



PARLAMENTO EUROPEO

2009 - 2014

Commissione per l'industria, la ricerca e l'energia

2010/0273(COD)

11.11.2011

PARERE

della commissione per l'industria, la ricerca e l'energia

destinato alla commissione per le libertà civili, la giustizia e gli affari interni

sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa agli
attacchi contro i sistemi di informazione, e che abroga la decisione quadro
2005/222/GAI del Consiglio
(COM(2010)0517 – C7-0293/2010 – 2010/0273(COD))

Relatore per parere: Christian Ehler

PA_Legam

EMENDAMENTI

La commissione per l'industria, la ricerca e l'energia invita la commissione per le libertà civili, la giustizia e gli affari interni, competente per il merito, a includere nella sua relazione i seguenti emendamenti:

Emendamento 1

Proposta di direttiva Considerando 1

Testo della Commissione

(1) L'obiettivo della presente direttiva è ravvicinare le legislazioni penali degli Stati membri nel settore degli attacchi contro i sistemi di informazione e migliorare la cooperazione fra le autorità giudiziarie le altre autorità competenti degli Stati membri, compresi la polizia e gli altri servizi specializzati incaricati dell'applicazione della legge.

Emendamento

(1) L'obiettivo della presente direttiva – **il quale forma parte della strategia generale dell'Unione volta a combattere la criminalità organizzata, ad aumentare la resilienza delle reti informatiche, a proteggere le infrastrutture di informazione critiche e a garantire la tutela dei dati** – è ravvicinare le legislazioni penali degli Stati membri nel settore degli attacchi contro i sistemi di informazione e migliorare la cooperazione fra le autorità giudiziarie **e** le altre autorità competenti degli Stati membri, compresi la polizia e gli altri servizi specializzati incaricati dell'applicazione della legge, **nonché la Commissione europea, Eurojust, Europol, i gruppi di pronto intervento informatico nazionali e unionali e l'Agenzia europea per la sicurezza delle reti e dell'informazione, onde consentire un approccio comune e globale a livello dell'Unione.**

Emendamento 2

Proposta di direttiva Considerando 1 bis (nuovo)

(1 bis) I sistemi informatici sono un elemento chiave dell'interazione politica, sociale ed economica in Europa. La società è fortemente e sempre più dipendente da tali sistemi. Il buon funzionamento e la sicurezza di questi sistemi in Europa sono fondamentali per lo sviluppo del mercato interno e di un'economia competitiva e innovativa. Tuttavia, oltre a recare grandi benefici, i sistemi di informazione comportano allo stesso tempo una serie di rischi per la nostra sicurezza a causa della loro complessità e vulnerabilità nei confronti di vari tipi di criminalità informatica. La sicurezza dei sistemi di informazione è pertanto una fonte di costante preoccupazione e richiede risposte efficaci da parte degli Stati membri e dell'Unione.

Emendamento 3

Proposta di direttiva Considerando 2

(2) Gli attacchi ai danni dei sistemi di informazione, **in particolare ad opera** della criminalità organizzata, sono una minaccia crescente, e la preoccupazione per la possibilità di attacchi terroristici o di matrice politica contro sistemi di informazione che fanno parte dell'infrastruttura critica degli Stati membri e dell'Unione è in aumento. Ciò costituisce una minaccia per la creazione di una società dell'informazione sicura e di uno spazio di libertà, sicurezza e giustizia, e richiede pertanto una risposta a livello di Unione europea.

(2) Gli attacchi ai danni dei sistemi di informazione **possono provenire da diversi soggetti, come terroristi, gruppi della criminalità organizzata, Stati o individui isolati. Tali attacchi** sono una minaccia crescente **per il funzionamento dei sistemi d'informazione nell'Unione e nel mondo**, e la preoccupazione per la possibilità di attacchi terroristici o di matrice politica contro sistemi di informazione che fanno parte dell'infrastruttura critica degli Stati membri e dell'Unione è in aumento. **Il carattere transfrontaliero di certi reati e il rischio e il costo relativamente bassi per i delinquenti, sommati ai grandi vantaggi che possono ottenere e ai danni che possono causare tramite gli attacchi,**

aumentano notevolmente il livello di minaccia. Ciò costituisce una minaccia per la creazione di una società dell'informazione sicura e di uno spazio di libertà, ***democrazia***, sicurezza e giustizia, ***pregiudica la creazione di un mercato interno digitale europeo*** e richiede pertanto una risposta a livello di Unione europea ***così come a livello internazionale, ad esempio attraverso la Convenzione del 2001 del Consiglio d'Europa sulla criminalità informatica.***

Emendamento 4

Proposta di direttiva Considerando 2 bis (nuovo)

Testo della Commissione

Emendamento

(2 bis) I recenti attacchi informatici perpetrati contro le reti o i sistemi di informazione europei hanno causato all'Unione considerevoli danni sul piano economico e della sicurezza.

Motivazione

In considerazione degli attacchi informatici perpetrati nel marzo 2011 contro le istituzioni europee nonché delle numerose violazioni commesse nel quadro dei sistemi europei di scambio delle quote di emissioni, che hanno portato a furti di milioni di euro in quote di emissioni.

Emendamento 5

Proposta di direttiva Considerando 3

Testo della Commissione

Emendamento

(3) Si registra chiaramente una tendenza a perpetrare attacchi su larga scala sempre più pericolosi e ricorrenti contro sistemi di informazione critici per lo Stato o per particolari funzioni del settore pubblico o privato. Questa tendenza va di pari passo

(3) Si registra chiaramente una tendenza a perpetrare attacchi su larga scala sempre più pericolosi e ricorrenti, ***tra cui attacchi distribuiti di "negazione del servizio" (Distributed Denial of Service - DDoS)***, contro sistemi di informazione critici per le

con **lo** sviluppo di strumenti sempre più sofisticati che possono essere usati dai criminali per lanciare attacchi informatici di vario tipo.

organizzazioni internazionali, per gli Stati, per l'Unione o per particolari funzioni del settore pubblico o privato. **Tali attacchi possono causare notevoli danni economici sia attraverso l'interruzione degli stessi sistemi di informazione e comunicazione sia attraverso la perdita o l'alterazione di informazioni riservate commercialmente importanti o di altri dati. Le PMI innovative, dipendenti dal corretto funzionamento e dalla disponibilità dei sistemi di informazione, e al contempo potenzialmente in grado di dedicare minori risorse alla sicurezza delle informazioni, rischiano di essere particolarmente colpite.** Questa tendenza va di pari passo con **il rapido** sviluppo **delle tecnologie dell'informazione e pertanto** di strumenti sempre più sofisticati che possono essere usati dai criminali per lanciare attacchi informatici di vario tipo, **alcuni dei quali dotati di un forte potenziale per causare danni economici e sociali.**

Emendamento 6

Proposta di direttiva Considerando 4

Testo della Commissione

(4) Per garantire un approccio coerente degli Stati membri nell'applicazione della presente direttiva è **importante** avere, in questo settore, definizioni comuni, in particolare **quelle** inerenti ai sistemi di informazione e ai dati informatici.

Emendamento

(4) Per garantire un approccio coerente **e uniforme** degli Stati membri nell'applicazione della presente direttiva è **fondamentale** avere, in questo settore, definizioni comuni, in particolare inerenti ai sistemi di informazione e ai dati informatici **nonché ai reati commessi contro i sistemi di informazione e i dati informatici.**

Emendamento 7

Proposta di direttiva Considerando 6

Testo della Commissione

(6) È necessario che gli Stati membri prevedano sanzioni per gli attacchi ai danni di sistemi di informazione, e che le sanzioni previste siano efficaci, proporzionate e dissuasive.

Emendamento

(6) Oltre alle misure adottate dagli Stati membri, dall'Unione e dal settore privato finalizzate ad aumentare la sicurezza e l'integrità dei sistemi di informazione così come a prevenire gli attacchi e a ridurre al minimo il loro impatto, è necessario che gli Stati membri prevedano *tanto misure efficaci intese a prevenire questi attacchi quanto* sanzioni *armonizzate* per gli attacchi ai danni di sistemi di informazione, *le quali dovrebbero rientrare nel quadro di più ampie strategie nazionali volte a dissuadere dal compiere siffatti attacchi e a combatterli*, e che le sanzioni previste siano efficaci, proporzionate e dissuasive. *La convergenza delle sanzioni e delle pene previste dagli Stati membri è necessaria a causa del carattere spesso transfrontaliero delle minacce e mira a ridurre le differenze tra gli Stati membri al momento di trattare i reati commessi nell'Unione.*

Emendamento 8

Proposta di direttiva Considerando 6 bis (nuovo)

Testo della Commissione

Emendamento

(6 bis) Gli Stati membri, l'Unione europea e il settore privato, in collaborazione con l'Agenzia europea per la sicurezza delle reti e dell'informazione, devono adottare misure volte ad aumentare la sicurezza e l'integrità dei sistemi di informazione nonché a prevenire gli attacchi e a ridurre al minimo il loro impatto.

Emendamento 9

Proposta di direttiva Considerando 8

Testo della Commissione

(8) Nelle sue conclusioni del 27-28 novembre 2008, il Consiglio ha invocato l'elaborazione di una nuova strategia con gli Stati membri e la Commissione, tenendo conto del contenuto della Convenzione del 2001 del Consiglio d'Europa sulla criminalità informatica. Tale Convenzione è il quadro giuridico di riferimento per la lotta contro la criminalità informatica, compresi gli attacchi contro i sistemi di informazione, e **su di essa si basa** la presente direttiva.

Emendamento

(8) Nelle sue conclusioni del 27-28 novembre 2008, il Consiglio ha invocato l'elaborazione di una nuova strategia con gli Stati membri e la Commissione, tenendo conto del contenuto della Convenzione del 2001 del Consiglio d'Europa sulla criminalità informatica. **Il Consiglio e la Commissione devono incoraggiare gli Stati membri che non hanno ancora ratificato la Convenzione a farlo il prima possibile.** Tale Convenzione è il quadro giuridico di riferimento per la lotta contro la criminalità informatica, compresi gli attacchi contro i sistemi di informazione, e **delle sue pertinenti disposizioni tiene conto** la presente direttiva.

Emendamento 10

Proposta di direttiva Considerando 10

Testo della Commissione

(10) La presente direttiva non intende prevedere la responsabilità penale qualora **gli atti ivi contemplati** siano **compiuti** senza dolo, ad esempio per effettuare un collaudo autorizzato o proteggere un sistema informatico.

Emendamento

(10) La presente direttiva non **contempla le azioni adottate allo scopo di garantire la sicurezza dei sistemi di informazione, come ad esempio la capacità di un sistema di informazione di resistere agli atti criminali di cui alla presente direttiva, o di rimuovere dai sistemi stessi gli strumenti utilizzati o destinati ad essere utilizzati per tali atti.** Essa non intende, **inoltre**, prevedere la responsabilità penale qualora siano **soddisfatti i criteri oggettivi dei reati previsti dalla presente direttiva, ma l'azione sia compiuta** senza dolo, ad esempio per effettuare un collaudo autorizzato o proteggere un sistema

informatico.

Motivazione

Dato il confine a volte labile fra accesso maligno e non maligno (aggiornamenti automatici, ecc.), l'emendamento mira a chiarire che, ad esempio, il funzionamento di software anti-virus o di strumenti di rimozione dei virus, o la messa in quarantena di dispositivi infetti, sono completamente al di fuori del campo di applicazione della direttiva.

Emendamento 11

Proposta di direttiva Considerando 11

Testo della Commissione

(11) La presente direttiva rafforza l'importanza delle reti, come la rete di punti di contatto del G8 o quella del Consiglio d'Europa, disponibili 24 ore su 24 e 7 giorni su 7 per lo scambio di informazioni allo scopo di assicurare un'assistenza immediata per le indagini o i procedimenti relativi a reati connessi a sistemi e dati informatici, o per la raccolta di prove **in formato elettronico** di un reato. Data la rapidità con cui possono essere lanciati gli attacchi su larga scala, occorre che gli Stati membri siano in grado di rispondere prontamente alle richieste urgenti provenienti da questa rete di punti di contatto. Tale assistenza deve consistere nel facilitare o nell'applicare direttamente misure come l'apporto di **consigli tecnici**, la conservazione dei dati, la raccolta di prove, la trasmissione di informazioni di carattere giuridico e la localizzazione dei sospetti.

Emendamento

(11) La presente direttiva rafforza l'importanza delle reti, come la rete di punti di contatto del G8 o quella del Consiglio d'Europa, disponibili 24 ore su 24 e 7 giorni su 7 per lo scambio di informazioni allo scopo di assicurare un'assistenza immediata per le indagini o i procedimenti relativi a reati connessi a sistemi e dati informatici, o per la raccolta di prove di un reato **o del tentativo di commettere un reato**. Data la rapidità con cui possono essere lanciati gli attacchi su larga scala, occorre che gli Stati membri, **l'Unione europea e l'Agenzia europea per la sicurezza delle reti e dell'informazione** siano in grado di rispondere prontamente **ed efficacemente** alle richieste urgenti provenienti da questa rete di punti di contatto. Tale assistenza deve consistere nel facilitare o nell'applicare direttamente misure come l'apporto di **assistenza tecnica, anche in ordine al ripristino della funzionalità dei sistemi di informazione**, la conservazione dei dati **in linea con i principi della protezione dei dati personali**, la raccolta di prove, la trasmissione di informazioni di carattere giuridico, **l'identificazione delle informazioni minacciate e/o carpite**, e la localizzazione **e l'identificazione** dei sospetti.

Emendamento 12

Proposta di direttiva Considerando 11 bis (nuovo)

Testo della Commissione

Emendamento

(11 bis) La cooperazione delle autorità pubbliche con il settore privato e con la società civile è di grande importanza per prevenire e combattere gli attacchi contro i sistemi di informazione. Occorre istituire un dialogo permanente con questi soggetti in considerazione del largo uso che fanno dei sistemi d'informazione, e della condivisione delle responsabilità necessaria per la stabilità e il buon funzionamento di tali sistemi. Migliorare la consapevolezza di tutti i soggetti coinvolti nell'utilizzo dei sistemi di informazione è importante al fine di creare una cultura della sicurezza informatica.

Emendamento 13

Proposta di direttiva Considerando 12

Testo della Commissione

Emendamento

(12) È necessario raccogliere dati sui reati contemplati dalla presente direttiva per ottenere un quadro più completo del problema a livello dell'Unione e contribuire così alla formulazione di risposte più efficaci. Grazie ai dati raccolti, inoltre, agenzie **specializzate** come Europol e l'Agenzia europea per la sicurezza delle reti e dell'informazione potranno valutare meglio la portata della criminalità informatica e lo stato della sicurezza delle reti e dell'informazione **in Europa**.

(12) È necessario raccogliere dati sui reati contemplati dalla presente direttiva per ottenere un quadro più completo del problema a livello dell'Unione e contribuire così alla formulazione di risposte più efficaci. **Gli Stati membri devono migliorare lo scambio di informazioni in merito agli attacchi contro i sistemi di informazione, con il sostegno della Commissione e dell'Agenzia europea per la sicurezza delle reti e dell'informazione.** Grazie ai dati raccolti, inoltre, agenzie **ed organi specializzati** come **i gruppi di pronto intervento degli Stati membri**

(CERT), Europol e l'Agenzia europea per la sicurezza delle reti e dell'informazione potranno valutare meglio la portata della criminalità informatica e lo stato della sicurezza delle reti e dell'informazione nell'Unione nonché assistere gli Stati membri nel fornire risposte agli incidenti in materia di sicurezza informatica. Una migliore conoscenza dei rischi presenti e futuri consentirà di adottare decisioni più appropriate per prevenire, combattere o limitare i danni causati dagli attacchi contro i sistemi di informazione.

Emendamento 14

Proposta di direttiva Considerando 12 bis (nuovo)

Testo della Commissione

Emendamento

(12 bis) Mentre la presente direttiva deve soddisfare severi requisiti in materia di certezza giuridica e prevedibilità del diritto penale, vi è anche la necessità – soddisfatta attraverso le disposizioni della presente direttiva sulla raccolta di dati, lo scambio di informazioni e l'obbligo per la Commissione di riferire regolarmente sulla sua applicazione e di formulare le proposte necessarie – di prevedere un meccanismo flessibile per permettere l'adattamento agli sviluppi futuri, che possa portare ad un ampliamento del campo di applicazione della presente direttiva. Tali sviluppi futuri comprendono tutti gli sviluppi tecnologici che consentono, ad esempio, un'applicazione più efficace nel settore degli attacchi contro i sistemi di informazione o che facilitano la prevenzione o l'attenuazione di tali attacchi.

Motivazione

Pur apprezzando l'introduzione di sanzioni, un approccio globale dell'Unione per contrastare

la criminalità informatica dovrebbe non solo concentrarsi sull'effettiva applicazione della legge, ma anche sviluppare strategie e strumenti per prevenire tali attività criminali.

Emendamento 15

Proposta di direttiva Considerando 12 ter (nuovo)

Testo della Commissione

Emendamento

(12 ter) L'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) dovrebbe svolgere un ruolo strategico nel quadro delle azioni di coordinamento tra gli Stati membri e le istituzioni dell'Unione. L'Agenzia potrebbe, ad esempio, essere incaricata di supervisionare lo scambio di informazioni tra detti soggetti, funzionando pertanto come punto di contatto unico e come organo di registrazione degli incidenti in materia di sicurezza informatica dell'Unione. L'Agenzia potrebbe inoltre essere incaricata di centralizzare a livello dell'Unione i dati statistici sui reati di cui alla presente direttiva e, fondandosi sui medesimi, di elaborare relazioni sulle condizioni di sicurezza dei sistemi di informazione e dei dati informatici nel territorio dell'Unione.

Emendamento 16

Proposta di direttiva Considerando 13

Testo della Commissione

Emendamento

(13) Le rilevanti lacune e le notevoli differenze nelle normative degli Stati membri nel campo degli attacchi contro i sistemi di informazione possono ostacolare la lotta contro la criminalità organizzata ed il terrorismo e complicare un'efficace cooperazione di polizia e giudiziaria in questo settore. Il carattere transnazionale e

(13) Le rilevanti lacune e le notevoli differenze nelle normative degli Stati membri nel campo degli attacchi contro i sistemi di informazione possono ostacolare la lotta contro la criminalità organizzata ed il terrorismo e complicare un'efficace cooperazione di polizia e giudiziaria in questo settore. Il carattere transnazionale e

senza frontiere dei moderni sistemi di informazione fa sì che gli attacchi contro tali sistemi abbiano una dimensione transnazionale, e rende evidente la necessità di adottare urgentemente azioni ulteriori per il ravvicinamento delle legislazioni penali in questo settore. L'adozione della decisione quadro 2009/948/GAI del Consiglio sulla prevenzione e la risoluzione dei conflitti relativi all'esercizio della giurisdizione nei procedimenti penali dovrebbe inoltre agevolare il coordinamento dell'azione penale nei casi di attacchi contro i sistemi di informazione.

senza frontiere dei moderni sistemi di informazione fa sì che gli attacchi contro tali sistemi abbiano una dimensione transnazionale, e rende evidente la necessità di adottare urgentemente azioni ulteriori **a livello dell'Unione** per il ravvicinamento delle legislazioni penali **nazionali** in questo settore. **Inoltre, l'Unione deve mirare a conseguire una maggiore cooperazione internazionale nel campo della sicurezza delle reti e dei sistemi di informazione, cui partecipino tutti i soggetti internazionali interessati.** L'adozione della decisione quadro 2009/948/GAI del Consiglio sulla prevenzione e la risoluzione dei conflitti relativi all'esercizio della giurisdizione nei procedimenti penali dovrebbe inoltre agevolare il coordinamento dell'azione penale nei casi di attacchi contro i sistemi di informazione.

Emendamento 17

Proposta di direttiva Articolo 1 – comma unico

Testo della Commissione

La presente direttiva introduce fattispecie di reato nel settore degli attacchi contro i sistemi di informazione e stabilisce norme minime per le relative sanzioni. Essa mira altresì a introdurre disposizioni comuni per impedire tali attacchi **e** migliorare la cooperazione **giudiziaria penale** europea in questo campo.

Emendamento

La presente direttiva introduce fattispecie di reato nel settore degli attacchi contro i sistemi di informazione e stabilisce norme minime **armonizzate** per le relative sanzioni. Essa mira altresì a introdurre disposizioni comuni **sia** per impedire **e combattere** tali attacchi **sia per** migliorare la cooperazione europea in questo campo, **in particolare in materia di giustizia penale.**

Emendamento 18

Proposta di direttiva Articolo 2 – lettera d

Testo della Commissione

(d) l'espressione "senza diritto" significa l'accesso o l'interferenza non autorizzati da parte di chi ha il diritto di proprietà o altro diritto sul sistema o una sua parte, ovvero non consentiti ai sensi **della legislazione** nazionale.

Emendamento

(d) l'espressione "senza diritto" significa l'accesso o l'interferenza non autorizzati da parte di chi ha il diritto di proprietà o altro diritto sul sistema o una sua parte, ovvero non consentiti ai sensi **del diritto** nazionale **o unionale**.

Emendamento 19

Proposta di direttiva
Articolo 7 – lettera b

Testo della Commissione

b) una password di un computer, un codice d'accesso, o informazioni simili che permettono di accedere in tutto o in parte a un sistema di informazione.

Emendamento

b) una password di un computer, un codice d'accesso, **un token di sicurezza digitale o fisico**, o informazioni simili che permettono di accedere in tutto o in parte a un sistema di informazione.

Emendamento 20

Proposta di direttiva
Articolo 8 – paragrafo 1 bis (nuovo)

Testo della Commissione

Emendamento

1 bis. Gli Stati membri provvedono a che la trasmissione non autorizzata di dati identificativi ad altre persone al fine di realizzare una delle operazioni di cui agli articoli da 3 a 7 costituisca reato.

Emendamento 21

Proposta di direttiva
Articolo 8 – paragrafo 1 ter (nuovo)

Testo della Commissione

Emendamento

1 ter. Gli Stati membri provvedono a che, qualora un atto previsto dagli articoli da 3

a 7 sia commesso da una persona che, nel quadro dell'esercizio delle sue funzioni, ha accesso ai sistemi di sicurezza inerenti ai sistemi di informazione, ciò costituisca una circostanza aggravante e l'atto in questione costituisca reato.

Emendamento 22

Proposta di direttiva Articolo 10 – paragrafo 2

Testo della Commissione

2. Gli Stati membri adottano le misure necessarie affinché i reati di cui agli articoli da 3 a 6 siano punibili con pene detentive non inferiori nel massimo ad anni cinque qualora siano stati commessi con strumenti concepiti per lanciare attacchi contro un gran numero di sistemi d'informazione o attacchi che causano danni ingenti, come perturbazioni dei servizi di sistema, costi finanziari o perdita di dati personali.

Emendamento

2. Gli Stati membri adottano le misure necessarie affinché i reati di cui agli articoli da 3 a 6 siano punibili con pene detentive non inferiori nel massimo ad anni cinque qualora siano stati commessi con strumenti concepiti per lanciare attacchi contro un gran numero di sistemi d'informazione o attacchi che causano danni ingenti, come perturbazioni dei servizi di sistema, costi finanziari o perdita di dati personali ***o di informazioni sensibili.***

Emendamento 23

Proposta di direttiva Articolo 13 – paragrafo 1 – lettera c

Testo della Commissione

(c) a beneficio di una persona giuridica ***che ha la sede legale*** nel territorio dello Stato membro interessato.

Emendamento

(c) a beneficio di una persona giuridica ***costituita*** nel territorio dello Stato membro interessato.

Emendamento 24

Proposta di direttiva Articolo 14 – paragrafo 1

Testo della Commissione

1. Per lo scambio delle informazioni relative ai reati di cui agli articoli da 3 a 8, fatte salve le disposizioni sulla protezione dei dati, gli Stati membri si servono della rete **esistente** di punti di contatto operativi 24 ore su 24 e 7 giorni su 7. Gli Stati membri provvedono inoltre a predisporre procedure per rispondere entro un massimo di otto ore alle richieste urgenti. La risposta **deve almeno indicare se, in che forma e quando sarà soddisfatta la richiesta di aiuto.**

Emendamento

1. Per lo scambio delle informazioni relative ai reati di cui agli articoli da 3 a 8, fatte salve le disposizioni sulla protezione dei dati, gli Stati membri **provvedono a predisporre un punto di contatto nazionale operativo e** si servono della rete di punti di contatto operativi 24 ore su 24 e 7 giorni su 7 **e inoltre trasmettono tali informazioni alla Commissione e all'Agenzia europea per la sicurezza delle reti e dell'informazione.** Gli Stati membri provvedono inoltre a predisporre procedure per rispondere entro un massimo di otto ore alle richieste urgenti. La risposta **è efficace e comprende, secondo il caso, l'agevolazione o l'attuazione diretta delle seguenti misure: l'apporto di consigli tecnici, anche in ordine al ripristino della funzionalità dei sistemi d'informazione, la conservazione dei dati in linea con i principi della protezione dei dati personali, la raccolta di prove, la trasmissione di informazioni di carattere giuridico, e la localizzazione e l'identificazione dei sospetti. I punti di contatto indicano in quale forma ed entro quanto tempo le richieste di assistenza saranno soddisfatte.**

Emendamento 25

Proposta di direttiva Articolo 14 – paragrafo 2

Testo della Commissione

2. Gli Stati membri informano la Commissione in merito al proprio punto di contatto operativo stabilito per lo scambio

Emendamento

2. Gli Stati membri informano la Commissione, **Eurojust e l'Agenzia europea per la sicurezza delle reti e**

d'informazioni sui reati di cui agli articoli da 3 a 8. La Commissione trasmette tali informazioni agli altri Stati membri.

dell'informazione in merito al proprio punto di contatto operativo stabilito per lo scambio d'informazioni sui reati di cui agli articoli da 3 a 8. La Commissione trasmette tali informazioni agli altri Stati membri.

Emendamento 26

Proposta di direttiva Articolo 15 – paragrafo 3

Testo della Commissione

3. Gli Stati membri trasmettono alla Commissione i dati raccolti ai sensi del presente articolo. Provvedono inoltre alla pubblicazione di una revisione consolidata di queste relazioni statistiche.

Emendamento

3. Gli Stati membri trasmettono alla Commissione, **a Europol e all'Agenzia europea per la sicurezza delle reti e dell'informazione** i dati raccolti ai sensi del presente articolo **e** provvedono inoltre alla pubblicazione di una revisione consolidata **periodica** di queste relazioni statistiche.

Emendamento 27

Proposta di direttiva Articolo 18 – paragrafo 1

Testo della Commissione

1. Entro [QUATTRO ANNI DALL'ADOZIONE], e successivamente ogni tre anni, la Commissione presenta al Parlamento europeo e al Consiglio una relazione sull'applicazione della presente direttiva negli Stati membri, corredata delle opportune proposte.

Emendamento

1. Entro [QUATTRO ANNI DALL'ADOZIONE], e successivamente ogni tre anni, la Commissione, **dopo aver consultato tutte le parti interessate**, presenta al Parlamento europeo e al Consiglio una relazione sull'applicazione della presente direttiva negli Stati membri, corredata delle opportune proposte. **Ogni relazione individua le soluzioni tecniche che consentono un'attuazione più efficace nell'Unione nel settore degli attacchi contro i sistemi di informazione, comprese le soluzioni tecniche che potrebbero servire a prevenire o a mitigare tali attacchi, e ne tiene conto per quanto riguarda qualsiasi proposta necessaria.**

Emendamento 28

Proposta di direttiva Articolo 18 – paragrafo 2

Testo della Commissione

2. Gli Stati membri trasmettono alla Commissione ogni informazione utile ai fini della relazione di cui al paragrafo 1. Tali informazioni comprendono una descrizione dettagliata delle misure legislative e non legislative adottate per l'attuazione della presente direttiva.

Emendamento

2. Gli Stati membri ***e l'Agenzia europea per la sicurezza delle reti e dell'informazione*** trasmettono alla Commissione ogni informazione utile ai fini della relazione di cui al paragrafo 1. Tali informazioni comprendono una descrizione dettagliata delle misure legislative e non legislative adottate per l'attuazione della presente direttiva.

PROCEDURA

Titolo	Attacchi contro i sistemi di informazione e abrogazione della decisione quadro 2005/222/GAI del Consiglio	
Riferimenti	COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)	
Commissione competente per il merito Annuncio in Aula	LIBE 7.10.2010	
Commissione(i) competente(i) per parere Annuncio in Aula	ITRE 7.10.2010	
Relatore(i) Nomina	Christian Ehler 24.11.2010	
Esame in commissione	13.4.2011	6.10.2011
Approvazione	10.11.2011	
Esito della votazione finale	+: 49 -: 0 0: 1	
Membri titolari presenti al momento della votazione finale	Ivo Belet, Bendt Bendtsen, Maria Da Graça Carvalho, Giles Chichester, Pilar del Castillo Vera, Christian Ehler, Ioan Enciu, Adam Gierek, Norbert Glante, Robert Goebbels, Fiona Hall, Jacky Hénin, Kent Johansson, Romana Jordan Cizelj, Lena Kolarska-Bobińska, Béla Kovács, Philippe Lamberts, Bogdan Kazimierz Marcinkiewicz, Marisa Matias, Judith A. Merkies, Angelika Niebler, Jaroslav Paška, Aldo Patriciello, Anni Podimata, Miloslav Ransdorf, Herbert Reul, Michèle Rivasi, Jens Rohde, Paul Rübig, Amalia Sartori, Francisco Sosa Wagner, Konrad Szymański, Michael Theurer, Ioannis A. Tsoukalas, Claude Turmes, Niki Tzavela, Marita Ulvskog, Vladimir Urutchev, Adina-Ioana Vălean	
Supplenti presenti al momento della votazione finale	Antonio Cancian, Jolanta Emilia Hibner, Yannick Jadot, Ivailo Kalfin, Bernd Lange, Werner Langen, Markus Pieper, Mario Pirillo, Hannes Swoboda, Silvia-Adriana Țicău	
Supplenti (art. 187, par. 2) presenti al momento della votazione finale	Eider Gardiazábal Rubial	