Consiglio dell'Unione europea

Bruxelles, 14 settembre 2017
(OR. en)

12211/17

CYBER 132
RELEX 767
JAI 790
ENFOPOL 413
TELECOM 212
MI 633
RECH 308

NOTA DI TRASMISSIONE

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	13 settembre 2017
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	JOIN(2017) 450 final
Oggetto:	COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL CONSIGLIO Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE

Si trasmette in allegato, per le delegazioni, il documento JOIN(2017) 450 final.

All.: JOIN(2017) 450 final

COMMISSIONE
EUROPEA

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

Bruxelles, 13.9.2017
JOIN(2017) 450 final

COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL CONSIGLIO

Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE

1. INTRODUZIONE

La cibersicurezza è essenziale sia per la nostra prosperità che per la nostra sicurezza. Vista la crescente dipendenza della nostra vita quotidiana e delle nostre economie dalle tecnologie digitali, siamo sempre più esposti. Gli incidenti di cibersicurezza si stanno diversificando in termini sia di responsabili sia di obiettivi perseguiti. Le attività informatiche dolose non solo minacciano le nostre economie e l'impegno verso il mercato unico digitale, ma anche il funzionamento stesso delle nostre democrazie, le nostre libertà e i nostri valori. La nostra sicurezza futura dipende dalla trasformazione della capacità di proteggere l'Unione dalle minacce cibernetiche: sia le infrastrutture civili che la capacità militare dipendono da sistemi digitali sicuri. Questo è stato riconosciuto dal Consiglio europeo del giugno 2017[1] e nella strategia globale per la politica estera e di sicurezza dell'Unione europea[2].

I rischi stanno aumentando in maniera esponenziale. Secondo alcuni studi l'impatto economico della cibercriminalità è aumentato di cinque volte tra il 2013 e il 2017 e potrebbe ancora quadruplicarsi entro il 2019[3]. I ransomware[4] hanno registrato un particolare incremento, con attacchi recenti[5] che riflettono il considerevole aumento dell'attività della cibercriminalità, ma non sono l'unica minaccia.

Le ciberminacce provengono da soggetti sia statali che non statali: spesso sono criminali motivati dal profitto, ma possono anche avere motivazioni politiche e strategiche. La minaccia criminale è intensificata dalla labilità del confine tra cibercriminalità e criminalità "tradizionale", in quanto i criminali utilizzano internet sia come modo per far crescere le loro attività sia come fonte per reperire nuovi metodi e strumenti di reato[6]. Eppure, nella stragrande maggioranza dei casi, le possibilità di rintracciare i criminali sono minime e quelle di poter procedere ad azioni penali ancor più esigue.

Allo stesso tempo, sempre più spesso gli attori statali raggiungono i loro obiettivi geopolitici non solo attraverso strumenti tradizionali come la forza militare, ma anche attraverso strumenti cibernetici più discreti, volti anche ad interferire nei processi democratici interni. È ormai ampiamente noto l'utilizzo del ciberspazio come terreno di guerra, da solo o nell'ambito di un approccio ibrido. Le campagne di disinformazione, le notizie false e le operazioni cibernetiche mirate ad infrastrutture critiche sono sempre più comuni e richiedono una risposta. Per questo motivo, nel documento di riflessione sul futuro della difesa europea[7] la Commissione ha sottolineato l'importanza della cooperazione nella ciberdifesa.

Se non miglioreremo sostanzialmente la nostra cibersicurezza, il rischio aumenterà in funzione della trasformazione digitale. Si prevede che nel 2020 decine di milioni di dispositivi dell'"internet delle cose" saranno connessi a Internet, ma la cibersicurezza non costituisce ancora una priorità nella loro progettazione[8]. L'impossibilità di proteggere i dispositivi che controlleranno le nostre reti elettriche, le nostre automobili nonché le reti dei trasporti, le

---

1 http://www.consilium.europa.eu/it/press/press-releases/2017/06/23-euco-conclusions/..

2 http://europa.eu/globalstrategy/.

3 Cfr. per esempio McAfee e Centro di studi strategici internazionali "Net losses: Estimating the Global Cost of Cybercrime" [Perdite nette: stima del costo globale della cibercriminalità], 2014.

4 Il ransomware è un tipo di software maligno che impedisce o limita l'accesso degli utenti al loro sistema, bloccando lo schermo del sistema o bloccando i file dell'utente fino al pagamento di un riscatto.

5 Nel maggio 2017 l'attacco ransomware WannaCry ha colpito più di 400 000 computer in più di 150 paesi. Un mese dopo l'attacco ransomware Petya ha colpito l'Ucraina e molte imprese nel mondo.

6 Europol, Valutazione della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità 2017.

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf.

8 IDC and TXT Solutions (2014), SMART 2013/0037 Cloud and IoT combination, studio per la Commissione europea.

fabbriche, la finanza, gli ospedali e le case potrebbe avere conseguenze devastanti e causare un danno enorme alla fiducia riposta dai consumatori nelle tecnologie emergenti. Il rischio di attacchi di matrice politica verso obiettivi civili, e di lacune nella ciberdifesa militare, aggrava ulteriormente la situazione.

L'approccio presentato nella presente comunicazione congiunta consentirà all'UE di affrontare meglio tali minacce. Rafforzerebbe la resilienza e l'autonomia strategica, promuovendo capacità in termini di tecnologie e competenze e contribuendo a costruire un mercato unico solido. Ciò richiede l'esistenza delle strutture idonee a creare una forte cibersicurezza e reagire quando necessario, con il pieno coinvolgimento di tutti gli attori chiave. L'approccio proposto costituirebbe inoltre un migliore deterrente dei ciberattacchi, intensificando il lavoro volto a rilevare, rintracciare e punire i responsabili. Terrebbe anche conto della dimensione globale sviluppando la cooperazione internazionale come piattaforma per la leadership dell'UE nella cibersicurezza. Tutto questo si fonda sugli approcci del mercato unico digitale, della strategia globale, dell'agenda europea sulla sicurezza[9], del quadro congiunto per contrastare le minacce ibride[10] e della comunicazione sull'istituzione del Fondo europeo per la difesa[11][12].

L'UE è già al lavoro su molte di queste questioni: è giunto il momento di far confluire i vari assi di intervento. Nel 2013 l'Unione ha definito la strategia per la cibersicurezza in cui ha stabilito una serie di assi fondamentali di intervento volti a migliorare la ciberresilienza[13]. I suoi principali obiettivi e principi di promozione di un ecosistema cibernetico affidabile, sicuro e aperto rimangono validi. Il contesto di minacce in continua evoluzione e sempre più profonde richiede però un'azione più incisiva per resistere agli attacchi e fare da deterrente in futuro[14].

L'UE si trova in una buona posizione per affrontare la questione della cibersicurezza, visto l'ambito di applicazione delle sue politiche e gli strumenti, le strutture e le capacità di cui dispone. Sebbene gli Stati membri rimangano responsabili della sicurezza nazionale, la portata e la natura transfrontaliera della minaccia giustificano ampiamente un'azione europea che fornisca incentivi e sostegno agli Stati membri perché sviluppino e mantengano capacità nazionali di cibersicurezza maggiori e migliori, costruendo allo stesso tempo una capacità a livello dell'Unione. Quest'approccio è concepito per spronare tutti gli attori – l'UE, gli Stati membri, le imprese e le persone – a dare alla cibersicurezza la priorità di cui ha bisogno per creare resilienza e dare una migliore risposta europea agli attacchi cibernetici. Indicherà iniziative concrete volte a rilevare e investigare qualsiasi forma di ciberincidente contro l'UE e i suoi Stati membri e rispondervi opportunamente, anche perseguendo i criminali. Permetterà un'azione esterna dell'UE volta a promuovere efficacemente la cibersicurezza sulla scena mondiale. Il risultato per l'Unione sarà una transizione da un approccio reattivo ad uno proattivo in tema di protezione della prosperità, della società e dei valori europei, così

---

9 COM(2015) 185 final.
10 JOIN(2016) 18 final.
11 COM(2017) 295.
12 Tale approccio è giustificato anche dalla consulenza scientifica indipendente fornita dal Gruppo di alto livello di consulenti scientifici del meccanismo di consulenza scientifica della Commissione europea (cfr. riferimenti infra).
13 JOIN(2013) 1 final. Una valutazione di tale strategia è disponibile nel documento SWD(2017) 295.
14 Salvo diversamente indicato, le proposte nella presente comunicazione non incidono sul bilancio. Qualsiasi iniziativa con implicazioni per il bilancio seguirà debitamente le procedure del bilancio annuale e non può pregiudicare il prossimo quadro finanziario pluriennale successivo al 2020.

come dei diritti e delle libertà fondamentali, rispondendo sia alle minacce esistenti che a quelle future.

2. RAFFORZAMENTO DELLA RESILIENZA DELL'UE AI CIBERATTACCHI

Una forte ciberresilienza richiede un approccio collettivo e di vasta portata. Ciò richiede strutture più solide ed efficaci volte a promuovere la cibersicurezza e a rispondere ai ciberattacchi negli Stati membri ma anche nelle istituzioni, nelle agenzie e negli organismi dell'UE. Richiede inoltre un approccio più completo e trasversale per rafforzare la ciberresilienza e l'autonomia strategica, con un solido mercato unico, importanti progressi nella capacità tecnologica nell'Unione e un numero molto più elevato di esperti qualificati. Il fulcro di tale approccio è un'accettazione più ampia del fatto che la cibersicurezza rappresenta una sfida sociale comune, motivo per cui dovrebbero essere coinvolti molteplici livelli dell'amministrazione pubblica, dell'economia e della società.

2.1 Rafforzamento dell'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione

L'**Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione** (ENISA) riveste un ruolo fondamentale nel rafforzamento della ciberresilienza e della risposta dell'Unione, tuttavia è limitata dal suo attuale mandato. La Commissione sta pertanto presentando un'ambiziosa proposta di riforma che include un **mandato permanente per l'agenzia**[15]. In questo modo l'ENISA potrà fornire sostegno agli Stati membri, alle istituzioni dell'Unione e alle imprese in settori chiave, compresa l'attuazione della direttiva sulla sicurezza delle reti e dei sistemi informativi ("direttiva NIS")[16] e del quadro di certificazione della cibersicurezza proposto.

L'ENISA riformata avrà un importante ruolo consultivo nell'elaborazione e nell'attuazione di politiche, anche promuovendo la coerenza tra le iniziative settoriali e la direttiva NIS e contribuendo a istituire centri di condivisione e di analisi delle informazioni in settori critici. L'ENISA aumenterà quantitativamente e qualitativamente la preparazione europea organizzando esercitazioni annuali di cibersicurezza paneuropee che combinino la risposta a diversi livelli. Sosterrà inoltre l'elaborazione della politica dell'UE sulla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione (TIC) e rivestirà un ruolo importante nell'intensificazione sia della cooperazione operativa sia della gestione delle crisi in tutta l'Unione. L'agenzia fungerà inoltre da punto di riferimento per le informazioni e le conoscenze nella comunità della cibersicurezza.

Una comprensione rapida e condivisa delle minacce e degli incidenti appena questi si verificano è un prerequisito per decidere se sia necessaria un'azione comune di mitigazione o risposta da parte dell'UE. Tale scambio di informazioni richiede il coinvolgimento di tutti gli attori interessati (organismi e agenzie dell'UE al pari degli Stati membri) a livello tecnico, operativo e strategico. In collaborazione con gli altri organismi competenti a livello degli Stati membri e dell'UE, in particolare la rete di gruppi di intervento per la sicurezza informatica in caso di incidente[17], CERT-UE, Europol e centro dell'UE di analisi dell'intelligence (INTCEN), l'ENISA contribuirà anche alla conoscenza situazionale a livello dell'Unione. Questo può confluire nell'intelligence e nell'elaborazione delle politiche riguardanti le minacce nel contesto del monitoraggio sistematico del panorama delle minacce e di una

[15] COM(2017) 477.

[16] Direttiva 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[17] Previsti all'articolo 9 della direttiva NIS.

cooperazione operativa efficace, così come nella risposta ad incidenti transfrontalieri su larga scala.

2.2 Verso un mercato unico della cibersicurezza

La crescita del mercato della cibersicurezza nell'Unione europea – in termini di prodotti, servizi e processi – è ostacolata in diversi modi. Un aspetto fondamentale è la mancanza di programmi di certificazione della cibersicurezza riconosciuti in tutta l'Unione che integrino parametri più elevati di resilienza nei prodotti in modo da sostenere la fiducia del mercato a livello dell'UE. La Commissione sta pertanto avanzando la proposta di istituire **un quadro europeo di certificazione della cibersicurezza**[18], il quale definirebbe la procedura per la creazione di programmi di certificazione della cibersicurezza a livello dell'UE a copertura di prodotti, servizi e/o sistemi, che adattino il livello di garanzia all'uso previsto (infrastrutture critiche o dispositivi di consumo)[19]. Tale quadro procurerebbe evidenti vantaggi alle imprese, che non dovrebbero espletare vari processi di certificazione diversi per operare a livello transnazionale, limitando così i costi amministrativi e finanziari. L'uso di programmi sviluppati nell'ambito di tale quadro favorirebbe inoltre la fiducia dei consumatori, con un certificato di conformità volto ad informare e rassicurare gli acquirenti e gli utilizzatori in merito alle proprietà di sicurezza dei prodotti e servizi che acquistano e utilizzano. Questo renderebbe gli elevati parametri di cibersicurezza una fonte di vantaggio competitivo. Il risultato incrementerebbe la resilienza poiché i prodotti e i servizi TIC sarebbero formalmente valutati in base a una serie definita di norme di cibersicurezza sviluppate in stretta correlazione con il più ampio lavoro in corso sulle norme delle TIC[20].

I programmi del suddetto quadro sarebbero volontari e non creerebbero alcun obbligo normativo immediato nei confronti dei fornitori o dei prestatori di servizi. I programmi non sarebbero in contrasto con gli eventuali obblighi di legge applicabili, come la normativa dell'UE sulla protezione dei dati.

Dopo aver istituito il quadro di certificazione la Commissione inviterà le parti interessate a concentrarsi su tre ambiti prioritari:

- sicurezza in applicazioni critiche o a rischio elevato[21]: i sistemi da cui dipendiamo nelle attività quotidiane, dalle automobili ai macchinari nelle fabbriche, dai sistemi più grandi come gli aeroplani e le centrali elettriche ai più piccoli come i dispositivi medici, stanno diventando sempre più digitali e interconnessi. I principali componenti TIC di tali prodotti e sistemi richiederebbero pertanto una rigorosa valutazione della sicurezza;

- cibersicurezza in prodotti digitali, reti, sistemi e servizi ampiamente diffusi utilizzati parimenti dai settori pubblico e privato al fine di difendersi da attacchi e rispettare gli obblighi normativi[22] – come la cifratura della posta elettronica, firewall e reti private

[18] COM(2017) 477.

[19] Un livello di garanzia indica il livello di rigore della valutazione della sicurezza ed è solitamente commisurato al livello di rischio associato a tali settori di applicazione o funzioni (ossia, è richiesto un livello più elevato di garanzia per i prodotti o servizi TIC utilizzati in settori di applicazione o funzioni ad alto rischio).

[20] COM(2016) 176.

[21] Un'eccezione esisterebbe nel caso in cui la certificazione obbligatoria o volontaria fosse disciplinata da altri atti dell'Unione.

[22] Per esempio la direttiva (UE) 2016/1148, il regolamento (UE) 2016/679, la direttiva (UE) 2015/2366 e altre proposte di atti legislativi come il codice europeo delle comunicazioni elettroniche: ciascuno prevede che le organizzazioni adottino misure di sicurezza adeguate per affrontare i corrispondenti rischi per la cibersicurezza.

virtuali; è fondamentale che l'uso diffuso di tali strumenti non comporti nuove fonti di rischio o nuove vulnerabilità;

- impiego di metodi di "sicurezza fin dalla progettazione" nei dispositivi di consumo di massa a basso costo, digitali e interconnessi che costituiscono l'internet delle cose; in questo quadro i programmi potrebbero essere utilizzati per segnalare che i prodotti sono costruiti utilizzando metodi all'avanguardia di sviluppo sicuro, che hanno superato adeguati test di sicurezza e che i fornitori si sono impegnati ad aggiornare il software nel caso in cui vengano scoperte nuove vulnerabilità o minacce.

Tali priorità dovrebbero tenere in particolare considerazione il panorama in evoluzione delle minacce di cibersicurezza, nonché l'importanza di servizi essenziali come i trasporti, l'energia, la sanità, le banche, le infrastrutture dei mercati finanziari, l'acqua potabile o l'infrastruttura digitale[23].

Sebbene non sia possibile garantire che un prodotto, sistema o servizio TIC sia sicuro al "100%", esistono numerosi difetti noti e ampiamente documentati nella progettazione dei prodotti TIC che possono essere sfruttati per eventuali attacchi. Un approccio di "sicurezza fin dalla progettazione" adottato dai produttori di dispositivi connessi, software e attrezzature informatiche permetterebbe di definire la questione della cibersicurezza prima di immettere nuovi prodotti sul mercato. Questo potrebbe rientrare nel principio di "responsabilità", da elaborare ulteriormente insieme agli operatori del settore, che potrebbe ridurre le vulnerabilità dei prodotti/software applicando una serie di metodi che vanno dalla progettazione ai test e alla verifica, inclusa la verifica formale ove applicabile, la manutenzione a lungo termine e l'utilizzo di processi sicuri lungo il ciclo di sviluppo, così come lo sviluppo di aggiornamenti e correzioni atti a risolvere vulnerabilità precedentemente nascoste e rapidi interventi di aggiornamento e riparazione[24]. Questo aumenterebbe inoltre la fiducia dei consumatori nei confronti dei prodotti digitali.

Occorre inoltre riconoscere l'importante ruolo dei ricercatori terzi in materia di sicurezza ai fini della scoperta di vulnerabilità nei prodotti e servizi esistenti e dovrebbero essere create le condizioni per consentire la divulgazione coordinata[25] delle vulnerabilità tra gli Stati membri, basandosi sulle migliori prassi[26] e sulle norme pertinenti[27].

Allo stesso tempo, **settori specifici** affrontano problemi specifici e dovrebbero quindi essere incoraggiati a sviluppare un approccio specifico proprio. In questo modo le strategie generali

---

[23] Settori che rientrano nell'ambito di applicazione della direttiva 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

[24] Cybersecurity in the European Digital Single Market [Cibersicurezza nel mercato unico digitale europeo], Gruppo di alto livello di consulenti scientifici, marzo 2017.

[25] La divulgazione coordinata delle vulnerabilità è una forma di cooperazione che facilita e consente ai ricercatori in materia di sicurezza di riferire le vulnerabilità al proprietario o al fornitore del sistema informativo, dando all'organizzazione l'opportunità di diagnosticare la vulnerabilità e porvi rimedio in modo corretto e tempestivo prima che le informazioni dettagliate sulla vulnerabilità vengano divulgate a terzi o al pubblico.

[26] Per esempio Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations [Guida di buone pratiche per la divulgazione di vulnerabilità. Dalle sfide alle raccomandazioni], ENISA, 2016.

[27] ISO/IEC 29147:2014 Information technology -- Security techniques -- Vulnerability disclosure [Tecnologia dell'informazione -- Tecniche di sicurezza -- Divulgazione di vulnerabilità].

di cibersicurezza sarebbero integrate da strategie di cibersicurezza settoriali in aree quali i servizi finanziari[28], l'energia, i trasporti e la sanità[29].

La Commissione ha già evidenziato le problematiche specifiche riguardanti la **responsabilità** emerse con le nuove tecnologie digitali[30] ed è in corso il lavoro di analisi delle implicazioni; i passi successivi saranno conclusi entro giugno 2018. La cibersicurezza fa sorgere problematiche riguardanti l'attribuzione dei danni per le imprese e le catene di approvvigionamento, la cui mancata gestione impedirà lo sviluppo di un solido mercato unico dei prodotti e dei servizi per la cibersicurezza.

Infine, lo sviluppo del mercato unico dell'UE dipende anche dal fatto che si tenga conto della cibersicurezza nelle politiche in materia di commercio e investimenti. L'effetto delle acquisizioni estere sulle tecnologie critiche – di cui la cibersicurezza è un importante esempio – costituisce un aspetto chiave nel quadro per **la selezione degli investimenti diretti esteri nell'Unione europea**[31], che mira a permettere la selezione degli investimenti da paesi terzi per motivi di sicurezza e ordine pubblico. Nella stessa ottica, gli obblighi di cibersicurezza hanno già creato barriere commerciali per i beni e i servizi dell'Unione in settori importanti in diverse economie di paesi terzi. Il quadro di certificazione della cibersicurezza dell'UE rafforzerà ulteriormente la posizione internazionale dell'Europa e dovrebbe essere integrato da sforzi continuativi verso l'elaborazione di norme globali di sicurezza elevata e accordi di mutuo riconoscimento.

2.3 Piena attuazione della direttiva sulla sicurezza delle reti e dei sistemi informativi

Poiché attualmente i principali strumenti per rafforzare la cibersicurezza si trovano nelle mani delle amministrazioni nazionali, l'UE ha riconosciuto la necessità di inasprire le norme. Vista la natura sempre più globalizzata, dipendente dal digitale e interconnessa di settori chiave come le banche, l'energia e i trasporti, raramente gli incidenti di cibersicurezza su larga scala colpiscono solo uno Stato membro.

La direttiva sulla sicurezza delle reti e dei sistemi informativi ("la direttiva NIS") è la prima normativa in materia di cibersicurezza adottata a livello dell'UE[32]. È stata elaborata per rafforzare la resilienza aumentando le capacità di cibersicurezza nazionali, favorendo una migliore cooperazione tra gli Stati membri e chiedendo alle imprese in importanti settori economici di adottare pratiche efficaci di gestione dei rischi e di segnalare gli incidenti gravi alle autorità nazionali. Tali obblighi si applicano anche a tre tipi di fornitori di servizi internet fondamentali: servizio nella nuvola (cloud computing), motori di ricerca e mercati online. L'ambizione è un approccio più solido e sistematico e un migliore flusso di informazioni.

La piena attuazione della direttiva da parte di tutti gli Stati membri entro maggio 2018 è essenziale per la ciberresilienza dell'Unione. Il processo è supportato dal lavoro collettivo degli Stati membri che darà come risultato, entro l'autunno 2017, orientamenti volti a sostenere un'attuazione più armonizzata, in particolare in relazione agli operatori di servizi essenziali. Nell'ambito di tale pacchetto la Commissione sta inoltre redigendo una

[28] L'imminente lavoro della Commissione sulla tecnologia finanziaria riguarderà la cibersicurezza per il settore finanziario.

[29] Nel settore dell'energia, ad esempio, che combina tecnologie dell'informazione molto vecchie e all'avanguardia, in particolare visti i requisiti di un contesto in tempo reale per la rete elettrica.

[30] COM(2017) 228.

[31] COM(2017) 478.

[32] Direttiva 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.

comunicazione[33] per la cibersicurezza allo scopo di sostenere gli Stati membri nelle attività indicando le loro migliori prassi di attuazione della direttiva e indicando orientamenti sul funzionamento pratico della direttiva.

Un ambito in cui occorrerà integrare la direttiva è il flusso di informazioni. Per esempio, la direttiva riguarda unicamente i settori strategici chiave, ma per logica un approccio analogo sarebbe necessario da parte di tutti i portatori d'interessi colpiti da ciberattacchi, in modo da giungere a una valutazione sistematica delle vulnerabilità e dei punti di accesso sfruttati dagli autori di tali attacchi. Inoltre la cooperazione e lo scambio di informazioni tra i settori pubblico e privato devono affrontare numerosi ostacoli. I governi e le autorità pubbliche sono riluttanti a condividere informazioni riguardanti la cibersicurezza per timore di compromettere la sicurezza o la competitività nazionale. Le imprese private sono riluttanti a condividere informazioni riguardanti le loro vulnerabilità cibernetiche e le perdite risultanti per timore di compromettere informazioni aziendali sensibili, di danneggiarsi la reputazione o di rischiare di violare norme in materia di protezione dei dati[34]. Occorre rafforzare la fiducia affinché i partenariati pubblico-privato sostengano una cooperazione e una condivisione di informazioni più ampia tra un numero maggiore di settori. Il ruolo dei centri di condivisione e di analisi delle informazioni è particolarmente importante nella creazione della fiducia necessaria per lo scambio di informazioni tra i settori pubblico e privato. Primi passi sono stati fatti in settori critici specifici come il trasporto aereo, attraverso la creazione del centro europeo per la cibersicurezza nell'aviazione,[35] e l'energia, sviluppando centri di condivisione e di analisi delle informazioni[36]. La Commissione contribuirà pienamente a tale approccio con il sostegno dell'ENISA, con la necessità di un'accelerazione in particolare nei settori che forniscono servizi essenziali identificati nella direttiva NIS.

2.4 Resilienza attraverso una rapida risposta alle emergenze

Quando si verifica un ciberattacco, una risposta rapida ed efficace può mitigarne l'impatto. Questo può anche dimostrare che le autorità pubbliche non sono impotenti di fronte ai ciberattacchi e può contribuire a rafforzare la fiducia. Per quanto riguarda la risposta delle istituzioni europee, gli aspetti cibernetici dovrebbero essere in primo luogo integrati nei meccanismi dell'UE di gestione delle crisi esistenti: i dispositivi integrati dell'UE per la risposta politica alle crisi, coordinati dalla presidenza del Consiglio,[37] e i sistemi di allarme rapido generali dell'UE[38]. La necessità di rispondere ad un incidente o un attacco cibernetico particolarmente grave potrebbe costituire una motivazione sufficiente perché uno Stato membro invochi la clausola di solidarietà dell'Unione[39].

---

33 COM(2017) 476.

34 Cybersecurity in the European Digital Single Market [Cibersicurezza nel mercato unico digitale europeo], Gruppo di alto livello di consulenti scientifici, marzo 2017. Una problematica specifica riguarda i segreti commerciali, in merito ai quali la comunicazione del luglio 2016 "Rafforzare il sistema di resilienza informatica dell'Europa" rilevava la reticenza nel segnalare il furto cibernetico di segreti commerciali e l'importanza di canali di segnalazione affidabili che assicurino la riservatezza.

35 https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

36 Si tratta di organizzazioni senza scopo di lucro e dirette dai loro membri, costituite da soggetti pubblici e privati allo scopo di condividere informazioni riguardanti minacce, rischi, prevenzione, mitigazione e risposta nel ciberspazio. Cfr. ad esempio i centri di condivisione e di analisi delle informazioni per l'energia europea (http://www.ee-isac.eu).

37 Consente il coordinamento delle risposte ad importanti crisi intersettoriali al massimo livello politico.

38 Consentono la condivisione interna di informazioni e il coordinamento in caso di insorgenza di crisi multi-settoriali o di minacce prevedibili o imminenti che richiedono un'azione a livello dell'UE.

39 A norma dell'articolo 222 del trattato sul funzionamento dell'Unione europea.

Una risposta rapida ed efficace si basa anche su un meccanismo rapido di scambio delle informazioni tra tutti gli attori principali a livello nazionale ed europeo, che a sua volta richiede chiarezza sui rispettivi ruoli e responsabilità. La Commissione ha consultato istituzioni e Stati membri in merito a un "programma" per stabilire un processo efficace per una risposta operativa a livello dell'Unione e degli Stati membri ad un ciberincidente su larga scala. Il **programma** presentato in una raccomandazione[40] in tale pacchetto spiega come la cibersicurezza venga integrata nei meccanismi in vigore di gestione delle crisi a livello dell'UE e definisce gli obiettivi e le modalità della cooperazione sia tra gli Stati membri sia tra gli Stati membri e le istituzioni, i servizi, le agenzie e gli organismi competenti dell'UE[41] in risposta agli incidenti e alle crisi di cibersicurezza su larga scala. La raccomandazione chiede inoltre agli Stati membri e alle istituzioni dell'UE di istituire un quadro di risposta alle crisi di cibersicurezza dell'UE volto a rendere operativo il programma. Il programma sarà testato regolarmente nel quadro di esercitazioni di gestione delle crisi connesse alla cibersicurezza e di altro genere[42], e aggiornato secondo necessità.

Dato che gli incidenti di cibersicurezza potrebbero incidere sostanzialmente sul funzionamento delle economie e sulla vita quotidiana della popolazione, una possibilità sarebbe di valutare la possibilità di un **Fondo di risposta alle emergenze di cibersicurezza**, seguendo l'esempio di altri meccanismi di crisi simili in altri settori normativi dell'UE. Questo consentirebbe agli Stati membri di chiedere aiuto a livello dell'UE durante o dopo incidenti gravi, purché lo Stato membro si sia dotato, prima dell'incidente, di un sistema prudente di cibersicurezza che comprenda la piena attuazione della direttiva NIS, una gestione matura dei rischi e quadri di vigilanza a livello nazionale. Tale fondo, che verrebbe a integrare i meccanismi in vigore di gestione delle crisi a livello dell'UE, potrebbe essere dotato di una capacità di risposta rapida nell'interesse della solidarietà e finanziare azioni specifiche di risposta ad emergenze come la sostituzione di attrezzature compromesse o l'utilizzo di strumenti di mitigazione o risposta, basandosi sulle competenze nazionali in modo analogo al meccanismo unionale di protezione civile.

2.5 Una rete di competenze sulla cibersicurezza con un centro europeo di ricerca e di competenza sulla cibersicurezza

Gli strumenti tecnologici di cibersicurezza sono risorse strategiche, oltre a rappresentare tecnologie chiave per la crescita futura. È nell'interesse strategico dell'UE garantire che l'Unione mantenga e sviluppi le capacità essenziali per tutelare al proprio interno l'economia, la società e la democrazia digitali, proteggere l'hardware e il software critici e fornire servizi fondamentali di cibersicurezza.

Il partenariato pubblico-privato sulla cibersicurezza[43] creato nel 2016 ha costituito un primo importante passo che genererà fino a 1,8 miliardi di euro di investimenti entro il 2020. L'entità dell'investimento in corso in altre parti del mondo[44] suggerisce tuttavia che l'UE deve fare di più in termini di investimenti e per superare la frammentazione delle capacità, attualmente sparpagliate in tutta l'Unione.

---

40 C(2017) 6100.

41 Compresi Europol, ENISA, squadra di pronto intervento informatico per le istituzioni, gli organismi e le agenzie dell'UE (CERT-EU) e centro dell'UE di analisi dell'intelligence (INTCEN).

42 Per esempio quelli condotti dall'ENISA: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

43 C(2016) 4400 final.

44 Gli Stati Uniti investiranno 19 miliardi di USD in cibersicurezza solo nel 2017, con un incremento del 35% rispetto al 2016. Casa Bianca, Segreteria alla stampa. "Fact Sheet: Cybersecurity National Action Plan" [Scheda informativa: Piano d'azione nazionale sulla cibersicurezza], 9 febbraio 2016.

L'UE può fornire valore aggiunto dati la sofisticatezza della tecnologia di cibersicurezza, l'investimento su larga scala richiesto e la necessità di soluzioni che funzionino in tutta l'Unione. Basandosi sul lavoro degli Stati membri e del partenariato pubblico-privato, un ulteriore passo consisterebbe nel rafforzare la capacità di cibersicurezza dell'UE attraverso una **rete di centri di competenza sulla cibersicurezza**[45] il cui fulcro sia un **centro europeo di ricerca e di competenza sulla cibersicurezza**. Tale rete e il suo centro stimolerebbero lo sviluppo e l'utilizzo di tecnologia nella cibersicurezza e integrerebbero l'impegno nella creazione di capacità in questo settore a livello dell'UE e nazionale. La Commissione avvierà una valutazione d'impatto per esaminare le opzioni disponibili – compresa la possibilità di istituire un'impresa comune – al fine di varare tale struttura nel 2018.

Come primo passo e modo per indirizzare il pensiero futuro, la Commissione proporrà l'istituzione di una fase pilota nell'ambito di Orizzonte 2020, al fine di contribuire a raccogliere i centri nazionali in una rete per dare nuovo slancio alle competenze in cibersicurezza e allo sviluppo tecnologico. Intende proporre a tale fine un'iniezione di fondi a breve termine per un importo di 50 milioni di euro. Quest'attività integrerà l'attuazione in corso del partenariato pubblico-privato sulla cibersicurezza.

Inizialmente l'attenzione della rete e del centro sarebbe rivolta principalmente a unire e plasmare gli sforzi di ricerca. Per sostenere lo sviluppo di capacità industriali, il centro potrebbe fungere da responsabile dei progetti sulle capacità, in grado di gestire progetti multinazionali. Questo darebbe uno stimolo aggiuntivo all'innovazione e alla competitività dell'industria dell'UE sulla scena globale nello sviluppo di tecnologie digitali di prossima generazione, tra cui intelligenza artificiale, informatica quantistica, *blockchain* e identità digitali sicure, così come nel garantire un accesso ai dati di massa per società con sede nell'UE: tutti aspetti fondamentali per il futuro della cibersicurezza. Il centro si baserebbe inoltre sul lavoro dell'UE per far crescere l'infrastruttura informatica ad alte prestazioni: questo è essenziale per l'analisi di grandi quantità di dati, la cifratura e la decifratura rapida di dati, il controllo delle identità, la simulazione di ciberattacchi e l'analisi di materiale video[46].

La rete di centri di competenza avrebbe inoltre le capacità di sostenere l'industria attraverso test e simulazioni finalizzati alla certificazione della cibersicurezza descritta nella sezione 2.2. Il suo coinvolgimento nell'intera gamma delle attività di cibersicurezza dell'UE assicurerebbe un aggiornamento continuo degli obiettivi a seconda delle esigenze. Il centro ambirebbe a promuovere norme di cibersicurezza di livello elevato non solo nella tecnologia e nei sistemi di cibersicurezza, ma anche nello sviluppo di capacità di alta qualità per professionisti, attraverso la fornitura di soluzioni e modelli per l'impegno nazionale nel lancio di capacità digitali. In questo senso rafforzerebbe anche le capacità di cibersicurezza a livello dell'UE e si baserebbe su sinergie, in particolare, con ENISA, CERT-UE, Europol e il possibile Fondo di risposta alle emergenze di cibersicurezza futuro e i CSIRT nazionali.

Un punto focale dell'attività della rete di competenza deve essere la mancanza di capacità europea nella valutazione della **cifratura** di prodotti e servizi utilizzati dai cittadini, dalle imprese e dalle amministrazioni pubbliche all'interno del mercato unico digitale. Una cifratura forte costituisce la base per quei sistemi di identificazione digitale sicura che rivestono un ruolo essenziale in una cibersicurezza efficace[47]; protegge inoltre la proprietà

[45] La rete includerebbe i centri di cibersicurezza esistenti e futuri istituiti negli Stati membri, i cui membri sarebbero solitamente organizzazioni e laboratori di ricerca pubblici.

[46] COM(2012) 45 final e COM(2016) 178 final.

[47] Già nell'ambito di Orizzonte 2020 la Commissione istituirà una nuova sfida per i Premi Orizzonte che assegnerà 4 milioni di euro alla migliore soluzione innovativa per metodi di autenticazione online senza soluzione di continuità.

intellettuale e consente di tutelare i diritti fondamentali come la libertà di espressione e la protezione dei dati personali e garantisce la sicurezza del commercio online[48].

Poiché i mercati della cibersicurezza civile e per la difesa dell'UE sono di fronte a sfide comuni[49] e condividono tecnologie a duplice uso che richiedono una stretta collaborazione in settori critici, potrebbe essere ulteriormente sviluppata una seconda fase della rete e del suo centro con una dimensione di ciberdifesa, nel pieno rispetto delle disposizioni del trattato riguardanti la politica di sicurezza e di difesa comune. Oltre ad essere incentrata sulla tecnologia, la dimensione di difesa potrebbe contribuire alla cooperazione tra gli Stati membri nel settore della ciberdifesa, comprendendo la condivisione di informazioni, la conoscenza situazionale, la creazione di competenze e reazioni coordinate e il sostegno allo sviluppo di capacità comuni da parte degli Stati membri. Potrebbe inoltre costituire una piattaforma che consenta agli Stati membri d'individuare le priorità della ciberdifesa dell'UE, esaminando soluzioni comuni, contribuendo allo sviluppo di strategie comuni, facilitando attività congiunte di formazione, esercitazioni e test sulla ciberdifesa a livello europeo e sostenendo il lavoro sulle tassonomie e le norme di ciberdifesa, in cui il centro avrebbe un ruolo di sostegno e di consulenza. Per portare avanti dette attività il centro dovrebbe collaborare strettamente e in piena complementarità con l'Agenzia europea per la difesa nel settore della ciberdifesa, così come con l'ENISA nel settore della ciberresilienza. Questa dimensione di difesa prenderebbe in considerazione il processo istituito dal documento di riflessione sul futuro della difesa europea.

L'elevato livello di resilienza necessario nella ciberdifesa richiede uno specifico indirizzamento degli sforzi della ricerca e delle tecnologie. I progetti o le tecnologie di ciberdifesa sviluppati dalle imprese potrebbero trarre vantaggio dai finanziamenti del Fondo europeo per la difesa per quanto riguarda sia la fase di ricerca che quella di sviluppo[50]. Settori specifici come i sistemi di cifratura basati sulle tecnologie quantistiche, sulla conoscenza situazionale cibernetica, sui sistemi di controllo biometrico dell'accesso, sulla rivelazione di *advanced persistent threat* (APT) o sul *data mining* potrebbero essere particolarmente rilevanti in questo contesto. L'Alta rappresentante, l'Agenzia europea per la difesa e la Commissione sosterranno gli Stati membri nell'individuazione di settori in cui potrebbero essere presi in considerazioni progetti di cibersicurezza comuni per un finanziamento da parte del Fondo europeo per la difesa.

2.6 Creazione di una solida base di competenze cibernetiche nell'UE

La cibersicurezza ha una forte dimensione educativa. Una cibersicurezza efficace dipende fortemente dalle capacità delle persone interessate. Tuttavia si prevede che nel 2022 il deficit di competenze di cibersicurezza tra i professionisti che lavorano nel settore privato in Europa raggiungerà 350 000 unità[51]. L'istruzione in materia di cibersicurezza dovrebbe essere sviluppata a tutti i livelli, a partire dalla normale formazione del personale del settore cibernetico, da una formazione aggiuntiva in cibersicurezza per tutti gli specialisti delle TIC e da nuovi piani formativi specifici in materia di cibersicurezza. Dovrebbero essere istituiti solidi centri accademici di competenza volti a soddisfare le richieste di istruzione e formazione accelerate, che potrebbero attingere agli orientamenti impartiti da un centro

[48] Cybersecurity in the European Digital Single Market [Cibersicurezza nel mercato unico digitale europeo], Gruppo di alto livello di consulenti scientifici, marzo 2017.

[49] "Study on synergies between the civilian and the defence cybersecurity markets" [Studio sulle sinergie tra i mercati della cibersicurezza civili e di difesa] (Optimity; SMART 2014-0059).

[50] Già adesso il programma europeo di sviluppo del settore industriale darà priorità a progetti di ciberdifesa e la ciberdifesa diventerà uno dei temi degli inviti a presentare proposte che saranno lanciati nel 2018.

[51] Global Information Security Workforce Study 2017. Il deficit globale è di 1,8 milioni.

europeo di ricerca e di competenza sulla cibersicurezza e dall'ENISA. L'obiettivo dovrebbe essere quello di rendere naturale la progettazione di prodotti e sistemi TIC che fin dall'inizio integrino principi di sicurezza. L'istruzione sulla cibersicurezza non dovrebbe essere limitata ai professionisti informatici, ma dovrebbe essere integrata nei piani formativi per altri settori, come l'ingegneria, la gestione aziendale o il diritto, nonché per percorsi educativi specifici di settore. Infine, gli insegnanti e gli alunni nell'istruzione primaria e secondaria dovrebbero essere sensibilizzati sulla criminalità informatica e la cibersicurezza quando acquisiscono competenze digitali a scuola.

Insieme agli Stati membri, anche l'UE dovrebbe contribuire basandosi sul lavoro della coalizione per le competenze e le occupazioni digitali[52] creando, ad esempio, programmi di apprendistato in cibersicurezza per le PMI.

2.7 Promozione dell'igiene e della consapevolezza cibernetiche

Visto che si ritiene che il 95% degli incidenti sia reso possibile da "qualche tipo di errore umano, intenzionale o meno"[53], è in gioco un forte fattore umano. La cibersicurezza è quindi una responsabilità di tutti. Ciò significa che il comportamento delle persone, delle aziende e delle amministrazioni pubbliche deve cambiare per garantire che tutti comprendano la minaccia e siano in possesso degli strumenti e delle competenze necessari al fine di rilevare rapidamente gli attacchi e proteggersi attivamente. Le persone devono sviluppare abitudini di igiene cibernetica, mentre le imprese e le organizzazioni devono adottare programmi adeguati di cibersicurezza basati sul rischio e aggiornarli regolarmente al fine di rispecchiare il di rischio in evoluzione.

La direttiva NIS stabilisce le responsabilità degli Stati membri non solo in termini di scambio di informazioni riguardanti i ciberattacchi a livello dell'UE ma anche di attuazione di strategie nazionali di cibersicurezza mature e di quadri di intervento sulla sicurezza della rete e dei sistemi informativi. Le amministrazioni pubbliche a livello dell'UE e nazionale dovrebbero svolgere un ulteriore ruolo motore nel portare avanti questi sforzi.

In primo luogo, gli Stati membri dovrebbero massimizzare la disponibilità di strumenti di cibersicurezza per le imprese e le persone. In particolare occorre un'azione più incisiva per prevenire e attutire le ripercussioni della cibercriminalità sugli utenti finali. Esiste già un esempio nel lavoro di Europol con la campagna "NoMoreRansom"[54], sviluppato attraverso una stretta collaborazione tra le autorità di contrasto e le società di cibersicurezza al fine di aiutare gli utenti a prevenire infezioni di ransomware e a decifrare i dati se sono vittime di un attacco. Programmi analoghi dovrebbero essere presentati per altri tipi di software maligni (malware) in altri settori e l'UE dovrebbe sviluppare un **portale unico per riunire tutti questi strumenti in uno sportello unico**, offrendo consulenza agli utenti sulla prevenzione e la rilevazione di software maligni e collegamenti a meccanismi di segnalazione.

In secondo luogo, gli Stati membri dovrebbero accelerare l'**uso di strumenti più sicuri dal punto di vista cibernetico nello sviluppo della pubblica amministrazione on line** e cogliere appieno i vantaggi della rete di competenze. Dovrebbe essere promossa l'adozione di mezzi sicuri di identificazione, basandosi sul quadro dell'UE di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno, che è in vigore dal 2016 e prevede un ambiente normativo prevedibile volto a consentire interazioni elettroniche sicure e

---

52 https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

53 IBM "The Cybersecurity Intelligence Index" [L'indice di intelligence sulla cibersicurezza] 2014, a cui si fa riferimento in Securitymagazine.com, 19 giugno 2014.

54 https://www.nomoreransom.org/.

fluide tra imprese, persone e autorità pubbliche[55] Inoltre le istituzioni pubbliche, in particolare quelle che forniscono servizi essenziali, dovrebbero assicurare che il loro personale sia formato nei settori legati alla cibersicurezza.

In terzo luogo, gli Stati dovrebbero fare della consapevolezza cibernetica una priorità nelle **campagne di sensibilizzazione**, incluse quelle destinate a scuole, università, comunità imprenditoriale e organismi di ricerca. Il mese della cibersicurezza che si celebra ogni anno ad ottobre con il coordinamento dell'ENISA sarà esteso per ottenere una diffusione maggiore come impegno di comunicazione comune a livello dell'UE e nazionale. Altrettanto importante è la sensibilizzazione in relazione alle **campagne di disinformazione** online e alle **notizie false** sui media sociali volte specificamente a danneggiare i processi democratici e i valori europei. Sebbene la responsabilità principale rimanga a livello nazionale – anche per le elezioni del Parlamento europeo – la messa in comune di competenze e la condivisione di esperienza a livello europeo si è dimostrata un valore aggiunto nel fornire un obiettivo di intervento[56].

Vi è inoltre un forte ruolo degli **operatori del settore** in generale, ma con particolare attenzione ai fornitori e ai produttori di servizi digitali. Il settore deve sostenere gli utenti (persone, imprese e pubbliche amministrazioni) con strumenti che consentano loro di assumersi la responsabilità delle proprie azioni online, rendendo chiaro che il mantenimento dell'igiene cibernetica rappresenta una parte indispensabile dell'offerta ai consumatori[57]. Per rilevare e rimuovere le vulnerabilità, il settore dovrebbe tendere a dotarsi di processi interni che trattino l'indagine, la categorizzazione e la risoluzione di vulnerabilità, indipendentemente dal fatto che la fonte di potenziale vulnerabilità sia esterna o interna all'impresa.

Azioni chiave

- Piena attuazione della direttiva sulla sicurezza delle reti e dei sistemi informativi
- Rapida adozione da parte del Parlamento europeo e del Consiglio del regolamento che stabilisce un nuovo mandato per l'ENISA e un quadro europeo di certificazione[58]
- Iniziativa congiunta della Commissione e del settore volta a definire il principio di "dovere di diligenza" per ridurre le vulnerabilità dei prodotti/del software e promuovere la "sicurezza fin dalla progettazione"
- Rapida attuazione del programma per la risposta agli incidenti transfrontalieri su larga scala
- Avvio di una valutazione d'impatto per studiare la possibilità che la Commissione presenti nel 2018 una proposta volta a istituire una rete di centri di competenza sulla cibersicurezza e un centro europeo di ricerca e di competenza sulla cibersicurezza, muovendo da una fase pilota immediata

[55] Regolamento (UE) n. 910/2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS) adottato il 23 luglio 2014. Inoltre la Commissione europea fornisce elementi costitutivi e strumenti per l'identificazione elettronica e l'interoperabilità della firma elettronica (ad esempio elenchi di fiducia di browser) attraverso il programma del meccanismo per collegare l'Europa.

[56] Un esempio è la task force East StratCom istituita nel 2015 dagli Stati membri e dall'Alta rappresentante per gestire le campagne di disinformazione in corso in Russia. La squadra è impegnata nello sviluppo di prodotti e campagne di comunicazione incentrate sulla spiegazione delle politiche europee nella regione del partenariato orientale.

[57] Alcuni produttori sono già abituati a questo concetto poiché parte della normativa europea sui prodotti (come la direttiva macchine 2006/42/CE) stabilisce i principi di "sicurezza fin dalla progettazione".

[58] COM(2017) 477.

- Sostegno agli Stati membri nell'individuazione dei settori in cui progetti comuni di cibersicurezza potrebbero essere presi in considerazione per ricevere sostegno dal Fondo europeo per la difesa
- Sportello unico a livello dell'UE per aiutare le vittime di ciberattacchi, che fornisca informazioni riguardanti le minacce più recenti e riunisca consigli pratici e strumenti di cibersicurezza
- Intervento degli Stati membri per integrare la cibersicurezza nei programmi di sviluppo delle competenze, nella pubblica amministrazione on line e in campagne di sensibilizzazione
- Intervento del settore per intensificare la formazione del personale in materia di cibersicurezza e adottare un approccio di "sicurezza fin dalla progettazione" per i prodotti, servizi e processi

3. CREAZIONE DI UNA DETERRENZA CIBERNETICA EFFICACE NELL'UE

Una deterrenza efficace comporta la creazione di un quadro di misure che siano sia credibili che dissuasive per i potenziali cibercriminali e autori di ciberattacchi. Fintanto che non avranno niente da temere a parte il fallimento dell'iniziativa, gli autori di ciberattacchi (siano essi non statali o statali) avranno pochi incentivi a desistere. Una risposta più efficace delle autorità di contrasto incentrata sull'individuazione, sulla tracciabilità e sul perseguimento dei cibercriminali è essenziale per creare una deterrenza efficace. A ciò si aggiunge la necessità che l'UE sostenga gli Stati membri nello sviluppo di capacità di cibersicurezza a duplice uso. Per i ciberattacchi la tendenza s'invertirà solo quando gli autori avranno più probabilità di essere arrestati e puniti per averli commessi. I ciberattacchi dovrebbero essere sottoposti tempestivamente a indagine e gli autori consegnati alla giustizia, o dovrebbero essere adottate azioni che permettano un'adeguata risposta politica o diplomatica. In caso di grave crisi con un'importante dimensione internazionale o di difesa, l'Alta rappresentante potrebbe presentare opzioni di adeguata risposta al Consiglio.

Un passo verso il miglioramento della risposta penale ai ciberattacchi è già stato fatto con l'adozione nel 2013 della direttiva relativa agli attacchi contro i sistemi di informazione[59], che ha stabilito norme minime riguardanti la definizione dei reati e delle sanzioni nel campo degli attacchi contro i sistemi di informazione e previsto misure operative volte a migliorare la cooperazione tra le autorità. La direttiva ha portato a progressi sostanziali per configurare come reato i ciberattacchi ad un livello comparabile in tutti gli Stati membri, il che facilita la cooperazione transfrontaliera fra le autorità di contrasto che indagano su questo tipo di reati. Tuttavia, esistono ancora margini d'azione perché la direttiva possa raggiungere le sue piene potenzialità, se gli Stati membri garantiranno l'attuazione completa di tutte le sue disposizioni[60]. La Commissione continuerà a fornire sostegno agli Stati membri per l'attuazione della direttiva e attualmente non vede alcuna necessità di proporre modifiche della stessa.

3.1 Identificazione dei malintenzionati

Al fine di aumentare le probabilità di consegnare alla giustizia gli autori di ciberattacchi, dobbiamo migliorare urgentemente la capacità di identificarli. Trovare informazioni utili per le indagini sulla cibercriminalità, soprattutto sotto forma di tracce digitali, costituisce una

[59] Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione.

[60] COM(2017) 474.

sfida importante per le autorità di contrasto. Dobbiamo pertanto aumentare la nostra capacità tecnologica di indagare efficacemente, anche potenziando con esperti del ciberspazio l'unità di lotta alla cibercriminalità di Europol. Europol è diventata un attore chiave nel sostegno alle indagini plurigiurisdizionali degli Stati membri. Dovrebbe diventare per le autorità di contrasto degli Stati membri un centro di competenza nelle indagini online e nell'informatica forense.

La pratica diffusa di mettere molteplici utenti – a volte migliaia – dietro un solo indirizzo IP rende molto difficile dal punto di vista tecnico indagare su comportamenti dolosi online. A volte rende anche necessario, ad esempio per reati gravi come la violenza sessuale su minori, indagare su un gran numero di utenti al fine di identificare un solo malintenzionato. L'UE pertanto incoraggerà la diffusione del nuovo protocollo (IPv6) in quanto consente l'assegnazione di un singolo utente per indirizzo IP, recando così chiari vantaggi alle indagini di contrasto e di cibersicurezza. Come primo passo per incoraggiare la diffusione, la Commissione integrerà l'obbligo di passare al protocollo IPv6 in tutte le sue politiche, inserendo requisiti in tal senso nel finanziamento di appalti, progetti e ricerche e sostenendo il necessario materiale formativo. Gli Stati membri dovrebbero altresì vagliare l'ipotesi di accordi volontari con i fornitori di servizi internet per promuovere la diffusione del protocollo IPv6.

Il Belgio è leader mondiale[61] *nel tasso di adozione del protocollo IPv6 anche grazie alla cooperazione pubblico-privato: i portatori d'interessi hanno vagliato l'ipotesi di limitare l'uso di un indirizzo IP a un massimo di 16 utenti nell'ambito di una misura di autoregolamentazione volontaria, che ha incentivato la transizione al protocollo IPv6*[62].

Più in generale, la responsabilità online dovrebbe essere promossa ulteriormente. Ciò comporta la promozione di misure volte a prevenire l'abuso dei nomi di dominio per la distribuzione di messaggi indesiderati o attacchi di *phishing*. A tal fine, la Commissione lavorerà per migliorare il funzionamento e la disponibilità e l'accuratezza delle informazioni nei sistemi dei nomi di dominio e nei WHOIS degli IP[63] in linea con gli sforzi dell'Internet Corporation for Assigned Names and Numbers[64].

3.2 Intensificazione della risposta delle autorità di contrasto

Indagare e **perseguire** efficacemente i reati favoriti dalla cibernetica costituisce un deterrente essenziale dei ciberattacchi. Il quadro procedurale attuale tuttavia deve essere adattato meglio all'era di internet[65]. La velocità dei ciberattacchi può avere il sopravvento sulle nostre procedure e creare particolari necessità di una rapida cooperazione transfrontaliera. A tal fine, come annunciato nell'ambito dell'agenda europea sulla sicurezza, all'inizio del 2018 la Commissione presenterà proposte per **facilitare l'accesso transfrontaliero a prove elettroniche**. Parallelamente, la Commissione sta attuando misure pratiche volte a migliorare l'accesso transfrontaliero alle prove elettroniche per indagini penali, compresi finanziamenti per la formazione in collaborazione transfrontaliera, lo sviluppo di una piattaforma elettronica

[61] https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

[62] http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

[63] Protocollo di interrogazione e risposta ampiamente utilizzato per interrogare le basi di dati che archiviano gli utenti registrati o gli assegnatari di una risorsa di Internet.

[64] L'Internet Corporation for Assigned Names and Numbers (ICANN) è un'organizzazione senza scopo di lucro responsabile di coordinare il mantenimento e le procedure di diverse basi di dati legate agli spazi nominativi di Internet.

[65] Solo per citare un esempio, il server (virtuale) della centrale di comando e controllo della botnet Avalanche spostava i server e i domini fisici ogni cinque minuti.

per lo scambio di informazioni all'interno dell'UE e la normazione di forme di cooperazione giudiziaria usate tra gli Stati Membri.

Un altro ostacolo all'efficace perseguimento è rappresentato dalle diverse procedure forensi degli Stati membri per la raccolta di prove elettroniche nelle indagini sui reati cibernetici. Quest'ostacolo potrebbe essere superato lavorando all'elaborazione di norme forensi comuni. Occorre inoltre rafforzare le capacità forensi al fine di sostenere la tracciabilità e l'attribuzione. Un passo consisterebbe nello sviluppare ulteriormente la capacità in Europol, adattando le risorse umane e di bilancio esistenti presso il Centro europeo per la lotta alla criminalità informatica di Europol per soddisfare la crescente esigenza di sostegno operativo nelle indagini transfrontaliere sulla cibercriminalità. Un altro sarebbe rispecchiare la suddetta enfasi sull'aspetto tecnologico per la cifratura, osservando come il suo abuso da parte dei criminali crei sfide significative nella lotta contro i reati gravi, compreso il terrorismo e la cibercriminalità. La Commissione proporrà i risultati delle attuali riflessioni sul **ruolo della cifratura nelle indagini penali**[66] entro ottobre 2017[67].

Vista la natura senza frontiere di internet, il quadro di cooperazione internazionale previsto dalla **convenzione di Budapest** del Consiglio d'Europa **sulla criminalità informatica**[68] offre a un gruppo eterogeneo di paesi l'opportunità di utilizzare uno standard giuridico ottimale per la diversa legislazione che disciplina la cibercriminalità. Attualmente è in fase di studio la possibile aggiunta di un protocollo alla convenzione[69], che potrebbe rappresentare anche un'utile opportunità per affrontare la questione dell'accesso transfrontaliero alle prove elettroniche nel contesto internazionale. Piuttosto che la creazione di nuovi strumenti giuridici internazionali in materia di cibercriminalità, l'UE chiede a tutti i paesi di stabilire un'adeguata normativa nazionale e di proseguire la cooperazione nel quadro internazionale vigente.

La disponibilità pervasiva di strumenti di anonimizzazione rende più facile ai criminali nascondersi. La "**darknet**"[70] ha aperto nuove modalità per i criminali per accedere a materiale pedopornografico, droghe o armi da fuoco, spesso con un rischio minimo di essere catturati[71]. Attualmente rappresenta anche una fonte fondamentale per gli strumenti utilizzati nella cibercriminalità, come i software maligni e gli strumenti di pirateria informatica. La Commissione, insieme alle parti interessate, analizzerà approcci nazionali allo scopo di identificare nuove soluzioni. Europol dovrebbe facilitare e sostenere le indagini sulla darknet,

---

66 Presidenza del Consiglio, Risultati del Consiglio "Giustizia e affari interni" dell'8 e 9 dicembre 2016, doc. n. 15391/16.

67 Ottava relazione sui progressi compiuti verso la creazione di un'autentica ed efficace Unione della sicurezza, del 29 giugno 2017, COM(2017) 354 final.

68 La convenzione è il primo trattato internazionale in materia di reati commessi tramite internet e altre reti informatiche, che tratta in particolare la violazione del diritto d'autore, le frodi informatiche, la pornografia infantile e le violazioni della sicurezza di rete. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Nel 2017 55 governi avevano ratificato o aderito alla convenzione del Consiglio d'Europa sulla criminalità informatica.

69 Mandato per l'elaborazione di un progetto di secondo protocollo aggiuntivo alla convenzione di Budapest sulla criminalità informatica, T-CY (2017)3.

70 La darknet è composta da contenuti su reti overlay che utilizzano internet ma richiedono software, configurazioni o autorizzazioni di accesso specifici. La darknet rappresenta una piccola parte del deep web, la parte del web non indicizzata da motori di ricerca.

71 Un'eccezione rilevante è la recente chiusura di due dei più grandi mercati criminali del dark web, AlphaBaye e Hansa: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

valutare le minacce e aiutare a determinare la giurisdizione e dare priorità a casi a rischio elevato; l'UE può svolgere un ruolo motore nel coordinamento dell'azione internazionale[72].

Un crescente settore di attività cibercriminali è l'uso fraudolento dei dati di carte di credito o altri mezzi elettronici di pagamento. Le credenziali di pagamento ottenute attraverso ciberattacchi diretti a siti di commercio elettronico o altre imprese legittime sono quindi commercializzate online e possono essere utilizzate da criminali per commettere frodi[73]. La Commissione sta presentando una proposta per accrescere la deterrenza attraverso una **direttiva relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti**[74]. Tale direttiva mira ad aggiornare le norme esistenti in questo settore e rafforzare la capacità delle autorità di contrasto di affrontare questa forma di criminalità.

Devono essere migliorate anche le capacità di indagine sulla cibercriminalità di cui dispongono le autorità di contrasto degli Stati membri, così come la comprensione dei reati favoriti dalla cibernetica e delle piste di indagine a disposizione di polizia e magistratura. Eurojust ed Europol contribuiscono a tale obiettivo e ad un maggior coordinamento, in stretta collaborazione con gruppi consultivi specializzati all'interno del centro per la lotta alla criminalità informatica di Europol e con le reti dei responsabili delle unità di lotta alla cibercriminalità e dei servizi di contrasto specializzati in cibercriminalità. La Commissione destinerà un finanziamento da 10,5 milioni di euro alla lotta contro la cibercriminalità, principalmente nell'ambito del **Fondo sicurezza interna – Polizia**. La formazione è un elemento importante e il Gruppo europeo di formazione e istruzione in materia di criminalità informatica ha redatto diversi materiali utili che adesso dovrebbero essere ampiamente diffusi per i professionisti delle autorità di contrasto con il sostegno dell'Agenzia dell'Unione europea per la formazione delle autorità di contrasto (CEPOL).

3.3 Cooperazione pubblico-privato contro la cibercriminalità

L'efficacia dei tradizionali meccanismi di contrasto è messa a dura prova dalle caratteristiche del mondo digitale, che consiste principalmente in infrastrutture di proprietà privata e molti operatori diversi in numerose giurisdizioni. Di conseguenza per le autorità pubbliche la cooperazione con il settore privato, anche con l'industria e la società civile, è fondamentale per combattere efficacemente la criminalità. In tale contesto anche il settore finanziario è fondamentale e la collaborazione dovrebbe essere intensificata. Dovrebbe per esempio essere rafforzato il ruolo delle unità di informazione finanziaria[75] nel contesto della cibercriminalità.

Alcuni Stati membri hanno già intrapreso iniziative fondamentali. Nei Paesi Bassi gli enti finanziari e le autorità di contrasto lavorano fianco a fianco sul problema delle frodi online e della cibercriminalità nella task force per la criminalità elettronica. Il centro di competenza tedesco contro la cibercriminalità rappresenta per i suoi membri il polo operativo in cui

[72] Europol riveste già un ruolo importante in questo ambito. Per un esempio recente si veda: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[73] I proventi di frodi sono un'importante fonte di reddito per la criminalità organizzata e costituiscono pertanto un fattore chiave per altre attività criminali come il terrorismo, il traffico di stupefacenti e la tratta di esseri umani.

[74] COM(2017) 489.

[75] Le unità di informazione finanziaria fungono da centri nazionali per la ricezione e l'analisi di segnalazioni di operazioni sospette e altre informazioni riguardanti il riciclaggio di denaro, reati base associati e il finanziamento del terrorismo, nonché per la diffusione dei risultati di tale analisi.

scambiare informazioni in stretta collaborazione con l'ufficio federale di polizia tedesco ed elaborare misure di protezione dalla cibercriminalità. 16 Stati membri[76] hanno creato centri di eccellenza contro la cibercriminalità volti a facilitare la cooperazione tra autorità di contrasto, mondo accademico e partner privati per l'elaborazione e lo scambio di migliori prassi, la formazione e la creazione di capacità.
La Commissione sostiene l'instaurazione di partenariati pubblico-privato e di meccanismi di cooperazione attraverso progetti dedicati come l'Online Fraud Cyber Centre and Experts Network[77], che attua un modello e uno standard di condivisione delle informazioni al fine di analizzare e attenuare i rischi di reati elettronici e le frodi online.

Nel contesto della cibercriminalità le imprese private devono essere in grado di condividere con le autorità di contrasto informazioni riguardanti incidenti concreti – compresi i dati personali – nel pieno rispetto delle norme in materia di protezione dei dati. La riforma della protezione dei dati dell'UE, che entrerà in vigore nel maggio 2018, prevede una serie di norme comuni che stabiliscono le condizioni in cui le autorità di contrasto e i soggetti privati possono collaborare. La Commissione europea collaborerà con il comitato europeo per la protezione dei dati e le parti interessate al fine di identificare le migliori prassi in questo settore e, se del caso, impartire orientamenti.

3.4 Intensificazione della risposta politica

Il **quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose**[78] ("pacchetto di strumenti della diplomazia informatica") approvato di recente stabilisce le misure da varare nell'ambito della politica estera e di sicurezza comune, comprese misure restrittive utilizzabili per rafforzare la risposta dell'UE ad attività che ne danneggiano gli interessi politici, di sicurezza ed economici. Il quadro costituisce un passo importante nello sviluppo di capacità di segnalazione e reazione a livello dell'UE e degli Stati membri. Aumenterà la nostra capacità di attribuire a un dato soggetto le attività informatiche dolose, allo scopo di influenzare il comportamento di potenziali aggressori, tenendo conto nel contempo della necessità di assicurare risposte proporzionate. L'attribuzione ad un attore statale o non statale rimane una decisione politica sovrana basata su informazioni provenienti da molteplici fonti. Il lavoro di attuazione sul quadro è attualmente in corso con gli Stati membri e verrebbe anche portato avanti in stretta collaborazione con il programma per una risposta ai ciberincidenti su larga scala[79]. La conoscenza situazionale necessaria per l'adozione di misure all'interno del quadro dovrebbe essere fusa, analizzata e condivisa da INTCEN[80], collaborando strettamente con gli Stati membri e le istituzioni dell'Unione.

3.5 Creazione di deterrenza di cibersicurezza attraverso la capacità di difesa degli Stati membri

Gli stati membri sviluppano già capacità di ciberdifesa. Inoltre, visto il labile confine tra la ciberdifesa e la cibersicurezza e il duplice uso degli strumenti e delle tecnologie cibernetiche,

---

[76] Austria, Belgio, Bulgaria, Cipro, Estonia, Francia, Germania, Grecia, Irlanda, Lituania, Polonia, Repubblica ceca, Regno Unito, Romania, Slovenia e Spagna .

[77] L'iniziativa EU-OF2CEN ambisce a consentire la condivisione sistematica a livello dell'UE delle informazioni riguardanti frodi su internet tra le banche e i servizi di contrasto per prevenire i pagamenti agli autori di frodi e a prestaconto e indagare e perseguire i perpetratori coinvolti. È cofinanziata dall'UE (Fondo sicurezza interna - Polizia).

[78] http://www.consilium.europa.eu/it/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

[79] C(2017) 6100.

[80] JOIN(2016) 018 final.

al pari della considerevole varietà di approccio tra gli Stati membri, l'UE è in una buona posizione per contribuire a promuovere sinergie tra gli sforzi militari e civili[81].

Gli Stati membri che hanno capacità di cibersicurezza più avanzate e intendono metterle in comune potrebbero prendere in considerazione, con il supporto dell'Alta rappresentante, della Commissione e dell'Agenzia europea per la difesa, di includere la ciberdifesa nel quadro di una "cooperazione strutturata permanente" (PESCO). Questo potrebbe essere sostenuto dal citato lavoro per incoraggiare le capacità industriali e l'autonomia strategica dell'UE. L'Unione europea può inoltre promuovere l'interoperabilità, anche facilitando lo sviluppo di capacità, il coordinamento di formazione e istruzione e gli sforzi di normazione del duplice uso.

Il quadro congiunto andrebbe altresì usato appieno al fine di rispondere alle minacce ibride, che spesso comprendono ciberattacchi, in particolare attraverso la cellula dell'UE per l'analisi delle minacce ibride e il centro europeo per la lotta contro le minacce ibride recentemente istituito a Helsinki, la cui missione consiste nell'incoraggiare il dialogo strategico e nel condurre ricerche e analisi.

L'UE darà nuova enfasi al quadro strategico dell'UE in materia di ciberdifesa del 2014[82] come strumento per integrare ulteriormente la cibersicurezza e la difesa nella politica di sicurezza e di difesa comune (PSDC). La ciberresilienza delle missioni e delle operazioni della PSDC sono di per sé essenziali: saranno sviluppate procedure standardizzate e capacità tecniche che potrebbero sostenere missioni e operazioni sia civili che militari e le rispettive strutture di capacità di pianificazione e condotta e i fornitori di servizi di tecnologia dell'informazione del SEAE. Al fine di far progredire la cooperazione fra gli Stati membri e orientare meglio gli sforzi dell'UE in quest'ambito, l'Agenzia europea per la difesa e il SEAE, in collaborazione con i servizi della Commissione, faciliteranno i contatti a livello strategico tra i responsabili delle politiche di ciberdifesa degli Stati membri. L'UE sosterrà inoltre lo sviluppo di soluzioni europee di cibersicurezza nell'ambito dell'impegno a favore di una base tecnologica e industriale europea di difesa. Questo include anche la promozione di cluster regionali di eccellenza nella cibersicurezza e nella difesa.

I servizi della Commissione, lavorando in stretta collaborazione con il SEAE, gli Stati membri e gli altri organismi competenti dell'UE, predisporranno entro il 2018 una **piattaforma di formazione ed istruzione in materia di ciberdifesa**, che integrerà il lavoro dell'Agenzia europea per la difesa in questo campo contribuendo a colmare l'attuale deficit di competenze nella cibersicurezza e nella ciberdifesa.

Azioni chiave

- Iniziativa della Commissione per l'accesso transfrontaliero alle prove elettroniche (inizio 2018)
- Rapida adozione da parte del Parlamento europeo e del Consiglio della proposta di direttiva relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti
- Introduzione dell'obbligo del protocollo IPv6 nel finanziamento di appalti, ricerche e progetti dell'UE; accordi volontari tra gli Stati membri e i fornitori di servizi internet per promuovere la diffusione del protocollo IPv6

[81] L'UE considera il ciberspazio un campo di operazioni come la terra, l'aria e il mare. Gli interventi di ciberdifesa includono altresì la protezione e la resilienza dei sistemi spaziali e dell'infrastruttura terreste correlata.

[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

- Nuova/maggiore enfasi in Europol sull'informatica forense e sul monitoraggio della darknet
- Attuazione del quadro per una risposta diplomatica congiunta dell'UE alle attività informatiche dolose
- Maggiore sostegno finanziario a progetti nazionali e transnazionali che promuovano la giustizia penale nel ciberspazio
- Varo nel 2018 di una piattaforma di istruzione relativa alla cibersicurezza per colmare l'attuale deficit di competenze in cibersicurezza e in ciberdifesa

4. RAFFORZAMENTO DELLA COOPERAZIONE INTERNAZIONALE IN MATERIA DI CIBERSICUREZZA

Guidata dai valori e dai diritti fondamentali dell'UE come la libertà di espressione e il diritto alla privacy e alla protezione dei dati personali, e dalla promozione di un ciberspazio aperto, libero e sicuro, la politica di cibersicurezza internazionale dell'UE intende affrontare la sfida in continua evoluzione di promuovere la stabilità cibernetica globale e di contribuire all'autonomia strategica dell'Europa nel ciberspazio.

4.1 Cibersicurezza nelle relazioni esterne

I dati indicano che in tutto il mondo le persone ravvisano nei ciberattacchi provenienti da altri paesi le principali minacce alla sicurezza nazionale[83]. Vista la natura globale della minaccia, instaurare e mantenere solide alleanze e partenariati con paesi terzi è fondamentale ai fini della prevenzione e della deterrenza dei ciberattacchi, che hanno un ruolo sempre più centrale nella stabilità e nella sicurezza internazionali. L'UE darà priorità all'istituzione di un quadro strategico di prevenzione dei conflitti e stabilità nel ciberspazio nelle attività bilaterali, regionali e multilaterali.

L'UE promuove fortemente la posizione secondo cui nel ciberspazio si applica il diritto internazionale, e in particolare la Carta delle Nazioni Unite. Ad integrazione delle norme vincolanti di diritto internazionale, l'UE approva le norme, le regole e i principi non vincolanti e volontari di comportamento responsabile dello Stato articolati dal gruppo di esperti governativi delle Nazioni Unite[84]; incoraggia inoltre l'elaborazione e l'attuazione di misure regionali di creazione della fiducia, sia nell'Organizzazione per la sicurezza e la cooperazione in Europa sia in altre regioni.

A livello bilaterale, saranno ulteriormente sviluppati i ciberdialoghi[85], che verranno integrati da sforzi volti a facilitare la cooperazione con i paesi terzi al fine di rafforzare i principi di diligenza dovuta e responsabilità dello Stato nel ciberspazio. Nelle attività internazionali l'UE darà la priorità alle questioni legate alla sicurezza internazionale nel ciberspazio, assicurando nel contempo che la cibersicurezza non diventi un pretesto per proteggere il mercato e limitare i diritti e le libertà fondamentali, compresa la libertà di espressione e di accesso alle informazioni. Un approccio completo alla cibersicurezza richiede il rispetto dei diritti umani, e l'UE continuerà a difendere i propri valori fondamentali nel mondo basandosi sui propri orientamenti in materia di diritti umani sulla libertà online[86]. A tale riguardo l'UE pone

[83] Spring 2017 Global Attitudes Survey, Pew Research Centre.
[84] A/68/98 e A/70/174.
[85] A settembre 2017 l'UE ha tenuto ciberdialoghi con gli Stati Uniti d'America, la Cina, il Giappone, la Repubblica di Corea e l'India.
[86] Orientamenti dell'UE in materia di diritti umani per la libertà di espressione online e offline.

l'enfasi sull'importanza del coinvolgimento di tutte le parti interessate nella governance di Internet.

La Commissione ha inoltre avanzato una proposta[87] per modernizzare i controlli delle esportazioni dell'UE, compresa l'introduzione di controlli sull'esportazione di tecnologie critiche di sorveglianza cibernetica che potrebbero essere all'origine di violazioni dei diritti umani o usate impropriamente contro la sicurezza dell'UE stessa, e intensificherà il dialogo con i paesi terzi ai fini della promozione della convergenza globale e di un comportamento responsabile in questo settore.

4.2 Creazione di capacità di cibersicurezza

La stabilità cibernetica globale dipende dalla capacità locale e nazionale di tutti i paesi di prevenire e reagire ai ciberincidenti e di investigare e perseguire i fatti di cibercriminalità. Sostenere gli sforzi volti a creare una resilienza nazionale nei paesi terzi aumenterà il livello di cibersicurezza a livello globale, con conseguenze positive per l'Unione. Il contrasto di minacce cibernetiche in rapida evoluzione indica la necessità di impegnarsi per lo sviluppo di formazione, politiche e normativa, nonché squadre di pronto intervento informatico e unità contro la cibercriminalità efficienti in tutti i paesi del mondo.

Dal 2013 l'UE svolge un ruolo motore nella creazione della capacità di cibersicurezza internazionale e nel collegamento sistematico di tale impegno con la cooperazione allo sviluppo. L'UE continuerà a promuovere un modello di creazione di capacità basato sui diritti, in linea con l'approccio Digital4Development[88]. Le priorità per la creazione di capacità saranno il vicinato dell'UE e i paesi in via di sviluppo che conoscono una connettività in rapida crescita e una rapida evoluzione delle minacce. L'impegno dell'Unione sarà complementare all'agenda per lo sviluppo dell'UE, alla luce dell'Agenda 2030 per lo sviluppo sostenibile, e agli sforzi complessivi per la creazione di capacità istituzionale.

Per migliorare la capacità dell'UE di mobilitare la sua competenza collettiva a supporto di tale creazione di capacità, dovrebbe essere istituita una rete specifica di sviluppo della capacità cibernetica dell'UE cui partecipino il SEAE, le autorità degli Stati membri competenti del ciberspazio, agenzie dell'UE, servizi della Commissione, mondo accademico e società civile. Saranno elaborati orientamenti sullo sviluppo della capacità cibernetica dell'UE, in modo da contribuire ad offrire orientamenti politici migliori e a stabilire le priorità per le attività dell'UE di assistenza ai paesi terzi.

L'Unione collaborerà inoltre con altri donatori in questo settore per evitare duplicazioni degli sforzi e per facilitare una creazione delle capacità più mirata in diverse regioni.

4.3 Cooperazione UE-NATO

Basandosi sui progressi sostanziali già compiuti, l'UE approfondirà la cooperazione con la NATO in materia di cibersicurezza, minacce ibride e difesa, come previsto nella dichiarazione congiunta dell'8 luglio 2016[89]. Tra le priorità rientrano la promozione dell'interoperabilità attraverso obblighi e norme coerenti di ciberdifesa, il rafforzamento della cooperazione in materia di formazione ed esercitazioni, l'armonizzazione dei requisiti formativi.

L'UE e la NATO promuoveranno inoltre la cooperazione nella ricerca e nell'innovazione in materia di ciberdifesa, muovendo dall'attuale accordo tecnico sullo scambio di informazioni

[87] COM(2016) 616.
[88] SWD(2017) 157.
[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.

di cibersicurezza tra i rispettivi organi responsabili della cibersicurezza[90]. Le recenti iniziative congiunte di contrasto delle minacce ibride, in particolare la cooperazione tra la cellula dell'UE per l'analisi delle minacce ibride e la sezione della NATO per l'analisi delle minacce ibride, dovrebbero essere sfruttate ulteriormente per rafforzare la resilienza e la risposta alle crisi cibernetiche. Un'ulteriore cooperazione tra l'UE e la NATO sarà promossa tramite esercitazioni di ciberdifesa, con il coinvolgimento del SEAE e altri organi dell'UE e gli omologhi della NATO, incluso il Centro di eccellenza per la ciberdifesa cooperativa della NATO di Tallinn. Per la prima volta la NATO e l'UE condurranno esercitazioni parallele e coordinate in risposta a uno scenario ibrido in cui la NATO assumerà la guida nel 2017 e l'UE nel 2018. La prossima relazione sulla cooperazione UE-NATO, che sarà presentata al rispettivo Consiglio nel dicembre 2017, offrirà l'occasione di prendere in considerazione le possibilità di ulteriore espansione della cooperazione, in particolare tramite mezzi di comunicazione comuni, sicuri e solidi tra tutte le istituzioni e gli organismi coinvolti, compresa l'ENISA.

Azioni chiave

- Portare avanti il quadro strategico per la prevenzione dei conflitti e la stabilità nel ciberspazio
- Sviluppare una nuova rete di creazione di capacità per sostenere i paesi terzi nella capacità di affrontare le ciberminacce e stabilire orientamenti per la creazione della capacità cibernetica dell'UE per stabilire la priorità delle iniziative dell'UE
- Portare avanti la cooperazione tra UE e NATO, compresa la partecipazione ad esercitazioni parallele e coordinate e una maggiore interoperabilità delle norme di cibersicurezza.

5. CONCLUSIONI

La preparazione cibernetica dell'UE è centrale sia per il mercato unico digitale che per la nostra Unione della sicurezza e della difesa. È imperativo aumentare la cibersicurezza e far fronte alle minacce nei confronti degli obiettivi sia civili che militari.

L'imminente summit digitale organizzato dalla Presidenza estone per il 29 settembre 2017 rappresenta un'opportunità per mostrare la determinazione comune di mettere la cibersicurezza al centro dell'UE nella sua dimensione di società digitale. Nell'ambito di tale impegno comune la Commissione chiede agli Stati membri di dichiarare come intendano agire nei settori in cui hanno la responsabilità principale. Questo dovrebbe includere il rafforzamento della cibersicurezza nelle seguenti modalità:

- garantendo la piena ed effettiva attuazione della direttiva NIS entro il 9 maggio 2018, nonché le risorse necessarie perché le autorità pubbliche responsabili della cibersicurezza svolgano efficacemente i loro compiti;
- applicando le stesse norme alle amministrazioni pubbliche, visto il ruolo che ricoprono nella società e nell'economia nel loro complesso;
- impartendo formazione sulla cibersicurezza nella pubblica amministrazione;
- dando la priorità alla consapevolezza cibernetica nelle campagne informative e inserendo la cibersicurezza nei piani formativi della formazione accademica e professionalizzante;
- sostenendo lo sviluppo di progetti di ciberdifesa tramite iniziative di "cooperazione strutturata permanente" (PESCO) e il Fondo europeo per la difesa.

[90] CERT-EU e NATO Computer Incident Response Capability (NCIRC).

La presente comunicazione congiunta ha esposto l'entità della sfida e la gamma di misure che l'UE può adottare. Ci serve un'Europa che sia resiliente, che possa proteggere la sua popolazione in modo efficace anticipando i possibili incidenti di cibersicurezza, costruendo una forte barriera protezione nelle sue strutture e nei suoi comportamenti, riprendendosi rapidamente dagli eventuali ciberattacchi e opponendo deterrenti a coloro che se ne rendono responsabili. La presente comunicazione propone misure mirate che rafforzeranno ulteriormente le strutture e le capacità di cibersicurezza dell'UE in modo coordinato, con la piena cooperazione degli Stati membri e delle diverse strutture dell'UE interessate e nel rispetto delle rispettive competenze e responsabilità. La sua attuazione darà una chiara dimostrazione del fatto che l'UE e gli Stati membri collaboreranno al fine di stabilire uno standard di cibersicurezza consono alle sfide sempre più acute cui l'Europa deve oggi far fronte.