La Politica di ciberdifesa dell'Unione europea. Comunicazione congiunta dalla Commissione e dell'Alto Rappresentante per gli affari esteri e la politica di sicurezza dell'UE

Dossier n° 11 -
13 marzo 2023

Tipo e numero atto	*Comunicazione congiunta dalla Commissione e dell'Alto Rappresentante per gli affari esteri e la politica di sicurezza dell'UE – JOIN(2022)49*
Data di adozione	*10 novembre 2022*
Settori di intervento	*Politica di sicurezza e di difesa comune; sicurezza delle infrastrutture critiche; Tecnologie dell'informazione, telecomunicazioni e trattamento dei dati*
Esame presso le istituzioni dell'UE	*La comunicazione è stata trasmessa al Consiglio ed al Parlamento europeo, che ancora deve avviarne l'esame*
Assegnazione	*Commissioni IV e IX*
Segnalazione da parte del Governo	*Sì*
Relazione del Governo ex art. 6 della legge 234	*No*

Finalità

La comunicazione **"*La politica di ciberdifesa dell'UE*"**, presentata dalla Commissione e dall'Alto Rappresentante il **10 novembre 2022**, propone una serie di **iniziative** volte alla **creazione** di una **capacità di ciberdifesa dell'UE a tutto spettro**, dalla ricerca al rilevamento, alla protezione ed alla risposta agli attacchi condotti da soggetti statali e non statali nell'ambito del ciberspazio, sulla base del **mandato ricevuto dal Consiglio** dell'UE nelle conclusioni del 23 maggio 2022 sulla **deterrenza informatica** dell'UE.

La creazione di una capacita di ciberdifesa dell'UE è una delle **priorità** indicate dalla **Bussola Strategica dell'UE**, approvata dal Consiglio del 21 marzo 2022.

Il **Consiglio europeo** nella riunione del **15 dicembre 2022** ha adottato delle **conclusioni** nelle quali, in particolare, ha **chiesto:** a) la definizione di una **politica forte dell'UE in materia di ciberdifesa**; b) **investimenti** per la cibersicurezza e la connettività spaziale, nonché per la resilienza delle infrastrutture critiche.

La comunicazione congiunta delinea **quattro linee di azione prioritarie**:

1. **promuovere un'azione comune** per rafforzare la ciberdifesa dell'UE rafforzando i **meccanismi di coordinamento fra attori nazionali e dell'UE**;
2. **mettere in sicurezza l'ecosistema di difesa dell'UE**;
3. **aumentare gli investimenti** in capacità di ciberdifesa;
4. promuovere **partenariati con Paesi terzi** per superare le sfide comuni.

Il contesto delle azioni per lo sviluppo di capacità di ciberdifesa dell'UE

La ciberdifesa dell'UE nel contesto globale

La comunicazione evidenzia come negli ultimi anni:

- si siano **intensificati i comportamenti dolosi di soggetti statali e non statali nel ciberspazio**, 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 dell'UE. Anche **l'aggressione militare della Russia contro l'Ucraina** ha evidenziato l'urgenza per l'UE di difendere i propri interessi nel ciberspazio;
- i **confini tra la dimensione civile e quella militare del ciberspazio vanno sfumandosi**, come dimostrano i recenti attacchi alle reti energetiche, alle infrastrutture di trasporto e di telecomunicazioni;
- sia **aumentata l'interdipendenza tra infrastrutture fisiche e digitali** e la possibilità che incidenti di cibersicurezza gravi possano perturbare o danneggiare le infrastrutture critiche;
- le **minacce alla cibersicurezza** rientrino 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** ed anche minare il **funzionamento delle democrazie**, anche attraverso **attacchi alle infrastrutture elettorali**.

A fronte di tale quadro, **l'UE deve assumersi maggiori responsabilità** per la propria sicurezza e gli **Stati membri** devono impegnarsi ad **aumentare gli investimenti** nelle capacità di ciberdifesa a tutto spettro.

La **prevenzione ed 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 poter essere **trasformati in intelligence utilizzabile**, che possa servire tanto per la cibersicurezza quanto per la ciberdifesa.

La comunicazione evidenzia come la **cooperazione tra le cibercomunità civili e della difesa** è alla base di una **migliore conoscenza situazionale comune** nel ciberspazio ed è cruciale per una **risposta coordinata alle crisi**.

Poiché le cibertecnologie presentano un forte **potenziale di duplice uso**, la comunicazione indica che le **industrie e le attività di ricerca e sviluppo** nel settore della **cibersicurezza** e della **ciberdifesa** devono **lavorare in modo molto più sinergico**.

La comunicazione indica, altresì, **l'importanza di una collaborazione con il settore privato** e, in particolare la necessità di **fornitori privati di fiducia** che agiscano come forza di riserva per la cibersicurezza per migliorare la risposta in caso di attacchi informatici.

Infine, considerata il carattere transnazionale delle minacce informatiche, si indica la **necessità di sviluppare partenariati** e reciprocamente vantaggiosi con i **Paesi che condividono gli stessi valori.**

Le iniziative dell'UE per il rafforzamento della ciberdifesa

Il quadro strategico dell'UE in materia di ciberdifesa del 2018

Il **19 novembre 2018**, il **Consiglio dell'UE** ha adottato una **versione aggiornata del quadro strategico dell'UE in materia di ciberdifesa**, che era stata inizialmente approvata dal Consiglio dell'UE il 18 novembre 2014, su mandato del Consiglio europeo del dicembre 2013.
Il quadro strategico riconosce il **ciberspazio** come il **quinto dominio operativo**, accanto a quelli terrestre, marittimo, aereo e spaziale, ed individua le seguenti **priorità**:

- promuovere lo **sviluppo delle capacità** di ciberdifesa degli Stati membri;

- rafforzare la **protezione dei sistemi di comunicazione e informazione nell'ambito della Politica di sicurezza e difesa** dell'UE;
- incentivare la **cooperazione civile-militare**;
- promuovere la dimensione europea di **ricerca e sviluppo nel settore della ciberdifesa**;
- incentivare una **cultura comune di ciberdifesa** in tutta l'UE attraverso attività di formazione, istruzione ed esercitazioni in materia di ciberdifesa;
- potenziare la **cooperazione con i partner internazionali.**

La Bussola strategica

La Bussola strategica dell'UE - il documento approvato dal Consiglio dell'UE il 21 marzo 2022 e poi dal Consiglio europeo del 24 e 25 marzo 2022, che definisce il quadro strategico delle azioni dell'UE nell'ambito della politica estera e di sicurezza per i prossimi anni – ha, in particolare, **impegnato l'UE e gli Stati membri a sviluppare ulteriormente la politica dell'UE in materia di ciberdifesa**.
La Bussola strategica indica le **seguenti priorità ed obiettivi**:

- è necessario **aumentare la cooperazione** tra gli **attori della ciberdifesa** dell'UE e degli Stati membri e s**viluppare meccanismi di mobilitazione delle capacità a livello dell'UE**, anche nel contesto delle **missioni e operazioni PSDC**;
- dovrà essere **rafforzata la cooperazione con partner** che condividono gli stessi principi nel settore della ciberdifesa, in particolare con la **NATO**, anche sostenendo i partner nel rafforzamento della loro ciberresilienza e, in caso di crisi informatiche, inviando esperti dell'UE e degli Stati membri per offrire assistenza;
- una **nuova normativa europea sulla ciberresilienza** dovrà rafforzare l'approccio comune dell'UE in **materia di infrastrutture informatiche**;
- verranno avviati lavori per la **creazione di un'infrastruttura europea di centri operativi di sicurezza**;
- in linea con la strategia dell'UE per la cibersicurezza del 2020, verrà **sviluppata la posizione in materia di deterrenza informatica dell'Unione** migliorando la capacità di prevenire gli attacchi informatici attraverso lo sviluppo e il potenziamento delle capacità, la formazione, le esercitazioni, un'accresciuta resilienza;
- si prevedono **esercitazioni periodiche nel settore informatico** per contribuire ad aumentare ulteriormente la solidarietà e l'assistenza reciproca;
- dovranno essere **rafforzate le capacità di intelligence informatica** per accrescere ciberresilienza dell'UE, fornendo anche un sostegno efficace alle missioni e operazioni PSDC in ambito civile e militare, come pure alle forze armate dell'UE;
- verrà promossa una **maggiore interoperabilità e condivisione di informazioni** attraverso la **cooperazione tra squadre di pronto intervento informatico militari** (**MilCERT**), come anche nello svolgimento di operazioni informatiche difensive;
- il **potenziamento della ciberdifesa** può dare un forte **impulso alla ricerca e all'innovazione**, stimolando la base industriale dell'UE.

Lo sviluppo delle capacità di ciberdifesa

Nella comunicazione congiunta della Commissione e dell'Alto Rappresentante "**sull'analisi delle carenze di investimenti nel settore della difesa e sulle prospettive di percorso"** (JOIN (2022) 24), del **18 maggio 2022,** tra le **capacità e medio e lungo termine** sulle quali si propone di lavorare per migliorare le capacità difesa dell'Europa vi è la **ciberdifesa** (gli altri 4 settori individuati come prioritari sono il settore aereo, quello terrestre, quello marittimo e lo spazio).

In particolare, nella comunicazione si afferma che "*in risposta al crescente rischio di attacchi informatici da parte di attori statali nel contesto della concorrenza geopolitica, l'UE e i suoi Stati membri potrebbero avviare lavori per giungere a una* ***capacità di ciberdifesa a tutto spettro*** *(dalla ricerca, individuazione e protezione alla risposta, comprese le capacità di difesa attiva). Ciò prevedrebbe capacità per la* ***conoscenza situazionale informatica*** *e la* ***condivisione di informazioni*** *(anche mediante potenziali sinergie con un'infrastruttura europea di "ciberscudo" dei centri operativi di sicurezza), un* ***comando e controllo ciberresiliente e interoperabile per le operazioni e le missioni militari, esercitazioni e formazioni di cibersicurezza*** *e* ***forze di riserva per la cibersicurezza a livello nazionale****".*

La deterrenza informatica dell'UE

Il **23 maggio 2022** il Consiglio ha adottato delle conclusioni sulla **deterrenza informatica** dell'UE nelle quali, osservando che la **ciberdifesa è in primo luogo una responsabilità nazionale:**

- **incoraggia gli Stati membri a** sviluppare ulteriormente le proprie **capacità di condurre operazioni di ciberdifesa**, comprese **misure proattive** per individuare e scoraggiare gli attacchi informatici **nonché proteggersi e difendersi** da questi ultimi ed anche per **fornire assistenza ad altri Stati membri e all'UE**;
- sottolinea che **l'ulteriore sviluppo di tali capacità** dovrebbe essere uno degli **obiettivi principali della futura politica dell'UE in materia di ciberdifesa** ed osserva che la politica dell'UE in materia di ciberdifesa dovrebbe tenere maggiormente conto del **ruolo che le istituzioni e gli organi competenti dell'UE possono svolgere** per intensificare la cooperazione tra gli attori della ciberdifesa dell'UE e degli Stati membri;
- sottolinea la necessità di **aumentare l'interoperabilità e la condivisione di informazioni** attraverso la cooperazione tra squadre di pronto intervento informatico militari (*Military Computer Emergency Readiness Team* - MilCERT) e sottolinea **l'importanza della cooperazione tra la rete MilCERT** e la rete civile dei ***CSIRT*** nazionali (*Computer Security Incident Response Team - CSIRT*) per migliorare la condivisione delle informazioni e la conoscenza situazionale;
- ribadisce la necessità di **integrare la dimensione informatica nella pianificazione e nello svolgimento delle missioni e operazioni PSDC**, anche potenziandone le capacità informatiche.

Il Consiglio europeo del 15 dicembre 2022

Il **Consiglio europeo** nella riunione del **15 dicembre 2022** ha adottato delle **conclusioni** sul tema della sicurezza e difesa nelle quali, per quanto riguarda in particolare l'ambito della **ciberdifesa**, ha **chiesto:**

- la **definizione di una politica forte dell'UE in materia di ciberdifesa** sulla base della recente comunicazione congiunta della Commissione e dell'alto rappresentante;
- **investimenti** in abilitanti strategici quali la **cibersicurezza e la connettività spaziale**, nonché nella **resilienza delle infrastrutture critiche**.

I progetti PESCO nel settore della ciberdifesa

Nell'ambito della **cooperazione strutturata permanente nel settore della difesa (PESCO)** - avviata nel dicembre 2017 fra 25 Stati membri, tra i quali l'Italia - si prevede l'impegno a intensificare la **cooperazione in materia di ciberdifesa**.

Con diretta implicazione della **ciberdifesa e cibersicurezza** sono in corso i seguenti **progetti PESCO**:

- creazione **gruppi di risposta rapida agli incidenti informatici e mutua assistenza** in materia di cibersicurezza (*Cyber Rapid Response Teams - CRRT*), progetto coordinato dalla Lituania, al quale **l'Italia non partecipa**;
- sviluppo di una **piattaforma per la condivisione delle informazioni in materia di minaccia informatica e di risposta** agli incidenti informatici (*Cyber Threats and Incident Response Information Sharing Platform - CTIRISP*) progetto coordinato dalla Grecia, al quale **l'Italia partecipa**;
- istituzione di un **centro di coordinamento nel settore informatico e dell'informazione** (*Cyber and Information Domain Coordination Center - CIDCC*), progetto coordinato dalla Germania, **al quale l'Italia non partecipa**;
- alla promozione di un **Poligono virtuale federato** (*Cyber Ranges Federations - CRF*), al fine di condividere e mettere in comune le capacità e migliorare la qualità degli addestramenti e delle esercitazioni in campo informatico, nonché utilizzare la federazione per scopi di ricerca e sviluppo in campo informatico, progetto coordinato dall'Estonia, **al quale l'Italia partecipa**;
- istituzione di una **Accademia e polo di innovazione dell'UE nel settore dell'informatica** (*EU CAIH*), progetto coordinato dal Portogallo, **al quale l'Italia non partecipa**;
- produzione di uno **studio di fattibilità sulle attuali capacità di guerra elettronica dell'UE** e delle lacune che devono essere colmate, progetto coordinato dalla Repubblica ceca, **al quale l'Italia non partecipa**.

Le iniziative dell'UE per la cibersicurezza e la resilienza delle infrastrutture critiche

Le recenti iniziative volta a rafforzare la ciberdifesa si collocano nel **contesto più ampio** delle iniziative già avviate dall'Unione volte a rafforzare la **cibersicurezza** e **resilienza delle infrastrutture critiche nell'UE**.

Gli **attacchi informatici** e la **criminalità informatica** stanno aumentando in tutta Europa in termini sia di quantità che di sofisticazione, una tendenza destinata a crescere in futuro, visto che si prevede che 22,3 miliardi di dispositivi in tutto il mondo saranno collegati all'internet delle cose entro il 2024 (cfr. i dati riportati sul sito del Consiglio).

Nel **dicembre 2020** la Commissione europea e il Servizio europeo per l'azione esterna (SEAE) hanno presentato una nuova strategia per la cibersicurezza, il cui obiettivo principale è quello di **rafforzare la resilienza dell'Europa** a fronte delle minacce informatiche e garantire che tutti i cittadini e le imprese possano beneficiare pienamente di servizi e strumenti digitali affidabili e attendibili. La nuova strategia include proposte concrete per l'introduzione di strumenti normativi, strategici e di investimento.

Per quanto riguarda la **normativa in materia cibersicurezza** si ricordano:

- il **regolamento UE sulla cibersicurezza**, entrato in vigore nel giugno 2019, che ha introdotto un **quadro unico di certificazione in tutta l'UE** e un mandato rafforzato per l'**Agenzia dell'UE per la cibersicurezza**;
  La nuova Agenzia dell'UE per la cibersicurezza si basa sulle strutture del suo predecessore, l'Agenzia europea per la sicurezza delle reti e dell'informazione (del quale ha adottato lo stesso acronimo ENISA), ma ha il compito di sostenere gli Stati membri, le istituzioni dell'UE e altre parti interessate nella gestione degli attacchi informatici.
- il regolamento che istituisce il **Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca**, adottato nell'aprile 2021. Sostenuto da una rete di centri nazionali di coordinamento, il nuovo Centro mira a: migliorare ulteriormente la ciberresilienza; contribuire alla diffusione delle tecnologie più recenti nel settore della cibersicurezza; sostenere le *start-up* e le PMI del settore della cibersicurezza; rafforzare la

ricerca e l'innovazione in materia di cibersicurezza; contribuire a colmare il divario di competenze in materia di cibersicurezza;

- la **direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione** (cosiddetta NIS 2 - *Security of network and information systems*), che abroga la direttiva (UE) 2016/1148 al fine di migliorare la resilienza e le capacità di risposta agli incidenti del settore pubblico e privato e dell'UE nel suo complesso. La direttiva è stata adottata il 28 novembre 2022 insieme a un regolamento sulla resilienza operativa digitale (regolamento DORA), che intende rafforzare la sicurezza informatica delle entità finanziarie quali banche, compagnie di assicurazione e imprese di investimento;
- la **direttiva sulla resilienza dei soggetti critici**, adottata in occasione del Consiglio giustizia e affari interni (GAI) dell'8 dicembre 2022;
- il **pacchetto di strumenti** (5G Toolbox) concordato dall'UE nel gennaio 2020 per fornire orientamenti ed individuare possibili misure comuni tese ad attenuare i principali rischi per la **cibersicurezza delle reti 5G;**
- **la proposta di regolamento che istituisce il programma dell'Unione per una connettività sicura per il periodo 2023-2027**, **approvata definitivamente dal Consiglio il 7 marzo 2023**. Il programma mira a far sì che l'Unione europea disponga di una propria costellazione di satelliti denominata "IRIS^2" (Infrastruttura per la resilienza, l'interconnettività e la sicurezza via satellite), che dovrebbe assicurare **servizi di comunicazione sicuri** entro il 2027. Il programma, con un importo totale di 2,4 miliardi di euro, fornirà **servizi governativi** che spazieranno dalla protezione delle infrastrutture critiche e la conoscenza situazionale al sostegno per le azioni esterne e la gestione delle crisi, ma anche la fornitura di servizi commerciali da parte del **settore privato**.

Relativamente ai finanziamenti per la cibersicurezza, nel quadro del **programma Europa digitale** per il periodo 2021-2027, l'UE si è impegnata a investire **1,6 miliardi di euro** in capacità di cibersicurezza e nell'ampia diffusione di infrastrutture e strumenti per la cibersicurezza in tutta l'UE a favore di pubbliche amministrazioni, imprese e singoli cittadini e **nell'ambito del programma di ricerca e innovazione Orizzonte Europa** ha stanziato **49 milioni di euro** per promuovere l'innovazione nei sistemi di cibersicurezza e privacy.

I contenuti della comunicazione sulla politica di ciberdifesa dell'UE

Al fine di sviluppare da un punto di vista operativo le indicazioni sopra illustrate volte al rafforzamento della ciberdifesa dell'UE, la comunicazione indica una **serie di iniziative** - suddivise in **azioni in materia di ciberdifesa** e azioni a **sostegno di soggetti civili** - articolate in **4 aree:**

1. **promuovere un'azione comune** per rafforzare la ciberdifesa dell'UE, rafforzando i **meccanismi di coordinamento fra attori nazionali e dell'UE**;
2. mettere in **sicurezza l'ecosistema della difesa**;
3. **aumentare gli investimenti** nelle capacità di ciberdifesa;
4. **cooperare con i Paesi partner** per affrontare le sfide comuni.

Promuovere un coordinamento comune per rafforzare la ciberdifesa dell'UE

La comunicazione indica le necessità di **rafforzare i meccanismi di coordinamento fra attori nazionali e dell'UE** nel settore della ciberdifesa, al fine di **intensificare lo scambio di informazioni** e la cooperazione fra le comunità militari e civili della ciberdifesa e sostenere maggiormente le missioni e le operazioni militari dell'UE nell'ambito della politica di sicurezza e di difesa comune-PSDC).
In particolare, sotto tale profilo, si indicano le seguenti azioni ed iniziative:

Azioni in materia di ciberdifesa

- istituire un **centro di coordinamento della ciberdifesa dell'UE (EUCDCC)** come **centro per la conoscenza situazionale militare comune**;
  L'Alto Rappresentante, sulla base del progetto della PESCO relativo al centro di coordinamento nel settore informatico e dell'informazione (CIDCC), sottoporrà all'esame degli Stati membri la proposta di istituzione dell'EUCDCC. Dovrebbero essere stabiliti collegamenti adeguati tra l'EUCDCC e il Centro UE di situazione e di intelligence (INTCEN), istituito presso il Servizio per l'azione esterna dell'UE (SEAE), nonché l'Intelligence dello Stato maggiore dell'UE. 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. L'UCDCC dovrebbe inoltre stabilire forme di cooperazione con il Centro di analisi e consapevolezza situazionale sulla cybersicurezza in via di costituzione presso la Commissione europea con il mandato di sostenere la consapevolezza situazionale e la risposta coordinata alle crisi, comprese quelle di natura ibrida.
- istituire una **conferenza dei comandanti per la sicurezza informatica dell'UE, che si dovrebbe riunire almeno due volte l'anno per discutere questioni operative e altri temi di interesse;**
  Tale conferenza si dovrebbe sviluppare sulla base del forum permanente che i comandanti per la sicurezza informatica dell'UE (CyberCo) hanno deciso di istituire al loro livello sulla base dei primi due incontri tenutisi a gennaio e a giugno 2022. 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 e per combinare esperienza militare e conoscenza situazionale civile a livello strategico e operativo.
- creazione della **rete operativa MICNET**, ossia la rete dei *Computer Emergency Response Team* militari nazionali (milCERT), e avviare iniziative per **stabilire una cooperazione con la rete dei** *Computer Security Incident Response Team* (CSIRT) civili nazionali;
  La rete MICNET, che sarà creata con il sostegno dell'Agenzia europea per la difesa (*European Defence Agency EDA*), avrà lo scopo di facilitare lo scambio di informazioni tra le milCERT e promuovere 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. In prospettiva, la MICNET dovrebbe, inoltre, **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'EDQ sosterrà infatti 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, inoltre, vagliato il **coinvolgimento del settore privato** nelle attività di condivisione di informazioni e di risposta agli incidenti. Si ricorda che il **CSIRT Italia** è stato istituito presso l'Agenzia per la cybersicurezza nazionale (ACN) con il compiti di: monitoraggio degli incidenti a livello nazionale; emissione di preallarmi, allerte, annunci e divulgazione di informazioni alle parti interessate in merito a rischi e incidenti; intervento in caso di incidente; analisi dinamica dei rischi e degli incidenti; sensibilizzazione situazionale; partecipazione alla rete dei CSIRT.
- sviluppare un **nuovo progetto quadro CyDef-X** che riunirà tutti gli Stati membri e servirà da **quadro di riferimento per le 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 PESCO *Cyber Rapid Response Teams - CRRT* già in corso (*v. supra*);

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 relativo progetto CRRT della PESCO. 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.

- vagliare le possibilità di **sviluppo ulteriore di progetti del Poligono virtuale federato**, sulla base del progetto PESCO *Cyber ranges federations – CRF* già in corso (*v. supra*);

Azioni a sostegno di soggetti civili

- preparare un'**iniziativa di cibersolidarietà dell'UE**, compresa la possibilità di apportare modifiche legislative al regolamento relativo 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 cibersicurezza** a livello di UE, con **servizi prestati da operatori privati** di fiducia;
  - effettuare prove presso **soggetti critici** al fine di **rilevarne potenziali vulnerabilità**.
    La Commissione ha avviato il 22 novembre 2022 un'iniziativa volta a promuovere la realizzazione di **un'infrastruttura dell'UE dei centri operativi di sicurezza nazionali (SOC),** con l'obiettivo 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. Il programma Europa digitale, attraverso una sua modifica legislativa, dovrebbe inoltre consentire di sostenere finanziariamente a più lungo termine, e a integrazione dei finanziamenti nazionali, appalti congiunti di strumenti e infrastrutture ultrasicuri di prossima generazione.
- vagliare lo sviluppo di **sistemi di certificazione della cibersicurezza** a livello UE per **l'industria** della cibersicurezza e le **imprese private**;
- migliorare la **cooperazione a livello strategico, operativo e tecnico** tra le **cibercomunità della ciberdifesa** e **quelle di altro tipo**.

Mettere in sicurezza l'ecosistema della difesa

Considerato che persino i componenti *software* non critici possono essere usati per attacchi informatici contro imprese o Governi, la comunicazione afferma la necessità di **lavorare ulteriormente alla normazione e certificazione della cibersicurezza** per mettere al riparo sia il settore civile sia quello militare. La comunicazione rileva, infatti, come le **forze armate dipendano in larga misura dalle infrastrutture critiche civili** per la mobilità, le comunicazioni o l'energia.

Nella comunicazione si osserva che gli **Stati membri stanno sviluppando** per i loro 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 e crea ostacoli all'assistenza reciproca**.

La comunicazione reputa anche necessario **promuovere maggiori sinergie tra i percorsi di normazione militari e civili**, dato che, per **l'industria**, il fatto di dover rispettare norme diverse per i clienti civili e per quelli militari aumenta i **costi di produzione** dei **prodotti a duplice uso**.

In particolare, sotto tale profilo, si indicano le seguenti azioni ed iniziative:

Azioni in materia di ciberdifesa

- sostenere gli Stati membri nello **sviluppo di raccomandazioni non giuridicamente vincolanti per la comunità della difesa**, ispirate alle disposizioni della direttiva NIS2 (*che non si applicano al settore della difesa*), al fine di contribuire a una maggiore maturità complessiva della ciberdifesa a livello nazionale;
  La direttiva NIS2, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, approvata lo scorso novembre e in corso di pubblicazione, abroga e sostituisce la direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (cosiddetta direttiva NIS1). La nuova direttiva NIS 2 contiene disposizioni volte a precisare e rafforzare gli obblighi già previsti dalla diretta NIS1 di adottare misure tecniche ed organizzative adeguate e proporzionate rispetto alla gestione dei rischi cyber e misure volte a prevenire e minimizzare l'impatto degli eventuali incidenti di sicurezza, ed estende l'ambito di applicazione delle sue disposizioni ad altre società e imprese, rispetto a quelle già previste dalla Direttiva NIS1.
- formulare **raccomandazioni sui requisiti di interoperabilità** per la ciberdifesa dell'UE;
  L'Agenzia europea per la difesa e lo Stato maggiore dell'UE svilupperanno raccomandazioni in merito a una serie di requisiti di interoperabilità della ciberdifesa dell'UE. L'armonizzazione dei requisiti per le capacità di ciberdifesa di prossima generazione potranno facilitare le attività di collaborazione ed eventualmente portare a iniziative di sviluppo e approvvigionamento congiunti.
- rafforzare la **cooperazione con tutti i soggetti** pertinenti in merito alle **norme** relative alla **difesa** nel quadro del Comitato europeo di normazione della difesa;
  Il **Comitato europeo di standardizzazione della difesa** (EDSC), costituito **presso l'EDA** nel 2020 ha il compito di sostenere e coordinare gli sforzi degli Stati membri per una maggiore standardizzazione della difesa europea con l'obiettivo di facilitare le missioni e le operazioni della PSDC e di rafforzare la base industriale e tecnologica della difesa europea (EDTIB).

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;
  Su richiesta del Consiglio, la Commissione, l'Alto rappresentante e il gruppo di cooperazione NIS stanno sviluppando scenari di rischio per la sicurezza delle infrastrutture digitali. L'attenzione si concentrerà innanzitutto sulla cibersicurezza nei **settori dell'energia, delle telecomunicazioni, dei trasporti e dello spazio**. Saranno inoltre preparate valutazioni mirate dei rischi di cibersicurezza 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**). 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 cibersicurezza delle infrastrutture critiche nel contesto del sistema energetico sono, invece, contenute nel piano d'azione dell'UE "Digitalizzare il sistema energetico", presentato dalla Commissione il 18 ottobre 2022. Mentre la **strategia spaziale dell'UE per la sicurezza e la difesa** annunciata nella bussola strategica delineerà ulteriori misure destinate a migliorare la solidità e la ciberresilienza delle infrastrutture spaziali e dei servizi collegati.
- promuovere la **cooperazione tra gli organismi di normazione civili e militari** per la definizione di **norme armonizzate per i prodotti a duplice uso**.
  Nella comunicazione si indica che gli Stati membri dovrebbero avvalersi di sistemi di certificazione della cibersicurezza e che 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 previsto nel piano d'azione sulle sinergie tra l'industria civile,

della difesa e dello spazio, la Commissione, intende, inoltre, presentare un **piano destinato a promuovere l'uso delle vigenti norme ibride civili/della difesa e lo sviluppo di nuove norme**. Dovrebbe, infine, essere ulteriormente sviluppata 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**, sfruttando al meglio a tal fine il **comitato europeo di normazione nel settore della difesa** istituito nell'ambito della Agenzia europea per la difesa (*v. supra*).

Aumentare gli investimenti nelle capacità di ciberdifesa

La comunicazione evidenzia come i **miglioramenti tecnologici siano essenziali** per **mantenere un vantaggio rispetto a concorrenti** e avversari e **ovviare alle vulnerabilità derivanti sia dalle dipendenze strategiche** e sia dalla **frammentazione della base industriale e tecnologica di difesa europea**.

La comunicazione constata che **l'industria dell'UE della difesa**, per quanto riguarda in particolare la ciberdifesa, si affida sostanzialmente a **soluzioni civili e a mercati esterni** e rileva le seguenti **criticità** che impediscono all'UE di avere una presenza forte a livello globale nell'ambito della cibersicurezza e ciberdifesa:

- sebbene i progressi tecnologici in ambito civile siano rapidi e il mercato dei prodotti civili per l'informazione e la cibersicurezza 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;
- la **frammentazione della base industriale e tecnologica di difesa** dell'UE (EDTIB) ne riduce notevolmente la capacità di migliorare la competitività, in quanto la maggior parte delle imprese che si occupano di cibersicurezza nell'UE sono **piccole e medie imprese** (PMI).

  La Commissione stima che il **numero totale di PMI** che nell'UE operano nelle catene di approvvigionamento multilivello e spesso transfrontaliere del settore della difesa sia pari a **2500**. Tali imprese servono clienti del settore della difesa e il **7,8 % delle loro attività riguarda il settore informatico**.

Per ovviare alle suddette criticità, la Commissione intende promuovere la **valorizzazione delle sinergie tra imprese civili e del settore della difesa** ed avviare un dialogo con il settore al fine di sviluppare l'industria dell'UE della ciberdifesa, coinvolgendo opportunamente l'Agenzia europea per la difesa.

A tal fine, nell'immediato, la comunicazione indica le necessità di avviare 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 ed indica che le **dipendenze critiche nel settore informatico**, 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.

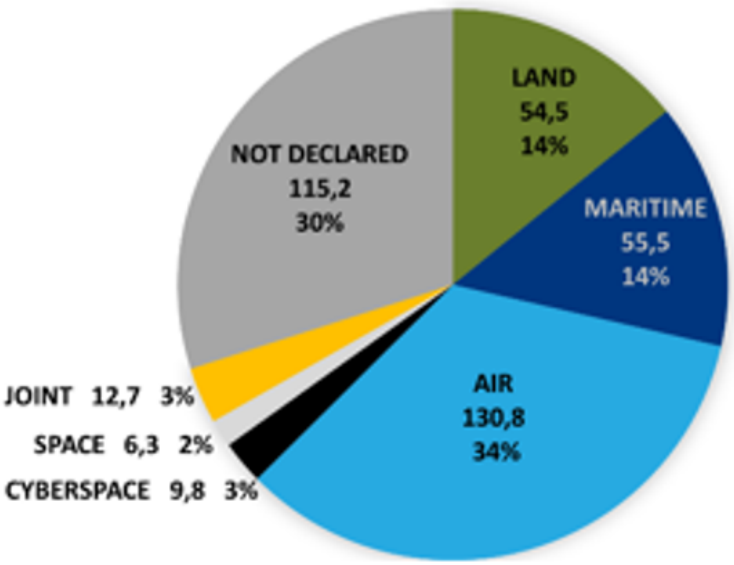
Allo stesso tempo la comunicazione ricorda che il **quadro dell'UE in materia di controllo degli investimenti esteri diretti** continuerà a essere **utilizzato per attenuare i rischi di acquisizioni** di tecnologie o soluzioni europee che presentano rischi in materia di difesa e sicurezza.

La comunicazione rileva, inoltre, che 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.

Sulla base di tale quadro nella comunicazione si indica la priorità per l'UE e gli Stati membri di **rafforzare la cooperazione e l'interoperabilità in materia di ciberdifesa sviluppando capacità congiunte** e **aumentare gli investimenti** in ricerca e sviluppo, collaborando tramite le

piattaforme di cooperazione e i meccanismi di finanziamento disponibili a livello di UE, quali la cooperazione strutturata permanente (PESCO) e il Fondo europeo per la difesa (FED), il programma di ricerca e sviluppo Orizzonte Europa e il programma Europa digitale.
La comunicazione **invita gli Stati membri** a prendere in considerazione l'elaborazione - nell'ambito del processo di revisione coordinata annuale sulla difesa (CARD) - 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 esistenti.
La Coordinated Annual Review on Defence (CARD) è un **processo di monitoraggio dei piani di difesa degli Stati membri dell'Unione Europea**, coordinato dall'Agenzia per la difesa europea per aiutare a coordinare le spese e identificare possibili progetti di collaborazione.
Nell'ultimo **rapporto sulla CARD**, presentato dall'Agenzia per la difesa europea il 2 dicembre 2022, si evidenzia che il **settore ciberspazio** è uno dei **domini operativi della difesa che riceve minori investimenti** da parte del complesso degli Stati membri dell'UE. Nel **periodo 2019-2025** per il ciberspazio sono previsti complessivamente **9,8 miliardi di euro di investimenti**, pari al circa il **3% degli investimenti complessivi** per l'intero periodo per il complesso degli altri domini operativi.
Il rapporto rileva che la **cooperazione in materia di difesa rimane l'eccezione piuttosto che la norma**. La CARD rileva che gli Stati membri attuano i loro piani in larga misura a livello nazionale, con **solo il 18% di tutti gli investimenti** in programmi di difesa **condotti in cooperazione** con altri Paesi dell'UE.

Totale degli investimenti previsti in miliardi di euro per dominio operativo per il periodo 2019-2025 dagli Stati membri dell'UE (Fonte 2022 Coordinated annual review on defence report)



Al fine di aumentare gli investimenti, la comunicazione indica le seguenti azioni ed **iniziative prioritarie**:
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;
  La comunicazione indica che nei prossimi anni il FED dedicherà particolare attenzione ai progetti di ricerca che riguardano nuove tecnologie sviluppate contro le minacce emergenti. Si ricorda che

fino **all'8% del bilancio del FED** *(circa 8 miliardi di euro per il periodo 2021-2027, di cui 5,3 miliardi lo sviluppo di capacità e 2,6 miliardi per progetti di ricerca a sviluppo)* è destinato a temi che riguardano le **tecnologie di rottura per la difesa**, compresi alcuni temi pertinenti per la ciberdifesa. Inoltre, data la rapidità di evoluzione della tecnologia, si considera opportuno ritagliare su misura le iniziative di ricerca e sviluppo tecnologico in collaborazione, in modo che i risultati possano essere incorporati più rapidamente nelle capacità esistenti e future. A tal fine, l'**EDA** e il **Centro europeo di competenza per la cibersicurezza (ECCC)** svilupperanno valutazioni strategiche 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** in merito alle rispettive priorità per le tecnologie di difesa e a duplice uso in ambito civile.

- definire una **tabella di marcia per le tecnologie in relazione alle cibertecnologie critiche per l'UE**;
  La tabella di marcia per le cibertecnologie critiche dovrebbe essere presentata nel 2023 dalla Commissione, assieme all'Agenzia europea per la difesa (EDA) e agli Stati membri, sulla base di consultazioni anche con il settore industriale. La tabella di marcia per le tecnologie dovrebbe individuare le cibertecnologie critiche per la sovranità tecnologica dell'UE, sia sul versante della ciberdifesa sia su quello della cibersicurezza, e mappare gli sviluppi tecnologici e le dipendenze strategiche, indicando iniziative per mitigare queste ultime.
- proporre percorsi per **ridurre le dipendenze** e **anticipare lo sviluppo tecnologico** al fine di aumentare la sovranità tecnologica e garantire la capacità d'agire utilizzando tutti gli strumenti dell'UE, compresi il programma Europa digitale, il programma Orizzonte Europa e il Fondo europeo per la difesa (FED);
  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 complessivo di 39 milioni di euro. Nel contesto delle azioni finanziate dal **Fondo europeo per la difesa** per il 2021 circa 40 milioni di euro sono stati destinati a **3 progetti collaborativi di ricerca e sviluppo nel settore della ciberdifesa** (ACTING, AInception, EU-GUARDIAN).
- sostenere lo sviluppo di un **quadro di certificazione delle competenze in materia di ciberdifesa**;
- mettere a punto **esercitazioni dell'UE in materia di ciberdifesa**.

Azioni a sostegno di soggetti civili

- istituire **un'accademia dell'UE 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;
  Tale iniziativa, avviata nel contesto dell'Anno europeo delle competenze 2023, è volta ad aumentare il numero di operatori professionali formati in cibersicurezza e sarà articolata in vari filoni d'azione (finanziamento, sostegno alle comunità, formazione e certificazione, coinvolgimento dei portatori di interessi, generazione di conoscenze). Verranno, inoltre previste modalità per facilitare lo **scambio di buone pratiche con l'Accademia europea per la sicurezza e la difesa** (AESD) per rafforzare le sinergie tra il settore militare e quello civile. La comunicazione rileva che l'Europa si trova di fronte a una **carenza allarmante di competenze informatiche** e riporta la stima dell'Organizzazione europea per la cibersicurezza (ECSO) per la quale già nel 2022 erano **necessari complessivamente 500.000 addetti**. La Commissione incoraggia, inoltre, gli **Stati membri a sviluppare programmi di istruzione specifici nel settore della ciberdifesa**, coinvolgendo istituzioni accademiche e di istruzione superiore (civili e militari) creando partenariati e progetti comuni e facilitando lo scambio di formatori e formandi.
- analizzare gli approcci alla **certificazione delle competenze informatiche**, cercando di promuovere sinergie e di colmare le lacune, anche attraverso i finanziamenti dell'UE.

Cooperare con i Paesi partner per affrontare le sfide comuni

La comunicazione evidenzia l'importanza della **cooperazione con i Paesi partner** che condividono gli stessi princìpi e valori, al fine di instaurare **partenariati per gestire le sfide comuni nell'ambito della ciberdifesa** che siano **reciprocamente vantaggiosi**.
In particolare, occorre rafforzare, in via prioritaria, il **partenariato strategico con la NATO** nel **settore della ciberdifesa**, nell'ambito del quale sono necessari ulteriori sforzi per lo sviluppo di soluzioni condivise in relazione a sfide e minacce comuni e **la cooperazione con i Paesi che condivido gli stessi principi**, in particolare gli **Stati Uniti** e i **Paesi candidati all'adesione,** fornendo anche sostegno allo sviluppo delle loro capacità di ciberdifesa.
Al momento l'UE ha concesso lo *status* di paese candidato all'adesione ai seguenti Paesi: Albania, Bosnia Erzegovina, Macedonia del Nord, Moldova, Montenegro, Serbia, Turchia e Ucraina.

In particolare, sotto tale profilo, si indicano le seguenti azioni ed iniziative:

Azioni in materia di ciberdifesa

- **rafforzare** la **cooperazione UE-NATO nel settore della ciberdifesa**, in termini di formazione, istruzione, conoscenza situazionale ed esercitazioni;
  In particolare, l'UE intende collaborare con la NATO per rafforzare **l'interoperabilità tecnica e procedurale** delle capacità di ciberdifesa, con la prospettiva di sinergie nello sviluppo e nell'impiego delle capacità di ciberdifesa. Si dovrebbe prestare particolare attenzione **all'interoperabilità delle norme**, al fine di promuovere l'interoperabilità dei sistemi di comunicazione e informazione militari, coinvolgendo se del caso il settore industriale. Verrà anche rafforzata la **cooperazione con la NATO nell'ambito della formazione**, sviluppando programmi, corsi ed esercitazioni comuni.
- includere la **ciberdifesa nei dialoghi a guida UE con i paesi partner** nel settore cibernetico e in materia di sicurezza e difesa e **cooperare con i paesi che condividono gli stessi principi**, anche nel contesto dello sviluppo di capacità in materia di ciberdifesa e ciberresilienza **e aumentare l'assistenza ai Paesi partner** per lo sviluppo di capacità in materia di ciberdifesa;
  La comunicazione indica come prioritario, in tale ambito, proseguire la **cooperazione con gli Stati Uniti** nell'ambito dei dialoghi già avviati nel settore cibernetico e in materia di sicurezza e difesa; continuare a **sostenere l'Ucraina**, anche avviando un dialogo sulle questioni informatiche; promuovere iniziative di sviluppo della capacità di ciberdifesa dei **paesi candidati all'adesione all'UE**, anche decidendo di prestare loro assistenza operativa;

Azioni a sostegno di soggetti civili

- rafforzare la **cooperazione UE-NATO nel campo della cibersicurezz**a per quanto riguarda la conoscenza situazionale, la risposta alle crisi, la protezione delle infrastrutture critiche, la normazione e la certificazione.
  L'UE e la NATO si impegneranno a migliorare la conoscenza situazionale reciproca, anche rafforzando la cooperazione tra capacità NATO di reazione a incidenti informatici (NCIRC) e la squadra di pronto intervento informatico per le istituzioni, gli organi e le agenzie dell'UE (CERT-UE).

Passi successivi

La Commissione e l'Alto rappresentante - anche nella sua veste di capo dell'Agenzia europea per la difesa - presenteranno annualmente al Consiglio dell'Unione europea una **relazione di**

monitoraggio e valutazione dello stato di attuazione delle azioni prospettate nella comunicazione congiunta, alla quale gli Stati membri sono invitati a contribuire.

Risoluzioni del Parlamento europeo

Il Parlamento europeo ha approvato, il 7 ottobre 2021, una risoluzione sullo **stato delle capacità di ciberdifesa dell'UE** nella quale in particolare:

- ricorda che la **ciberdifesa ha una dimensione sia militare che civile e richiede pertanto maggiore cooperazione, sinergie e coerenza tra gli strumenti**, sottolineando la necessità di analizzare e discutere, innanzitutto, i **problemi di cooperazione e coordinamento**, ma anche le **lacune riguardanti le risorse umane e tecniche** a livello sia nazionale sia dell'UE;
- rammenta che il **miglioramento delle capacità di ciberdifesa**, dato il loro frequente carattere "**a duplice uso**", **esige anche competenze civili nel campo della sicurezza delle reti e dell'informazione**, sottolineando che la proliferazione di sistemi a duplice uso disponibili in commercio può presentare sfide in termini di sfruttamento dei sistemi da parte di un numero crescente di attori ostili statali e non statali ed **invita la Commissione e gli Stati membri a utilizzare diverse leve, tra cui la certificazione e la vigilanza sulla responsabilità degli attori privati**;
- invita a procedere a **un'ulteriore integrazione della cibersicurezza nei meccanismi di risposta alle crisi dell'UE e a creare un collegamento tra le iniziative, le strutture e le procedure esistenti nelle varie comunità informatiche** al fine di rafforzare l'assistenza reciproca e la cooperazione operativa tra gli Stati membri, in particolare in caso di gravi attacchi informatici, così da aumentare l'interoperabilità e sviluppare una comprensione comune della ciberdifesa;
- chiede una **maggiore cooperazione UE-NATO**, in particolare per quanto riguarda i **requisiti di interoperabilità** in materia di ciberdifesa, **cercando possibili complementarità** e possibilità di **rafforzare le capacità in modo reciprocamente vantaggioso**, **evitando duplicazioni** e riconoscendo le rispettive responsabilità;
- chiede un più stretto **coordinamento in materia di ciberdifesa tra gli Stati membri, le istituzioni dell'UE, gli alleati della NATO, le Nazioni Unite e l'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE)** e sottolinea inoltre l'importanza della **cooperazione con i paesi dell'immediato vicinato dell'UE**, con particolare riferimento ai paesi dei **Balcani occidentali e del Partenariato orientale**;
- sottolinea l'importanza di dotarsi un **partenariato solido nel settore informatico con il Regno Unito** ed invita la Commissione a valutare la possibilità di rilanciare un processo finalizzato alla conclusione di un quadro formale e strutturato per la futura cooperazione in tale ambito;
- sottolinea l'importanza della **cooperazione con i Parlamenti nazionali** ai fini dello scambio delle migliori prassi nell'ambito della ciberdifesa.

Il Parlamento europeo, nell'ambito della risoluzione del 18 gennaio 2023 sull'**attuazione della politica di sicurezza e di difesa comune – relazione annuale 2022,** in particolare:

- **accoglie con favore la comunicazione congiunta sulla politica di ciberdifesa dell'UE** e chiede che gli **strumenti esistenti dell'Unione siano resi operativi** affinché possano contribuire più efficacemente alla prevenzione e al contrasto delle minacce ibride;
- invita l'Unione e i suoi Stati membri a migliorare le loro capacità di individuare le minacce ibride, sottolineando la necessità di **sviluppare ulteriormente la politica e le capacità dell'Unione in materia di ciberdifesa**, compresa la creazione di gruppi di risposta rapida agli incidenti informatici;

- sottolinea la necessità di **aiutare**, in stretta **collaborazione con la NATO**, i paesi partner dei **Balcani occidentali e del partenariato orientale a contrastare efficacemente gli attacchi informatici** e la guerra ibrida;
- sottolinea che, per combattere le **crescenti minacce e l'aumento delle narrative anti-europee da parte di paesi terz**i, l'UE deve **intensificare i suoi sforzi tesi a fornire sostegno, formazione e rafforzamento delle capacità con i paesi partner** che condividono gli stessi principi.

Esame presso le istituzioni europee

La comunicazione è stata trasmessa al Consiglio ed al Parlamento europeo, che ancora deve avviarne l'esame.

Esame presso altri Parlamenti nazionali

Sulla base dei dati forniti dal **sito IPEX**, l'esame della comunicazione è stato è stato **completato** dal **Bundestag tedesco** e **avviato** dalla **Camera dei Rappresentati del Belgio**, dal **Parlamento danese**, dal **Consiglio nazionale della Slovacchia**, dal **Sejm Polacco**.