



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

Bruxelles, 10.11.2022
JOIN(2022) 49 final

**COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL
CONSIGLIO**

La politica di ciberdifesa dell'UE

I. INTRODUZIONE

Il ritorno della guerra in Europa, con l'aggressione militare ingiustificata e non provocata della Russia contro l'Ucraina, è stato un campanello d'allarme per tutti coloro che mettono in discussione l'approccio dell'UE alla sicurezza e alla difesa, la sua capacità di promuovere la propria visione e di difendere i propri interessi, anche nel cibernazio. I regimi autoritari cercano di sfidare e minare l'ordine internazionale basato sulle regole nel cibernazio, trasformandolo in un contesto sempre più conteso al pari di terra, mare, aria e spazio. Negli ultimi anni si sono intensificati i comportamenti dolosi di soggetti statali e non statali nel cibernazio, compreso un numero crescente di attacchi informatici che hanno preso di mira infrastrutture critiche militari e civili sia nell'UE sia nel contesto delle missioni e operazioni dispiegate sul terreno.

I confini tra la dimensione civile e quella militare del cibernazio vanno sfumandosi, come dimostrano i recenti attacchi alle reti energetiche, alle infrastrutture di trasporto e alle risorse spaziali. Emerge l'interdipendenza tra infrastrutture fisiche e digitali e la possibilità che incidenti di cibersicurezza gravi possano perturbare o danneggiare le infrastrutture critiche. Si tratta di un forte richiamo del fatto che l'UE necessita di una stretta cooperazione militare e civile nel cibernazio per diventare un fornitore di sicurezza più forte.

L'UE deve assumersi maggiori responsabilità per la propria sicurezza. Ciò richiede forze armate europee moderne e interoperabili. Gli Stati membri devono quindi impegnarsi, urgentemente e in via prioritaria, ad aumentare gli investimenti nelle capacità di ciberdifesa a tutto spettro, comprese quelle attive. Pur mantenendo fermo l'impegno al rispetto del diritto e delle norme internazionali nel cibernazio, l'UE dovrebbe segnalare la volontà di utilizzare tali capacità in modo coordinato in caso di attacco informatico a uno Stato membro.

Per riuscire l'UE deve munirsi di una propria sovranità tecnologica e digitale nel settore informatico. La capacità d'azione dell'UE dipenderà dalla sua capacità di padroneggiare e sviluppare tecnologie all'avanguardia per la cibersicurezza e la ciberdifesa al suo interno. Poiché le cibertecnologie presentano un forte potenziale di duplice uso, le industrie e le attività di ricerca e sviluppo e di innovazione nel settore della cibersicurezza e della ciberdifesa devono lavorare in modo molto più sinergico per sviluppare capacità migliori.

La prevenzione e il rilevamento comuni costituiscono un aspetto importante delle capacità di difesa dell'Unione. L'UE deve essere in grado di rilevare gli attacchi nelle loro fasi iniziali. I dati di rilevamento devono essere trasformati in intelligence utilizzabile, che possa servire tanto per la cibersicurezza quanto per la ciberdifesa. La cooperazione tra le cybercomunità civili e della difesa è alla base di una migliore conoscenza situazionale comune nel cibernazio ed è altrettanto cruciale per una risposta coordinata alle crisi a livello tanto tecnico quanto operativo.

Il conflitto armato in Ucraina ha dimostrato altresì il valore di una stretta collaborazione con il settore privato e la necessità di avere accesso a fornitori privati di fiducia che agiscono come forza di riserva per la cibersicurezza per migliorare la risposta in caso di attacchi informatici gravi. Di conseguenza è necessario garantire che gli Stati membri possano fare affidamento sul sostegno di forze di riserva fidate per la cibersicurezza e che ciò avvenga in modo sicuro e coordinato.

La presente comunicazione congiunta, pur basandosi sul quadro strategico in materia di ciberdifesa¹, propone una strategia ambiziosa destinata a consentire all'UE e ai suoi Stati membri di agire con fiducia nelle proprie possibilità e con assertività nel cyberspazio. Mira a potenziare le capacità di ciberdifesa attraverso l'azione individuale o congiunta degli Stati membri nonché a rafforzare il coordinamento e la cooperazione tra le cibercomunità dell'UE. Agirà a sostegno della riduzione delle dipendenze strategiche dell'UE in relazione alle cibertecnologie critiche e rafforzerà la base industriale e tecnologica di difesa europea (EDTIB). La politica stabilirà le regole del gioco dell'UE e proporrà modalità per rafforzare nella ciberdifesa la solidarietà che sta al centro stesso dell'UE, nonché per cooperare con il settore privato al fine di migliorare la risposta in caso di attacchi informatici gravi. Data la transnazionalità delle minacce informatiche, svilupperà partenariati personalizzati e reciprocamente vantaggiosi nel settore della ciberdifesa, anche in relazione allo sviluppo di capacità di ciberdifesa, e migliorerà la ciberresilienza dei paesi partner.

Come proposto nella bussola strategica per la sicurezza e la difesa² adottata dal Consiglio nel marzo 2022, la presente politica di ciberdifesa rafforzerà quindi, utilizzando tutti i mezzi disponibili, la capacità di prevenzione, rilevamento, difesa, recupero e deterrenza in relazione ad attacchi informatici rivolti contro l'UE e i suoi Stati membri. Ciò è in linea con le priorità digitali della Commissione, con l'ambizione di cui alla strategia dell'UE in materia di cibersicurezza del 2020³, con l'annuncio della presidente von der Leyen nel discorso sullo stato dell'Unione del 2021⁴ e con le conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica⁵ del 23 maggio 2022. La comunicazione congiunta del 2022 sulle carenze di investimenti nel settore della difesa⁶ ha incoraggiato l'UE e gli Stati membri ad avviare i lavori per la creazione di una capacità di ciberdifesa a tutto spettro, dalla ricerca al rilevamento e alla protezione fino alla risposta.

II. CIBERDIFESA DELL'UE PER PROTEZIONE, RILEVAMENTO, DETERRENZA E DIFESA DAGLI ATTACCHI INFORMATICI

1. Intervenire insieme a rafforzamento della ciberdifesa

Gli attacchi informatici hanno spesso natura transfrontaliera e possono comportare ripercussioni fisiche su infrastrutture critiche nell'UE. Gli incidenti di cibersicurezza gravi possono avere effetti troppo perturbatori perché un singolo o più Stati membri colpiti possano gestirli da soli. Possono rientrare nel contesto di attacchi ibridi di portata più ampia condotti da paesi terzi con l'obiettivo di destabilizzare l'economia e la società, indebolire le infrastrutture critiche necessarie a garantire la sicurezza dell'UE oppure minare e danneggiare il funzionamento delle democrazie, anche attraverso attacchi alle infrastrutture elettorali.

¹ Quadro strategico dell'UE in materia di ciberdifesa (aggiornamento 2018), 19 novembre 2018, <https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/it/pdf>.

² [Una bussola strategica per la sicurezza e la difesa - Per un'Unione europea che protegge i suoi cittadini, i suoi valori e i suoi interessi e contribuisce alla pace e alla sicurezza internazionali.](#)

³ La strategia dell'UE in materia di cibersicurezza per il decennio digitale ([JOIN\(2020\) 18 final](#)).

⁴ https://ec.europa.eu/commission/presscorner/detail/it/SPEECH_21_4701.

⁵ [9364/22](#).

⁶ [JOIN\(2022\) 24 final](#).

Nel 2018 l'UE ha individuato il ciberspazio come dominio operativo militare. Il documento "Visione e strategia militari sul ciberspazio come dominio operativo"⁷, adottato nel 2021, stabilisce le condizioni quadro e descrive le finalità, le modalità e i mezzi necessari per utilizzare il ciberspazio come dominio operativo a sostegno delle operazioni della politica di sicurezza e di difesa comune (PSDC) dell'UE. La ciberdifesa e l'impiego delle capacità corrispondenti nell'intero spettro delle operazioni militari nel ciberspazio sono una prerogativa nazionale degli Stati membri, pur basandosi su un ecosistema più ampio che comprende una solida base industriale sostenuta dallo sviluppo di capacità a livello UE.

La comunità della ciberdifesa dell'UE, costituita da autorità della difesa degli Stati membri e sostenuta da istituzioni, organi e organismi dell'UE, presenta talune specificità rispetto alle altre cibercomunità⁸ e segue un modello di governance diverso. L'assenza di un quadro consolidato per lo scambio di informazioni e la cooperazione tra le squadre militari di pronto intervento informatico (milCERT) dell'UE, anche a sostegno delle missioni e operazioni militari della PSDC, risulta problematica in considerazione dell'accresciuto livello di minacce informatiche da parte di soggetti statali e non statali.

Tutti i soggetti interessati ricaveranno elevato valore aggiunto dalla cooperazione tra le cibercomunità delle sfere civile, diplomatica e di contrasto e le omologhe del settore della difesa. Fondamentale è quindi porre le condizioni abilitanti la collaborazione mettendo a disposizione mezzi idonei e sicuri per lo scambio di informazioni e organizzando esercitazioni e altre attività che creino fiducia e una visione comune.

Attualmente l'assistenza operativa reciproca tra gli Stati membri è limitata. Dovrebbe essere vagliata l'ipotesi di un'ulteriore espansione in tutta l'UE del concetto di gruppi di reazione rapida agli incidenti informatici, sulla base dei gruppi di risposta rapida agli incidenti informatici e mutua assistenza in materia di cibersicurezza (CRRT)⁹ del collegato progetto di cooperazione strutturata permanente (PESCO), anche nel contesto dell'articolo 42, paragrafo 7, del trattato sull'Unione europea (TUE)¹⁰ ("clausola di assistenza reciproca") e dell'articolo 222 del trattato sul funzionamento dell'Unione europea (TFUE)¹¹ ("clausola di solidarietà"). Analogamente, uno degli insegnamenti tratti dal successo della ciberdifesa ucraina nel contesto della guerra di aggressione della Russia è il ruolo decisivo svolto dal settore privato. È opportuno quindi vagliare in quale misura anche il settore privato possa contribuire a migliorare la risposta a incidenti informatici.

1.1 Rafforzare la conoscenza situazionale comune e il coordinamento all'interno della comunità della difesa

Data l'entità del rischio associato agli attacchi informatici, gli Stati membri devono disporre della più completa conoscenza situazionale collettiva, compresa la capacità di rilevamento precoce, nonché delle risorse per rispondere adeguatamente e recuperare in modo solidale e coordinato.

⁷ EEAS(2021) 706 REV4.

⁸ Cibercomunità delle sfere civile, diplomatica e di contrasto.

⁹ Gruppi di risposta rapida agli incidenti informatici e mutua assistenza in materia di cibersicurezza.

¹⁰ Trattato sull'Unione europea, versione consolidata (GU C 326 del 26.10.2012, pag. 1).

¹¹ Trattato sul funzionamento dell'Unione europea, versione consolidata (GU C 326 del 26.10.2012, pag. 1).

Per quanto riguarda la conoscenza situazionale militare, è necessario istituire un **centro di coordinamento della ciberdifesa dell'UE (EUCDCC)** che sostenga una maggiore conoscenza situazionale all'interno della comunità della difesa, di cui facciano parte tutti i comandanti militari UE della PSDC. L'alto rappresentante sottoporrà all'esame degli Stati membri la proposta di istituzione dell'EUCDCC, sulla base del progetto della PESCO relativo al centro di coordinamento nel settore informatico e dell'informazione (CIDCC)¹². L'obiettivo è fornire un'analisi olistica del ciber spazio, dell'ambiente elettromagnetico e del dominio cognitivo, riunendo diverse fonti di informazione a livello strategico e operativo militare. Dovrebbero essere stabiliti collegamenti adeguati tra l'EUCDCC e il Centro UE di situazione e di intelligence (INTCEN), nonché l'Intelligence dello Stato maggiore dell'UE, nel contesto del quadro della capacità unica di analisi dell'intelligence. Oltre alle fonti di informazione esterne, l'EUCDCC dovrebbe istituire e integrare un sistema indipendente di sensori informatici attivi per rafforzare il monitoraggio dei nodi di proprietà dell'UE che supportano missioni e operazioni militari della PSDC. Fornirà maggiori capacità di rilevamento e dovrebbe creare una nuova stratificazione di informazioni per migliorare ulteriormente la base informativa ai fini della valutazione dei rischi informatici e della conoscenza situazionale.

A tal fine sono necessarie capacità che consentano e assicurino la creazione e il mantenimento di un quadro del ciber spazio operativo 24 ore su 24, 7 giorni su 7 e, ove possibile, riconosciuto, comprese le operazioni informatiche in corso e imminenti tanto degli avversari quanto delle forze amiche. Tale quadro contribuirebbe alla pianificazione e alla conduzione di missioni e operazioni militari della PSDC dell'UE. Diventerà quindi il contributo militare destinato a rendere l'UE più consapevole e reattiva nei confronti di atti dolosi nel ciber spazio.

Per migliorare la fiducia e per scambiare informazioni strategiche attendibili e tempestive sui grandi incidenti informatici, sarà ulteriormente sviluppata e rafforzata la **conferenza dei comandanti per la sicurezza informatica dell'UE**¹³. Forte del supporto di segreteria dell'AED e della partecipazione dello Stato maggiore dell'UE, la conferenza si riunirà almeno due volte l'anno per discutere questioni operative e altri temi d'interesse.

Sarà creata una rete operativa per le **milCERT (MICNET)** con il sostegno dell'AED. Tutti gli Stati membri sono esortati a partecipare alla MICNET, che dovrebbe diventare operativa nel gennaio 2023.

Facilitando lo scambio di informazioni tra le milCERT, la MICNET promuoverà una risposta più solida e coordinata alle minacce informatiche che colpiscono sistemi di difesa nell'UE, compresi quelli impiegati nelle missioni e operazioni militari della PSDC. La MICNET consentirà di mantenere nel tempo i processi di formazione e l'individuazione continua di requisiti nuovi per la comunità delle milCERT. Nei prossimi quattro anni l'AED svilupperà, in collaborazione con gli Stati membri, un'infrastruttura di condivisione delle informazioni, con i collegati strumenti e procedure, al fine di sostenere la condivisione di informazioni tra le milCERT. La MICNET costituirà il quadro di un'esercitazione annuale per sottoporre a prova, convalidare e individuare requisiti e soluzioni nuovi.

¹² Il progetto mira a sviluppare, istituire e gestire un centro multinazionale di coordinamento nel settore informatico e dell'informazione (CIDCC) come elemento militare multinazionale permanente.

¹³ Sulla base dei primi due incontri delle conferenze dei comandanti per la sicurezza informatica dell'UE (CyberCo) tenutisi a gennaio e a giugno 2022, i comandanti per la sicurezza informatica dell'UE hanno deciso di istituire un forum permanente al loro livello.

1.2 Miglioramento del coordinamento con le comunità civili

La MICNET dovrebbe fungere da quadro e infrastruttura per la condivisione di informazioni tra i diversi livelli della comunità della ciberdifesa e i portatori di interessi esterni.

Via via che la MICNET raggiungerà un grado più avanzato di maturità, l'AED sosterrà gli Stati membri nel vagliare opzioni di collaborazione con la rete di **gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT)**, che riunisce i CSIRT nazionali e la squadra di pronto intervento informatico delle istituzioni, organi e organismi dell'Unione europea (CERT-UE). Tale collaborazione potrebbe contemplare riunioni ed esercitazioni congiunte. Dovrebbe essere vagliato il coinvolgimento del settore privato nelle attività di condivisione di informazioni e di risposta agli incidenti.

Ai fini di una maggiore efficienza nella gestione delle crisi informatiche, la conferenza dei comandanti per la sicurezza informatica dell'UE dovrebbe interagire con la rete europea delle organizzazioni di collegamento per le crisi informatiche (CyCLONe), che riunisce Stati membri e Commissione a sostegno del coordinamento e della gestione degli incidenti di cibersicurezza su vasta scala nell'UE. L'interazione combinerà esperienza militare e conoscenza situazionale civile a livello strategico e operativo.

Sebbene l'EUCDCC sia inteso come snodo di raccolta, analisi, valutazione e infine divulgazione di informazioni relative alla ciberdifesa, in particolare per le missioni e le operazioni militari della PSDC, è ipotizzabile anche un suo collegamento con la task force interistituzionale per le crisi informatiche¹⁴, istituita per garantire un processo decisionale informato e una risposta coordinata delle istituzioni, organi e organismi dell'UE alle grandi crisi informatiche a livello strategico e operativo.

L'EUCDCC può anche scambiare informazioni d'interesse con il centro di situazione e di analisi informatiche, attualmente in via di costituzione presso la Commissione, con il sostegno dell'ENISA e del CERT-UE, e incaricato di fornire analisi e un sostegno più efficace nella gestione delle crisi.

La mancanza di strumenti e piattaforme di comunicazione sicura da tutti condivisi o interoperabili tra gli Stati membri e le istituzioni, organi e organismi dell'UE competenti rimane un ostacolo importante. La Commissione e le istituzioni pertinenti stanno mappando gli strumenti di comunicazione sicura nel settore informatico esistenti. Basandosi su questa mappatura degli strumenti esistenti, a fine 2022 la Commissione presenterà raccomandazioni al Consiglio affinché siano decisi gli interventi futuri.

Cibersolidarietà dell'UE a sostegno di capacità di rilevamento comune e conoscenza situazionale più forti

Le azioni a sostegno di soggetti civili possono aumentare ulteriormente la conoscenza situazionale comune. La comunità della ciberdifesa potrà trarre beneficio dalle maggiori

¹⁴ Gruppo informale che comprende i servizi competenti della Commissione, il servizio europeo per l'azione esterna (SEAE), l'agenzia dell'Unione europea per la cibersicurezza (ENISA), il CERT-UE ed Europol, copresieduto da Commissione e alto rappresentante.

capacità di rilevamento e di conoscenza situazionale sviluppate nel settore civile per la protezione delle infrastrutture critiche dell'UE. A tal fine la Commissione prepara un'iniziativa volta a promuovere la realizzazione di un'infrastruttura unionale dei centri operativi di sicurezza (SOC). Questa prima fase, che partirà nelle prossime settimane, sarà poi ampliata e dispiegata su più vasta scala¹⁵, con il fine ultimo di istituire varie piattaforme multinazionali dei SOC, raggruppanti ciascuna SOC nazionali, con l'ausilio del programma Europa digitale¹⁶ a integrazione dei finanziamenti nazionali. Una modifica legislativa del programma Europa digitale consentirebbe di sostenere finanziariamente a più lungo termine gli appalti congiunti di strumenti e infrastrutture ultrasicuri di prossima generazione. La prospettata infrastruttura dei SOC dell'UE sarebbe così in grado di migliorare le capacità collettive di rilevamento valendosi delle più moderne forme di intelligenza artificiale e analisi dei dati, con copertura delle reti di comunicazione civili. Grazie a questa generazione di intelligence sulle minacce informatiche attivabile sarebbe possibile allertare tempestivamente autorità e soggetti d'interesse così che siano in grado di rilevare gli incidenti gravi e rispondervi efficacemente. Scala e copertura dell'infrastruttura dipenderanno dai finanziamenti complessivi mobilitabili a livello nazionale e, subordinatamente al bilancio disponibile nell'ambito del quadro finanziario pluriennale, a livello di Unione.

Tali SOC multinazionali potrebbero altresì consentire la partecipazione di soggetti del settore della difesa, istituendo un "pilastro della difesa" in termini di governance e di tipo di informazioni condivise. Il "pilastro della difesa" sarebbe sviluppato in collaborazione con l'alto rappresentante e potrebbe prevedere un meccanismo dedicato per lo scambio di informazioni con i soggetti militari, compreso l'EUCDCC, per il quale potrebbero essere sviluppate norme di sicurezza a livello di difesa.

La cibersolidarietà dell'UE nella preparazione, nella risposta e nel recupero

Gli incidenti di cibersicurezza gravi hanno spesso effetti troppo perturbatori perché un singolo Stato membro o più Stati membri colpiti possano gestirli da soli. In tali casi gli Stati membri devono poter ricorrere all'assistenza e alla solidarietà reciproche, anche nel contesto dell'articolo 42, paragrafo 7, TUE e dell'articolo 222 TFUE. L'alto rappresentante vaglierà, in collaborazione con la Commissione e gli Stati membri, le possibilità di **espansione del concetto di gruppi di reazione rapida agli incidenti informatici (CRRT)**, sulla base del collegato progetto CRRT della PESCO, al fine di sostenere meglio gli Stati membri dell'UE nonché le missioni e le operazioni della PSDC. Il ruolo di tali gruppi sarebbe quello di fornire un'assistenza a breve termine mirata e personalizzata, su richiesta e in base alle esigenze specifiche di ciascun caso. Potrebbe includere altresì, se pertinente, opzioni di sostegno da parte di partner privati di fiducia al fine di garantire efficienza nelle azioni di risposta e recupero.

Nel contesto dell'iniziativa dell'UE per la cibersolidarietà, la Commissione sta preparando azioni destinate a rafforzare l'opera di preparazione e risposta in tutta l'UE, anche tramite la **sperimentazione di soggetti essenziali che presiedono all'esercizio di infrastrutture critiche per individuare le potenziali vulnerabilità sulla scorta di valutazioni del rischio**

¹⁵ La strategia dell'UE in materia di cibersicurezza per il decennio digitale, (JOIN(2020) 18 final) e la strategia dell'UE per l'Unione della sicurezza (COM(2020) 605 final).

¹⁶ Conformemente al regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio, del 29 aprile 2021, che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240 (GU L 166 dell'11.5.2021, pag. 1), fatte salve possibili modifiche.

effettuate a livello UE, muovendo dalle iniziative già avviate dalla Commissione insieme all'ENISA, e tramite azioni di risposta agli incidenti per attutire l'impatto degli incidenti gravi, aiutare un recupero immediato e/o ripristinare il funzionamento dei servizi essenziali¹⁷.

L'iniziativa dell'UE per la cibersolidarietà potrebbe sostenere la **costituzione graduale di una forza di riserva per la cibersicurezza a livello di UE, con servizi prestati da operatori privati di fiducia**, pronta a intervenire su richiesta degli Stati membri in caso di incidenti transfrontalieri rilevanti. Si dovrebbero indicare chiaramente ruoli e responsabilità in totale coordinamento con gli organismi esistenti, così che il sostegno della riserva per la cibersicurezza a livello di UE si diriga laddove necessario e integri altre potenziali forme di assistenza. Sebbene la sfera d'azione e la ripartizione dei costi degli interventi specifici dipendano dalla disponibilità di finanziamenti unionali, la stessa disponibilità e preparazione della riserva a livello di UE apporterebbe già valore aggiunto. Per garantire un livello elevato di fiducia, la Commissione vaglierà anche le possibilità di sostegno allo sviluppo di sistemi di certificazione di cibersicurezza per tali imprese private.

Le esercitazioni costituiscono un aspetto chiave dello sviluppo della preparazione, in quanto promuovono lo sviluppo di una base di conoscenze e di una visione comuni della ciberdifesa, che a loro volta migliorano la preparazione operativa. Le esercitazioni comuni in materia di ciberdifesa svilupperanno altresì interoperabilità e fiducia tra i portatori di interessi, anche al fine di sostenere le missioni e le operazioni militari della PSDC. Sulla base della serie CYBER PHALANX¹⁸ e delle esercitazioni delle milCERT, l'**AED istituirà un nuovo progetto CyDef-X, che riunirà tutti gli Stati membri e servirà di quadro di riferimento per le esercitazioni dell'UE in materia di ciberdifesa**. Il progetto potrebbe servire per esercitazioni sull'assistenza reciproca in virtù dell'articolo 42, paragrafo 7, TUE. Si dovrebbe vagliare l'uso di ambienti di prova, addestramento ed esercitazioni dedicati alla ciberdifesa (ad esempio il Poligono virtuale federato), anche attraverso il ricorso al progetto del Poligono virtuale federato della PESCO¹⁹.

Le esercitazioni possono svolgere un ruolo importante per migliorare la cooperazione tra soggetti civili e militari. Nell'organizzare le esercitazioni, l'ENISA, l'AED e gli altri soggetti pertinenti dovrebbero quindi considerare sistematicamente la possibilità di includere partecipanti appartenenti ad altre cibercomunità.

Nel contesto del rafforzamento delle capacità dell'UE di prevenzione, deterrenza e risposta agli attacchi informatici, e in linea con la strategia del 2020 dell'UE in materia di cibersicurezza e con la bussola strategica, nel 2023 l'alto rappresentante proporrà opzioni per l'ulteriore rafforzamento del pacchetto di strumenti della diplomazia informatica dell'UE²⁰, attingendo agli elementi della posizione dell'Unione in materia di deterrenza informatica e agli insegnamenti tratti dall'attuazione di tale pacchetto sin dalla sua istituzione.

¹⁷ [Appello di Nevers a rafforzare le capacità di cibersicurezza dell'UE](#).

¹⁸ <https://eda.europa.eu/publications-and-data/factsheets/factsheet-cyber-phalanx>.

¹⁹ <https://www.pesco.europa.eu/project/cyber-ranges-federations-crf/>.

²⁰ Conclusioni del Consiglio su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica").

Azioni in materia di ciberdifesa

- Istituire un centro di coordinamento della ciberdifesa dell'UE come centro per la conoscenza situazionale militare comune e vagliare le modalità di cooperazione con il centro di situazione e di analisi informatiche della Commissione.
- Sviluppare e rafforzare ulteriormente la conferenza dei comandanti per la sicurezza informatica dell'UE.
- Incoraggiare gli Stati membri a partecipare attivamente alla MICNET, ossia la rete dei CERT militari, e a lavorare per stabilire una cooperazione con la rete dei CSIRT civili.
- Sviluppare un nuovo progetto quadro CyDef-X a sostegno delle esercitazioni di ciberdifesa a livello UE.
- Vagliare le possibilità di sviluppo ulteriore del concetto di gruppi di reazione rapida agli incidenti informatici, sulla base del progetto CRRT della PESCO.
- Vagliare le possibilità di sviluppo ulteriore di progetti del Poligono virtuale federato.

Azioni a sostegno di soggetti civili

- Preparare un'iniziativa di cibersolidarietà dell'UE, compresa una possibile legge per apportare modifiche legislative al programma Europa digitale al fine di:
 - rafforzare le capacità comuni dell'UE in materia di rilevamento, conoscenza situazionale e risposta;
 - sviluppare gradualmente una forza di riserva per la cibersecurity a livello di UE, con servizi prestati da operatori privati di fiducia;
 - sostenere le prove presso soggetti critici al fine di rilevare potenziali vulnerabilità basate sulle valutazioni del rischio effettuate a livello UE.
- Vagliare lo sviluppo di sistemi di certificazione della cibersecurity a livello UE per l'industria della cibersecurity e le imprese private.
- Migliorare la cooperazione a livello strategico, operativo e tecnico tra le cybercomunità della ciberdifesa e quelle di altro tipo.

2. Mettere in sicurezza l'ecosistema di difesa dell'UE

Negli ultimi anni il numero di attacchi informatici è aumentato sensibilmente, compreso quello degli attacchi alle catene di approvvigionamento con finalità di ciberspionaggio, ransomware o di perturbazione. Nel 2020 l'attacco alla catena di approvvigionamento SolarWinds²¹ ha interessato più di 18 000 organizzazioni a livello globale, tra cui agenzie governative, grandi imprese e imprese del settore della difesa. Lo sfruttamento di una vulnerabilità nel software log4j di Apache²² ha messo in evidenza il fatto che anche componenti software non considerati a rischio elevato o critici possono essere trasformati in armi per sferrare con successo nell'UE attacchi ai danni di grandi imprese o amministrazioni pubbliche, anche nel settore della difesa. Ciò dimostra l'evidente necessità di rafforzare ulteriormente la ciberresilienza dei soggetti che

²¹ <https://cybernews.com/security/solarwinds-hack-the-mystery-of-one-of-the-biggest-cyberattacks-ever/>.

²² <https://english.ncsc.nl/topics/log4j-vulnerability>.

operano nell'ecosistema della difesa dell'UE, compresi i soggetti militari, l'industria della difesa e gli operatori privati.

Le forze armate dipendono in larga misura dalle infrastrutture critiche civili per la mobilità, le comunicazioni o l'energia. L'attacco russo alla rete satellitare KA-SAT²³, che ha interrotto le comunicazioni per diverse autorità pubbliche così come per le forze armate ucraine, è un esempio di tale interrelazione che dimostra la necessità di mettere in sicurezza le infrastrutture critiche.

Per affrontare le questioni relative alla sicurezza dei loro sistemi di comunicazione e informazione, gli Stati membri stanno sviluppando per i sistemi militari norme e requisiti di sicurezza propri, che non sempre tengono conto della necessità di interoperabilità né dell'esistenza di norme civili per i prodotti a duplice uso. Ciò incide negativamente sulla capacità degli Stati membri di agire assieme nel ciberspazio, anche nel contesto delle missioni e operazioni militari della PSDC, e crea ostacoli all'assistenza reciproca. Inoltre è necessario promuovere sinergie maggiori tra i percorsi di normazione militari e civili, dato che, per l'industria, il fatto di dover rispettare norme simili ma diverse per i clienti civili e per quelli militari aumenta i costi di produzione nello sviluppo dei prodotti a duplice uso.

2.1. Migliorare la ciberresilienza dell'ecosistema della difesa

Il rafforzamento della ciberresilienza dell'ecosistema della difesa richiede interventi e investimenti mirati da parte di un'ampia serie di soggetti, dalle infrastrutture militari degli Stati membri e dalle missioni e operazioni della PSDC alle infrastrutture critiche, all'industria della difesa e ai soggetti pertinenti che si occupano di ricerca.

Ai fini del successo delle missioni e operazioni della PSDC si devono proteggere le informazioni necessarie per un processo decisionale informato. L'UE e gli Stati membri devono rafforzare ulteriormente le strutture militari di comando e controllo e sviluppare e rendere sicure le infrastrutture. Ciò vale anche per la consultazione politico-militare nelle prime fasi della gestione delle crisi ai fini di un impiego efficace del quartier generale del comando del livello operativo, compresa la capacità militare di pianificazione e condotta (MPCC). La questione sarà affrontata in particolare attraverso l'ulteriore sviluppo della rete operativa WAN dell'UE.

Nel contesto delle missioni e delle operazioni militari, i soggetti del settore della ciberdifesa si trovano a gestire informazioni in formati diversi e con classificazioni diverse, provenienti da fonti diverse. È quindi massimamente importante l'applicazione, con il sostegno dell'industria, di tecnologie sicure e allo stato dell'arte quali l'intelligenza artificiale.

La sicurezza dell'infrastruttura dei sistemi di comunicazione e informazione deve essere migliorata applicando procedure di gestione concordate, così da favorire tra i portatori di interessi la fiducia nell'integrità delle informazioni disponibili. L'alto rappresentante - anche nella sua veste di capo dell'AED - assisterà, con il sostegno della Commissione, gli Stati

²³ Dichiarazione dell'alto rappresentante a nome dell'Unione europea sulle attività informatiche malevole condotte da hacker e gruppi di hacker nel contesto dell'aggressione della Russia nei confronti dell'Ucraina: <https://www.consilium.europa.eu/it/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/>.

membri nell'elaborazione di **raccomandazioni non giuridicamente vincolanti per la comunità della difesa, ispirate alla direttiva relativa a misure per un livello comune elevato di cibersecurity nell'Unione (NIS2)**²⁴, in quanto la difesa è esclusa dall'ambito di applicazione della direttiva. Ciò contribuirà ad aumentare la maturità complessiva della ciberdifesa.

La proposta della Commissione relativa a una legge sulla ciberresilienza²⁵, che mira a stabilire requisiti di cibersecurity per i prodotti con elementi digitali, ridurrà ulteriormente le possibilità di attacco nel contesto dei prodotti a duplice uso impiegati, ad esempio nei sistemi di comunicazione e informazione, dall'industria della difesa e da soggetti governativi del settore della difesa. Secondo la proposta, i fabbricanti sarebbero tenuti a segnalare, entro 24 ore, le vulnerabilità attivamente sfruttate all'ENISA, la quale provvederà quindi ad informare i CSIRT nazionali pertinenti. A questo proposito sarebbe importante che la comunità della difesa fosse informata tempestivamente delle vulnerabilità presenti nei prodotti con elementi digitali e delle eventuali patch e misure di attenuazione disponibili e/o applicate.

A maggior ragione in considerazione della dipendenza delle forze militari da infrastrutture critiche civili è **necessario aumentare ulteriormente la protezione delle infrastrutture critiche contro gli attacchi informatici su larga scala**. Su richiesta del Consiglio²⁶, la Commissione, l'alto rappresentante e il gruppo di cooperazione NIS²⁷ stanno sviluppando scenari di rischio per la sicurezza delle infrastrutture digitali. L'attenzione si concentrerà innanzitutto sulla cibersecurity nei settori dell'energia, delle telecomunicazioni, dei trasporti e dello spazio. Saranno inoltre preparate valutazioni mirate dei rischi di cibersecurity per le infrastrutture e le reti di comunicazione nell'UE (comprese le infrastrutture fisse e mobili, i satelliti, i cavi sottomarini, l'instradamento in internet)²⁸. Per quanto concerne la protezione delle infrastrutture critiche dalle minacce provocate dall'uomo, comprese quelle ibride, la proposta di raccomandazione del Consiglio su un approccio coordinato dell'Unione per rafforzare la resilienza delle infrastrutture critiche²⁹ invita gli Stati membri a garantire, tra l'altro, prove di stress e un coordinamento delle crisi adeguati. La questione dell'infrastruttura critica marittima, compresa la protezione dei cavi sottomarini su cui transitano i dati, sarà affrontata ulteriormente nel contesto dell'imminente revisione della strategia per la sicurezza marittima dell'UE e del relativo piano d'azione. Ulteriori azioni destinate a rafforzare la cibersecurity delle infrastrutture critiche nel contesto del sistema energetico sono contenute nel piano d'azione dell'UE "Digitalizzare il sistema energetico"³⁰.

²⁴ Direttiva relativa a misure per un livello comune elevato di cibersecurity nell'Unione, che abroga la direttiva (UE) 2016/1148, che è stata concordata recentemente dai legislatori e la cui adozione formale è attesa entro l'anno.

²⁵ Proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersecurity per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 ([COM\(2022\) 454 final](#)).

²⁶ Conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica (ST09364/22), 23 maggio 2022.

²⁷ <https://digital-strategy.ec.europa.eu/it/policies/nis-cooperation-group>.

²⁸ [Appello di Nevers a rafforzare le capacità di cibersecurity dell'UE](#).

²⁹ Proposta di raccomandazione del Consiglio su un approccio coordinato dell'Unione per rafforzare la resilienza delle infrastrutture critiche ([COM\(2022\) 551 final](#)).

³⁰ Digitalizzare il sistema energetico - Piano d'azione dell'UE (COM(2022) 552 final).

I servizi spaziali sono sempre più importanti per la difesa, che si tratti di sorveglianza, conoscenza situazionale, precisione del posizionamento o comunicazioni ultrasicure. Di conseguenza costituiscono risorse strategiche fondamentali per la sovranità tecnologica. Perturbazioni dei servizi spaziali potrebbero incidere notevolmente sui sistemi di difesa, ma anche sulla società e sull'economia nel loro complesso. La resilienza di tali servizi è essenziale ai fini della resilienza complessiva della ciberdifesa, in quanto possono essere oggetto di attacchi dolosi. In particolare, come si è visto con gli attacchi alle reti KA-SAT, i sistemi spaziali sono sempre più esposti a minacce informatiche che possono compromettere la disponibilità o la continuità dei servizi spaziali, circostanza che genera un rischio per gli interessi strategici di sicurezza dell'UE nel settore spaziale così come per le capacità spaziali che consentono e assistono la ciberdifesa. La strategia spaziale dell'UE per la sicurezza e la difesa annunciata nella bussola strategica³¹ delinea le misure destinate a migliorare la solidità e la ciberresilienza delle infrastrutture spaziali e dei collegati servizi, così come a scoraggiare e rispondere a qualsiasi minaccia posta nei confronti dei sistemi e servizi spaziali sensibili nell'UE, in particolare le minacce informatiche.

La Commissione invita gli Stati membri ad attuare con urgenza le misure raccomandate nel pacchetto di strumenti dell'UE sulla cibersicurezza 5G³². Gli Stati membri che non hanno ancora adottato restrizioni sui fornitori a rischio elevato dovrebbero procedere in tal senso senza ulteriori indugi, considerato che il tempo perso può aumentare la vulnerabilità delle reti nell'UE. Tali rischi possono interessare le risorse militari e incidere sul contesto generale della difesa degli Stati membri.

Per quanto concerne la **ciberresilienza dell'industria europea della difesa e dei soggetti che si occupano di ricerca e sviluppo nel settore della difesa**, si tratta di soggetti che rientrano nell'ambito di applicazione della direttiva NIS2, fatto salvo il caso in cui siano esplicitamente esclusi dagli Stati membri, e che si ritroverebbero quindi a dover disporre di un programma di gestione dei rischi di cibersicurezza comprensivo della sicurezza delle catene di approvvigionamento e della segnalazione di incidenti. Poiché il settore privato svolge un ruolo importante nell'erogazione di servizi di cibersicurezza nell'ecosistema della difesa, gli Stati membri dovrebbero avvalersi di sistemi di certificazione della cibersicurezza. Potrebbe essere vagliata la possibilità di istituire un **sistema dell'UE di certificazione della cibersicurezza per le imprese che forniscono servizi all'industria della difesa**, come modo per introdurre un livello armonizzato di fiducia nel mercato sfruttando l'esperienza dell'ENISA.

2.2. Garantire l'interoperabilità della ciberdifesa UE e la coerenza delle norme

L'interoperabilità e l'omogeneità sono requisiti importanti da considerare sin dalla fase di progettazione delle capacità di ciberdifesa, tenendo conto anche degli insegnamenti tratti dalle missioni e dalle operazioni in corso, individuati sotto la guida dello Stato maggiore dell'UE, con il sostegno dell'AED. I principi, i processi e le norme concordati nella rete delle missioni federate³³ dovrebbero fornire gli elementi guida per lo sviluppo di capacità nazionali di ciberdifesa al fine di garantire l'interoperabilità.

³¹ Una bussola strategica per la sicurezza e la difesa, 21 marzo 2022, https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf.

³² Cibersicurezza delle reti 5G - Pacchetto di strumenti dell'UE di misure di attenuazione dei rischi | Plasmare il futuro digitale dell'Europa (europa.eu).

³³ <https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx>.

Le attività di collaborazione possono essere facilitate dall'armonizzazione dei requisiti per le capacità di ciberdifesa di prossima generazione, che potrebbe eventualmente portare a iniziative di sviluppo e approvvigionamento congiunti e al sostegno integrato del ciclo di vita. Per questo motivo l'AED e lo Stato maggiore dell'UE svilupperanno **raccomandazioni in merito a una serie di requisiti di interoperabilità della ciberdifesa dell'UE**. Tali requisiti devono essere presi in considerazione in tutti gli orizzonti di pianificazione al fine di garantire tutti gli aspetti della normazione come fattore abilitante critico per l'interoperabilità. I requisiti per le prove, la valutazione e la certificazione sono altri fattori abilitanti critici.

Nella proposta legge sulla ciberresilienza³⁴ saranno sviluppate norme armonizzate per la cibersecurity dei prodotti e componenti hardware e software. Tali norme riguarderanno tutti i prodotti civili e a duplice uso aventi elementi digitali, che costituiscono una parte consistente dei prodotti impiegati nel settore della difesa. Ove possibile la Commissione incoraggerà la coerenza con le norme in materia di cibersecurity dei prodotti digitali seguite nel settore della difesa. Come stabilito nel piano d'azione sulle sinergie tra l'industria civile, della difesa e dello spazio³⁵ (il "piano d'azione sulle sinergie"), la Commissione presenterà, in stretta collaborazione con i principali portatori di interessi, un piano destinato a promuovere l'uso delle vigenti norme ibride civili/della difesa e lo sviluppo di norme nuove. La cooperazione tra tutti i portatori di interessi, comprese le organizzazioni europee di normazione, l'Organizzazione del Trattato del Nord Atlantico (NATO) e altri partner, dovrebbe essere sviluppata ulteriormente sfruttando al meglio a tal fine il comitato europeo di normazione nel settore della difesa. In maniera analoga, quando gli organismi di normazione militare sviluppano norme nuove relative alla cibersecurity dei prodotti con elementi digitali destinati all'uso nel settore della difesa, dovrebbero prendere a riferimento le norme armonizzate sviluppate ai sensi della legge sulla ciberresilienza³⁶.

Azioni in materia di ciberdifesa

- Sostenere gli Stati membri nello sviluppo di raccomandazioni non giuridicamente vincolanti per la comunità della difesa, ispirate alla NIS2, al fine di contribuire a una maggiore maturità complessiva della ciberdifesa a livello nazionale.
- Formulare raccomandazioni sui requisiti di interoperabilità per la ciberdifesa dell'UE.
- Rafforzare la cooperazione con tutti i soggetti pertinenti in merito alle norme relative alla difesa nel quadro del comitato europeo di normazione della difesa.

Azioni a sostegno di soggetti civili

- Delineare scenari di rischio per le infrastrutture critiche rilevanti per la comunicazione e la mobilità militari, al fine di orientare le azioni di preparazione, anche mediante test di penetrazione.

³⁴ COM(2022) 454 final.

³⁵ COM(2021) 70 final.

³⁶ Sono attualmente in corso lavori di normazione in relazione ai requisiti di cibersecurity per le apparecchiature radio, sulla base del regolamento delegato (UE) 2022/30. Qualora la Commissione abroghi o modifichi tale regolamento delegato in maniera tale da determinare la cessazione dell'applicazione a determinati prodotti soggetti alla legge sulla ciberresilienza, la Commissione e gli organismi europei di normazione dovrebbero tener conto del lavoro di normazione svolto nel contesto della decisione di esecuzione C(2022) 5637 della Commissione relativa alla richiesta di normazione per il suddetto regolamento delegato in relazione alla preparazione e allo sviluppo di norme armonizzate destinate a facilitare l'attuazione della legge sulla ciberresilienza.

- Promuovere la cooperazione tra gli organismi di normazione civili e militari per la definizione di norme armonizzate per i prodotti a duplice uso.

3. Investire in capacità di ciberdifesa

Negli ultimi anni, gli investimenti a favore della ciberdifesa dell'UE sono aumentati a fronte di un aumento delle attività informatiche dolose da parte di soggetti statali e non statali. È fondamentale che l'UE rafforzi le capacità di ciberdifesa. La guerra di aggressione della Russia nei confronti dell'Ucraina acuisce ulteriormente la necessità di aumentare gli investimenti, così che gli Stati membri dispongano di capacità di ciberdifesa allo stato dell'arte, tanto fisse quanto dispiegabili.

I miglioramenti tecnologici sono essenziali per mantenere un vantaggio rispetto a concorrenti e avversari, che investono anch'essi massicciamente in tecnologie nuove. Di conseguenza l'UE e gli Stati membri devono altresì rafforzare la cooperazione e l'interoperabilità in materia di ciberdifesa sviluppando capacità congiunte e aumentando gli investimenti in ricerca e sviluppo.

È necessario ovviare alle vulnerabilità derivanti dalle dipendenze strategiche e dalla frammentazione dell'EDTIB³⁷. In particolare le capacità e le competenze sono essenziali per affrancarsi dalle dipendenze strategiche in materia di cibersicurezza e ciberdifesa in Europa. Per rimanere in grado di apportare soluzioni ad alta tecnologia in un contesto globale, l'industria europea della difesa deve mantenere le competenze essenziali e acquisirne di nuove³⁸. La mancanza di competenze ha ripercussioni negative sul settore della difesa, in quanto ostacola lo sviluppo di capacità in tutti i settori. Tutte le azioni saranno perfettamente in linea con gli approcci annunciati nel piano d'azione sulle sinergie, nella tabella di marcia per le tecnologie critiche per la sicurezza e la difesa ("tabella di marcia")³⁹ e nell'analisi delle carenze⁴⁰.

3.1. Sviluppare capacità di ciberdifesa allo stato dell'arte e a tutto spettro

Agli Stati membri spettano la responsabilità e la competenza per l'uso delle capacità di ciberdifesa, mentre l'UE svolge un ruolo importante nel sostenere l'ulteriore sviluppo di capacità militari specifiche nello spettro della dottrina, dell'organizzazione, dell'addestramento, dei materiali, del personale, della leadership, delle strutture e dell'interoperabilità (DOTMLPF-I) al fine di creare libertà d'azione nel ciberspazio. È necessario unificare ulteriormente l'approccio alla ciberdifesa in tutti i domini di capacità e adattarlo al mutevole contesto geopolitico. Di conseguenza si devono individuare gli elementi mancanti nelle capacità esistenti e sostenere lo sviluppo coordinato e misurabile di capacità nuove.

³⁷ Ad esempio quelle indicate nell'analisi delle carenze di investimenti nel settore della difesa.

³⁸ Sono state avviate diverse iniziative, ad esempio il partenariato europeo per le competenze nel settore della difesa.

³⁹ Nella tabella di marcia per le tecnologie critiche la Commissione ha invitato a rafforzare la cooperazione sulle tecnologie critiche per la sicurezza e la difesa a lungo termine dell'Europa nonché gli sforzi volti a ridurre le relative dipendenze strategiche.

⁴⁰ Comunicazione congiunta sull'analisi delle carenze di investimenti nel settore della difesa e sulle prospettive di percorso, nella quale la Commissione e l'alto rappresentante hanno proposto diverse misure destinate a garantire che l'industria dell'UE sia debitamente attrezzata per fornire prestazioni tanto a breve quanto a lungo termine.

Tuttavia il livello di partecipazione degli Stati membri a progetti di collaborazione per lo sviluppo della ciberdifesa rimane ad oggi insufficiente e dovrebbe essere aumentato per massimizzarne l'impatto a livello UE. Tutti gli Stati membri devono aumentare gli investimenti nello sviluppo di capacità di ciberdifesa a tutto spettro e svilupparle in modo collaborativo. Gli Stati membri dovrebbero prendere in considerazione **l'elaborazione di una serie di impegni volontari per lo sviluppo di capacità nazionali di ciberdifesa** e di capacità multinazionali al di là dei progetti di ciberdifesa della PESCO esistenti⁴¹. Il processo di revisione coordinata annuale sulla difesa (CARD) potrebbe essere utilizzato per avviare un dialogo con gli Stati membri in merito ai requisiti di ciberdifesa e agli obiettivi nazionali per lo sviluppo delle capacità di ciberdifesa, nonché per valutare l'attuazione degli impegni. La Commissione sostiene e cofinanzia, mediante il Fondo europeo per la difesa (FED), lo sviluppo di capacità di ciberdifesa a tutto spettro e la ricerca in tale ambito, anche in relazione a capacità di difesa attiva. La Commissione ha già aumentato gli investimenti nella ciberdifesa attraverso il FED, il che dovrebbe portare allo sviluppo di strumenti europei comuni e/o interoperabili per le operazioni nel ciberspazio e la gestione degli incidenti, le operazioni difensive e le misure preventive delle guerre dell'informazione nonché il miglioramento della resilienza dei sistemi di comunicazione e informazione. Quest'attività tocca settori quali la conoscenza situazionale in ambito informatico, la caccia alle minacce in tempo reale e le capacità operative di risposta, nonché le capacità operative informatiche e le esercitazioni e attività di formazione in ambito informatico⁴². Affinché gli Stati membri siano in grado di condurre operazioni informatiche congiunte, nei prossimi anni il FED sosterrà le operazioni di risposta e le capacità operative informatiche. Infine gli Stati membri sono incoraggiati a partecipare attivamente ai diversi consessi di cooperazione e a utilizzare tutti gli strumenti istituiti a livello UE, compreso il gruppo di progetto dell'AED sulla ciberdifesa⁴³.

La revisione in corso delle priorità di sviluppo delle capacità dell'UE del 2018⁴⁴ offre un'occasione tempestiva per definire le priorità aggiornate dello sviluppo cooperativo e collaborativo, il che consentirà a sua volta un aumento dello sviluppo di capacità cooperative. La revisione della priorità specifica della ciberdifesa dovrebbe tenere conto dell'esito della revisione coordinata annuale sulla difesa del 2022, nonché dei risultati dell'analisi delle carenze presentata agli Stati membri nel maggio del 2022. Successivamente la revisione coordinata annuale sulla difesa offrirà un quadro periodico per passare in rassegna i progressi compiuti nell'attuazione di questa priorità aggiornata a livello nazionale e vagliare le nuove opzioni emergenti per lo sviluppo collaborativo di capacità di ciberdifesa con gli Stati membri. Le

⁴¹ Gruppi di risposta rapida agli incidenti informatici e mutua assistenza in materia di cibersicurezza (CRRT), centro di coordinamento nel settore informatico e dell'informazione (CIDCC), piattaforma per la condivisione delle informazioni in materia di minaccia informatica e di risposta agli incidenti informatici (CTIRISP), Poligono virtuale federato (CRF), accademia e polo di innovazione dell'UE nel settore dell'informatica (EU CAIH).

⁴² Nel contesto del programma europeo di sviluppo del settore industriale della difesa (EDIDP) sono stati finanziati 6 progetti (PANDORA, DISCRETION, CYBER4DE, ECYSAP, SMOTANET e HERMES) per un importo di 39 milioni di EUR. Nel contesto del FED 2021 quasi 40 milioni di EUR saranno destinati a 3 progetti collaborativi di ricerca e sviluppo nel settore della ciberdifesa selezionati per il finanziamento (ACTING, AInception, EU-GUARDIAN).

⁴³ Il gruppo di progetto sulla ciberdifesa mette a disposizione degli Stati membri un forum per discutere di questioni di ciberdifesa aventi implicazioni militari.

⁴⁴ Scheda informativa del piano di sviluppo delle capacità dell'AED (28.6.2018): [scheda informativa del piano di sviluppo delle capacità](#).

priorità aggiornate di sviluppo delle capacità UE serviranno di riferimento fondamentale per i progetti della PESCO in materia di ciberdifesa.

A questo proposito, muovendo dal mandato del comitato militare dell'UE, lo Stato maggiore dell'UE svilupperà, in stretto coordinamento con gli Stati membri, il piano di attuazione delle operazioni nel settore informatico, al fine di tracciare una panoramica dello stato di attuazione delle capacità di ciberdifesa e di sostenere gli Stati membri ai fini di un migliore allineamento di iniziative e attività. Le iniziative si basano sul concetto di ciberdifesa dell'UE per le operazioni e le missioni militari a guida UE, il che rispecchia la definizione delle priorità di cui al piano di sviluppo delle capacità.

Potenziamento delle attività di ricerca sulle tecnologie chiave per la ciberdifesa

Al fine di mantenere capacità di ciberdifesa allo stato dell'arte, è necessario rimanere al passo con gli sviluppi tecnologici e le relative applicazioni nei sistemi di difesa, con particolare riferimento alle tecnologie emergenti e di rottura (ad esempio l'intelligenza artificiale, la crittografia e il calcolo quantistico)⁴⁵. In particolare, l'UE deve investire nella crittografia post-quantistica per garantire la persistenza della sicurezza dei suoi sistemi di difesa. Data la rapidità di evoluzione della tecnologia, occorre ritagliare su misura le iniziative di ricerca e sviluppo tecnologico in collaborazione, al fine di conseguire un livello di preparazione tecnologica sufficientemente avanzato così che i risultati possano essere incorporati più rapidamente nelle capacità esistenti e future.

Nel quadro del FED la Commissione finanzia l'innovazione tecnologica per la difesa e sostiene lo sviluppo di tecnologie emergenti e di rottura nonché di tecnologie all'avanguardia, anche per la ciberdifesa. Fino all'8 % del bilancio del FED è destinato a temi che riguardano le tecnologie di rottura per la difesa, compresi alcuni temi pertinenti per la ciberdifesa. Nei prossimi anni il FED dedicherà particolare attenzione alle azioni e ai progetti di ricerca che riguardano tecnologie nuove sviluppate contro le minacce emergenti e in evoluzione, nonché l'aumento della resilienza e della cibersicurezza e la relativa integrazione nelle capacità di difesa.

In linea con il piano d'azione sulle tecnologie emergenti e di rottura⁴⁶, l'AED informerà annualmente gli Stati membri in merito al panorama delle tecnologie emergenti, comprese quelle applicabili alla ciberdifesa. Svilupperà altresì la valutazione strategica europea delle tecnologie emergenti e di rottura al fine di sostenere gli Stati membri nell'adozione di orientamenti strategici a lungo termine, individuando sinergie e possibilità di collaborazione. Il Centro europeo di competenza per la cibersicurezza (ECCC) adotterà un'agenda strategica per gli investimenti nei settori chiave della cibersicurezza, che a sua volta guiderà la preparazione dei programmi di lavoro futuri dei programmi Europa digitale e Orizzonte Europa in relazione alla cibersicurezza, sostenendo rispettivamente la ricerca, l'innovazione e l'adozione da parte del mercato. Al fine di favorire le sinergie l'ECCC e l'AED concorderanno modalità operative per facilitare la condivisione di informazioni tra i membri del rispettivo personale in merito alle rispettive priorità per le tecnologie di difesa e a duplice uso in ambito civile.

⁴⁵ Indicate nel programma di ricerca in materia di ciberdifesa e nell'agenda strategica di ricerca onnicomprensiva (OSRA).

⁴⁶ Il documento "Tecnologie emergenti e di rottura: un piano d'azione basato sulle capacità" è stato approvato il 16 dicembre 2021 dal comitato direttivo dell'AED nella composizione dei direttori per la Ricerca e la tecnologia.

Agire in base alle esigenze tecnologiche per la ciberdifesa

Sono necessari ulteriori interventi e iniziative di coordinamento al fine di garantire che la rapida evoluzione tecnologica nel settore informatico sia recepita celermente dal settore della difesa. Rientra in questo contesto l'intensificazione delle iniziative volte a individuare le tecnologie critiche per la difesa e la cibersicurezza cui attribuire priorità ai fini della riduzione delle dipendenze tecnologiche dell'UE e a stabilire se gli strumenti di definizione delle priorità e di finanziamento vigenti permettano una risposta sufficiente a tali dipendenze.

A tal fine la Commissione, assieme all'Agenzia europea per la difesa (AED) e agli Stati membri, proporrà nel 2023 una **tabella di marcia per le cibertecnologie critiche** sulla base di consultazioni in materia, se del caso anche con il settore industriale. La tabella di marcia per le tecnologie individuerà le cibertecnologie importanti per la sovranità tecnologica dell'UE, tratterà tanto la ciberdifesa quanto la cibersicurezza, mapperà gli sviluppi tecnologici e le dipendenze strategiche ed agirà per mitigare queste ultime. Informerà le priorità strategiche degli strumenti di finanziamento dell'UE e proporrà di sfruttare appieno i programmi di ricerca e sviluppo di capacità del contesto civile e della difesa e gli strumenti di finanziamento corrispondenti, in linea con le rispettive norme in materia di governance. Proporrà ulteriori modalità per incoraggiare lo sviluppo della ricerca, lo sviluppo tecnologico e l'innovazione a duplice uso in materia di cibersicurezza e ciberdifesa a livello di UE e di Stati membri.

In tale contesto, nel 2023 la Commissione⁴⁷ valuterà, in collaborazione con l'ECDC e l'AED, le tecnologie che sono già state individuate come critiche ai fini della ciberdifesa e, possibilmente con il sostegno dell'Osservatorio sulle tecnologie critiche, proseguirà l'opera di mappatura e individuazione delle dipendenze esistenti⁴⁸. A tal fine terrà conto del lavoro svolto nel contesto del documento annuale di monitoraggio dell'AED⁴⁹ e della valutazione strategica europea delle tecnologie emergenti e di rottura⁵⁰. L'ECDC potrebbe lanciare un progetto di sostegno alle politiche dedicato in grado di alimentare il processo di definizione di tabelle di marcia per le tecnologie e riunire e coinvolgere i pertinenti portatori di interessi della sfera civile e di quella militare.

Nel contesto delle attività delineate nel piano d'azione sulle sinergie, nella tabella di marcia e nell'analisi delle carenze, sono già in corso diverse azioni volte a rafforzare le sinergie per sfruttare meglio il pieno potenziale delle tecnologie a duplice uso, anche nel settore informatico.

Gli Stati membri sono incoraggiati a fare pieno uso delle iniziative esistenti a sostegno della ricerca e dello sviluppo tecnologico, in particolare, per la difesa, i gruppi dell'AED sulla

⁴⁷ Compreso il Centro comune di ricerca (JRC).

⁴⁸ Osservatorio sulle tecnologie critiche, annunciato nel piano d'azione sulle sinergie tra l'industria civile, della difesa e dello spazio.

⁴⁹ Prima fase del piano d'azione 2021 sulle tecnologie emergenti e di rottura dell'AED.

⁵⁰ Seconda fase del piano d'azione 2021 dell'AED.

tecnologia per le capacità di difesa⁵¹ e i relativi elementi tecnologici dell'OSRA⁵², il quadro ad hoc dell'AED⁵³, il FED e la PESCO. Per le tecnologie civili e a duplice uso, l'ECCC e la Rete possono gestire progetti aventi una dimensione tanto di difesa quanto civile, come stabilito dall'applicabile base giuridica⁵⁴. Come annunciato nel piano d'azione sulle sinergie e nella tabella di marcia, la Commissione cercherà inoltre di rafforzare le sinergie tra le attività dell'ECCC e del FED in materia di cibernsicurezza e ciberdifesa, in linea con le norme del FED in materia di governance.

3.2. Un'industria europea della difesa agile, competitiva e innovativa

L'UE necessita di un'industria europea della difesa forte, agile, competitiva e innovativa, in grado di fornire uno spettro completo di capacità di difesa allo stato dell'arte, comprese le capacità di ciberdifesa. Tuttavia, per quanto riguarda la ciberdifesa, attualmente l'industria dell'UE della difesa si affida sostanzialmente a soluzioni civili e a mercati esterni per fornire soluzioni allo stato dell'arte. Sebbene i progressi tecnologici in ambito civile siano rapidi e il mercato dei prodotti civili per l'informazione e la cibernsicurezza sia in rapida crescita, esistono requisiti militari specifici che non sono soddisfatti dai normali prodotti civili. Parti importanti dell'hardware e del software attualmente utilizzati per la ciberdifesa non sono prodotte nell'UE, il che può creare dipendenze a livello industriale e tecnologico. All'UE manca altresì una presenza forte nel settore globale della cibernsicurezza e della ciberdifesa. La notevole frammentazione dell'EDTIB ne riduce notevolmente la capacità di migliorare la competitività⁵⁵, in quanto la maggior parte delle imprese che si occupano di cibernsicurezza nell'UE sono piccole e medie imprese (PMI)⁵⁶. Disporre di capacità industriale dotata di sovranità tecnologica è un aspetto essenziale per la capacità d'azione dell'UE.

L'UE sta sostenendo lo sviluppo di un'EDTIB forte attraverso una serie di programmi e iniziative. Mentre il FED finanzia l'innovazione tecnologica per la difesa e sostiene lo sviluppo di tecnologie che da ultimo portino a capacità militari all'avanguardia sviluppate

⁵¹ Le CapTech offrono agli esperti degli Stati membri un forum per la creazione di reti e un quadro flessibile per i progetti collaborativi. Ulteriori informazioni sulle CapTech relative al settore informatico (Settore informatico, Informazione, Componenti) sono disponibili all'indirizzo: [https://eda.europa.eu/what-we-do/research-technology/capability-technology-areas-\(captechs\)](https://eda.europa.eu/what-we-do/research-technology/capability-technology-areas-(captechs)).

⁵² L'OSRA mappa i settori della ricerca e della tecnologia pertinenti per la difesa e specifica in dettaglio le possibilità concrete di collaborazione. Esistono 17 elementi tecnologici aventi le proprie tabelle di marcia per le tecnologie associate alle cibertecnologie che trattano la conoscenza situazionale in relazione alla ciberdifesa, la protezione dei sistemi di comunicazione militari, l'elaborazione di informazioni da fonti eterogenee, la modellazione e la simulazione, l'informatica quantistica e la crittografia, oltre a vagliare le sinergie tra operazioni informatiche e guerra elettronica. L'intelligenza artificiale e i megadati (*big data*) svolgono un ruolo fondamentale nell'elaborazione delle informazioni.

⁵³ Il quadro ad hoc dell'AED è definito dalla decisione del Consiglio (PESC) 2015/1835. Attualmente sono in fase di esecuzione 6 progetti con elementi cibertecnologici, per un importo di circa 20 milioni di EUR (ANQUOR, CERERE, AED SOC 2, MASFAD II, PASEI II, ASSAI).

⁵⁴ Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cibernsicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.

⁵⁵ Come rilevato nella comunicazione congiunta sull'analisi delle carenze di investimenti nel settore della difesa e sulle prospettive di percorso.

⁵⁶ Il numero totale di PMI che nell'UE operano nelle catene di approvvigionamento multilivello e spesso transfrontaliere del settore della difesa è stimato a 2 500. Tali imprese servono clienti del settore della difesa e il 7,8 % delle loro attività riguarda il settore informatico.

congiuntamente e contribuiscano alla competitività dell'industria della difesa dell'UE, i programmi Orizzonte Europa ed Europa digitale sostengono la ricerca in materia di cibersecurity e lo sviluppo di tecnologie a duplice uso, tra cui il calcolo quantistico, la crittografia, il cloud protetto e l'intelligenza artificiale⁵⁷.

Ulteriori azioni dovrebbero affrontare le questioni relative alle tecnologie critiche per la ciberdifesa e alle esigenze industriali indicate dalla **tabella di marcia per le cibertecnologie critiche**. Occorre individuare flussi di sostegno adeguati, ad esempio per stimolare le iniziative comuni in materia di appalti ricorrendo al futuro programma europeo di investimenti nel settore della difesa, oppure per facilitare l'accesso a capitale e prestiti mediante il Fondo europeo per gli investimenti e la Banca europea per gli investimenti.

Al fine di disporre di un'EDTIB forte, è necessario garantire lo sfruttamento e la valorizzazione delle sinergie tra imprese civili e del settore della difesa. Le azioni di innovazione proposte nel contesto del sistema di innovazione nel settore della difesa dell'UE (EUDIS), tra cui la sensibilizzazione delle PMI e la prospezione tecnologica, potrebbero avere ripercussioni positive per l'industria dell'UE della difesa e per l'EDTIB.

La Commissione avvierà un dialogo con il settore al fine di sviluppare l'industria dell'UE della ciberdifesa, coinvolgendo opportunamente l'AED.

La Commissione e l'alto rappresentante propongono di mettere in atto varie misure che attrezzino l'industria a ottenere risultati a breve e lungo termine. Ciò comporta, nell'immediato, una mappatura accurata delle capacità produttive dell'UE nel settore della difesa, al fine di individuare con precisione le carenze e gli ambiti nei quali è necessario un potenziamento.

Le dipendenze critiche nel settore informatico, come quelle che possono essere individuate nelle tabelle di marcia sulle tecnologie, potrebbero essere superate anche mediante il nuovo Fondo per la sovranità europea annunciato dalla presidente von der Leyen nel discorso sullo Stato dell'Unione di settembre 2022.

Il quadro dell'UE in materia di controllo degli investimenti esteri diretti continuerà a essere utilizzato per attenuare i rischi di acquisizioni di tecnologie o soluzioni europee che presentano rischi in materia di difesa e sicurezza. Gli Stati membri che non hanno ancora istituito meccanismi di controllo nazionali dovrebbero procedere in tal senso senza indugio.

3.3. Forza lavoro dell'UE nel settore della ciberdifesa

L'Europa si trova di fronte a una carenza effettiva e allarmante di competenze informatiche: l'Organizzazione europea per la cibersecurity (ECSSO) stima che già ora, nel 2022, siano necessari complessivamente 500 000 addetti. Tale carenza di competenze ostacola la capacità dell'UE di sviluppare tecnologie nuove e di difendere le infrastrutture critiche. Per gli enti pubblici quali i ministeri della Difesa e le forze armate, la forte concorrenza in termini di competenze e gli stipendi allettanti offerti dal settore privato aggravano ulteriormente le difficoltà di attrarre e trattenere talenti informatici.

⁵⁷ Il programma Orizzonte Europa prevede che le sinergie con il FED andranno a beneficio della ricerca in ambito civile e di difesa, anche se le attività del programma quadro si concentreranno esclusivamente sulle applicazioni civili.

Nel contesto dell'Anno europeo delle competenze 2023 **la Commissione avvierà l'iniziativa per un'accademia delle competenze informatiche**. Si tratta di un'iniziativa multicomparto finalizzata ad aumentare il numero di operatori professionali formati in cibersecurity, nella quale convoglieranno le numerose iniziative in materia di competenze informatiche e si esplicheranno il coordinamento, l'integrazione e una comunicazione comune al riguardo. Articolata in vari filoni d'azione (finanziamento, sostegno alle comunità, formazione e certificazione, coinvolgimento dei portatori di interessi, generazione di conoscenze), l'accademia delle competenze informatiche sarà anche in grado di apportare benefici alla forza lavoro del settore della ciberdifesa. L'Accademia europea per la sicurezza e la difesa (AESD) vaglierà le modalità per facilitare lo scambio di buone pratiche e ulteriori sinergie tra il settore militare e quello civile per quanto concerne la formazione e lo sviluppo di competenze militari specifiche per il ciberspazio.

Sulla base di un'analisi dei requisiti di formazione dell'UE e delle esigenze di formazione, l'AESD, l'AED e gli Stati membri svilupperanno ulteriormente e organizzeranno attività di formazione ed esercitazioni in materia di ciberdifesa per le istituzioni dell'UE, le operazioni e le missioni della PSDC e i funzionari degli Stati membri. Al fine di generare ulteriori capacità di formazione sarà vagliata altresì l'ipotesi di un ulteriore **sviluppo della piattaforma informatica dell'AESD in materia di istruzione, formazione, valutazione ed esercitazioni (ETEE)**. In tale contesto dovrebbero figurare altresì corsi di formazione per settori operativi specifici e operazioni multisettoriali. Si dovrebbero ricercare sinergie in particolare con il progetto di accademia e polo di innovazione dell'UE nel settore dell'informatica (EU CAIH) della PESCO⁵⁸.

Gli Stati membri sono incoraggiati a sviluppare programmi di istruzione specifici nel settore della ciberdifesa, coinvolgendo istituzioni accademiche e di istruzione superiore (civili e militari) al fine di sviluppare e creare programmi di formazione comuni in materia di ciberdifesa, condividendo le migliori pratiche, creando partenariati e progetti comuni e facilitando lo scambio di formatori e formandi. Al fine di garantire l'interoperabilità e una cultura comune in tutta l'UE, l'AESD promuoverà uno scambio tra gli Stati membri attraverso l'ETEE.

Gli Stati membri dovrebbero potenziare e allargare la cooperazione tra i soggetti coinvolti nella formazione e nell'istruzione mediante l'abbinamento degli aspetti civili e militari nel settore tecnico, operativo, strategico e giuridico, gettando le basi per la creazione di programmi di formazione comuni e standardizzati a livelli diversi per le comunità civile, delle autorità di contrasto, diplomatica e della ciberdifesa. Gli Stati membri dovrebbero interagire con gli erogatori di formazione del settore privato europeo, così come con le istituzioni accademiche, al fine di aumentare i livelli di competenza e abilità del personale coinvolto nelle missioni e operazioni militari della PSDC.

Tra gli Stati membri, le istituzioni, organi e organismi dell'UE, i partner internazionali e altri soggetti, compresi il settore privato e il mondo accademico, dovrebbe essere inoltre promossa la cooperazione in merito a livelli di formazione e certificazione in materia di ciberdifesa. Basandosi su iniziative esistenti nel settore civile quale il quadro europeo in materia di competenze nel settore della cibersecurity (ECSF) sviluppato dall'ENISA, l'AESD elaborerà

⁵⁸ <https://www.pesco.europa.eu/project/eu-cyber-academia-and-innovation-hub-eu-caih/>.

un quadro di certificazione delle competenze in materia di ciberdifesa. La Commissione prenderà in considerazione altresì gli approcci per la certificazione delle competenze informatiche disponibili sul mercato e nelle università, cercando, attraverso l'accademia delle competenze informatiche, di stimolare sinergie tra tali approcci e di colmare le lacune, in particolare con finanziamenti mirati dell'UE.

Azioni in materia di ciberdifesa

- Mettere a punto una valutazione strategica delle tecnologie emergenti e di rottura per sostenere le decisioni strategiche di investimento a lungo termine.
- Definire una tabella di marcia per le tecnologie in relazione alle cibertecnologie critiche per l'UE che comprenda le tecnologie critiche per la ciberdifesa e la cibersicurezza al fine di valutare il grado di dipendenza.
- Proporre percorsi per ridurre le dipendenze utilizzando tutti gli strumenti dell'UE, compresi il programma Europa digitale, il programma Orizzonte Europa e il FED, e anticipare lo sviluppo tecnologico per aumentare la sovranità tecnologica e garantire la capacità d'agire.
- Sostenere lo sviluppo di un quadro di certificazione delle competenze in materia di ciberdifesa.
- Mettere a punto esercitazioni dell'UE in materia di ciberdifesa e vagliare le modalità per sviluppare ulteriormente la piattaforma informatica ETEE dell'AESD al fine di generare maggiori capacità di formazione.

Azioni a sostegno di soggetti civili

- Istituire un'accademia unionale delle competenze informatiche, tenendo presenti i bisogni di competenze specifiche nei diversi profili professionali e settori di attività, anche per quanto riguarda la forza lavoro nel settore della difesa.
- Analizzare gli approcci alla certificazione delle competenze informatiche, cercando di promuovere sinergie e di colmare le lacune, anche attraverso i finanziamenti dell'UE.

4. Stringere partenariati per superare le sfide comuni

I partner trarranno beneficio da un'UE più capace e resiliente nel ciberspazio, così come dall'assistenza e dallo sviluppo di capacità in materia di ciberdifesa che l'Unione apporterà tramite i suoi strumenti pertinenti. L'UE cercherà di istituire partenariati personalizzati nel settore della ciberdifesa, laddove questi siano reciprocamente vantaggiosi. I partenariati in materia di ciberdifesa s'iscriveranno anche nel contesto della partecipazione dei paesi partner alle missioni e operazioni militari della PSDC.

Ove opportuno, tale attività si baserà sui dialoghi esistenti nel settore cibernetico, nonché sui dialoghi in materia di sicurezza e difesa. L'alto rappresentante vaglierà altresì le sinergie tra la **rete informale della diplomazia informatica dell'UE e la rete degli addetti alla difesa presso le delegazioni UE.**

4.1. Collaborazione con la NATO

Il partenariato strategico dell'UE con la NATO resta essenziale ai fini della sicurezza euro-atlantica, come sottolineato nella bussola strategica e nel concetto strategico del 2022 della NATO⁵⁹. L'UE rimane pienamente impegnata a rafforzare tale partenariato fondamentale, anche nel settore della ciberdifesa; devono essere compiuti ulteriori passi verso lo sviluppo di soluzioni condivise in relazione a minacce e sfide comuni. In conformità con le dichiarazioni congiunte di Varsavia e Bruxelles in merito alla cooperazione UE-NATO⁶⁰ e sulla base dei principi di trasparenza, reciprocità e inclusività, apertura e autonomia decisionale di entrambe le organizzazioni, la cibersecurity e la ciberdifesa costituiscono uno dei settori prioritari dell'UE per la cooperazione.

Sulla base della reciprocità, l'UE continuerà gli scambi con la NATO in merito al quadro concettuale militare relativo all'integrazione degli aspetti di ciberdifesa nella pianificazione e nella conduzione di missioni e operazioni militari della PSDC. L'UE si adopererà per conseguire la massima compatibilità con i concetti e la dottrina della NATO in materia di ciberdifesa.

Per quanto concerne la forte domanda di capacità di ciberdifesa, l'UE promuoverà sinergie e complementarità con la NATO al di là dei confini organizzativi e nazionali. L'UE collaborerà con la NATO per rafforzare l'interoperabilità tecnica e procedurale delle capacità di ciberdifesa, compreso lo sviluppo di capacità in linea con l'iniziativa della rete delle missioni federate. Si aprirà così la strada allo sviluppo e all'impiego potenziali e sinergici delle capacità di ciberdifesa. Si dovrebbe prestare particolare attenzione all'interoperabilità delle norme, contribuendo alla ciberresilienza e all'interoperabilità dei sistemi di comunicazione e informazione militari, coinvolgendo se del caso il settore industriale.

Al fine di fornire una formazione coerente al rispettivo personale addetto alla ciberdifesa, l'UE rafforzerà se del caso la cooperazione con la NATO anche in materia di armonizzazione delle esigenze di formazione e di analisi dei requisiti, sviluppando programmi di formazione, corsi ed esercitazioni comuni. Sulla base dei principi di reciprocità e non discriminazione, l'AESD aprirà al personale della NATO i corsi di formazione in ciberdifesa e creerà una piattaforma per pubblicizzare i corsi comuni. L'UE promuoverà la partecipazione del personale della NATO alle esercitazioni in ambito informatico e a quelle in materia di gestione delle crisi con elementi informatici.

L'UE e la NATO si impegneranno inoltre a migliorare ulteriormente la conoscenza situazionale reciproca e a vagliare le possibilità di coordinamento, anche rafforzando la cooperazione tra capacità NATO di reazione a incidenti informatici (NCIRC) e il CERT-UE. Al fine di promuovere la cooperazione in merito agli aspetti e alle implicazioni informatiche della gestione e della risposta alle crisi, l'UE contribuirà allo scambio tra membri del personale nel contesto di iniziative militari, civili e comuni e, se del caso, allo sviluppo di sinergie potenziali dei rispettivi quadri e delle rispettive iniziative di gestione delle crisi, anche nel caso di incidenti su larga scala. Con l'obiettivo di garantire la complementarità reciproca ed evitare inutili duplicazioni di sforzi, l'UE cercherà di intensificare la cooperazione e lo scambio di

⁵⁹ <https://www.nato.int/strategic-concept/>.

⁶⁰ Firmate rispettivamente nel 2016 e nel 2018.

informazioni con la NATO in merito alle iniziative di sviluppo di capacità di ciberdifesa nei paesi partner.

4.2. Cooperazione con partner che condividono gli stessi principi

L'alto rappresentante includerà in maniera più sistematica le questioni di ciberdifesa nei dialoghi esistenti e futuri con i partner nel settore cibernetico e in materia di sicurezza e difesa. Via via che gli aspetti della ciberdifesa si svilupperanno nel contesto dei dialoghi bilaterali, aumenterà la possibilità di introdurre le questioni della ciberdifesa in altri assetti di cooperazione con i partner dell'UE.

Il partenariato strategico dell'UE con gli **Stati Uniti d'America** continuerà ad approfondire la cooperazione reciprocamente vantaggiosa in materia di sicurezza e difesa, anche attraverso lo scambio strutturato di informazioni sulla conoscenza situazionale. I dialoghi UE-USA nel settore cibernetico e i dialoghi UE-USA in materia di sicurezza e difesa, che si tengono periodicamente, confermano l'esistenza di un forte partenariato transatlantico. L'alto rappresentante introdurrà in tali dialoghi, laddove opportuno, gli aspetti pertinenti della ciberdifesa.

Insieme ai partner internazionali, l'UE continuerà a sostenere l'**Ucraina**, anche con un dialogo sulle questioni informatiche. In considerazione dell'esperienza dell'Ucraina nello sviluppo di capacità di resilienza e di ciberdifesa, lo scambio di buone pratiche in materia di ciberdifesa, comprese le informazioni sul panorama delle minacce e la conoscenza situazionale nonché i pertinenti sviluppi politici, è di interesse comune, proseguirà e sarà ampliato.

I partner che condividono gli stessi principi svolgono un ruolo importante nel mantenere un ciberspazio globale, aperto, stabile e sicuro e possono integrare la capacità dell'UE di prevenzione, scoraggiamento, deterrenza e risposta a comportamenti dolosi nel ciberspazio. L'UE rimane aperta a un'interazione vasta, ambiziosa e reciprocamente vantaggiosa in materia di sicurezza e difesa con tutti i partner che condividono gli stessi principi, anche per quanto riguarda la ciberdifesa,

4.3. Sostegno allo sviluppo di capacità di ciberdifesa a favore dei paesi partner

Le sfide globali e regionali hanno aumentato l'interdipendenza reciproca dell'UE e dei suoi partner e hanno evidenziato la necessità di stabilire partenariati più stretti in materia di sicurezza e difesa. Si tratta di un aspetto particolarmente rilevante per i paesi candidati all'adesione all'UE. I recenti attacchi informatici su larga scala mettono in evidenza la necessità di rafforzare l'interazione e il partenariato dell'UE in materia di sicurezza e ciberdifesa muovendo dai programmi esistenti. Data la transnazionalità delle minacce informatiche, il rafforzamento della ciberresilienza dei paesi partner, soprattutto di quelli con un grado inferiore di maturità informatica, contribuirà a rendere il ciberspazio più sicuro e protetto. Di conseguenza l'UE sarebbe maggiormente in grado di prevenire, rilevare e scoraggiare gli attacchi informatici e di difendersi da essi. L'UE rafforzerà la cooperazione in materia di sicurezza e difesa con i paesi partner al fine di potenziarne la ciberresilienza, anche tramite i dialoghi esistenti. Ove applicabile e reciprocamente vantaggioso, l'UE si impegnerà nelle iniziative di sviluppo delle capacità di ciberdifesa dei partner, in particolare in quelle dei paesi candidati all'adesione all'UE allineati con la politica estera e di sicurezza comune dell'UE e con la politica di sicurezza e di difesa comune. Ciò potrebbe includere il sostegno a favore di quadri strategici e legislativi, la formazione, la consulenza, il tutoraggio e l'equipaggiamento delle

forze armate e di sicurezza dei partner. Gli Stati membri potrebbero decidere di prestare ai partner assistenza operativa in materia di ciberdifesa. L'UE aiuterà i partner a rafforzare la capacità di contribuire alle missioni e operazioni militari della PSDC, in quanto si tratta di un apporto prezioso allo sforzo comune di promuovere la pace e la sicurezza.

Lo strumento europeo per la pace (EPF) continuerà a sostenere le iniziative dell'UE volte a contribuire allo sviluppo di capacità di difesa, ciberdifesa inclusa, nei paesi partner, in particolare nel vicinato dell'UE, integrando le attività di gestione delle crisi della PSDC. A questo proposito, ove necessario l'UE collegherà meglio l'assistenza alla ciberdifesa con lo sviluppo di capacità civili in materia di cibersicurezza, in particolare tramite il comitato dell'UE per lo sviluppo delle capacità informatiche. Ai fini del successo delle azioni di sviluppo di capacità in materia di ciberdifesa e di cibersicurezza sarà necessario un coordinamento efficiente tra i programmi e gli strumenti pertinenti dell'UE, compreso l'EPF, e gli Stati membri.

Nel fornire sostegno ai paesi partner nello sviluppo di capacità in materia di ciberdifesa, l'UE lavorerà a stretto contatto con gli altri donatori per sviluppare piattaforme di conoscenza situazionale e di coordinamento al fine di fornire il miglior sostegno personalizzato possibile e di garantire la coerenza e la non duplicazione degli sforzi.

Azioni in materia di ciberdifesa

- Rafforzare la cooperazione UE-NATO nel settore della ciberdifesa, in termini di formazione, istruzione, conoscenza situazionale ed esercitazioni.
- Includere la ciberdifesa nei dialoghi a guida UE con i paesi partner nel settore cibernetico e in materia di sicurezza e difesa.
- Cooperare con i paesi che condividono gli stessi principi, anche nel contesto dello sviluppo di capacità in materia di ciberdifesa e ciberresilienza.
- Aumentare l'assistenza ai partner per lo sviluppo di capacità in materia di ciberdifesa, anche attraverso lo strumento europeo per la pace (EPF), **in particolare nel vicinato dell'UE e a sostegno dei paesi candidati all'adesione all'UE.**

Azioni a sostegno di soggetti civili

- Rafforzare la cooperazione UE-NATO nel campo della cibersicurezza per quanto riguarda la conoscenza situazionale, la risposta alle crisi, la protezione delle infrastrutture critiche, la normazione e la certificazione.

III. CONCLUSIONI

L'alto rappresentante, anche nella sua veste di capo dell'AED, e la Commissione invitano gli Stati membri a sviluppare gli aspetti d'interesse della politica di ciberdifesa e si coordineranno con gli Stati membri per individuare le misure pratiche di attuazione. In cooperazione con gli Stati membri potrebbe essere stabilito un piano di attuazione. I risultati dell'attuazione della politica di ciberdifesa dell'UE concorreranno al conseguimento degli obiettivi generali della strategia dell'UE per la cibersecurity e della bussola strategica.

Al Consiglio sarà presentata annualmente una relazione di monitoraggio e valutazione dello stato di attuazione della politica di ciberdifesa. Gli Stati membri sono invitati a contribuire alla relazione comunicando l'andamento dell'attuazione che fa capo a misure nazionali o cooperative.