle esigenze di **formazione**. È un dato di fatto che lo sviluppo tecnologico rende necessaria una formazione continua delle autorità giudiziarie e di contrasto sui vari aspetti della cibercriminalità. È pertanto previsto un contributo finanziario maggiore e più coordinato dell'UE a favore di programmi di formazione multinazionali. Inoltre la Commissione, in stretta cooperazione con gli Stati membri e altri organi competenti quali Europol, Eurojust, l'Accademia europea di polizia (CEPOL) e la rete europea di formazione giudiziaria (REFG), si adopererà per coordinare e collegare a livello dell'UE tutti i programmi di formazione pertinenti.

Nel 2007 la Commissione organizzerà una **riunione** di esperti in materia di contrasto degli Stati membri, di Europol, della CEPOL e dell'REFG per discutere come migliorare la cooperazione strategica e operativa e la formazione in materia di cibercriminalità in Europa. Tra i vari temi, l'istituzione di un punto di contatto permanente dell'UE per lo scambio di informazioni e di una piattaforma UE di formazione sulla cibercriminalità. Quella del 2007 sarà la prima di una serie di riunioni programmate per il prossimo futuro.

3.2. Rafforzamento del dialogo con l'industria

Sia il settore pubblico che quello privato hanno interesse a elaborare insieme metodi per individuare e prevenire i danni causati dalle attività criminali. La partecipazione congiunta dei settori pubblico e privato, basata sulla fiducia reciproca e sull'obiettivo comune di ridurre tali danni, promette di essere un mezzo efficace per migliorare la sicurezza, anche nella lotta alla cibercriminalità. Gli aspetti pubblico/privato della politica della Commissione sulla cibercriminalità saranno integrati, a tempo debito, in una politica globale dell'UE, già programmata, sul dialogo tra i settori pubblico e privato, che riguarderà l'intero ambito della sicurezza europea. A portare avanti tale politica sarà, in particolare, il forum europeo per la sicurezza, la ricerca e l'innovazione che la Commissione intende creare prossimamente e che raggrupperà gli attori interessati dei settori pubblico e privato.

Lo sviluppo delle moderne tecnologie dell'informazione e dei moderni sistemi di comunicazione elettronica è controllato in larga misura da operatori privati. Società private valutano le minacce, stabiliscono programmi per contrastare la criminalità e sviluppano soluzioni tecniche per prevenire le attività criminali. L'industria ha dimostrato grande disponibilità ad aiutare le autorità pubbliche nella lotta alla cibercriminalità, soprattutto alla pornografia infantile[17] e altri tipi di contenuti illegali su Internet.

Un'altra questione riguarda l'apparente mancanza di un flusso di scambio di informazioni, conoscenze specializzate e migliori pratiche tra il settore pubblico e quello privato. Per proteggere modelli e segreti commerciali, gli operatori del settore privato sono spesso restii, o non obbligati per legge, a comunicare alle autorità di contrasto informazioni pertinenti sui reati subiti. Eppure, queste informazioni possono essere necessarie alle autorità pubbliche per elaborare una politica di lotta alla criminalità efficiente e appropriata. Le soluzioni per migliorare lo scambio intersettoriale di informazioni saranno esaminate anche alla luce delle norme vigenti in materia di protezione dei dati personali.

---

[17] Un esempio recente di cooperazione in questo settore è la cooperazione tra le autorità di contrasto e le società di carte di credito, nell'ambito della quale queste ultime hanno aiutato i servizi di polizia a localizzare acquirenti di pornografia infantile on line.

La Commissione svolge già un ruolo importante in varie strutture pubblico/privato di lotta alla cibercriminalità, come il gruppo di esperti nella prevenzione delle frodi[18]. È in effetti persuasa che una politica generale di lotta alla cibercriminalità, per essere efficace, deve anche prevedere una strategia di cooperazione tra operatori dei settori pubblico e privato, incluse le organizzazioni della società civile.

Per ampliare la cooperazione pubblico/privato in questo settore, la Commissione organizzerà nel 2007 una conferenza destinata agli esperti in materia di contrasto e ai rappresentanti del settore privato, specie Internet Service Providers (ISP), per discutere come migliorare la cooperazione operativa tra i settori pubblico e privato in Europa[19]. La conferenza tratterà tutti i temi che possono apportare un valore aggiunto a entrambi i settori, ma si soffermerà soprattutto sui seguenti aspetti:

- miglioramento della cooperazione operativa nella lotta contro le attività e i contenuti illegali su Internet, riguardanti in particolare il terrorismo, il materiale pedopornografico e altre attività illegali particolarmente sensibili dal punto di vista della tutela dell'infanzia;

- conclusione di accordi tra settori pubblico e privato per bloccare in tutta l'UE i siti a contenuto illegale, in particolare materiale pedopornografico;

- elaborazione di un modello europeo per la condivisione di informazioni necessarie e pertinenti tra i settori pubblico e privato, per promuovere un clima di fiducia reciproca e tener conto degli interessi di tutte le parti;

- istituzione di una rete di punti di contatto per le attività di contrasto del settore privato e di quello pubblico.

3.3. Legislazione

Non è ancora opportuno procedere a un'armonizzazione generale delle definizioni di reato e delle disposizioni penali nazionali in materia di cibercriminalità, dati i diversi tipi di illecito rientranti in questa nozione. Poiché l'efficacia della cooperazione tra le autorità di contrasto spesso dipende dall'esistenza di definizioni di reato almeno in parte armonizzate, armonizzare la legislazione degli Stati membri resta un obiettivo a lungo termine[20]. Per quanto riguarda alcune definizioni fondamentali di reato, un importante passo avanti si è avuto con la decisione quadro relativa agli attacchi contro i sistemi di informazione. Come precedentemente esposto, da allora sono comparse nuove minacce e la Commissione sta seguendo con attenzione questa evoluzione, essendo importante valutare di continuo l'esigenza di ulteriori atti normativi. Il monitoraggio dell'evoluzione delle minacce è svolto in stretto coordinamento con il programma europeo per la protezione delle infrastrutture critiche.

---

18 Cfr. http://ec.europa.eu/internal_market/payments/fraud/index_en.htm

19 La conferenza potrebbe essere considerata il seguito del forum dell'UE presentato al punto 6.4 della comunicazione sulla criminalità informatica.

20 Questo obiettivo a lungo termine è già stato menzionato a pagina 3 della comunicazione del 2001.

È invece opportuno soppesare sin d'ora l'opportunità di strumenti normativi contro la cibercriminalità. Un problema particolare per il quale potrebbe essere necessario legiferare riguarda i reati informatici connessi al **furto di identità**. In generale, con "furto di identità" si intende l'uso di dati di identificazione personale, come il numero di carta di credito, per commettere altri reati. Nella maggior parte degli Stati membri l'autore sarebbe più probabilmente perseguito per frode, o per un altro reato, che per furto di identità: il primo è considerato infatti un reato più grave. Il furto di identità in quanto tale non costituisce fattispecie di reato in tutti gli Stati membri. Poiché però è spesso più facile provare il reato di furto di identità che quello di frode, la cooperazione fra le autorità di contrasto dell'UE sarebbe agevolata se tutti gli Stati membri considerassero reato il furto di identità. Nel 2007 la Commissione avvierà consultazioni per valutare l'opportunità di legiferare al riguardo.

3.4. Elaborazione di statistiche

È comunemente ammesso che lo stato attuale delle informazioni sulla frequenza dei reati è largamente inadeguato, in particolare che sono necessari sensibili miglioramenti per poter comparare i dati tra Stati membri. Nella comunicazione del 7 agosto 2006, intitolata *"Elaborazione di una coerente strategia globale per la misurazione della criminalità e della giustizia penale: piano d'azione dell'UE per il 2006-2010"*[21], la Commissione ha esposto un piano quinquennale ambizioso per affrontare il problema. Il gruppo di esperti istituito dal piano d'azione sarebbe la sede adeguata per elaborare indicatori pertinenti e misurare l'estensione della cibercriminalità.

4. PROSPETTIVE

È intenzione della Commissione sviluppare tale politica generale di lotta contro la cibercriminalità. Tuttavia, le sue competenze in materia penale sono limitate, quindi tale politica può solo integrare le misure decise dagli Stati membri e da altri organi. Le misure più importanti (ciascuna delle quali implicherà l'uso di uno, alcuni o tutti gli strumenti esposti al punto 3) riceveranno il sostegno del programma finanziario "Prevenzione e lotta contro la criminalità".

4.1. La lotta contro la cibercriminalità in generale

- Instaurare una cooperazione operativa rafforzata fra autorità di contrasto e giudiziarie degli Stati membri. Questa azione sarà avviata organizzando un'apposita riunione di esperti nel 2007 e potrà comportare l'istituzione di un punto di contatto centrale dell'UE per la cibercriminalità.

- Aumentare il contributo finanziario a favore delle iniziative dirette a migliorare la formazione delle autorità di contrasto e giudiziarie che trattano i casi di cibercriminalità e a prendere le misure per coordinare tutti gli sforzi di formazione multinazionali creando una piattaforma di formazione dell'UE.

- Incoraggiare gli Stati membri e tutte le autorità pubbliche a impegnarsi seriamente a prendere provvedimenti efficaci contro la cibercriminalità e a stanziare risorse sufficienti a tal fine.

---

[21] COM(2006) 437, 7.8.2006.

- Sostenere la ricerca che contribuisce alla lotta contro la cibercriminalità.

- Organizzare almeno una grande conferenza (nel 2007) con le autorità di contrasto e gli operatori privati per avviare la cooperazione nella lotta contro le attività illegali su Internet attraverso o contro le reti elettroniche e per promuovere uno scambio più efficace di informazioni a carattere non personale; prevedere progetti concreti di cooperazione pubblico/privato che diano seguito alle conclusioni della conferenza del 2007.

- Avviare azioni pubblico/privato, e parteciparvi, che sensibilizzino, soprattutto i consumatori, ai costi e ai pericoli della cibercriminalità, evitando di minare la fiducia dei consumatori e degli utenti concentrandosi solo sugli aspetti negativi della sicurezza.

- Promuovere la cooperazione internazionale globale nella lotta contro la cibercriminalità e parteciparvi attivamente.

- Avviare e sostenere, anche finanziariamente, progetti internazionali conformi alla politica della Commissione in questo settore, ad esempio quelli gestiti dal G8 e coerenti con i documenti strategici nazionali e regionali (per quanto riguarda la cooperazione con i paesi terzi).

- Prendere misure concrete per incoraggiare tutti gli Stati membri e i paesi terzi interessati a ratificare la convenzione del Consiglio d'Europa sulla cibercriminalità e il relativo protocollo addizionale, e considerare la possibilità che la Comunità diventi parte di tale convenzione.

- Esaminare, assieme agli Stati membri, il fenomeno degli attacchi coordinati e su larga scala contro le infrastrutture di informazione degli Stati membri, al fine di prevenirli e combatterli, anche con risposte coordinate, e condividere le informazioni e le migliori pratiche.

4.2. Lotta contro i reati tradizionali su reti elettroniche

- Avviare un'analisi approfondita per approntare una proposta legislativa specifica dell'UE contro il furto di identità.

- Promuovere lo sviluppo di tecniche e procedure per combattere la frode e il commercio illegale su Internet, anche con progetti di cooperazione pubblico/privato.

- Proseguire e sviluppare i lavori in settori mirati specifici, sul modello del gruppo di esperti nella prevenzione delle frodi per quanto riguarda la lotta contro le frodi relative ai mezzi di pagamento diversi dai contanti sulle reti elettroniche.

4.3. Contenuti illegali

- Continuare a sviluppare misure contro contenuti illegali specifici, primi fra tutti il materiale pedopornografico e l'incitamento al terrorismo, provvedendo al follow up della decisione quadro relativa alla lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile.

- Invitare gli Stati membri a stanziare risorse finanziarie sufficienti per rafforzare il lavoro degli organi di contrasto, prestando particolare attenzione all'individuazione delle vittime di materiale pedopornografico on line.

- Avviare e sostenere azioni di lotta contro i contenuti illegali che possono incitare i minori ad adottare comportamenti violenti o gravemente illegali, come certi tipi di videogiochi on line estremamente violenti.

- Avviare e promuovere il dialogo tra gli Stati membri e con i paesi terzi sulle tecniche di lotta contro i contenuti illegali e sulle procedure per chiudere siti Internet illegali, anche in vista dell'eventuale conclusione di accordi formali con paesi vicini e altri paesi.

- Concludere accordi volontari e convenzioni a livello dell'UE tra autorità pubbliche e operatori privati, in particolare ISP, sulle procedure per bloccare e chiudere i siti Internet illegali.

4.4. Follow-up

La presente comunicazione espone, come tappe future, una serie di azioni per migliorare le strutture di cooperazione nell'UE. La Commissione darà seguito a tali azioni, valuterà i progressi nella realizzazione delle attività e ne riferirà al Consiglio e al Parlamento.