COMMISSIONE
EUROPEA

ALTA RAPPRESENTANTE
DELL'UNIONE EUROPEA
PER GLI AFFARI ESTERI
E LA POLITICA DI SICUREZZA

Bruxelles, 7.2.2013
JOIN(2013) 1 final

COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

Strategia dell'Unione europea per la cibersicurezza:

un ciberspazio aperto e sicuro

COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

Strategia dell'Unione europea per la cibersicurezza:

un ciberspazio aperto e sicuro

1. INTRODUZIONE

1.1. Contesto

Negli ultimi due decenni internet, e più in generale il ciberspazio, hanno avuto un impatto impressionante su tutti gli strati della società. La nostra vita quotidiana, i diritti fondamentali, le interazioni sociali e le economie dipendono dal funzionamento impeccabile delle tecnologie dell'informazione e della comunicazione. Un ciberspazio aperto e libero ha promosso l'inclusione politica e sociale in tutto il mondo, ha abbattuto le barriere tra paesi, comunità e cittadini rendendo possibili l'interazione e lo scambio di informazioni e di idee in tutto il pianeta, ha creato un forum di libertà di espressione e esercizio dei diritti fondamentali e ha conferito potere partecipativo ai cittadini nella loro ricerca di una società democratica e più giusta, come è avvenuto in modo clamoroso durante la cd. Primavera araba.

Perché il ciberspazio rimanga aperto e libero è necessario che nell'ambiente online si applichino le stesse norme, gli stessi principi e gli stessi valori che l'Unione europea difende offline. Occorre tutelare nel ciberspazio i diritti fondamentali, la democrazia e lo Stato di diritto. La nostra libertà e la nostra prosperità dipendono sempre più dalla solidità e dall'innovazione di internet, che continuerà a fiorire a patto che l'innovazione del settore privato e la società civile ne guidino la crescita. Ma la libertà online presuppone la sicurezza. È necessario che il ciberspazio sia protetto da incidenti, attività dolose e abusi: gli Stati hanno un ruolo decisivo nella garanzia della libertà e della sicurezza del ciberspazio. I loro compiti sono numerosi: salvaguardare l'apertura e l'accessibilità, rispettare e proteggere i diritti fondamentali online e preservare l'affidabilità e l'interoperabilità di internet. D'altro canto, il settore privato è proprietario e fa funzionare quote notevoli di ciberspazio, per cui la riuscita di qualsiasi iniziativa in questo settore presuppone il riconoscimento del suo ruolo motore.

La tecnologia dell'informazione e delle comunicazioni è diventata la spina dorsale della crescita economica e una risorsa critica da cui dipendono tutti i settori dell'economia: oggi queste tecnologie sono alla base dei sistemi complessi che fanno funzionare le nostre economie in settori essenziali come la finanza, la sanità, l'energia e i trasporti, mentre molti modelli di impresa si fondano sulla disponibilità ininterrotta di internet e sul corretto funzionamento dei sistemi informativi.

Con il completamento del mercato unico digitale il PIL dell'UE potrebbe aumentare di quasi 500 miliardi all'anno[1], ossia in media 1 000 euro pro capite. Il decollo delle nuove tecnologie connesse, come i pagamenti elettronici, l'informatica nella nuvola o la comunicazione da macchina a macchina[2], presuppone la fiducia e l'affidamento dei cittadini. Purtroppo

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf

[2] Ad esempio l'inserimento di sensori nelle piante per comunicare al sistema di irrigazione che è ora di annaffiare.

un'indagine di Eurobarometro del 2012[3] ha dimostrato che quasi un terzo dei cittadini europei non si fidano a usare internet per operazioni bancarie o acquisti. La stragrande maggioranza degli intervistati ha anche affermato di evitare di rendere pubblici i propri dati personali online per questioni di sicurezza. A livello dell'Unione, più di un internauta su dieci è già stato vittima di frodi online.

L'esperienza degli anni recenti dimostra che il mondo digitale, oltre a procurare enormi vantaggi, presenta anche vulnerabilità. Gli incidenti a carico della cibersicurezza[4], intenzionali o fortuiti, che stanno crescendo ad un ritmo allarmante, sono suscettibili di perturbare la fornitura di servizi essenziali che diamo per scontati, come la distribuzione idrica, le cure sanitarie, l'elettricità o i servizi mobili. Le minacce possono essere di varia origine, come attacchi criminali, di natura politica o terroristica, o commissionati da uno Stato, oppure essere causate da calamità naturali e errori non intenzionali.

L'economia dell'UE già conosce i reati cibernetici[5] messi a segno contro il settore privato e le persone. I cibercriminali si avvalgono di metodi sempre più sofisticati per infiltrarsi nei sistemi informativi, rubare dati critici o ricattare imprese. L'aumento dello spionaggio economico e di attività sponsorizzate dagli Stati nel ciberspazio dà origine ad una nuova categoria di minacce per gli Stati e le imprese dell'UE.

Anche al di fuori dell'UE gli Stati possono abusare del ciberspazio per sorvegliare e controllare i propri cittadini. L'UE può combattere questa situazione promuovendo la libertà in linea e garantendo il rispetto dei diritti fondamentali online.

Tutti questi fattori spiegano perché i governi di tutto il mondo hanno iniziato a sviluppare strategie in materia di cibersicurezza e a considerare il ciberspazio come una questione internazionale sempre più importante. È tempo che anche l'Unione europea intensifichi i propri interventi in questo campo. La presente proposta di strategia dell'Unione europea per la cibersicurezza, presentata dalla Commissione e dall'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza (l'Alto rappresentante), delinea la visione dell'UE in questo campo, chiarisce i ruoli e le responsabilità e definisce gli interventi necessari per una protezione effettiva e forte e per la promozione dei diritti dei cittadini, nell'intento di fare dell'ambiente online dell'Unione l'ambiente in linea più sicuro al mondo.

1.2. Principi della cibersicurezza

Per le sue qualità di strumento di comunicazione senza confini e multistrato internet è diventata uno degli strumenti più potenti di progresso planetario, non soggetto a sorveglianza o regolamentazione statale. Se da un lato il settore privato dovrà continuare a svolgere un ruolo motore nella costruzione e nella gestione quotidiana di internet, dall'altro si sta facendo sempre più pressante la necessità di fissare obblighi di trasparenza, rendicontazione e

---

3 Indagine speciale Eurobarometro 390 del 2012 sulla cibersicurezza.

4 La cibersicurezza si riferisce comunemente alle precauzioni e agli interventi che si possono prendere per proteggere il ciberdominio, in campo sia civile che militare, nei confronti delle minacce associate o che possono nuocere alle loro reti e infrastrutture di informazione interdipendenti. La cibersicurezza si propone di salvaguardare la disponibilità e l'integrità delle reti e dell'infrastruttura e la riservatezza delle informazioni che esse contengono.

5 Il reato cibernetico o cibercrimine si riferisce comunemente a un'ampia gamma di attività criminali diverse in cui i sistemi informativi e i sistemi informatici costituiscono o l'arma primaria o il bersaglio primario. Il cibercrimine comprende reati tradizionali (ad es. frode, contraffazione o furto di identità), reati connessi ai contenuti (ad es. distribuzione in linea di materiale pedopornografico o incitamento all'odio razziale) e reati peculiari ai sistemi informatici e ai sistemi informativi (ad es. attacchi contro i sistemi informativi, rifiuto di servizio o software maligni (malware).

sicurezza. La presente strategia chiarisce i principi ai quali dovrebbe essere ispirata la politica in materia di cibersicurezza a livello unionale e internazionale.

I valori costitutivi dell'UE valgono sia nel mondo del digitale che nel mondo fisico

Le stesse leggi e le stesse norme che si applicano in altri settori della nostra vita quotidiana si applicano anche nel ciberspazio.

Protezione dei diritti fondamentali, della libertà di espressione, dei dati personali e della vita privata

La cibersicurezza può essere solida ed efficace solo se si basa sui diritti e sulle libertà fondamentali sancite dalla Carta dei diritti fondamentali dell'Unione europea e sui valori costitutivi dell'Unione. Viceversa, non è possibile assicurare i diritti delle persone senza disporre di reti e sistemi sicuri. Qualunque scambio di informazioni ai fini della cibersicurezza, dove siano in gioco dati personali deve rispettare la legislazione dell'UE in materia di protezione dei dati e tenere pienamente conto dei diritti delle persone in questo campo.

Accesso per tutti

Se si pensa a quanto il mondo digitale pervada ogni attività sociale è evidente come un accesso limitato o inesistente a internet e l'analfabetismo digitale siano pregiudizievoli per i cittadini. Tutti dovrebbero avere accesso a internet e a un flusso continuo di informazioni. L'accesso sicuro per tutti presuppone l'integrità e la sicurezza di internet.

Governance partecipativa, democratica ed efficiente

Il mondo digitale non è controllato da un'entità singola: attualmente sono parecchi i soggetti interessati, tra cui entità commerciali e non governative, implicati nella gestione quotidiana delle risorse, dei protocolli e delle norme di internet e nel futuro sviluppo della rete. L'UE ribadisce l'importanza di ciascun soggetto interessato nell'attuale modello di governance e appoggia questo approccio partecipativo alla governance di internet[6].

Responsabilità condivisa per garantire la sicurezza

La crescente dipendenza dalle tecnologie dell'informazione e delle comunicazioni in tutti i campi della vita umana ha creato vulnerabilità che è necessario definire adeguatamente, analizzare in profondità, riparare o ridurre. Tutti gli attori implicati, siano essi autorità pubbliche, settore privato o singoli cittadini, devono riconoscere questa responsabilità condivisa, attivarsi per proteggersi e se necessario assicurare una risposta coordinata per rafforzare la cibersicurezza.

2. AZIONI E PRIORITÀ STRATEGICHE

L'UE ha il compito di salvaguardare un ambiente online che offra la massima libertà e sicurezza possibile per tutti. Pur riconoscendo che spetta in primo luogo agli Stati membri il compito di affrontare le sfide di sicurezza nel ciberspazio, la presente strategia propone interventi specifici che possono rafforzare l'efficienza complessiva dell'UE. Questi interventi

[6] V. anche COM(2009) 277, Comunicazione della Commissione al Parlamento Europeo e al Consiglio – "Governance di internet : le prossime tappe"

sono proiettati sia nel breve che nel lungo termine, comprendono una serie di strumenti strategici[7] e coinvolgono vari tipi di attori, dalle istituzioni dell'UE, agli Stati membri, all'industria.

La visione dell'UE delineata nella presente strategia si articola intorno a cinque priorità strategiche per affrontare le sfide sopra descritte:

- raggiungere la ciberresilienza;
- ridurre drasticamente il cibercrimine;
- sviluppare una politica e capacità di ciberdifesa connesse alla Politica di sicurezza e di difesa comune (PSDC);
- sviluppare le risorse industriali e tecnologiche per la cibersicurezza;
- creare una politica internazionale coerente dell'Unione europea sul ciberspazio e promuovere i valori costitutivi dell'UE.

2.1. Raggiungere la ciberresilienza

Per promuovere la ciberresilienza nell'UE le autorità pubbliche e il settore privato devono sviluppare capacità e cooperare efficacemente. Basandosi sui risultati positivi ottenuti grazie alle attività realizzate finora[8], gli ulteriori interventi dell'UE possono contribuire in particolare a contrastare i rischi e le minacce cibernetiche aventi dimensione transfrontaliera e a preparare a una risposta coordinata in situazioni di emergenza. In questo modo si sosterrà concretamente il corretto funzionamento del mercato interno e si rafforzerà la sicurezza interna dell'UE.

Senza un considerevole sforzo di rafforzamento delle capacità e delle risorse pubbliche e private, nonché dei procedimenti per prevenire, individuare e trattare gli incidenti a carico della cibersicurezza, l'Europa resterà vulnerabile. Per questo la Commissione ha elaborato una politica in materia di sicurezza delle reti e dell'informazione (SRI)[9]. L'**Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA)** è stata costituita nel 2004[10] e attualmente il Consiglio e il Parlamento stanno esaminando un nuovo regolamento destinato a rafforzare l'ENISA e ad aggiornarne il mandato[11]. Inoltre, la direttiva quadro sulle comunicazioni elettroniche fa obbligo ai fornitori di comunicazioni elettroniche[12] di gestire adeguatamente i rischi sulle loro reti e di segnalare importanti violazioni di sicurezza. La legislazione dell'Unione in materia di protezione dei dati[13] impone poi ai responsabili del trattamento dei dati di garantire il rispetto degli obblighi e delle garanzie in materia di

---

7 Le azioni connesse allo scambio di informazioni se sono in gioco dati personali devono rispettare la legislazione dell'UE in materia di protezione dei dati.

8 Si vedano i riferimenti nella presente comunicazione e nel documento di lavoro dei servizi della Commissione sulla valutazione di impatto che accompagna la proposta della Commissione relativa ad una direttiva sulla sicurezza delle reti e dell'informazione, in particolare le sezioni 4.1.4, 5.2 e gli allegati 2, 6 e 8.

9 Nel 2001 la Commissione ha adottato una comunicazione "Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo" (COM(2001) 298); nel 2006 ha adottato "Una strategia per una società dell'informazione sicura" (COM(2006) 251). Dal 2009 la Commissione ha adottato anche un piano di azione e una comunicazione "Proteggere le infrastrutture critiche informatizzate" (COM(2009) 149, approvata dalla risoluzione del Consiglio 2009/C 321/01 e COM(2011) 163, approvata dalle conclusioni del Consiglio 10299/11).

10 Regolamento (CE) n. 460/2004.

11 COM(2010) 521. Le azioni proposte nella presente strategia non comportano modifiche del mandato attuale o futuro dell'ENISA.

12 Articoli 13 *bis* e 13 *ter* della direttiva 2002/21/CE.

13 Articolo 17 della direttiva 95/46/CE; articolo 4 della direttiva 2002/58/CE.

protezione dei dati, anche mediante l'adozione di misure connesse alla sicurezza e, nel settore dei servizi di comunicazione elettronica accessibili al pubblico, di notificare alle autorità nazionali competenti gli incidenti che comportano violazioni di dati personali.

Nonostante i progressi compiuti grazie a impegni assunti su base volontaria, continuano a esistere lacune nell'UE, soprattutto in termini di capacità nazionali, di coordinamento in caso di incidenti che coinvolgono più paesi e di coinvolgimento e preparazione del settore privato. La presente strategia è accompagnata da una proposta **legislativa** destinata in particolare a:

- stabilire obblighi minimi comuni in materia di SRI a livello nazionale, in base ai quali gli Stati membri sarebbero tenuti a designare autorità nazionali competenti in materia di SRI, costituire squadre CERT performanti e adottare una strategia nazionale e un piano di collaborazione nazionale in materia di SRI. La creazione di capacità e il coordinamento riguardano anche le istituzioni dell'UE: nel 2012 è stata costituita su base permanente una squadra di pronto intervento informatico (in seguito "CERT-UE") responsabile della sicurezza dei sistemi IT delle istituzioni, delle agenzie e degli organismi dell'UE;
- costituire meccanismi coordinati di prevenzione, individuazione, mitigazione e risposta, che permettano lo scambio di informazioni e l'assistenza reciproca tra le autorità nazionali competenti in materia di SRI. Le autorità nazionali competenti in materia di SRI dovranno garantire un'adeguata collaborazione a livello UE, in particolare sulla base di un piano unionale di collaborazione in materia di SRI, per rispondere in particolare agli incidenti cibernetici aventi dimensione transnazionale. Tale collaborazione poggerà anche sui progressi compiuti nell'ambito del Forum europeo degli Stati membri (EFMS)[14] che ha organizzato discussioni e scambi produttivi sulla politica pubblica in materia di sicurezza delle reti e dell'informazione e che potrà essere integrato nel meccanismo di cooperazione, una volta costituito;
- migliorare la preparazione e l'impegno del settore privato. Poiché la vasta maggioranza delle reti e dei sistemi informativi sono di proprietà privata e sono operati da privati, è essenziale coinvolgere maggiormente il settore privato nel rafforzamento della cibersicurezza. Il settore privato dovrebbe elaborare, a livello tecnico, capacità proprie di ciberresilienza e scambiare buone pratiche a livello intersettoriale. Anche il settore pubblico dovrebbe beneficiare degli strumenti messi a punto dall'industria per rispondere agli incidenti, individuare le cause e condurre indagini di polizia scientifica.

Tuttavia, continuano a non esistere incentivi efficaci che incoraggino gli attori privati a fornire dati attendibili sull'esistenza di incidenti a carico della SRI o sul loro impatto, ad abbracciare una cultura di gestione del rischio o a investire in soluzioni di sicurezza. La legislazione proposta mira pertanto a garantire che gli attori di una serie di settori cruciali (come l'energia, i trasporti, le banche, le borse, i facilitatori di servizi internet e le amministrazioni pubbliche) valutino i rischi di cibersicurezza che corrono, garantiscano l'affidabilità e la resilienza delle loro reti e dei loro sistemi informativi attraverso una gestione appropriata del rischio e scambino le informazioni richieste con le autorità nazionali competenti in materia di SRI. L'accoglimento di una cultura della cibersicurezza potrebbe rafforzare le opportunità commerciali e la competitività del settore privato e trasformare la cibersicurezza in un argomento di vendita.

[14] Il Forum europeo degli Stati membri è stato lanciato con la comunicazione COM(2009) 149 come piattaforma per promuovere la discussione tra le autorità pubbliche degli Stati membri in materia di buone pratiche sulla sicurezza e sulla resilienza delle infrastrutture critiche informatizzate.

I suddetti soggetti sarebbero tenuti a segnalare alle autorità nazionali competenti in materia di SRI gli incidenti aventi un impatto significativo sulla continuità di servizi essenziali e della fornitura di beni che dipendono dalle reti e dai sistemi informativi.

Le autorità nazionali competenti in materia di SRI dovrebbero collaborare e scambiare informazioni con altri organismi di regolamentazione, in particolare con le autorità garanti della protezione dei dati personali. Le autorità nazionali competenti in materia di SRI dovrebbero, a loro volta, notificare alle autorità di contrasto gli incidenti di cui sospettano la natura dolosa grave. Le autorità nazionali competenti dovrebbero anche pubblicare regolarmente su un apposito sito web informazioni non riservate in merito a preallarmi in corso relativi a rischi o incidenti e alle risposte coordinate adottate. Gli obblighi legali non dovrebbero però sostituire, né impedire, la collaborazione volontaria e informale, anche tra settori pubblico e privato, destinata a rafforzare i livelli di sicurezza e gli scambi di informazioni e buone pratiche. In particolare, il partenariato europeo pubblico-privato per la resilienza (EP3R[15]) costituisce una valida piattaforma a livello dell'UE che dovrebbe essere ulteriormente sviluppata.

Il meccanismo per collegare l'Europa (CEF)[16] fornirebbe il sostegno finanziario a infrastrutture di base che collegano le capacità in materia di SRI degli Stati membri rendendo più agevole la cooperazione in tutta l'Unione.

Infine, per poter simulare la collaborazione tra Stati membri e settore privato è fondamentale organizzare a livello dell'Unione esercitazioni sui ciberincidenti. La prima esercitazione che ha visto la partecipazione degli Stati membri è stata realizzata nel 2010 (Cyber Europe 2010), mentre una seconda esercitazione, a cui ha partecipato anche il settore privato, si è svolta nell'ottobre 2012 (Cyber Europe 2012). Nel novembre 2011 si è svolto un esercizio di simulazione UE-USA (Cyber Atlantic 2011). Nei prossimi anni sono programmate altre esercitazioni anche con partner internazionali.

La Commissione intende:

- portare avanti le attività, eseguite dal proprio Centro comune di ricerca in stretto coordinamento con le autorità degli Stati membri e i proprietari/operatori di infrastrutture critiche, di individuazione delle vulnerabilità, sul piano della sicurezza delle reti e dell'informazione, delle infrastrutture critiche europee e di stimolo all'elaborazione di sistemi resilienti;
- lanciare all'inizio del 2013 un progetto pilota finanziato dall'UE[17] per la lotta contro le cd. **botnet (reti di bot) e i software maligni (malware),** destinato fornire un quadro di coordinamento e collaborazione tra gli Stati membri dell'UE, organismi del settore privato, come i fornitori di servizi internet, e partner

[15] Il partenariato europeo pubblico-privato per la resilienza è stato lanciato con la comunicazione COM(2009) 149. La piattaforma ha avviato i lavori e rafforzato la collaborazione tra i settori pubblico e privato in merito all'individuazione degli aspetti, delle risorse, delle funzioni e degli obblighi di base in materia di resilienza e in merito alle esigenze e ai meccanismi di collaborazione necessari per rispondere a perturbazioni su ampia scala a carico delle comunicazioni elettroniche.

[16] https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. Linea di bilancio CEF 09.03.02 – Reti di telecomunicazioni (promuovere l'interconnessione e l'interoperabilità dei servizi pubblici nazionali online nonché l'accesso a tali reti).

[17] CIP-ICT PSP-2012-6, 325188, dotato di un bilancio globale di 15 Mio EUR, di cui il finanziamento UE ammonta a 7,7 Mio EUR.

internazionali.

La Commissione chiede all'ENISA di:

- assistere gli Stati membri nello sviluppo di **capacità nazionali di ciberresilienza** forti, in particolare creando competenze in materia di sicurezza e resilienza dei sistemi industriali di controllo e delle infrastrutture dei trasporti e dell'energia;
- esaminare nel 2013 la fattibilità della creazione di gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) per i sistemi industriali di controllo nell'UE;
- continuare a dare supporto agli Stati membri e alle istituzioni dell'UE nella realizzazione periodica di **esercitazioni paneuropee sui ciberincidenti,** che costituiranno anche la base operativa per la partecipazione dell'UE a esercitazioni internazionali sugli incidenti informatici.

La Commissione invita il Parlamento europeo e il Consiglio a:

- **adottare** rapidamente la proposta di direttiva relativa a un **livello comune elevato di sicurezza delle reti e dell'informazione (SRI)** nell'Unione, che affronta i temi delle capacità e della preparazione a livello nazionale, della collaborazione a livello dell'UE, dell'adozione di prassi di gestione del rischio e scambio di informazioni in materia di sicurezza delle reti e dell'informazione.

La Commissione chiede all'industria:

- di porsi alla guida degli **investimenti** per raggiungere un elevato livello di cibersicurezza e sviluppare buone pratiche e scambi di informazioni all'interno del settore e con le autorità pubbliche, allo scopo di garantire una protezione forte ed efficace di beni e individui, in particolare nell'ambito di partenariati pubblico-privati come EP3R e Trust in Digital Life (TDL)[18].

Sensibilizzazione

Garantire la cibersicurezza è una responsabilità comune. Gli utenti finali hanno un ruolo fondamentale per la garanzia della sicurezza delle reti e dei sistemi informativi: perciò devono essere sensibilizzati ai rischi che corrono online ed essere responsabilizzati perché prendano semplici misure necessarie per premunirsi contro tali rischi.

In anni recenti sono state elaborate varie iniziative che devono essere portate avanti. In particolare, l'ENISA è stata impegnata in un'opera di sensibilizzazione attraverso la pubblicazione di relazioni, l'organizzazione di seminari con esperti e lo sviluppo di partenariati pubblico-privati. Anche Europol, Eurojust e le autorità nazionali responsabili della protezione dei dati sono attivi nell'opera di sensibilizzazione. Nell'ottobre 2012 l'ENISA ha condotto, insieme ad alcuni Stati membri, il "Mese della cibersicurezza europea". La sensibilizzazione è uno dei settori che sta portando avanti il gruppo di lavoro UE-USA sulla

[18] http://www.trustindigitallife.eu/

cibersicurezza e il cibercrimine[19] ed è un aspetto essenziale nell'ambito del programma Safer Internet[20] (che si incentra sulla sicurezza dei bambini in linea).

La Commissione chiede all'ENISA di:

- proporre nel 2013 una tabella di marcia per la creazione di una "patente di sicurezza delle reti e dell'informazione" come programma di certificazione volontaria, destinato a promuovere il rafforzamento delle competenze e delle qualifiche dei professionisti informatici (ad es. amministratori di siti web).

La Commissione intende:

- organizzare nel 2014, con il sostegno dell'ENISA, un **campionato** di cibersicurezza per studenti universitari che concorreranno con la presentazione di soluzioni per la sicurezza delle reti e dell'informazione.

La Commissione invita gli Stati membri[21] a:

- organizzare ogni anno, a partire dal 2013, un **mese della cibersicurezza,** con il sostegno dell'ENISA e il coinvolgimento del settore privato, per sensibilizzare gli utenti finali. A partire dal 2014 sarà organizzato un mese della cibersicurezza concomitante nell'UE e negli USA;
- rafforzare l'**impegno nazionale in materia di istruzione e formazione sulla sicurezza delle reti e dell'informazione** attraverso l'introduzione di: formazioni sulla SRI nelle scuole entro il 2014; formazioni sulla SRI, sullo sviluppo di software sicuri e sulla protezione dei dati personali per gli studenti di informatica; una formazione di base in materia di SRI per il personale delle pubbliche amministrazioni.

La Commissione invita l'industria a:

- promuovere la **sensibilizzazione alla cibersicurezza a tutti i livelli**, sia nella prassi interna che nei rapporti con la clientela. In particolare è necessario che il settore rifletta a come conferire maggiori doveri di rendicontazione sulla cibersicurezza agli amministratori delegati e ai consigli di amministrazione.

2.2. Ridurre drasticamente il cibercrimine

Più viviamo nel mondo digitale, più aumentano le occasioni da sfruttare per i ciberdelinquenti. Il cibercrimine, che miete ogni giorno più di un milione di vittime nel mondo, rappresenta una delle forme di delinquenza che si diffonde più rapidamente. I ciberdelinquenti e le reti del cibercrimine diventano sempre più sofisticati: per questo

[19] Questo gruppo di lavoro, costituito in occasione del vertice UE-USA del novembre 2010 (MEMO/10/597), ha il compito di sviluppare approcci collaborativi in tutta una serie di problematiche relative alla cibersicurezza e al cibercrimine.

[20] Il programma Safer Internet finanzia una rete di ONG attive nel campo del benessere dei bambini online, una rete di autorità di contrasto che si scambiano informazioni e buone pratiche relative allo sfruttamento criminale di internet per la diffusione di materiale sugli abusi sessuali di cui sono vittima i bambini e una rete di ricercatori che raccoglie informazioni sugli usi, i rischi e le conseguenze delle tecnologie online per la vita dei bambini.

[21] Anche con la partecipazione delle autorità nazionali competenti, tra cui le autorità competenti in materia di SRI e di protezione dei dati.

dobbiamo avere gli strumenti operativi giusti e le capacità necessarie per fronteggiarli. I reati informatici presentano profitti elevati e scarsi rischi e spesso i delinquenti sfruttano l'anonimato dei domini dei siti web. Il cibercrimine non conosce confini; l'estensione planetaria di internet implica che l'attività di contrasto deve essere coordinata e sostenuta dalla collaborazione transnazionale per rispondere a questa crescente minaccia.

Una legislazione solida ed efficace

L'Unione europea e gli Stati membri hanno bisogno di una legislazione solida ed efficace per affrontare il cibercrimine. La convenzione del Consiglio d'Europa sulla criminalità informatica, nota come convenzione di Budapest, è un trattato internazionale vincolante che rappresenta un quadro efficace per l'adozione delle legislazioni nazionali.

L'Unione europea ha già adottato disposizioni legislative in materia di cibercriminalità, tra cui una direttiva relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile[22]. L'UE sta inoltre per adottare una direttiva sugli attacchi contro i sistemi informativi in particolare mediante l'uso delle cd. *botnet*.

La Commissione intende:

- garantire il pronto recepimento e la rapida attuazione delle direttive relative al cibercrimine;
- premere sugli Stati membri che non hanno ancora ratificato la **convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica** perché la ratifichino e ne attuino le disposizioni quanto prima.

Rafforzamento delle capacità operative di lotta alla cibercriminalità

Le tecniche del cibercrimine evolvono con una rapidità impressionante: ne consegue che le autorità di contrasto non possono combattere il cibercrimine con strumenti operativi datati. Oggi non tutti gli Stati membri dell'UE dispongono delle capacità operative necessarie per rispondere efficacemente al cibercrimine. Tutti gli Stati membri devono dotarsi di unità nazionali efficaci contro la cibercriminalità.

[22] Direttiva 2011/93/UE che ha sostituito la decisione quadro 2004/68/GAI.

La Commissione intende:

- attraverso i propri programmi di finanziamento[23] aiutare gli Stati membri **a individuare le lacune e a rafforzare le capacità** di indagine e lotta alla cibercriminalità. La Commissione sosterrà inoltre gli organismi che fanno da ponte tra gli istituti di ricerca/università, le autorità di contrasto e il settore privato, analogamente al lavoro svolto attualmente dai centri di eccellenza contro la criminalità informatica finanziati dalla Commissione e già costituiti in alcuni Stati membri;
- coordinare, insieme gli Stati membri, gli sforzi di individuazione delle buone pratiche e delle migliori tecniche disponibili, anche con il supporto del CCR, per lottare contro la cibercriminalità (ad es. lo sviluppo e l'uso di strumenti di polizia scientifica e l'analisi delle minacce);
- collaborare strettamente con il **Centro europeo per la lotta alla criminalità informatica (EC3)** di recente creazione, **con Europol e con Eurojust** per armonizzare gli approcci strategici con le migliori pratiche sul fronte operativo.

Migliore coordinamento a livello UE

A complemento del lavoro degli Stati membri l'UE può facilitare un'impostazione coordinata e collaborativa, riunendo le autorità di contrasto e le autorità giudiziarie oltre che i soggetti interessati, pubblici e privati, dell'Unione e di altri paesi.

La Commissione intende:

- sostenere l'attività del **Centro europeo per la lotta alla criminalità informatica (EC3)** di recente creazione in quanto punto focale europeo di lotta contro la cibercriminalità. Il centro EC3 svolgerà un lavoro di analisi e di intelligence, assisterà le indagini, offrirà tecniche forensi di alto livello, agevolerà la collaborazione, creerà canali di scambio di informazioni tra le autorità competenti degli Stati membri, il settore privato e gli altri soggetti interessati e diventerà gradualmente il portavoce della comunità delle autorità di contrasto[24];
- sostenere le iniziative volte ad assegnare un più ampio dovere di rendicontazione alle autorità di registrazione dei nomi di dominio e garantire l'accuratezza delle informazioni sulla proprietà del sito web, in particolare sulla base delle raccomandazioni in materia di controllo dell'attuazione delle leggi destinate alla *Internet Corporation for Assigned Names and Numbers* (ICANN), in conformità al diritto dell'Unione, comprese le norme sulla protezione dei dati;
- in base alla legislazione recente, continuare a rafforzare l'attività dell'Unione per contrastare gli abusi sessuali perpetrati sui bambini online. La Commissione ha adottato una Strategia europea per un'internet migliore per i ragazzi[25] e insieme a

[23] Per il 2013, nell'ambito del programma di prevenzione e lotta contro la criminalità (ISEC). Dopo il 2013, nell'ambito del Fondo Sicurezza interna (nuovo strumento del quadro finanziario pluriennale).

[24] Il 28 marzo 2012 la Commissione europea ha adottato una comunicazione "Lotta alla criminalità nell'era digitale: istituzione di un Centro europeo per la lotta alla criminalità informatica".

[25] COM(2012) 196 definitivo.

paesi dell'UE e non UE ha lanciato una **Alleanza mondiale contro l'abuso sessuale di minori online**[26]. L'Alleanza è un mezzo a disposizione degli Stati membri per attivare nuovi interventi col sostegno della Commissione e del Centro europeo per la lotta alla criminalità informatica (EC3).

La Commissione chiede a Europol (EC3):

- in un primo tempo, di concentrare il sostegno operativo e in termini di analisi a favore delle indagini degli Stati membri sulla criminalità informatica, per concorrere a smantellare e distruggere le reti criminali in primo luogo nei settori degli abusi sessuali sui bambini, delle frodi nei pagamenti online, delle reti botnet e dell'intrusione;
- di produrre relazioni periodiche, strategiche e operative, sulle tendenze e sulle minacce emergenti, per individuare le priorità e mirare l'azione investigativa delle squadre contro la cibercriminalità negli Stati membri.

La Commissione chiede all'Accademia europea di polizia (CEPOL), in collaborazione con Europol:

- di coordinare la concezione e la pianificazione di corsi di formazione destinati a dotare le autorità di contrasto delle conoscenze e della perizia necessarie per lottare efficacemente contro il cibercrimine.

La Commissione chiede a Eurojust:

- di individuare i principali ostacoli alla cooperazione giudiziaria sulle indagini in materia di cibercriminalità e al coordinamento tra gli Stati membri e con i paesi terzi e di sostenere le indagini e il perseguimento del cibercrimine a livello operativo e strategico, nonché di eseguire attività di formazione in questo campo.

La Commissione chiede a Eurojust e Europol (EC3):

- di collaborare strettamente, tra l'altro mediante scambi di informazioni, per rendere più efficace la lotta al cibercrimine, in conformità ai rispettivi mandati e alle rispettive competenze.

2.3. Sviluppare una politica e capacità di ciberdifesa connesse al quadro della Politica di sicurezza e di difesa comune (PSDC)

Le attività a favore della cibersicurezza nell'Unione europea coinvolgono anche la dimensione della ciberdifesa. Per aumentare la resilienza dei sistemi informativi e di comunicazione che supportano gli interessi della difesa e della sicurezza nazionale degli Stati membri, lo sviluppo di capacità di ciberdifesa dovrebbe concentrarsi sulle attività di individuazione, risposta e recupero nei confronti di ciberminacce sofisticate.

Le varie sfaccettature delle minacce richiedono un rafforzamento delle sinergie tra approcci civili e militari alla protezione di ciberstrutture critiche. Questi interventi dovrebbero essere sostenuti da attività di ricerca e sviluppo e da una collaborazione più stretta tra governi,

[26] Conclusioni del Consiglio su un'Alleanza mondiale contro l'abuso sessuale dei minori online (dichiarazione comune UE-USA) del 7 e 8 giugno 2012 e dichiarazione sull'istituzione di un'Alleanza mondiale contro l'abuso sessuale di minori online (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm)

settore privato e settore accademico nell'UE. Per evitare duplicazioni, l'UE esplorerà come l'UE e la NATO possano unire e rendere complementari le rispettive attività destinate a migliorare la resilienza di infrastrutture critiche statali, di difesa e di informazione dalle quali sono dipendenti i membri di entrambe le organizzazioni.

L'Alto rappresentante si focalizzerà sulle seguenti attività cruciali e invita gli Stati membri e l'Agenzia europea per la difesa a collaborare per:

- valutare i requisiti operativi in materia di ciberdifiesa dell'UE e promuovere lo sviluppo di capacità di ciberdifesa e di tecnologie relative tutti gli aspetti dello sviluppo delle capacità, in particolare la dottrina, la leadership, l'organizzazione, il personale, la formazione, la tecnologia, l'infrastruttura, la logistica e l'interoperabilità;

- elaborare un quadro politico della ciberdifesa dell'UE per proteggere le reti nell'ambito di operazioni e missioni PSDC, comprendente la gestione dinamica del rischio, una migliore analisi delle minacce e un migliore scambio di informazioni; migliorare le occasioni di formazione e di esercitazione dei militari nell'ambito della ciberdifesa nei contesti europeo e multinazionale, inserendo l'integrazione degli aspetti della ciberdifesa negli attuali programmi di esercitazione;

- promuovere il dialogo e il coordinamento tra gli attori civili e militari nell'UE, con particolare riferimento allo scambio di buone pratiche e di informazioni, ai preallarmi, alla risposta agli incidenti, all'analisi del rischio, alla sensibilizzazione e alla prioritarizzazione della cibersicurezza;

- curare il dialogo con i partner internazionali, in particolare la NATO, con altre organizzazioni internazionali e centri di eccellenza multinazionali, per garantire capacità efficaci di difesa, individuare settori di cooperazione ed evitare duplicazioni degli sforzi.

2.4. Sviluppare le risorse industriali e tecnologiche per la cibersicurezza

In Europa esistono capacità eccellenti di ricerca e sviluppo, ma molti dei leader mondiali che offrono prodotti e servizi TIC innovativi sono stabiliti fuori dell'UE. Si corre il rischio che l'Europa diventi non solo eccessivamente dipendente da TIC prodotte altrove, ma anche da soluzioni di sicurezza sviluppate fuori dai suoi confini. È fondamentale garantire che i componenti hardware e software prodotti nell'UE e nei paesi terzi, che sono usati da servizi e infrastrutture critiche e sempre di più dai dispositivi mobili, siano affidabili, sicuri e garantiscano la protezione dei dati personali.

Promuovere un mercato unico dei prodotti della cibersicurezza

Si può raggiungere un livello elevato di sicurezza solo se tutti, nella catena del valore (produttori di attrezzature, sviluppatori di software, fornitori di servizi della società dell'informazione) fanno della sicurezza una priorità. A quanto pare[27], tuttavia, molti attori continuano a guardare alla sicurezza solo come a una formalità supplementare e la domanda di soluzioni di sicurezza è limitata. Sono necessari adeguati requisiti di efficacia della cibersicurezza, che devono essere rispettati lungo tutta la catena del valore dei prodotti TIC utilizzati in Europa. Perché il settore privato garantisca un livello elevato di cibersicurezza sono necessari incentivi, come ad es. etichette che indicano prestazioni adeguate di

[27] V. il documento di lavoro dei servizi della Commissione relativo alla valutazione d'impatto che accompagna la proposta di direttiva sulla sicurezza delle reti e dell'informazione, sezione 4.1.5.2.

cibersicurezza, che permetterebbero alle imprese con buone prestazioni di cibersicurezza e con una buona esperienza di sfruttare queste credenziali a fini di vendita e trarne un vantaggio competitivo. Anche gli obblighi previsti dalla proposta direttiva in materia di sicurezza delle reti e dell'informazione contribuirebbero notevolmente a incrementare la competitività delle imprese nei settori considerati.

Occorrerebbe anche incentivare una domanda a livello europeo di prodotti altamente sicuri. Innanzitutto, la presente strategia mira a rafforzare la collaborazione e la trasparenza sulla sicurezza dei prodotti TIC. Essa esorta a creare una piattaforma che riunisca i soggetti europei interessati, pubblici e privati, per individuare le buone pratiche in materia di cibersicurezza lungo tutta la catena del valore e creare condizioni di mercato favorevoli allo sviluppo e all'adozione di soluzioni TIC sicure. Un primo obiettivo importante dovrebbero essere la creazione di incentivi per un'appropriata gestione del rischio e l'adozione di soluzioni e norme di sicurezza; inoltre si dovrebbero possibilmente elaborare regimi volontari di certificazione a livello dell'UE basandosi sui regimi esistenti nell'Unione e a livello internazionale. La Commissione incoraggerà l'adozione di approcci coerenti tra gli Stati membri per evitare disparità che potrebbero ledere le imprese a causa del loro luogo di stabilimento.

In secondo luogo, la Commissione appoggerà l'elaborazione di norme di sicurezza e contribuirà alla creazione di regimi di certificazione volontaria a livello dell'UE nel settore dell'informatica nella nuvola, tenendo debitamente in considerazione la necessità di garantire la protezione dei dati. Ci si dovrà concentrare sulla sicurezza della catena di approvvigionamento, in particolare in settori economici critici (sistema industriale di controllo, infrastruttura dell'energia e dei trasporti). Quest'opera dovrà poggiare sul lavoro di standardizzazione in corso di realizzazione da parte degli organismi europei di normazione (CEN, CENELEC e ETSI)[28], del gruppo di coordinamento per la cibersicurezza, nonché sulle competenze dell'ENISA, della Commissione e degli altri attori coinvolti.

La Commissione intende:

- lanciare nel 2013 una **piattaforma pubblico-privata sulle soluzioni materia di sicurezza delle reti e dell'informazione** per elaborare incentivi all'adozione di soluzioni TIC sicure e all'applicazione, ai prodotti TIC utilizzati in Europa, del criterio delle buone prestazioni di cibersicurezza;
- proporre nel 2014 raccomandazioni per garantire la cibersicurezza lungo tutta la catena del valore TIC, mettendo a frutto i lavori della suddetta piattaforma,
- esaminare in che modo i principali fornitori di hardware e software TIC potrebbero informare le autorità nazionali competenti sulle vulnerabilità individuate che potrebbero avere significative implicazioni di sicurezza.

La Commissione chiede all'ENISA di:

- elaborare, in collaborazione con le autorità nazionali competenti, le parti interessate, gli organismi internazionali ed europei di normazione e il Centro comune di ricerca della Commissione europea, **orientamenti tecnici e raccomandazioni per l'adozione di norme e buone pratiche in materia di SRI** nei settori pubblico e privato.

[28] In particolare nell'ambito della norma M/490 per le reti intelligenti per la prima serie di norme relative ad una rete intelligente e un'architettura di riferimento.

La Commissione invita le parti interessate pubbliche e private a:

- incoraggiare l'elaborazione e l'adozione di **norme di sicurezza** promosse dall'industria, di norme tecniche e di principi che garantiscono la sicurezza e la protezione della vita privata fin dalla progettazione, da parte dei fabbricanti di prodotti e dei fornitori di servizi TIC, inclusi i fornitori di servizi nella nuvola; le nuove generazioni di software e hardware dovrebbero essere dotate di **dispositivi di sicurezza più efficaci, incorporati e facili da usare**;
- elaborare norme promosse dall'industria sulla prestazione delle imprese in materia di cibersicurezza e migliorare le informazioni disponibili per il pubblico, mettendo a punto **etichette di sicurezza** o marchi per aiutare gli utenti a esplorare il mercato.

Rafforzare gli investimenti in R&S e l'innovazione

La R&S può essere il supporto di una politica industriale forte, promuovere un settore europeo delle TIC affidabile, dare impulso al mercato interno e ridurre la dipendenza europea dalle tecnologie straniere. La R&S dovrebbe ovviare alle lacune tecnologiche della sicurezza delle TIC, prepararci ad affrontare le sfide di sicurezza di nuova generazione, tenendo conto della costante evoluzione delle esigenze degli utenti, e sfruttare i vantaggi delle tecnologie a doppio uso. Dovrebbe anche continuare a supportare lo sviluppo della crittografia. A ciò devono aggiungersi iniziative per tradurre i risultati della R&S in soluzioni commerciali, grazie ai necessari incentivi e alla creazione delle condizioni politiche favorevoli.

L'UE dovrebbe sfruttare al meglio lo strumento Orizzonte 2020[29] del programma quadro per la ricerca e l'innovazione tecnologica che sarà lanciato nel 2014. La proposta della Commissione contiene obiettivi specifici per l'affidabilità delle TIC e la lotta al cibercrimine, che sono in linea con la presente strategia. Orizzonte 2020 darà sostegno alla ricerca sulla sicurezza connessa alle tecnologie TIC emergenti, offrirà soluzioni relative ai sistemi, servizi e applicazioni TIC sicuri su tutta la linea, fornirà incentivi per l'attuazione e l'adozione delle soluzioni esistenti e affronterà l'interoperabilità tra le reti e i sistemi informativi. A livello dell'UE si provvederà in particolare ad ottimizzare e coordinare meglio i vari programmi di finanziamento (Orizzonte 2020, Fondo Sicurezza interna, ricerca della Agenzia europea per la difesa, compreso il quadro europeo di cooperazione).

La Commissione intende:

- usare Orizzonte 2020 per affrontare una serie di aspetti di sicurezza e tutela della vita privata nelle TIC, dalla R&S all'innovazione e alla divulgazione dei suoi risultati. Orizzonte 2020 svilupperà anche strumenti per combattere le attività criminali e terroristiche che prendono di mira l'ambiente cibernetico;
- creare meccanismi per migliorare il coordinamento delle agende di ricerca delle istituzioni dell'Unione europea e degli Stati membri e incentivi perché gli Stati

[29] Orizzonte 2020 è lo strumento finanziario che attua l'iniziativa faro della strategia Europa 2020 dal titolo "L'Unione dell'innovazione", volta a garantire la competitività dell'UE a livello mondiale. Il nuovo programma quadro per la ricerca e l'innovazione tecnologica, che andrà dal 2014 al 2020, rientra nell'impegno comune di creare nuovi posti di lavoro e crescita in Europa.

membri investano di più in R&S.

La Commissione invita gli Stati membri a:

- elaborare, entro la fine del 2013, buone pratiche per sfruttare il **potere di acquisto delle pubbliche amministrazioni** (ad es. tramite appalti pubblici) per stimolare lo sviluppo e la diffusione di funzioni di sicurezza nei prodotti e servizi TIC;
- incoraggiare il coinvolgimento precoce dell'industria e dell'università nello sviluppo e nel coordinamento delle soluzioni, sfruttando al meglio la base industriale europea e le connesse innovazioni tecnologiche della R&S e coordinando le agende di ricerca delle istituzioni civili e militari.

La Commissione chiede a Europol e all'ENISA di:

- individuare le tendenze in atto e le esigenze connesse all'evoluzione della cibercriminalità e dei modelli di cibersicurezza per elaborare adeguati strumenti e tecnologie digitali per le tecniche forensi.

La Commissione invita le parti interessate pubbliche e private a:

- elaborare, in collaborazione con il settore delle assicurazioni, **metriche armonizzate di calcolo dei premi di rischio** che permetterebbero alle imprese che hanno investito nella sicurezza di beneficiare di premi di rischio inferiori.

2.5. Creare una politica internazionale coerente dell'Unione europea sul ciberspazio e promuovere i valori costitutivi dell'UE

Preservare l'apertura, la libertà e la sicurezza del ciberspazio è una sfida mondiale che l'UE deve cogliere insieme ai partner e alle organizzazioni internazionali interessati, al settore privato e alla società civile.

Nella propria politica internazionale sul ciberspazio l'UE dovrà proporsi di promuovere l'apertura e la libertà di internet, di incoraggiare le iniziative per l'elaborazione di regole di condotta e di applicare nel ciberspazio le leggi internazionali vigenti. L'UE si adopererà anche per colmare il divario digitale e parteciperà attivamente alle iniziative internazionali di creazione di capacità in materia di cibersicurezza. L'impegno internazionale dell'UE in questo settore sarà ispirato ai suoi valori costitutivi, come la dignità umana, la libertà, la democrazia, l'uguaglianza, lo Stato di diritto e il rispetto dei diritti fondamentali.

Integrazione delle problematiche del ciberspazio nelle relazioni esterne dell'UE e nella politica estera e di sicurezza comune

La Commissione, l'Alto rappresentante e gli Stati membri sono chiamati ad elaborare una politica internazionale dell'UE in materia di ciberspazio coerente e mirante ad aumentare l'impegno e a intensificare le relazioni con i principali partner e le principali organizzazioni internazionali, come pure con il settore privato e la società civile. Le consultazioni dell'UE con i partner internazionali sugli aspetti della cibersicurezza e della cibercriminalità dovrebbero essere organizzate, coordinate ed attuate in modo da creare un valore aggiunto rispetto ai dialoghi bilaterali che si svolgono attualmente tra gli Stati membri dell'UE e i paesi terzi. L'UE porrà un nuovo accento sul dialogo con i paesi terzi, in particolare con i partner che si trovano su posizioni affini e condividono i valori dell'UE. L'Unione promuoverà il raggiungimento di un livello elevato di protezione dei dati, in particolare in caso di trasferimento di dati personali a un paese terzo. Per affrontare le sfide mondiali nel

ciberspazio l'UE chiederà una collaborazione più stretta da parte delle organizzazioni attive in questo settore come il Consiglio d'Europa, l'OCSE, le Nazioni Unite, l'OSCE, la NATO, l'UA, l'ASEAN e l'OSA. A livello bilaterale è particolarmente importante la cooperazione con gli Stati Uniti, che sarà ulteriormente sviluppata in particolare nel contesto del gruppo di lavoro UE-USA sulla cibersicurezza e il cibercrimine.

Uno degli elementi basilari della politica internazionale dell'UE in questo campo sarà la promozione del ciberspazio come uno spazio di libertà e di diritti fondamentali. L'espansione dell'accesso a internet deve far progredire le riforme democratiche e promuoverne la diffusione in tutto il mondo. Una maggiore connettività a livello mondiale dovrà essere esente da censura o da una sorveglianza di massa. L'Unione dovrà promuovere la responsabilità sociale delle imprese[30] e avviare iniziative internazionali per migliorare il coordinamento mondiale in questo campo.

La responsabilità di un ciberspazio più sicuro incombe a tutti i protagonisti della società globale dell'informazione, dai singoli cittadini agli Stati. L'UE sostiene il tentativo di definire regole di condotta nel ciberspazio che dovrebbero essere rispettate da tutte le parti interessate. Proprio come l'UE si aspetta che i cittadini rispettino i doveri civici, le responsabilità sociali e le leggi quando sono online, così anche gli Stati devono rispettare le norme e le leggi vigenti. Per quanto riguarda la sicurezza internazionale, l'UE incoraggia l'elaborazione di misure di rafforzamento della fiducia nella cibersicurezza, destinate ad aumentare la trasparenza e a ridurre il rischio che il comportamento degli Stati sia frainteso.

L'Unione non chiede la creazione di un nuovo strumento giuridico internazionale riguardante le questioni della cibersicurezza.

Gli obblighi giuridici contenuti nel Patto internazionale relativo ai diritti civili e politici, nella Convenzione europea dei diritti dell'uomo e nella Carta dei diritti fondamentali dell'Unione europea devono essere rispettati anche online. L'UE si adopererà per far sì che queste disposizioni siano rispettate anche nel ciberspazio.

Per contrastare la cibercriminalità, la convenzione di Budapest è uno strumento aperto alla ratifica da parte dei paesi terzi, che offre un modello per l'elaborazione della legislazione nazionale in materia di cibercriminalità e costituisce una base di cooperazione internazionale in questo campo.

In caso di conflitti armati che si estendano al ciberspazio, si applicherà il diritto dei conflitti armati e, per quanto di ragione, il diritto internazionale umanitario.

Sviluppo di capacità per la cibersicurezza e di infrastrutture di informazione resilienti nei paesi terzi

L'armonioso funzionamento delle infrastrutture soggiacenti che offrono e facilitano i servizi di comunicazione beneficerà dei vantaggi di una maggiore cooperazione internazionale, che può assumere la forma di scambi di buone pratiche e di informazioni, di preallarmi, di esercitazioni comuni di gestione degli incidenti ecc.. Per contribuire al raggiungimento di questo obiettivo l'UE intensificherà le attività internazionali in corso per rafforzare le reti di collaborazione per la protezione delle infrastrutture critiche informatizzate, alle quali partecipano le autorità pubbliche e il settore privato.

[30] "Strategia rinnovata dell'UE per il periodo 2011-14 in materia di responsabilità sociale delle imprese", COM(2011) 681 definitivo.

Non tutti i paesi del mondo beneficiano degli effetti positivi di internet per mancanza di un accesso aperto, sicuro, interoperabile e affidabile. Per questo l'Unione europea continuerà ad appoggiare gli sforzi dei paesi che cercano di dare ai loro cittadini maggiori possibilità di accesso e di uso di internet, di assicurarne l'integrità e la sicurezza e di combattere efficacemente il cibercrimine.

In collaborazione con gli Stati membri, la Commissione e l'Alto rappresentante intendono:

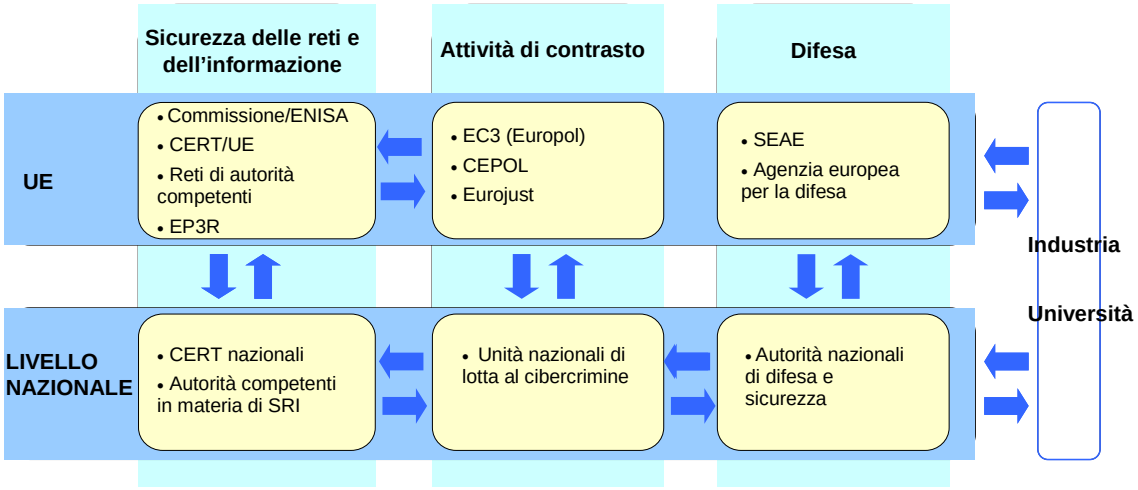
- adoperarsi per elaborare una politica internazionale dell'UE coerente in materia di ciberspazio per aumentare l'impegno con i principali partner e le principali organizzazioni internazionali, per inserire le materie connesse alla cibersicurezza nella PESC e per migliorare il coordinamento di aspetti di portata globale;
- appoggiare l'elaborazione di regole di condotta e di misure di creazione di capacità nel settore della cibersicurezza; facilitare il dialogo sulle modalità di applicazione delle leggi internazionali vigenti nel ciberspazio e promuovere la convenzione di Budapest per combattere la cibercriminalità;
- sostenere la promozione e la protezione dei diritti fondamentali, incluso l'accesso all'informazione e la libertà di espressione, in particolare: a) elaborando nuove linee guida pubbliche sulla libertà d'espressione online e offline; b) monitorando l'esportazione di prodotti o servizi che potrebbero essere usati per la censura o la sorveglianza di massa online; c) elaborando misure e strumenti per espandere l'accesso, l'apertura e la resilienza di internet, per contrastare la censura o la sorveglianza di massa attraverso le tecnologie della comunicazione; d) dando ai soggetti interessati il potere di utilizzare la tecnologia delle comunicazioni per promuovere i diritti fondamentali;
- impegnarsi con i partner e le organizzazioni internazionali, il settore privato e la società civile a sostenere i paesi terzi nella creazione di capacità globali per migliorare l'accesso all'informazione e a un'internet aperta, prevenire e contrastare le minacce cibernetiche, compresi gli eventi accidentali, la cibercriminalità e il ciberterrorismo e sviluppare il coordinamento tra i donatori per guidare le iniziative di creazione di capacità;
- utilizzare i diversi strumenti di aiuto dell'UE a favore della creazione di capacità di cibersicurezza, inclusa l'assistenza alla formazione del personale delle autorità di contrasto, delle autorità giudiziarie e del personale tecnico in modo da renderlo in grado di affrontare le ciberminacce; appoggiare la creazione di politiche, strategie e istituzioni nazionali nei paesi terzi;
- aumentare il coordinamento delle politiche e lo scambio di informazioni attraverso le reti internazionali per la protezione delle infrastrutture critiche informatizzate, come la rete *Meridian*, nonché la collaborazione tra le autorità competenti in materia di SRI e altri soggetti.

3. RUOLI E RESPONSABILITÀ

In un'economia e in una società digitale interconnesse i ciberincidenti non conoscono confini. Tutti gli attori, dalle autorità competenti in materia di SRI, alle squadre CERT, alle autorità di contrasto e all'industria, devono assumersi le loro responsabilità a livello sia nazionale che

unionale e collaborare per rafforzare la cibersicurezza. Dato che possono essere implicati diversi ordinamenti giuridici e diverse giurisdizioni, la grossa sfida per l'Unione è chiarire i ruoli e le responsabilità dei numerosi attori partecipanti.

Data la complessità della materia e la varietà dei soggetti coinvolti, una supervisione europea esercitata centralmente non costituisce la risposta giusta. Le amministrazioni nazionali occupano una posizione migliore per organizzare la prevenzione e la risposta ai ciberincidenti e ai ciberattacchi e creare contatti diretti con il settore privato attraverso i loro quadri giuridici e canali precostituiti. Contemporaneamente, però, data la natura transnazionale, potenziale o reale, dei rischi, un'efficace risposta nazionale richiederebbe in molti casi un coinvolgimento a livello dell'UE. Per far fronte alla cibersicurezza in maniera complessiva, le attività dovrebbero articolarsi intorno a tre pilastri fondamentali — la SRI, l'attività di contrasto e la difesa — anch'essi funzionanti all'interno di quadri giuridici diversi:



3.1. Coordinamento tra autorità competenti in materia di SRI, squadre CERT, autorità di contrasto e difesa

Livello nazionale

Gli Stati membri dovrebbero disporre, già oggi o in seguito alla presente strategia, di strutture per garantire la ciberresilienza, far fronte alla cibercriminalità e provvedere alla difesa e dovrebbero raggiungere il livello di capacità necessario per trattare i ciberincidenti. Tuttavia, dato il numero di soggetti che possono avere responsabilità operative nei vari aspetti della cibersicurezza e data l'importanza del coinvolgimento del settore privato, è necessario a livello nazionale ottimizzare il coordinamento tra i vari ministeri. Gli Stati membri dovrebbero stabilire, nella propria strategia nazionale in materia di cibersicurezza, i ruoli e le responsabilità dei vari soggetti nazionali.

Lo scambio di informazioni tra i soggetti nazionali e con il settore privato dovrebbe essere incoraggiato per permettere agli Stati membri e al settore privato di mantenere una visione globale delle varie minacce e comprendere meglio le nuove tendenze e le nuove tecniche utilizzate per commettere ciberattacchi e per potervi reagire più prontamente. Nella definizione di piani di collaborazione nazionali in materia di SRI da attivare in caso di incidente, gli Stati membri dovrebbero essere in grado di assegnare con precisione ruoli e responsabilità e ottimizzare gli interventi di risposta.

Livello dell'UE

Come per il livello nazionale, anche a livello dell'UE la cibersicurezza è una materia di competenza di una serie di attori. In particolare l'ENISA, Europol/EC3 e l'Agenzia europea per la difesa (AED) sono tre agenzie attive rispettivamente nel campo della sicurezza delle reti e dell'informazione, dell'attività di contrasto e della difesa. Queste agenzie hanno consigli di amministrazione in cui gli Stati membri sono rappresentati e offrono piattaforme di coordinamento livello dell'UE.

È necessario incoraggiare il coordinamento e la collaborazione tra l'ENISA, Europol/EC3 e l'Agenzia europea per la difesa (AED) in una serie di settori in cui hanno competenze comuni, in particolare per quanto riguarda l'analisi delle tendenze, la valutazione del rischio, la formazione e lo scambio di buone pratiche. Nel collaborare, tali agenzie conserveranno le proprie specificità. Insieme alla squadra CERT-UE, alla Commissione e agli Stati membri esse dovranno contribuire allo sviluppo di una comunità fidata di esperti tecnici e politici nel settore.

I canali informali di coordinamento e collaborazione saranno completati da legami più strutturati. Il personale militare dell'Unione europea e la squadra di progetto dell'AED per la ciberdifesa possono fungere da vettore di coordinamento della difesa. Il Consiglio di programma di Europol/EC3 riunirà tra gli altri EUROJUST, CEPOL, gli Stati membri[31], l'ENISA e la Commissione, offrendo loro la possibilità di condividere le loro competenze distinte e far sì che gli interventi di EC3 siano eseguiti in partenariato, riconoscendo l'esperienza aggiuntiva degli altri partecipanti e nel rispetto dei mandati di ognuno. Il nuovo mandato dell'ENISA dovrebbe permettere di rafforzare i legami con Europol e con i soggetti interessati dell'industria. E, non da ultimo, la proposta legislativa della Commissione in materia di sicurezza delle reti e dell'informazione (SRI) prevede la creazione di un quadro di cooperazione attraverso una rete di autorità nazionali competenti in materia di SRI e lo scambio di informazioni tra queste ultime autorità e le autorità di contrasto.

Livello internazionale

La Commissione e l'Alto rappresentante assicurano, insieme agli Stati membri, un intervento internazionale coordinato nel campo della cibersicurezza. Nel farlo essi si impegneranno a promuovere i valori costitutivi dell'UE e un uso pacifico, aperto e trasparente delle cibertecnologie. La Commissione, l'Alto rappresentante e gli Stati membri avviano un dialogo politico con i partner internazionali e con organizzazioni internazionali come il Consiglio d'Europa, l'OCSE, l'OSCE, la NATO e l'ONU.

3.2. Sostegno dell'UE in caso di ciberincidente o ciberattacco grave

I ciberincidenti o i ciberattacchi gravi sono suscettibili di avere ripercussioni sugli Stati, sulle imprese e sui cittadini dell'UE. In esito alla presente strategia e in particolare alla proposta direttiva in materia di SRI, ci si aspetta un miglioramento della prevenzione, dell'individuazione e della risposta ai ciberincidenti e un maggiore e più regolare scambio di informazioni tra gli Stati membri e la Commissione in merito a incidenti e ciberattacchi gravi. Tuttavia, i meccanismi di risposta saranno diversi in funzione della natura, della portata e delle ripercussioni transfrontaliere dell'incidente.

[31] Attraverso una rappresentanza nella task force dell'UE sulla cibercriminalità, costituita dai capi delle unità di lotta al cibercrimine degli Stati membri.

Se l'incidente ha un impatto grave sulla continuità operativa, la direttiva in materia di SRI propone di attivare i piani nazionali di collaborazione in materia di SRI o il corrispondente piano unionale, in funzione della portata nazionale o transfrontaliera dell'incidente. In questo contesto, si farebbe ricorso alla rete di autorità competenti in materia di SRI per scambiarsi informazioni e assistenza. Questo permetterebbe di preservare o riparare le reti e i servizi colpiti.

Se l'incidente sembra essere di natura dolosa, Europol/EC3 dovrebbe esserne informato per potere, insieme alle autorità di contrasto dei paesi colpiti, avviare un'indagine, salvaguardare le prove, individuare gli autori e in definitiva assicurarsi che essi siano perseguiti.

Se l'incidente sembra connesso ad attività di ciberspionaggio o un attacco commissionato da uno Stato, oppure se ha implicazioni per la sicurezza nazionale, le autorità nazionali responsabili della sicurezza e della difesa allerteranno i loro omologhi perché sappiano che sono sotto attacco e possano difendersi. In tal caso saranno attivati meccanismi di preallarme e, se necessario, meccanismi di gestione delle crisi o altri procedimenti. Il verificarsi di ciberincidenti o ciberattacchi particolarmente gravi costituirebbe un motivo sufficiente perché uno Stato membro invochi la clausola di solidarietà (articolo 222 del trattato sul funzionamento dell'Unione europea).

Se l'incidente sembra aver compromesso dati personali, occorre coinvolgere le autorità nazionali responsabili della protezione dei dati o l'autorità nazionale di regolamentazione a norma della direttiva 2002/58/CE.

Infine, per il trattamento dei ciberincidenti e dei ciberattacchi saranno preziose le reti di contatto e l'assistenza dei partner internazionali, che possono consistere nella mitigazione tecnica, in indagini penali o nell'attivazione del meccanismo di gestione e risposta alle crisi.

4. CONCLUSIONI E SEGUITO

La presente proposta di strategia per la cibersicurezza dell'Unione europea, presentata dalla Commissione e dall'Alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, delinea la visione dell'UE e gli interventi necessari, basati su una protezione forte e una promozione efficace dei diritti dei cittadini, nell'intento di fare dell'ambiente online dell'Unione l'ambiente in linea più sicuro al mondo[32].

Questa visione può diventare realtà soltanto attraverso un autentico partenariato tra i molti soggetti partecipanti, in cui tutti si assumano le proprie responsabilità e possano affrontare le sfide future.

La Commissione e l'Alto rappresentante invitano pertanto il Consiglio e il Parlamento europeo ad approvare la strategia e a contribuire a realizzare gli interventi ivi descritti. Sono

[32] Il finanziamento della strategia sarà realizzato nei limiti degli importi previsti per ciascuno dei settori di attività (CEF, Orizzonte 2020, Fondo Sicurezza interna, PESC e cooperazione con i paesi terzi, in particolare lo Strumento di stabilità), come indicato nella proposta della Commissione di Quadro finanziario pluriennale 2014-2020 (fatta salva l'approvazione da parte dell'autorità di bilancio e fatti salvi gli importi finali del QFP per il periodo 2014-2020). Per quanto riguarda la necessità di garantire la compatibilità generale col numero di posti disponibili per le agenzie decentrate e i sottomassimali per le agenzie decentrate per ciascun capitolo di spesa nel prossimo QFP, le agenzie (CEPOL, AED, ENISA, EUROJUST e EUROPOL/EC3), alle quali in virtù della presente comunicazione sono affidati nuovi compiti, saranno incoraggiate ad espletarli nella misura in cui sia stata stabilita l'effettiva capacità dell'agenzia di assorbire maggiori risorse e dopo aver esplorato tutte le possibilità di riassegnazione.

necessari anche un forte sostegno e un forte impegno da parte del settore privato e della società civile, che sono i protagonisti principali del rafforzamento del nostro livello di sicurezza e di protezione dei diritti dei cittadini.

È venuto il momento di agire. La Commissione e l'Alto rappresentante sono determinati a lavorare insieme a tutti i soggetti partecipanti per garantire la sicurezza necessaria in Europa. Per la pronta attuazione della presente strategia e la sua valutazione in vista dei possibili sviluppi, tra 12 mesi la Commissione e l'Alto rappresentante riuniranno tutti i soggetti interessati nell'ambito di una conferenza di alto livello in cui procederanno alla valutazione dei progressi compiuti.