Consiglio dell'Unione europea

Bruxelles, 19 novembre 2018
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
in data:	19 novembre 2018
Destinatario:	delegazioni
Oggetto:	Quadro strategico dell'UE in materia di ciberdifesa (aggiornamento 2018)

Si allega per le delegazioni il quadro strategico dell'UE in materia di ciberdifesa (aggiornamento 2018), adottato dal Consiglio nella 3652ª sessione del 19 novembre 2018.

ALLEGATO

QUADRO STRATEGICO DELL'UE IN MATERIA DI CIBERDIFESA

(AGGIORNATO NEL 2018)

Ambito di applicazione e obiettivi

Per rispondere alle mutevoli sfide in materia di sicurezza, l'UE e i suoi Stati membri devono rafforzare la ciberresilienza e sviluppare solide capacità di cibersicurezza e ciberdifesa.

Il quadro strategico dell'UE in materia di ciberdifesa sostiene lo sviluppo delle capacità di ciberdifesa degli Stati membri dell'UE come pure il rafforzamento della ciberprotezione dell'infrastruttura di sicurezza e difesa dell'UE, fatte salve le legislazioni nazionali degli Stati membri e la legislazione dell'UE, incluso, laddove definito, l'ambito di applicazione della ciberdifesa.

Il ciberspazio è il quinto dominio operativo che si affianca a quello terrestre, marittimo, aereo e spaziale. L'efficace attuazione delle missioni e operazioni dell'UE dipende sempre più da un accesso ininterrotto a un ciberspazio sicuro e richiede pertanto capacità operative informatiche solide e resilienti.

Obiettivo dell'aggiornato quadro strategico in materia di ciberdifesa è sviluppare ulteriormente la politica di ciberdifesa dell'UE tenendo conto degli opportuni sviluppi in altre sedi e settori pertinenti nonché dell'attuazione del suddetto quadro dal 2014. Il quadro strategico individua i settori prioritari per la ciberdifesa e chiarisce il ruolo dei vari attori europei, nel pieno rispetto delle responsabilità e delle competenze degli attori dell'Unione e degli Stati membri come pure del quadro istituzionale dell'UE e della sua autonomia decisionale.

Contesto

Nelle conclusioni del Consiglio europeo di dicembre 2013 sulla PSDC e in quelle del Consiglio di novembre 2013 sulla PSDC si chiedeva lo sviluppo di un quadro strategico dell'UE in materia di ciberdifesa, basato su una proposta dell'alto rappresentante, in cooperazione con la Commissione europea e l'Agenzia europea per la difesa (AED). Il quadro strategico dell'UE in materia di ciberdifesa è stato adottato dal Consiglio il 18 novembre 2014[1] e da allora, attraverso la sua attuazione, risultati concreti hanno contribuito a rafforzare in modo significativo le capacità di ciberdifesa degli Stati membri. Nell'ambito della relazione annuale 2017 sull'attuazione del quadro strategico in materia di ciberdifesa[2] e tenuto conto delle iniziative dell'UE nel settore della sicurezza e della difesa, segnatamente la revisione coordinata annuale sulla difesa (CARD), la cooperazione strutturata permanente (PESCO), il Fondo europeo per la difesa e il patto sulla dimensione civile della PSDC, come pure la revisione 2018 del piano di sviluppo delle capacità (CDP) e del piano di sviluppo delle capacità civili, gli Stati membri hanno chiesto un aggiornamento del quadro strategico dell'UE in materia di ciberdifesa.

La cibersicurezza è una priorità della strategia globale per la politica estera e di sicurezza dell'Unione europea, come pure del livello di ambizione dell'UE[3]. La strategia globale pone l'accento sulla necessità di accrescere le capacità di proteggere l'UE e i suoi cittadini e di rispondere alle crisi esterne, nonché di rafforzare l'UE in quanto comunità di sicurezza. In questo contesto gli sforzi in materia di sicurezza e difesa dovrebbero inoltre rafforzare il ruolo strategico dell'UE e la sua capacità di agire autonomamente, se e quando necessario, e con i partner, quando possibile. Detti obiettivi richiedono una maggiore cooperazione nello sviluppo di capacità che promuoverà l'efficacia e l'interoperabilità delle capacità civili e militari che ne derivano.

---

1 Documento del Consiglio 15585/14, 18.11.2014.
2 Documento del Consiglio 15870/17, 19.12.2017.
3 Conclusioni del Consiglio sull'attuazione della strategia globale dell'UE nel settore della sicurezza e della difesa, 14.11.2016.

L'insieme comune di proposte per l'attuazione della dichiarazione congiunta del presidente del Consiglio europeo, del presidente della Commissione europea e del Segretario generale dell'Organizzazione del Trattato del Nord Atlantico, firmata a Varsavia l'8 luglio 2016,[4] contiene azioni concrete per accrescere la cooperazione tra l'UE e la NATO in materia di cibersicurezza e ciberdifesa, anche nell'ambito delle missioni e operazioni, nonché in materia di sviluppo di capacità di ciberdifesa, ricerca e tecnologia, formazione, istruzione, esercitazioni e integrazione degli aspetti informatici nella gestione delle crisi. Tale cooperazione avviene nel pieno rispetto dei principi di apertura, trasparenza, inclusività, reciprocità e autonomia decisionale dell'UE. Un accordo tecnico tra la squadra di pronto intervento informatico dell'Unione europea (CERT-UE) e la capacità NATO di reazione a incidenti informatici (NCIRC), siglato nel febbraio 2016, sta facilitando la condivisione di informazioni tecniche per migliorare la prevenzione, l'individuazione e la risposta ai ciberincidenti in ambo le organizzazioni.

È opportuno ricordare che alcune politiche dell'UE contribuiscono agli obiettivi della politica di ciberdifesa di cui al presente documento. Questo quadro strategico tiene conto inoltre delle normative, delle politiche e del supporto tecnologico pertinenti in ambito civile. Nel luglio 2016 ad esempio il Parlamento europeo e il Consiglio hanno adottato la direttiva sulla sicurezza delle reti e dell'informazione[5] (NIS), che accrescerà il grado di preparazione generale degli Stati membri in caso di minacce informatiche e rafforzerà la cooperazione a livello dell'UE. La direttiva stabilisce misure volte a conseguire un livello comune elevato di sicurezza della rete e dei sistemi informativi nell'Unione così da migliorare il funzionamento del mercato interno. Il termine per il recepimento della direttiva scadeva il 9 maggio 2018.

---

4 Conclusioni del Consiglio sull'attuazione della dichiarazione congiunta del presidente del Consiglio europeo, del presidente della Commissione europea e del Segretario generale dell'Organizzazione del Trattato del Nord Atlantico (6 dicembre 2016, doc. 15283/16; 5 dicembre 2017, doc. 14802/17).

5 Direttiva (UE) 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, GU L 194 del 19.7.2016, pag. 1.

La proposta di regolamento UE sulla cibersicurezza, presentata nel settembre 2017, include il nuovo mandato dell'agenzia dell'UE per la cibersicurezza (ENISA) nonché l'istituzione di un quadro europeo di certificazione. Una volta instaurato, il quadro di certificazione dovrebbe supportare standard elevati relativi a processi, prodotti e servizi TIC, oltre a essere fonte di vantaggi competitivi e accrescere la fiducia di consumatori e acquirenti. La Commissione ha inoltre adottato un altro provvedimento nel settembre 2017 per preparare l'UE all'eventualità di un incidente transfrontaliero su vasta scala in materia di cibersicurezza (il "piano") e sta attualmente lavorando con gli Stati membri e altri organismi, istituzioni e agenzie allo sviluppo di un quadro europeo di cooperazione in caso di crisi di cibersicurezza, procedendo alla messa in pratica e alla documentazione relativa a tutti gli attori, processi e procedure pertinenti nell'ambito degli attuali meccanismi dell'UE di gestione delle crisi e delle catastrofi, in particolare i dispositivi integrati dell'UE per la risposta politica alle crisi.

Le conclusioni del Consiglio di novembre 2016 su come rafforzare il sistema di resilienza informatica dell'Europa delineavano l'obiettivo comune di contribuire, anche nel ciberspazio, all'autonomia strategica dell'UE, come indicato nelle conclusioni del Consiglio di novembre 2016 sulla strategia globale per la politica estera e di sicurezza dell'Unione europea. Il Consiglio europeo ha ribadito questo messaggio nel giugno 2018 e ha altresì sottolineato la necessità di rafforzare le capacità di combattere le minacce alla cibersicurezza provenienti dall'esterno dell'UE.

Nel 2017 il Consiglio ha adottato un quadro relativo a una risposta diplomatica comune dell'UE alle attività informatiche dolose (il "pacchetto di strumenti della diplomazia informatica")[6]. Il quadro dovrebbe incoraggiare la cooperazione, facilitare la riduzione delle minacce e influenzare il comportamento dei potenziali aggressori sul lungo periodo. Esso si avvale delle misure in ambito PESC, comprese le misure restrittive, per prevenire e rispondere alle attività informatiche dolose. I soggetti che compiono attività informatiche dolose devono rendere conto delle proprie azioni e gli Stati membri dell'UE sono incoraggiati a sviluppare ulteriormente la propria capacità di rispondere ad attività informatiche dolose in modo coordinato e in linea con il pacchetto di strumenti della diplomazia informatica. Gli Stati non dovrebbero portare avanti o sostenere consapevolmente attività nell'ambito delle tecnologie dell'informazione e della comunicazione che siano contrarie ai loro obblighi a norma del diritto internazionale; inoltre, non dovrebbero consentire consapevolmente l'utilizzo dei rispettivi territori per atti illeciti a livello internazionale compiuti mediante l'uso delle tecnologie dell'informazione e della comunicazione.

Nel settembre 2017 la Commissione e l'AR/VP hanno presentato una comunicazione congiunta[7] in ambito di cibersicurezza volta a mitigare i rischi derivanti dalle nuove minacce. Il testo include la ciberdifesa fra le principali aree di azione e il quadro strategico dell'UE in materia di ciberdifesa rappresenta uno dei pilastri della sua concreta attuazione[8].

Nelle conclusioni del Consiglio di novembre 2017 sulle questioni in materia di cibersicurezza vengono riconosciuti i crescenti legami tra cibersicurezza e difesa e viene chiesto di rafforzare la cooperazione in materia di ciberdifesa, anche promuovendo la cooperazione tra le comunità incaricate della risposta agli incidenti civili e militari. Viene inoltre sottolineato che un incidente o una crisi cibernetica particolarmente grave potrebbe costituire una motivazione sufficiente perché uno Stato membro invochi la clausola di solidarietà e/o la clausola di assistenza reciproca dell'UE.

---

6 Conclusioni del Consiglio su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica"), doc. 9916/17, 7 giugno 2017.

7 Comunicazione congiunta al Parlamento europeo e al Consiglio: Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE (13 settembre 2017, JOIN(2017) 450 final).

8 Conclusioni del Consiglio sulla comunicazione congiunta al Parlamento europeo e al Consiglio: Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE (20 novembre 2017, doc. 14435/17).

L'11 dicembre 2017 è stata avviata la cooperazione strutturata permanente (PESCO). Questo quadro di cooperazione ambizioso, vincolante e inclusivo è stato stabilito fra 25 Stati membri e prevede l'impegno a intensificare gli sforzi di cooperazione in materia di ciberdifesa nonché i relativi progetti in ambito PESCO. Il primo insieme di progetti individuato dagli Stati membri partecipanti alla PESCO nel 2017 comprende due progetti relativi alla ciberdifesa: i "gruppi di risposta rapida agli incidenti informatici e mutua assistenza in materia di cibersicurezza" e la "piattaforma per la condivisione delle informazioni in materia di minaccia informatica e di risposta agli incidenti informatici". Sono previsti ulteriori insiemi di progetti in ambito PESCO. La PESCO svilupperà capacità di ciberdifesa e rafforzerà dunque la cooperazione tra gli Stati membri partecipanti, oltre ad accrescere l'interoperabilità.

Il piano di sviluppo delle capacità dell'UE aggiornato (CDP), approvato dal comitato direttivo dell'AED nel giugno 2018, definisce la ciberdifesa quale elemento chiave, riconoscendo la necessità di operazioni informatiche di natura difensiva in qualsiasi contesto operativo sulla base di sofisticate conoscenze situazionali attuali e predittive nell'ambito del ciberspazio, compresa la capacità di combinare grandi quantità di dati e intelligence da numerose fonti per contribuire a un rapido processo decisionale e a una maggiore automazione della raccolta e dell'analisi dei dati nonché delle procedure di supporto alla presa di decisioni. Il CDP 2018 individua le priorità in termini di capacità di ciberdifesa nei seguenti settori: cooperazione e sinergie con i pertinenti attori nell'ambito della ciberdifesa e della cibersicurezza; attività di ricerca e tecnologia in materia di ciberdifesa; quadri di ingegneria dei sistemi per le operazioni informatiche; istruzione, formazione, esercitazioni e valutazione (ETEE); risposta alle sfide in materia di ciberdifesa nel dominio aereo, spaziale, marittimo e terrestre.

Infine, negli ultimi anni è emersa chiaramente la necessità che la comunità internazionale prevenga conflitti, cooperi e stabilizzi il ciberspazio. L'UE promuove, in stretta cooperazione con altre organizzazioni internazionali, in particolare le Nazioni Unite, l'OSCE e il Forum regionale dell'ASEAN, un quadro strategico per la prevenzione dei conflitti, la cooperazione e la stabilità nel ciberspazio, che comprende i) l'applicazione del diritto internazionale, in particolare della Carta delle Nazioni Unite in tutti i suoi elementi, nel ciberspazio; ii) il rispetto delle norme, delle regole e dei principi universali non vincolanti per un comportamento responsabile da parte degli Stati; iii) lo sviluppo e l'attuazione di misure regionali di rafforzamento della fiducia (CBM). Il quadro strategico in materia di ciberdifesa dovrebbe sostenere anche questo sforzo.

Priorità

Nell'ambito dell'aggiornamento del quadro strategico dell'UE in materia di ciberdifesa sono state individuate sei priorità. Uno degli obiettivi principali di tale quadro strategico è lo sviluppo di capacità di ciberdifesa, nonché la protezione delle reti di comunicazione e informazione UE PSDC. Tra gli altri settori prioritari si annoverano la formazione e le esercitazioni, la ricerca e la tecnologia, la cooperazione civile-militare e la cooperazione internazionale. Nel campo della formazione, si pone l'accento sul potenziamento della formazione in materia di ciberdifesa rivolta agli Stati membri e della formazione in materia di consapevolezza cibernetica rivolta alla catena di comando PSDC. È inoltre importante che la dimensione cibernetica sia adeguatamente trattata nelle esercitazioni allo scopo di rafforzare la capacità dell'UE di reagire a crisi cibernetiche e ibride, migliorando le procedure decisionali e la disponibilità delle informazioni. Il ciberspazio è un ambito in rapida evoluzione ed è necessario sostenere i nuovi sviluppi tecnologici in ambito sia civile che militare. La cooperazione civile-militare nel settore informatico è essenziale per assicurare una risposta coerente alle minacce informatiche. Non da ultimo, il rafforzamento della cooperazione con i partner internazionali potrebbe contribuire a rafforzare la cibersicurezza all'interno e all'esterno dell'UE, nonché a promuovere i principi e i valori dell'UE.

Il presente quadro delinea le proposte e le opportunità di coordinamento fra i pertinenti organismi, istituzioni e agenzie dell'UE e riflette l'importante ruolo svolto dal settore privato nello sviluppo di tecnologie per la cibersicurezza e la ciberdifesa.

Inoltre, il quadro strategico in materia di ciberdifesa sostiene l'integrazione della cibersicurezza nei meccanismi dell'Unione di gestione delle crisi, nel contesto dei quali, per affrontare gli effetti di una crisi cibernetica, possono essere d'applicazione le pertinenti disposizioni del trattato sull'Unione europea e del trattato sul funzionamento dell'Unione europea[9].

1. Sostegno allo sviluppo delle capacità di ciberdifesa degli Stati membri

Lo sviluppo delle capacità e delle tecnologie di ciberdifesa dovrebbe abbracciare tutti gli aspetti dello sviluppo di capacità, inclusi dottrina, leadership, organizzazione, personale, formazione, industria, tecnologia, infrastruttura, logistica e interoperabilità. A tal fine, gli Stati membri dovrebbero intensificare i loro sforzi per conseguire una capacità effettiva di ciberdifesa. Il SEAE, la Commissione e l'AED dovrebbero collaborare e sostenere tali sforzi.

La valutazione costante delle vulnerabilità delle infrastrutture d'informazione a sostegno delle missioni ed operazioni PSDC risulta necessaria, insieme con una conoscenza quasi in tempo reale dell'efficacia della protezione. Dal punto di vista operativo, uno dei principali ambiti delle attività di ciberdifesa cui prestare attenzione sarà il mantenimento della disponibilità, dell'integrità e della riservatezza delle reti di comunicazione e informazione PSDC, salvo se altrimenti specificato nel mandato dell'operazione o della missione in causa. In aggiunta, il SEAE, in collaborazione con gli Stati membri, intensificherà l'integrazione di capacità in ambito informatico nelle missioni e operazioni PSDC.

I soggetti che compiono attività informatiche dolose devono rendere conto delle proprie azioni. È importante che gli Stati membri, con il sostegno del SEAE, favoriscano la cooperazione reciproca per rispondere alle attività informatiche dolose. Lo sviluppo del pacchetto di strumenti della diplomazia informatica mira a contribuire a raggiungere tale risposta comune. Sulla base del pacchetto di strumenti della diplomazia informatica, il SEAE e l'AED organizzeranno esercitazioni periodiche in cui gli Stati membri dell'UE potranno mettere in pratica tale aspetto.

---

[9] Articolo 222 del TFUE e articolo 42, paragrafo 7, del TUE, tenuto in debita considerazione l'articolo 17 del TUE.

Considerando che nella legislazione nazionale degli Stati membri e nella legislazione dell'UE l'ambito di applicazione della ciberdifesa, ove e quando definito, è ampio e diversificato, è necessario sviluppare una visione aggregata comune in merito all'ambito di applicazione della ciberdifesa.

Dal momento che le operazioni militari PSDC fanno affidamento sull'infrastruttura di C4 (comando, controllo, telecomunicazioni ed informatica) messa a disposizione dagli Stati membri, è necessario un certo grado di convergenza strategica nella pianificazione dei requisiti di ciberdifesa per l'infrastruttura d'informazione.

Basandosi sui lavori della squadra di progetto dell'AED per la ciberdifesa per lo sviluppo delle capacità di ciberdifesa, l'AED e gli Stati membri:

- ricorreranno al CDP e ad altri strumenti, quali la CARD, che agevolano e sostengono la cooperazione tra Stati membri allo scopo di migliorare il grado di convergenza nella pianificazione dei requisiti di ciberdifesa degli Stati membri a livello strategico, segnatamente per quanto riguarda: monitoraggio, conoscenza situazionale, prevenzione, individuazione e protezione, scambio di informazioni, capacità d'analisi in campo forense e di software dannosi (malware), insegnamenti tratti, limitazione dei danni, capacità di ripresa dinamica, archiviazione distribuita dei dati e back-up dei dati;
- sosterranno i progetti, attuali e futuri, di messa in comune e condivisione connessi con la ciberdifesa per le operazioni militari (ad es. in campo forense, di sviluppo dell'interoperabilità e di definizione delle norme);
- svilupperanno una serie standard di obiettivi e requisiti che definiscano il livello minimo di cibersicurezza e di fiducia che gli Stati membri devono raggiungere, basandosi sulle esperienze maturate a livello di UE.

Il SEAE e l'AED:

- faciliteranno gli scambi tra Stati membri relativamente alle dottrine nazionali in materia di ciberdifesa, nonché ai programmi di reclutamento, mantenimento in servizio e riserve di personale orientati alla ciberdifesa.

L'AED:

- esaminerà i diversi ambiti di applicazione dei requisiti militari in materia di ciberdifesa nelle legislazioni nazionali e nelle migliori prassi degli Stati membri. Il principale obiettivo dello studio sarà lo sviluppo di un'architettura d'impresa per la ciberdifesa al fine di includere l'ambito di applicazione, le funzionalità e i requisiti al riguardo impiegati dagli Stati membri sulla base della legislazione nazionale e dell'UE.

Su base volontaria, gli Stati membri:

- miglioreranno la cooperazione tra le CERT militari allo scopo di rendere più efficace la prevenzione e il trattamento degli incidenti;
- si avvarranno della PESCO per rafforzare ulteriormente la cooperazione in materia di ciberdifesa, compresi nuovi progetti;
- si avvarranno del Fondo europeo per la difesa per sviluppare congiuntamente capacità di ciberdifesa;
- svilupperanno una visione comune sull'applicazione della clausola di assistenza reciproca nel settore informatico, preservandone nel contempo la flessibilità;
- elaboreranno requisiti di base in materia di ciberdifesa per l'infrastruttura d'informazione;
- nella misura in cui il miglioramento delle capacità di ciberdifesa dipende dalle competenze civili nel campo della sicurezza delle reti e dell'informazione, si avvarranno dell'assistenza dell'ENISA, delle autorità degli Stati membri riunite nel gruppo di cooperazione NIS e di altre eventuali entità a livello dell'UE con competenze in materia di cibersicurezza civile.

Gli Stati membri, il SEAE/Stato maggiore dell'UE, l'AESD e l'AED:

- prenderanno in esame la possibilità di predisporre formazioni in materia di ciberdifesa, nella prospettiva di una certificazione dei gruppi tattici dell'UE.

La Commissione, in collaborazione con gli Stati membri:

- terrà in considerazione la ciberdifesa nei programmi di lavoro del programma europeo di sviluppo del settore industriale della difesa e del Fondo europeo per la difesa.

2. Rafforzamento della protezione dei sistemi di comunicazione e informazione PSDC utilizzati da entità dell'UE

Fatto salvo il ruolo della squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie europee (CERT-UE) quale struttura di coordinamento centrale della risposta a incidenti informatici per tutte le istituzioni, organi e agenzie dell'Unione e nel quadro delle regole applicabili del bilancio dell'Unione, il SEAE elaborerà una definizione adeguata e autonoma degli aspetti attinenti alla difesa della sicurezza e delle reti e svilupperà la propria capacità in termini di sicurezza TI. Essa mirerà a migliorare la resilienza delle reti SEAE in ambito PSDC, incentrandosi in particolare su prevenzione, individuazione, risposta agli incidenti, conoscenza situazionale, scambio di informazioni e meccanismi di allarme rapido.

La protezione dei sistemi di comunicazione e informazione del SEAE e lo sviluppo delle capacità in materia di sicurezza della tecnologia dell'informazione (TI) sono responsabilità della direzione generale del bilancio e dell'amministrazione (BA) del SEAE. Lo Stato maggiore dell'Unione europea (EUMS), la direzione gestione delle crisi e pianificazione (CMPD) e la capacità civile di pianificazione e condotta (CPCC) renderanno inoltre disponibili ulteriori risorse dedicate e sostegno. La capacità di sicurezza TI contemplerà sistemi sia classificati che non classificati e formerà parte integrante delle entità operative attuali.

È anche necessario snellire le regole di sicurezza per i sistemi d'informazione forniti dai diversi attori istituzionali dell'UE durante la condotta di missioni e operazioni PSDC. In questo contesto, si potrebbe prendere in considerazione una catena di comando unificata con l'obiettivo di migliorare la resilienza delle reti usate per la PSDC.

Per un migliore coordinamento e per rafforzare la protezione e la resilienza dei sistemi e delle reti di comunicazione e informazione PSDC, nel 2017 è stato creato in seno al SEAE un comitato di governance informatica facente capo al Segretario generale del SEAE.

Il SEAE/BA:

- rafforzerà la capacità di sicurezza TI all'interno del SEAE, sulla base delle capacità e procedure tecniche esistenti, con particolare attenzione a prevenzione, individuazione, risposta agli incidenti, conoscenza situazionale, scambio di informazioni e meccanismi di allarme rapido. Sarà potenziata ulteriormente una strategia di cooperazione con la CERT-UE e le capacità di cibersicurezza dell'UE esistenti.

Il SEAE/BA, congiuntamente all'EUMS, all'MPCC, alla CMPD e alla CPCC:

- svilupperanno strategie e orientamenti coerenti in materia di sicurezza TI, prendendo anche in considerazione i requisiti tecnici per la ciberdifesa di strutture, missioni e operazioni nel contesto PSDC, tenendo presenti i quadri e le politiche di cooperazione vigenti in ambito UE allo scopo di raggiungere la convergenza di norme, politiche e organizzazione.

Il SEAE/Capacità unica di analisi dell'intelligence (SIAC):

- basandosi sulle strutture esistenti, rafforzerà la sua valutazione della ciberminaccia e la capacità d'intelligence nell'ottica di individuare nuovi ciberrischi e fornire periodiche valutazioni del rischio sulla base di una valutazione strategica della minaccia e di informazioni quasi in tempo reale sugli incidenti coordinate tra le pertinenti strutture dell'UE e rese accessibili a diversi livelli di classificazione.

Il SEAE/SIAC e la CERT-UE:

- promuoveranno lo scambio di informazioni in tempo reale tra gli Stati membri e le pertinenti entità UE sulla ciberminaccia. A tale scopo, saranno sviluppati, tra le pertinenti autorità nazionali ed europee, attraverso un approccio volontario basato sulla cooperazione già esistente, meccanismi per lo scambio di informazioni e misure volte a rafforzare la fiducia.

Il SEAE/EUMS e l'MPCC:

- svilupperanno ulteriormente e integreranno, nella pianificazione a livello strategico, un concetto di ciberdifesa per le missioni e operazioni militari PSDC;
- svilupperanno, in cooperazione con il comando operativo, una procedura operativa standard generica in ambito informatico a livello operativo.

Il SEAE/CPCC e la CMPD:

- svilupperanno ulteriormente e integreranno, nella pianificazione strategica, un concetto di ciberdifesa per le missioni civili PSDC;
- rafforzeranno le capacità di ciberdifesa delle missioni civili PSDC basandosi sulle infrastrutture esistenti e promuovendo la normalizzazione e l'armonizzazione delle tecnologie utilizzate nelle missioni e operazioni PSDC, avvalendosi, se del caso, delle competenze della CERT-UE, dell'ENISA e dell'AED;
- nel processo di rafforzamento della dimensione civile della PSDC, esamineranno ulteriormente la possibilità di un sostegno alle nazioni ospitanti in fatto di cibersicurezza mediante le missioni civili PSDC.

Il SEAE:

- svilupperà ulteriormente i requisiti comuni per le missioni e le operazioni militari e civili PSDC;
- rafforzerà il coordinamento della ciberdifesa allo scopo di realizzare gli obiettivi connessi con la protezione delle reti usate dagli attori istituzionali UE che supportano la PSDC, basandosi sulle esperienze già maturate a livello dell'UE;
- esaminerà periodicamente i requisiti in termini di risorse e altre decisioni strategiche in materia sulla scorta dell'evoluzione dello scenario della minaccia, in consultazione con gli Stati membri e altre istituzioni dell'UE.

3. Promozione della cooperazione civile-militare

Il ciberspazio è un ambito in rapida evoluzione: è necessario che gli sviluppi tecnologici siano rafforzati da sistemi di sicurezza, sia in ambito civile che militare. Nella misura del possibile, è opportuno prevedere il coordinamento tra gli ambiti civile e militare nei casi in cui sviluppi tecnologici analoghi possano apportare soluzioni per applicazioni sia civili che militari. In altri casi le capacità militari e i sistemi d'arma sono talmente specifici che non è possibile applicarli alle tecnologie civili. Fatte salve l'organizzazione e la legislazione interne degli Stati membri, la cooperazione civile-militare nel ciberdominio può essere presa in considerazione ad esempio ai fini dello scambio di migliori prassi, dei meccanismi per lo scambio di informazioni e di allarme rapido, delle valutazioni dei rischi in materia di risposta in caso d'incidente, delle iniziative di sensibilizzazione nonché delle attività di formazione e delle esercitazioni.

Il miglioramento della cibersicurezza civile è un fattore importante che contribuisce alla resilienza complessiva della sicurezza delle reti e dell'informazione. La direttiva NIS aumenta il grado di preparazione a livello nazionale e rafforza la cooperazione tra Stati membri a livello dell'Unione sia sotto il profilo strategico che operativo. La cooperazione coinvolge le autorità nazionali preposte alla supervisione delle politiche in materia di cibersicurezza, come pure le CERT nazionali e la CERT-UE. La cooperazione tra le CERT civili e militari dovrebbe essere rafforzata tenendo in debita considerazione tali sviluppi. Il nuovo regolamento europeo sulla cibersicurezza è volto a migliorare la resilienza dell'Europa ai ciberattacchi e a instaurare un quadro per la certificazione della cibersicurezza di prodotti e servizi al fine di accrescere la fiducia negli aspetti civili della sfera digitale.

L'AED, l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA), il Centro europeo per la lotta alla criminalità informatica (EC3) e la CERT-UE, insieme ad altri pertinenti organi e agenzie dell'UE, nell'ambito dei rispettivi mandati e senza sovrapporsi alle competenze degli Stati membri, nonché gli Stati membri, sono incoraggiati a rafforzare la cooperazione nei settori seguenti:

- sviluppo di profili di competenza comuni in materia di cibersicurezza e ciberdifesa sulla base delle migliori prassi internazionali e della certificazione usata dalle istituzioni, organi e organismi dell'UE, tenendo conto anche delle norme di certificazione del settore privato;
- contributo all'ulteriore sviluppo e all'adattamento delle norme tecniche e organizzative del settore pubblico in materia di cibersicurezza e ciberdifesa per l'uso nel settore della sicurezza e della difesa. Ove necessario prendere le mosse dai lavori in corso di ENISA ed AED;
- creazione o sviluppo ulteriore di meccanismi e modalità di lavoro per scambiare le migliori prassi in particolare in materia di istruzione, formazione ed esercitazioni nonché della ricerca e sviluppo e in altri settori di possibile sinergia civile-militare;
- messa a frutto delle esperienze esistenti nell'UE nel campo della prevenzione, delle indagini e delle capacità forensi in ordine alla cibercriminalità e relativo uso rafforzato nello sviluppo di capacità di ciberdifesa.

Su base volontaria, gli Stati membri:

- rafforzano la cooperazione tra le CERT civili e militari degli Stati membri.

Il SEAE, la Commissione e gli Stati membri:

- includono la ciberdifesa nelle procedure dell'UE di gestione delle crisi e delle catastrofi (tramite il "piano").

4. Ricerca e tecnologia

Gli operatori dell'infrastruttura e dei servizi TIC (Tecnologie dell'informazione e della comunicazione) per finalità civili e di difesa sono confrontati a problematiche di cibersicurezza simili, a motivo di requisiti di capacità tecnologici ed operativi comuni. Le esigenze R&T comuni e i requisiti comuni per i sistemi sono previsti in anticipo per migliorare l'interoperabilità dei sistemi nel lungo periodo come pure per ridurre i costi dello sviluppo di soluzioni. Realizzare economie di scala è necessario per far fronte al numero crescente di minacce e vulnerabilità, il che faciliterà d'altra parte la salvaguardia e la crescita di un'industria europea della ciberdifesa competitiva.

Lo sviluppo di capacità di ciberdifesa presenta un'importante dimensione R&T. Nel quadro dell'agenda per la ricerca in materia di ciberdifesa (*Cyber Defence Research Agenda* - CDRA) l'AED ha fornito una solida base per la fissazione delle priorità in ordine al futuro finanziamento R&T nell'ambito del quadro intergovernativo. La conseguente agenda strategica per la ricerca, sviluppata con il pertinente gruppo di lavoro ad hoc dell'AED, stabilisce con cognizione le priorità nell'ambito delle tecnologie informatiche necessarie in ambito militare, individuando nel contempo le opportunità per un duplice uso a livello di sforzi e investimenti indipendentemente dal contesto (nazionale, multinazionale o finanziato dall'UE).

È essenziale sviluppare in Europa capacità tecnologiche per mitigare le minacce e le vulnerabilità. L'industria resterà il motore primario per la tecnologia e l'innovazione connesse alla ciberdifesa. Tra i settori da approfondire figurano: crittografia, sistemi integrati sicuri, individuazione di software dannosi, tecniche di simulazione e visualizzazione, protezione delle reti e dei sistemi di comunicazione, tecnologie di identificazione e autenticazione. È altresì importante promuovere in Europa una catena di approvvigionamento industriale competitiva sotto il profilo della cibersicurezza sostenendo il coinvolgimento delle piccole e medie imprese (PMI).

Fare in modo che l'Europa possa stare al passo dei concorrenti internazionali per quanto riguarda le capacità tecnologiche in ambito informatico dipende anche dalla nostra capacità di stimolare l'innovazione pionieristica con strumenti nazionali e dell'UE, come il Consiglio europeo per l'innovazione.

Per agevolare la cooperazione civile-militare nello sviluppo delle capacità di ciberdifesa, rafforzare la base industriale e tecnologica di difesa europea[10] e contribuire all'autonomia strategica dell'UE anche nel settore del ciberspazio, ove e quando necessario e insieme a partner ogniqualvolta sia possibile,

l'AED, la Commissione e gli Stati membri:

- ricercheranno sinergie degli sforzi R&T nel settore militare con i programmi civili di ricerca e sviluppo, in particolare quelli relativi all'innovazione pionieristica, e prenderanno in considerazione la dimensione di cibersicurezza e ciberdifesa nell'attuazione dell'azione preparatoria sulla ricerca connessa con la difesa;
- metteranno in comune le agende per la ricerca sulla cibersicurezza (ad esempio l'agenda strategica per la ricerca sulla cibersicurezza dell'Agenzia europea per la difesa) e condivideranno le tabelle di marcia e le azioni che ne deriveranno; a tal fine sarà sviluppata un'agenda per la ricerca intersettoriale in materia di ciberdifesa in stretta cooperazione con la Commissione e gli Stati membri;
- contribuiranno a migliorare l'integrazione delle dimensioni di cibersicurezza e ciberdifesa nei programmi con una dimensione di sicurezza e di difesa a duplice uso, ad esempio il programma di ricerca sulla gestione del traffico aereo nel cielo unico europeo (SESAR).

[10] Comunicazione "Verso un settore della difesa e della sicurezza più concorrenziale ed efficiente", COM (2013) 542.

La Commissione intende:

- prendere in considerazione la creazione di un centro europeo di competenza per l'industria, la tecnologia e la ricerca nel settore della cibersicurezza con una rete di centri nazionali di coordinamento per sostenere le capacità tecnologiche e industriali di cibersicurezza e per aumentare la competitività dell'industria della cibersicurezza dell'Unione, assicurando la complementarietà ed evitando duplicazioni con la rete dei centri di competenza sulla cibersicurezza e con altre agenzie dell'UE. Tra l'altro, il centro dovrebbe promuovere la cooperazione tra le applicazioni e le tecnologie civili e di difesa, lavorando a stretto contatto e in piena complementarità con l'Agenzia europea per la difesa nel settore della ciberdifesa;
- sostenere lo sviluppo di ecosistemi industriali e poli di innovazione che abbracciano l'intera catena di valore nel settore della sicurezza attingendo alle conoscenze del mondo accademico, all'innovazione nelle PMI e alla produzione industriale.

La Commissione, in collaborazione con gli Stati membri, intende:

- includere le questioni di ciberdifesa negli inviti a presentare proposte dell'azione preparatoria sulla ricerca connessa con la difesa;
- includere la ciberdifesa nei punti oggetto di inviti a presentare proposte nell'ambito del Fondo europeo per la difesa;
- sostenere la coerenza strategica dell'UE per assicurare che gli aspetti strategici e tecnici della ciberprotezione dell'UE restino al primo posto dell'innovazione tecnologica e siano armonizzati in tutta l'UE (capacità di analisi e valutazione della ciberminaccia, iniziative "sicurezza fin dalla progettazione", gestione delle dipendenze per l'accesso alla tecnologia, ecc.).

5. Miglioramento delle opportunità di formazione, istruzione ed esercitazione

Onde aumentare il grado di preparazione per far fronte alle ciberminacce e sviluppare una cultura comune di ciberdifesa in tutta l'UE, anche a vantaggio delle missioni e delle operazioni dell'UE, occorre migliorare le opportunità di formazione in ordine alla ciberdifesa. È fondamentale che i bilanci per l'istruzione e la formazione siano usati con efficienza offrendo nel contempo la massima qualità possibile. Saranno di importanza cruciale la messa in comune e la condivisione dell'istruzione e della formazione in ciberdifesa a livello europeo.

L'Accademia europea per la sicurezza e la difesa (AESD), il SEAE, l'AED, la Commissione e gli Stati membri:

- sulla base dell'analisi dei bisogni formativi in ciberdifesa dell'AED e delle esperienze acquisite dall'AESD nella formazione in cibersicurezza, approntеranno interventi di formazione e istruzione in materia PSDC per pubblici diversi, tra cui il SEAE, il personale delle missioni e delle operazioni PSDC e i funzionari degli Stati membri, che dovrebbero anche affrontare i problemi di mantenimento del personale qualificato sul breve, medio e lungo periodo;
- proporranno l'avvio di un dialogo in materia di ciberdifesa sugli standard e la certificazione della formazione da portare avanti con gli Stati membri, le istituzioni dell'UE, i paesi terzi e altre organizzazioni internazionali, nonché il settore privato;
- collaboreranno con i formatori del settore privato europeo, nonché con le istituzioni accademiche, per aumentare competenze e conoscenze specialistiche del personale impegnato in missioni e operazioni PSDC.

L'AESD:

- svilupperà ulteriormente la piattaforma informatica in materia di istruzione, formazione, valutazione ed esercitazioni costituita in seno all'AESD (piattaforma informatica ETEE);
- creerà sinergie con i programmi di formazione di altri soggetti interessati, ad esempio ENISA, Europol, Accademia europea di polizia (CEPOL) e Centro di eccellenza per la ciberdifesa cooperativa della NATO;
- vaglierà la possibilità di svolgere programmi di formazione congiunti AESD-NATO in materia di ciberdifesa aperti a tutti gli Stati membri dell'UE allo scopo di promuovere una cultura di ciberdifesa condivisa.

La Commissione:

- valuterà le opzioni per aumentare le possibilità di formazione e di istruzione all'interno degli Stati membri individuate dalla piattaforma informatica ETEE.

L'AED:

- svilupperà ulteriormente i corsi AED, in collaborazione con l'AESD, per rispondere ai requisiti degli Stati membri relativamente a istruzione, formazione ed esercitazioni in materia di ciberdifesa;
- sosterrà la piattaforma informatica ETEE, tra l'altro integrando progressivamente i moduli di istruzione, formazione, valutazione ed esercitazioni informatiche sviluppati nel quadro dell'AED.

Il SEAE e gli Stati membri:

- seguiranno i meccanismi stabiliti di certificazione AESD per i programmi di formazione in stretta cooperazione con i servizi competenti nelle istituzioni, negli organismi e nelle agenzie dell'UE, sulla base degli standard e delle conoscenze esistenti; prenderanno in considerazione la definizione di moduli specifici di ciberdifesa nel quadro dell'iniziativa Erasmus militare.

Occorre migliorare le opportunità di esercitazione di ciberdifesa all'indirizzo degli attori PSDC militari e civili. Le esercitazioni congiunte fungono da strumento per sviluppare una comune conoscenza e visione della ciberdifesa. Le forze nazionali saranno così in grado di migliorare la prontezza ad operare in un contesto multinazionale. La condotta di esercitazioni di ciberdifesa comuni produrrà inoltre interoperabilità e creerà fiducia.

Il SEAE, l'AED, la CERT-UE e gli Stati membri si concentreranno sulla promozione degli elementi di ciberdifesa nelle esercitazioni in ambito PSDC e in altri ambiti:

- integrare la dimensione di ciberdifesa negli scenari di esercitazione esistenti per *MILEX* e *MULTILAYER*;
- organizzare periodicamente esercitazioni strategiche/politiche come *CYBRID 2017* in coordinamento con l'esercitazione parallela e coordinata (PACE) a guida UE, nonché esercitazioni tecnico-operative come *DEFNET*;
- sviluppare, se del caso, un'esercitazione di ciberdifesa dedicata UE PSDC e vagliare la possibilità di un eventuale coordinamento con esercitazioni paneuropee di cibersicurezza quali *Cyber Europe*, organizzate da ENISA;
- continuare a partecipare ad altre esercitazioni multinazionali di ciberdifesa come *Locked Shields*;
- invitare alle esercitazioni i pertinenti partner internazionali, ad esempio la NATO, in conformità del quadro politico dell'UE sulle esercitazioni;
- organizzare esercitazioni periodiche, sulla base del pacchetto di strumenti della diplomazia informatica, durante le quali gli Stati membri possano allenarsi a rispondere alle attività informatiche dolose.

6. Potenziamento della cooperazione con i pertinenti partner internazionali

Nel quadro della cooperazione internazionale occorre assicurare un dialogo con i partner internazionali, nello specifico la NATO e altre organizzazioni internazionali, al fine di contribuire allo sviluppo di effettive capacità di ciberdifesa. Si dovrebbe ricercare una maggiore corrispondenza con il lavoro svolto nel quadro dell'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE) e delle Nazioni Unite (ONU) al fine di proporre un quadro strategico per la prevenzione dei conflitti, la cooperazione e la stabilità nel ciberspazio.

Nell'UE esiste la volontà politica di cooperare maggiormente con la NATO in merito alla ciberdifesa nello sviluppo di capacità di ciberdifesa forti e resilienti, secondo quanto richiesto dalla dichiarazione congiunta del presidente del Consiglio europeo, del presidente della Commissione europea e del Segretario generale dell'Organizzazione del Trattato del Nord Atlantico, firmata a Varsavia l'8 luglio 2016. Consultazioni periodiche a livello di personale, briefing incrociati ed eventualmente riunioni del Gruppo politico-militare con i pertinenti comitati NATO contribuiranno ad evitare una duplicazione inutile e a garantire coerenza e complementarietà di sforzi, in linea con il quadro summenzionato.

Il SEAE e l'AED, insieme con gli Stati membri, svilupperanno ulteriormente la cooperazione in materia di ciberdifesa tra l'UE e la NATO, nel rispetto del quadro istituzionale e dell'autonomia decisionale di tali organizzazioni:

- intensificazione delle attività in corso nel quadro dell'attuazione della dichiarazione congiunta del presidente del Consiglio europeo, del presidente della Commissione europea e del Segretario generale dell'Organizzazione del Trattato del Nord Atlantico;
- scambio di migliori prassi nella gestione delle crisi e nella ciberdifesa delle missioni e operazioni militari e civili;
- lavoro sulla coerenza dei risultati nello sviluppo dei requisiti di capacità di ciberdifesa in caso di sovrapposizioni, in particolare nello sviluppo a lungo termine;
- ulteriore ricorso al quadro di cooperazione dell'AED con il Centro di eccellenza per la ciberdifesa cooperativa della NATO quale piattaforma iniziale per una maggiore collaborazione nei progetti multinazionali di ciberdifesa, sulla base di opportune valutazioni.

L'AESD, il SEAE e l'AED:

- coopereranno maggiormente sui concetti per la formazione e l'istruzione, nonché le esercitazioni, in materia di ciberdifesa;
- assicureranno la reciproca partecipazione del personale alle esercitazioni, in linea con il quadro concordato.

La CERT-UE:

- sfrutterà ulteriormente l'accordo tecnico concluso con la NCIRC (capacità NATO di reazione a incidenti informatici) allo scopo di migliorare la conoscenza situazionale, lo scambio di informazioni e i meccanismi di allarme rapido e anticipare le minacce che potrebbero colpire entrambe le organizzazioni.

Per quanto riguarda le altre organizzazioni internazionali e i pertinenti partner internazionali dell'UE, il SEAE e gli Stati membri, se del caso:

- seguiranno gli sviluppi strategici e terranno consultazioni sulle questioni relative alla ciberdifesa con i partner internazionali (organizzazioni internazionali e paesi terzi);
- vaglieranno le possibilità di cooperazione sulle questioni di ciberdifesa, anche con i paesi terzi che partecipano alle missioni e operazioni PSDC;
- promuoveranno, in seno alle pertinenti organizzazioni internazionali, in particolare l'ONU, l'OSCE e il Forum regionale dell'ASEAN, l'applicazione del diritto internazionale vigente, in particolare della Carta delle Nazioni Unite nella sua interezza, nel ciberspazio, lo sviluppo e l'attuazione di norme universali non vincolanti per un comportamento responsabile da parte degli Stati, nonché misure regionali di rafforzamento della fiducia (CBM) tra gli Stati al fine di aumentare la trasparenza e ridurre il rischio che il comportamento degli Stati sia frainteso.

La Commissione e il SEAE:

- se del caso, sosterranno lo sviluppo delle capacità dei partner dell'UE in ambito informatico attraverso lo strumento inteso a contribuire alla stabilità e alla pace (IcSP) modificato.

Seguito

Nell'ambito del coordinamento da parte del SEAE dell'attuazione del quadro strategico in materia di ciberdifesa, il SEAE, l'AED e la Commissione dovrebbero presentare al Gruppo politico-militare, con la partecipazione dei membri del Gruppo orizzontale "Questioni riguardanti il ciberspazio", e al comitato politico e di sicurezza una relazione annuale sullo stato di avanzamento dei lavori che comprenda i sei settori illustrati in precedenza, al fine di valutare l'attuazione di detto quadro strategico. Sarà inoltre effettuata una presentazione orale semestrale.

È fondamentale che all'evoluzione della ciberminaccia corrisponda l'individuazione di nuovi requisiti in materia di ciberdifesa, da includere successivamente nel quadro strategico in materia di ciberdifesa. La prossima revisione di tale quadro dovrebbe essere presentata entro la metà del 2022 in stretta consultazione con gli Stati membri.