Consiglio
dell'Unione europea

Bruxelles, 22 maggio 2023
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
Destinatario:	Delegazioni
n. doc. prec.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Oggetto:	Conclusioni del Consiglio sulla politica di ciberdifesa dell'UE

Si allegano per le delegazioni le conclusioni del Consiglio sulla politica ciberdifesa dell'UE, approvate dal Consiglio nella sessione del 22 maggio 2023.

Conclusioni del Consiglio sulla politica di ciberdifesa dell'UE

1. Basandosi sul quadro strategico in materia di ciberdifesa del 2014 e sul suo aggiornamento del 2018, il Consiglio accoglie con favore l'ambiziosa comunicazione congiunta sulla politica di ciberdifesa dell'UE, che mira a investire ulteriormente nelle nostre forze armate moderne e interoperabili, nelle tecnologie all'avanguardia e nelle capacità di ciberdifesa allo stato dell'arte, nonché a potenziare i partenariati per superare le sfide comuni. Il ciberspazio è diventato un campo di competizione strategica, in un momento di crescente dipendenza dalle tecnologie digitali. È pertanto essenziale mantenere un ciberspazio aperto, libero, stabile e sicuro. L'uso delle operazioni informatiche che hanno consentito e accompagnato la guerra di aggressione non provocata e ingiustificata della Russia contro l'Ucraina incide sulla stabilità e sulla sicurezza globali, rappresenta un notevole rischio di escalation e si somma all'aumento già significativo delle attività informatiche malevole al di fuori del contesto dei conflitti armati negli ultimi anni.

2. La guerra in Ucraina ha fornito un nuovo contesto strategico e ha confermato la necessità che l'UE, i suoi Stati membri e i loro partner rafforzino ulteriormente la resilienza dell'UE per far fronte alle minacce informatiche e aumentino la nostra cibersicurezza e ciberdifesa comuni contro i comportamenti malevoli e gli atti di aggressione nel ciberspazio. La comunicazione congiunta sulla politica di ciberdifesa dell'UE mostra la nostra determinazione a prevedere misure immediate e a lungo termine per garantire la libertà d'azione nel ciberspazio e rispondere agli autori delle minacce che attuano, tra l'altro, tentativi di intrusione, interruzione o distruzione dei sistemi informativi e di rete dell'UE e dei suoi partner. A integrazione della strategia dell'UE in materia di cibersicurezza e in linea con la bussola strategica, la comunicazione congiunta rappresenta un passo significativo verso l'approccio a tutto spettro dell'UE alla resilienza, alla risposta, alla prevenzione dei conflitti, alla cooperazione e alla stabilità nel ciberspazio. In tale contesto, il Consiglio sottolinea la necessità di risposte appropriate e coerenti da parte dell'UE, dei suoi Stati membri e dei loro partner e attende inoltre con interesse la revisione degli orientamenti di attuazione del pacchetto di strumenti della diplomazia informatica dell'UE quale ulteriore passo avanti fondamentale nell'evoluzione della posizione dell'UE in materia di deterrenza informatica.

3. Il Consiglio sottolinea che anche i recenti attacchi informatici contro infrastrutture critiche europee, la rapida evoluzione del panorama delle minacce informatiche e il ritmo sostenuto dello sviluppo tecnologico dimostrano la necessità di rafforzare il coordinamento e la cooperazione civili-militari, evidenziando al contempo che non esiste alcuna gerarchia tra le comunità civile e militare.
   La politica di ciberdifesa dell'UE consente all'UE e ai suoi Stati membri di rafforzare la loro capacità di proteggere, individuare, difendere e scoraggiare, sfruttando adeguatamente l'intera gamma di opzioni difensive a disposizione delle comunità civile e militare per la sicurezza e la difesa dell'UE in senso lato, conformemente al diritto internazionale, compresi il diritto dei diritti umani e il diritto internazionale umanitario.

4. Sebbene la sicurezza nazionale, anche nel settore informatico, rimanga di esclusiva responsabilità di ciascuno Stato membro, come indicato all'articolo 4, paragrafo 2, TUE, il Consiglio sottolinea nel contempo la necessità di realizzare investimenti sostanziali, in forma individuale e collaborativa, nel rafforzamento della resilienza e nella diffusione di capacità di ciberdifesa a tutto spettro, sfruttando le reti di cooperazione e gli incentivi finanziari dell'UE. Il Consiglio sottolinea la necessità di rafforzare ulteriormente le azioni degli Stati membri e delle istituzioni, degli organi e degli organismi dell'UE al fine di proteggere l'Unione, i nostri cittadini, le istituzioni, gli organi e gli organismi dell'UE, nonché le missioni e operazioni PSDC nel ciberspazio. Evidenzia inoltre l'importanza di potenziare la resilienza dell'UE nel ciberspazio sviluppando capacità di ciberdifesa e rafforzando la cooperazione con un ecosistema privato affidabile.

I. **Intervenire insieme a rafforzamento della ciberdifesa**

5. Il Consiglio ribadisce che un processo incrementale, trasparente e inclusivo è essenziale per rafforzare la fiducia, che è di fondamentale importanza per l'ulteriore sviluppo di un quadro dell'UE per la gestione delle crisi informatiche, da realizzare in linea con la tabella di marcia per la gestione delle crisi informatiche elaborata in sede di Consiglio. Il Consiglio ribadisce la necessità di continuare a rafforzare la nostra capacità di individuare e scoraggiare gli attacchi informatici nonché proteggerci e difenderci da essi attraverso una migliore conoscenza situazionale, lo sviluppo e il potenziamento delle capacità, la formazione, le esercitazioni, un'accresciuta resilienza e reagendo con fermezza agli attacchi informatici contro l'Unione, i suoi Stati membri e le sue istituzioni, i suoi organi e i suoi organismi, nonché le missioni e operazioni PSDC, mediante l'utilizzo di tutti i mezzi appropriati. Nel farlo, il Consiglio incoraggia l'alto rappresentante e la Commissione a ridurre la complessità nel settore informatico, a evitare inutili duplicazioni e ad assicurare la cooperazione e le sinergie con le iniziative esistenti. Occorre rafforzare la cooperazione e il coordinamento tra gli attori della ciberdifesa dell'UE e degli Stati membri e interni all'UE e agli Stati membri, tra le cibercomunità militari e civili e tra un ecosistema pubblico e un ecosistema privato affidabile. In tale contesto, gli Stati membri sono incoraggiati a esplorare e rafforzare ulteriormente i meccanismi di coordinamento nazionale civile-militare, ad agevolare la condivisione volontaria comune delle informazioni, a condividere gli insegnamenti tratti, a contribuire allo sviluppo di norme interoperabili, a realizzare valutazioni dei rischi ed elaborare scenari di rischio, nonché a effettuare esercitazioni congiunte, in particolare a livello europeo, nel pieno rispetto delle disposizioni della direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (NIS 2).

6. Riconoscendo gli sforzi volti a potenziare ulteriormente la resilienza dell'Unione per mezzo della direttiva NIS 2 e della direttiva sulla resilienza dei soggetti critici (CER), il Consiglio ribadisce la sua raccomandazione su un approccio coordinato a livello dell'UE per rafforzare la resilienza delle infrastrutture critiche[1]. Sollecita l'adozione di misure intese a potenziare ulteriormente la resilienza dei soggetti critici, delle infrastrutture critiche e dei prodotti e servizi critici, osservando nel contempo che la corretta attuazione della NIS 2 continua a costituire il passo più importante. Pur trattandosi prevalentemente di una responsabilità civile, questo aspetto contribuisce anche al rafforzamento della ciberdifesa. In tale contesto, le istituzioni, gli organi e gli organismi dell'UE e gli Stati membri sono incoraggiati a sostenere l'ulteriore sviluppo e la diffusione di meccanismi di coordinamento a livello dell'UE, sia nuovi che esistenti, come pure delle valutazioni, degli accertamenti e degli scenari del rischio, della condivisione volontaria comune delle informazioni e delle esercitazioni, secondo modalità che apportino valore aggiunto ed evitino inutili duplicazioni con le iniziative esistenti.

7. Nell'ottica di rafforzare ulteriormente la fiducia, consolidare la cooperazione e facilitare lo scambio tempestivo di informazioni in ordine agli incidenti informatici significativi e su vasta scala che hanno ripercussioni sui sistemi di difesa, il Consiglio accoglie con favore l'iniziativa di continuare a sviluppare la conferenza dei comandanti per la sicurezza informatica dell'UE, che sarà organizzata da ciascuna presidenza del Consiglio dell'UE con il sostegno dell'Agenzia europea per la difesa (AED) e la partecipazione del servizio europeo per l'azione esterna (SEAE). Il Consiglio incoraggia tutti gli Stati membri a partecipare a tali riunioni. Per rafforzare la resilienza dell'UE nei confronti degli incidenti di cibersicurezza su vasta scala, il Consiglio invita la rete UE delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) e la conferenza dei comandanti per la sicurezza informatica dell'UE a individuare le possibili modalità con cui cooperare e trarre beneficio da una prospettiva militare e civile congiunta.

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

8. Nell'ottica di promuovere una risposta più solida e coordinata a livello dell'UE, il Consiglio si compiace dell'istituzione della rete operativa delle squadre militari di pronto intervento informatico dell'UE (MICNET) e attende con interesse che essa raggiunga la capacità operativa iniziale entro la metà del 2024, al fine di potenziare la condivisione di informazioni tecniche sugli incidenti informatici che hanno ripercussioni sui sistemi di difesa tra gli Stati membri partecipanti. Il Consiglio incoraggia tutti gli Stati membri a partecipare a MICNET onde garantire l'efficacia della rete. Invita inoltre gli Stati membri a basarsi sugli insegnamenti tratti dalla rete di gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) e incoraggia vivamente la creazione, al momento opportuno, di un meccanismo efficace di cooperazione e coordinamento tra le due reti, nel pieno rispetto dei meccanismi di governance e delle componenti di ciascuna entità.

9. Alla luce dell'aumento delle attività informatiche malevole da parte di attori statali e non statali contro le operazioni e missioni PSDC dell'UE, il Consiglio invita l'UE e i suoi Stati membri a rafforzare le rispettive capacità di difesa e garanzia delle operazioni e missioni PSDC. A tale riguardo, il Consiglio accoglie con favore gli obiettivi intesi a promuovere ulteriormente la protezione delle reti e delle strutture militari dell'UE, in linea, tra l'altro, con la visione e la strategia militari dell'UE sul ciberspazio come dominio operativo[2].

[2] EEAS(2021) 706 REV 4.

10. Il Consiglio ribadisce le conclusioni del Consiglio del maggio 2022[3] e la necessità di investire nella nostra assistenza reciproca ai sensi dell'articolo 42, punto 7, TUE, nonché la clausola di solidarietà di cui all'articolo 222 TFUE. Sottolinea l'importanza di approfondire ulteriormente la comprensione comune, da parte dell'UE e dei suoi Stati membri, dell'attuazione dell'articolo 42, punto 7, anche in scenari complessi che implichino un attacco informatico, compatibilmente con i principi pertinenti del diritto internazionale. Accoglie con favore la possibilità, su esplicita richiesta dello Stato membro o degli Stati membri interessati, di ricevere sostegno da parte dell'UE qualora si verifichi un attacco informatico, fatto salvo il carattere specifico della politica di sicurezza e di difesa di taluni Stati membri.

11. Il Consiglio sottolinea i progressi compiuti nel progetto PESCO relativo ai gruppi di risposta rapida agli incidenti informatici e mutua assistenza in materia di cibersicurezza (CRRT) e la sua disponibilità ad agire su richiesta quale capacità di risposta alle esigenze degli Stati membri e dell'UE, a sostegno delle missioni e operazioni PSDC e per fornire assistenza ai partner dell'UE. Accoglie con favore l'ulteriore sviluppo delle capacità dei CRRT in ambito PESCO, dei gruppi nazionali di risposta agli incidenti informatici e, se del caso, delle capacità aggiuntive di risposta agli incidenti, quali i futuri gruppi di risposta rapida alle minacce ibride, come previsto nella bussola strategica, anche promuovendo il loro coordinamento e la loro cooperazione a livello dell'UE.

---

[3] Conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, 23 maggio 2022 , doc. 9364/22.

12. Il Consiglio si compiace del lavoro del centro di coordinamento nel settore informatico e dell'informazione (CIDCC) nel quadro del progetto PESCO, che mira a fornire una capacità militare atta a raccogliere e analizzare informazioni pertinenti in vista di un quadro operativo comune in materia di ciberspazio. Si compiace inoltre della proposta di integrare la dimostrazione di concetto – qualora abbia buon esito come centro di coordinamento dell'informazione – in un centro di coordinamento della ciberdifesa dell'UE (EUCDCC) a partire dal 2025, al fine di rafforzare il coordinamento e la conoscenza situazionale, in particolare dei comandanti delle missioni e operazioni PSDC dell'UE, e rafforzare la più ampia architettura di comando e controllo dell'UE. Il Consiglio invita l'alto rappresentante a presentare un concetto e una tabella di marcia per l'istituzione dell'EUCDCC, traendo insegnamenti da analoghe entità internazionali, individuando le risorse necessarie, evitando inutili duplicazioni e cercando la complementarità con il più ampio quadro dell'UE in materia di cibersicurezza.

13. Il Consiglio sottolinea l'importanza della cooperazione in materia di intelligence strategica sulle minacce e sulle attività informatiche e invita gli Stati membri, attraverso le rispettive autorità competenti, a continuare a contribuire ai lavori dell'INTCEN dell'UE, della direzione "Intelligence" dell'EUMS e degli Stati membri nell'ambito della capacità unica di analisi dell'intelligence (SIAC). Sottolinea inoltre l'importanza di rafforzare le nostre capacità di intelligence informatica per accrescere la nostra resilienza informatica e le nostre risposte, nonché per fornire un sostegno efficace alle nostre missioni e operazioni PSDC in ambito civile e militare, come pure alle nostre forze armate e alla capacità della SIAC nel settore informatico, sulla base di contributi volontari degli Stati membri in materia di intelligence e fatte salve le loro competenze.

14. Il Consiglio prende atto del centro di situazione e analisi informatiche della Commissione europea inteso a rafforzare la conoscenza situazionale della Commissione. Sottolinea l'importanza di instaurare una cooperazione reciprocamente vantaggiosa tra tale centro e altre istituzioni e altri organi e organismi dell'UE, in particolare l'ENISA e il CERT-UE. Rimarca inoltre l'importanza di garantire una stretta cooperazione con le reti di cooperazione dell'UE nello sviluppo della conoscenza situazionale, come pure di rispettare la riservatezza. Rileva la necessità di consolidare la conoscenza situazionale comune a livello dell'UE e di sviluppare ulteriormente il quadro dell'UE per la gestione delle crisi informatiche, evitando nel contempo inutili duplicazioni degli sforzi.

15. Il Consiglio ricorda che l'istruzione, la formazione e le esercitazioni in materia di cibersicurezza sono essenziali per garantire la preparazione e l'efficacia e accoglie con favore le attività nazionali come pure le attività fornite dall'UE attraverso l'Accademia europea per la sicurezza e la difesa (AESD), l'AED, l'ENISA e i progetti PESCO in corso, quali il Poligono virtuale federato e l'Accademia e polo di innovazione dell'UE nel settore dell'informatica (EU CAIH). Al fine di intensificare ulteriormente tali sforzi, il Consiglio attende con interesse l'istituzione del progetto quadro CyDef-X dell'AED, volto a sincronizzare le esercitazioni di ciberdifesa e a prestarvi sostegno. Il Consiglio incoraggia l'AED a esaminare, in stretta cooperazione con gli Stati membri e il SEAE, in che modo CyDef-X potrebbe fornire ulteriore sostegno a esercitazioni quali CYBER PHALANX, anche per quanto riguarda l'assistenza reciproca ai sensi dell'articolo 42, paragrafo 7, TUE e la clausola di solidarietà di cui all'articolo 222 TFUE, nonché con la Commissione e l'ENISA per quanto riguarda le esercitazioni civili. Incoraggia inoltre l'utilizzo e l'ulteriore sviluppo, nell'ambito di CyDef-X, degli ambienti di test ed esercitazione di ciberdifesa esistenti, come il Poligono virtuale federato. Per garantire un processo decisionale agile ed efficiente in caso di crisi informatica, il Consiglio sottolinea l'importanza di procedere a periodiche esercitazioni di simulazione per il livello decisionale degli Stati membri.

16. Il Consiglio prende atto della proposta di regolamento sulla cibersolidarietà e dell'intenzione di rafforzare le capacità di individuazione delle minacce e degli incidenti di cibersicurezza nell'UE e di risposta agli stessi. Il Consiglio sottolinea che le proposte in questo settore possono essere efficaci solo se allineate ai quadri e alle esigenze in materia di gestione delle crisi degli Stati membri. Rimarca l'importanza di sottoporre a verifiche le infrastrutture critiche per individuare potenziali vulnerabilità, qualora ciò sia ritenuto utile, come competenza nazionale, tenendo conto delle valutazioni del rischio disponibili a livello dell'UE.

17. Il Consiglio prende atto della proposta della Commissione di istituire un meccanismo per le emergenze di cibersicurezza, che potrebbe supportare la disponibilità di servizi di cibersicurezza da parte di operatori privati di fiducia per assistere, su richiesta, gli Stati membri in caso di incidenti di cibersicurezza su vasta scala, sottolineando nel contempo la necessità di potenziare l'industria europea della cibersicurezza con il sostegno del Centro europeo di competenza per la cibersicurezza (ECCC) quale pilastro essenziale per rendere operativo tale meccanismo. Il Consiglio sottolinea il ruolo chiave di ciascuno Stato membro nel monitoraggio e nella valutazione delle proprie esigenze nazionali.

II. **Mettere in sicurezza l'ecosistema di difesa dell'UE**

18. Il Consiglio ricorda l'incoraggiamento rivolto agli Stati membri affinché sviluppino ulteriormente le proprie capacità di condurre operazioni di ciberdifesa, comprese, se del caso, misure di difesa proattive finalizzate a individuare e scoraggiare gli attacchi informatici nonché a difendersi e proteggersi da essi. Considerato che la direttiva NIS 2 non si applica agli enti della pubblica amministrazione che svolgono le loro attività nel settore della difesa, il Consiglio invita l'AED, con il sostegno della Commissione e del SEAE ove opportuno, ad assistere gli Stati membri nell'elaborazione di raccomandazioni volontarie giuridicamente non vincolanti ispirate alla direttiva NIS 2 al fine di potenziare la cibersicurezza nella comunità della difesa e invita tutti gli Stati membri a impegnarsi attivamente in tal senso. Tali raccomandazioni dovrebbero tenere conto degli sforzi analoghi intrapresi in altri ambiti.

19. Come riconosciuto nella bussola strategica, la capacità di agire dell'UE dipende dalla sua capacità di ridurre le sue dipendenze strategiche in tutte le capacità nel settore della ciberdifesa e le catene di approvvigionamento, nonché di sviluppare e padroneggiare tecnologie di ciberdifesa all'avanguardia. In quest'ottica, occorre anche rafforzare la base industriale e tecnologica di difesa europea in tutta l'UE e la sua capacità di cooperare con i partner nel mondo che condividono gli stessi principi, su una base di reciprocità al fine di assicurare benefici per tutti. Il Consiglio invita pertanto le industrie della cibersicurezza e della ciberdifesa a cooperare strettamente per creare sinergie con l'obiettivo di sviluppare e fornire capacità di ciberdifesa a tutto spettro. Il Consiglio invita la Commissione, in stretta collaborazione con l'ECCC, se del caso, a sostenere ulteriormente lo sviluppo di una base industriale e tecnologica di ciberdifesa europea, ivi comprese le piccole e medie imprese (PMI), che sia forte, agile, competitiva a livello mondiale e innovativa, attraverso ulteriori investimenti e azioni strategiche.

20. Considerando l'importanza dell'interoperabilità e dell'omogeneità delle capacità di ciberdifesa, anche per quanto riguarda lo sviluppo collaborativo di capacità di ciberdifesa di prossima generazione, il Consiglio invita l'AED e lo Stato maggiore dell'UE a lavorare su una serie di requisiti di interoperabilità in materia di ciberdifesa dell'UE, che prendano le mosse dai principi, dai processi e dalle norme esistenti stabiliti in particolare nel quadro dell'Organizzazione del trattato del Nord Atlantico (NATO) e siano compatibili con essi. Il Consiglio invita inoltre gli Stati membri a valutare, nel quadro del comitato europeo di normazione nel settore della difesa, se possano essere necessarie specifiche norme volontarie per i sistemi di difesa, in stretta cooperazione con tutti i pertinenti portatori di interessi, tra cui, se del caso, le organizzazioni europee di normazione e la NATO.

21. Il Consiglio accoglie con favore gli sforzi profusi dalla Commissione per presentare un piano volto a promuovere il ricorso a norme esistenti per usi di ciberdifesa e cibersicurezza civile, nonché l'elaborazione di nuove norme volontarie. Sottolinea la necessità di allineare, se del caso, le norme in materia di cibersicurezza e ciberdifesa. Riconosce che tali norme volontarie potrebbero essere utili per le industrie della cibersicurezza e della ciberdifesa dell'UE e sollecita una più stretta collaborazione tra gli organismi di normazione civili e quelli nel settore della difesa.

22. Il Consiglio chiede che siano elaborate rapidamente raccomandazioni basate sulla mappatura degli strumenti esistenti per comunicazioni sicure nel settore informatico effettuata dalla Commissione e dalle istituzioni competenti. Ove possibile, le raccomandazioni dovrebbero essere allineate alle iniziative esistenti in materia di condivisione delle informazioni e dovrebbero altresì tenere conto dei rischi posti dalle tecnologie emergenti e di rottura per gli attuali metodi di cifratura.

23. Oltre a ciò, il Consiglio accoglie con favore i lavori iniziali intrapresi sulla valutazione e sugli scenari di rischio in corso di elaborazione da parte della Commissione, dell'alto rappresentante e dal gruppo di cooperazione NIS in relazione, per cominciare, ai settori dell'energia e delle telecomunicazioni, su richiesta del Consiglio. Il Consiglio riconosce che sono in fase di preparazione anche valutazioni mirate dei rischi di cibersicurezza per le infrastrutture e le reti di comunicazione nell'UE. Ribadisce che è di fondamentale importanza raggiungere una comprensione comune dei possibili impatti degli incidenti informatici non solo tra gli Stati membri, ma anche tra le istituzioni, gli organi e gli organismi dell'UE. Il Consiglio invita pertanto i suddetti attori a provvedere affinché le valutazioni e gli scenari di rischio e le successive raccomandazioni siano presi in considerazione nella definizione e nella classificazione in ordine di priorità delle misure e del sostegno, a livello dell'UE e, se del caso, nazionale. Il Consiglio chiede inoltre che tutti i soggetti pertinenti tengano conto degli scenari di rischio nei processi di valutazione del rischio come pure nello sviluppo delle esercitazioni di cibersicurezza.

III. **Investire in capacità di ciberdifesa**

24. Il Consiglio esorta gli Stati membri ad accrescere gli investimenti per realizzare, mantenere e sviluppare ulteriormente capacità di ciberdifesa interoperabili. Sostiene l'elaborazione di una serie di impegni volontari per l'ulteriore sviluppo delle capacità nazionali di ciberdifesa, tenendo conto di iniziative analoghe intraprese in altri quadri.

25. Il Consiglio invita gli Stati membri e l'AED a cogliere l'opportunità offerta dalla revisione del piano di sviluppo delle capacità per fissare un elevato livello di ambizione riguardo allo sviluppo della ciberdifesa collaborativa a livello dell'UE. Incoraggia inoltre gli Stati membri a basarsi sulla serie aggiornata di priorità e sui relativi impegni PESCO per accrescere il loro livello di coinvolgimento in progetti di collaborazione per lo sviluppo di capacità di ciberdifesa dell'UE, riconoscendo il vantaggio diretto dei progetti di collaborazione a livello dell'UE per sostenere lo sviluppo delle capacità nazionali di ciberdifesa.

26. Il Consiglio accoglie con favore gli sforzi di ricerca collaborativa a livello dell'UE volti a esplorare le possibili applicazioni nei sistemi di difesa delle tecnologie emergenti e di rottura, rilevando altresì la necessità di garantire che tali sviluppi tecnologici siano rapidamente integrati nelle capacità esistenti e future. Esorta gli Stati membri e l'industria dell'UE a sfruttare al meglio le opportunità di ricerca collaborativa a livello dell'UE, ad esempio nel quadro dell'AED, nei progetti PESCO in corso, come l'Accademia e polo di innovazione dell'UE nel settore dell'informatica (EU CAIH), nel quadro del Fondo europeo per la difesa e, ove opportuno, di Orizzonte Europa e del programma Europa digitale per i progetti a duplice uso. Inoltre, il Consiglio accoglie con favore l'utilizzo dei quadri dedicati per sostenere l'innovazione nel settore della difesa mediante gli spin-in del settore civile, segnatamente il sistema UE di innovazione nel settore della difesa e il polo di innovazione nel settore della difesa. Incoraggia inoltre l'ECCC e l'AED a stipulare un accordo operativo in modo da facilitare lo scambio di informazioni tra i relativi membri del personale sulle rispettive priorità riguardanti le tecnologie civili, a duplice uso e di difesa, al fine di creare sinergie ed evitare duplicazioni.

27. Il Consiglio accoglie con favore l'intenzione della Commissione di elaborare, in cooperazione con l'AED e l'ECCC conformemente ai rispettivi mandati, con gli Stati membri e in consultazione con i pertinenti portatori di interessi quali l'industria, una tabella di marcia tecnologica per le cibertecnologie critiche che, attraverso l'individuazione delle cibertecnologie critiche, la mappatura degli sviluppi tecnologici e le dipendenze strategiche, offra modalità per ridurle, a sostegno dell'autonomia strategica e della sovranità tecnologica dell'UE, preservando nel contempo un'economia aperta. Il Consiglio rileva che la tabella di marcia tecnologica per le cibertecnologie critiche può guidare le priorità strategiche per gli strumenti di finanziamento dell'UE, rimanendo nel contempo in linea con le rispettive modalità in vigore per tali strumenti. Ricorda che l'UE dovrebbe perseguire una politica industriale europea ambiziosa e assertiva per creare un contesto imprenditoriale sostenibile, attraente e competitivo, che possa anche consentire ai soggetti europei nel settore informatico di espandersi.

28. Il Consiglio apprezza l'intenzione di colmare il significativo divario di competenze in materia di cibersicurezza attirando nuovi professionisti, comprese le donne, attraverso il miglioramento del livello delle competenze e la riqualificazione e investendo in formazioni ed esercitazioni — nonché organizzandole — per dar vita a una forza lavoro nel settore della cibersicurezza che sia diversificata e inclusiva. Riconoscendo le sfide che l'UE si trova ad affrontare per quanto riguarda il capitale umano nell'ambito della cibersicurezza e della ciberdifesa, il Consiglio accoglie con favore l'iniziativa dell'accademia per le competenze in materia di cibersicurezza, da cui può trarre vantaggio anche la forza lavoro nel settore della ciberdifesa.

29. Il Consiglio invita gli Stati membri a scambiarsi informazioni sulle migliori pratiche per sviluppare professionisti qualificati in materia di cibersicurezza, sfruttando le sinergie tra le iniziative militari, civili e delle autorità di contrasto e invita l'AESD, con il sostegno e l'esperienza dell'AED e dell'ENISA, a valutare alternative per migliorare lo scambio di migliori pratiche e ulteriori sinergie tra il settore militare e quello civile per quanto concerne la formazione e lo sviluppo di competenze di difesa precipue del settore informatico.

30. Il Consiglio sottolinea l'importanza di raggiungere una comprensione comune della composizione della forza lavoro nel settore della cibersicurezza e delle competenze associate al fine di individuare e colmare le lacune nel mercato del lavoro della cibersicurezza, come pure la necessità di coinvolgere tutti i portatori di interessi, compresi gli Stati membri e l'industria. Il Consiglio riconosce che la definizione di indicatori per monitorare il mercato del lavoro della cibersicurezza contribuirebbe a individuare il fabbisogno di competenze in materia di cibersicurezza e a dirigere i fondi in modo opportuno, concorrendo nel contempo a soddisfare gli obblighi connessi alle politiche, in particolare quelli derivanti dalla direttiva NIS 2. Il Consiglio accoglie con favore la proposta relativa a un quadro di certificazione delle competenze in materia di ciberdifesa e invita l'alto rappresentante, in qualità di capo dell'AESD, a svilupparlo, in cooperazione con il SEAE, la Commissione e gli Stati membri, facendo leva su iniziative civili.

IV. **Stringere partenariati per superare le sfide comuni**

31. Il Consiglio invita l'alto rappresentante e la Commissione a rafforzare e portare avanti la cooperazione e a valutare l'opportunità di partenariati reciprocamente vantaggiosi e su misura in materia di politiche di ciberdifesa, anche per quanto riguarda lo sviluppo di capacità di ciberdifesa attraverso lo strumento europeo per la pace (EPF). A tal fine, il punto "ciberdifesa" dovrebbe essere aggiunto ai dialoghi e alle consultazioni dell'UE in materia di cibersicurezza nonché alle consultazioni generali in materia di sicurezza e difesa con i partner. Oltre a ciò, occorre rafforzare i dialoghi e la collaborazione con il settore privato. Il Consiglio sottolinea che la collaborazione internazionale su norme e certificazione in materia di cibersicurezza costituirebbe un valore aggiunto per l'industria europea. Accoglie pertanto con favore l'impegno della Commissione a fare di questo aspetto una parte essenziale dei dialoghi dell'UE in materia di cibersicurezza con i paesi terzi e le organizzazioni internazionali.

32. Il Consiglio sottolinea l'importanza della cooperazione internazionale per prevenire o ridurre i rischi di conflitto nel ciberspazio, specie attraverso l'ulteriore sviluppo e messa in opera di misure volte a rafforzare la fiducia (CBM) a livello regionale e internazionale, anche a livello di Nazioni Unite, nonché l'importanza di continuare a incoraggiare l'uso delle CBM informatiche esistenti, ad esempio in seno all'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE), anche in tempi di tensioni internazionali.
L'UE e i suoi Stati membri rimarcano che il diritto internazionale vigente si applica al ciberspazio ed evidenziano l'importanza di proseguire gli sforzi per sostenere e promuovere il quadro delle Nazioni Unite per il comportamento responsabile degli Stati e di adoperarsi per la sua attuazione, anche attraverso l'istituzione del programma d'azione per promuovere un comportamento responsabile degli Stati nel ciberspazio.

33. In linea con le dichiarazioni congiunte sulla cooperazione UE-NATO, il Consiglio invita l'alto rappresentante, anche in qualità di capo dell'AED, e la Commissione a rafforzare, approfondire e ampliare ulteriormente il partenariato con la NATO nel settore della cibersicurezza, nel pieno rispetto dei principi di inclusività, reciprocità, apertura reciproca e trasparenza, come pure dell'autonomia decisionale di ambo le organizzazioni. Pur tenendo conto della necessità di garantire sforzi complementari e coordinati con il massimo coinvolgimento possibile degli Stati membri che non fanno parte della NATO ed evitare inutili duplicazioni, il Consiglio chiede di stabilire legami ai rispettivi livelli tra l'UE e la NATO per quanto riguarda la formazione, l'istruzione, la conoscenza situazionale, le esercitazioni e le piattaforme di R&S, e di ricercare possibili sinergie tra i corrispettivi impegni volontari per lo sviluppo delle capacità nazionali di ciberdifesa e i quadri di gestione delle crisi, la protezione delle infrastrutture critiche e il rafforzamento degli scambi di conoscenza situazionale, le risposte coordinate alle attività informatiche malevole e le iniziative di sviluppo di capacità nei paesi terzi. Questo comprende l'accordo tecnico tra la capacità NATO di reazione a incidenti informatici (NCIRC) e la squadra di pronto intervento informatico dell'Unione europea (CERT-UE), così come un dialogo politico rafforzato su questioni di ciberdifesa a tutti i livelli.

V. **Conclusione**

34. Sulla base delle conclusioni del Consiglio sulla politica di ciberdifesa dell'UE, il Consiglio invita l'alto rappresentante e la Commissione a elaborare, in vista dell'approvazione degli Stati membri, un piano di attuazione di tale politica entro il secondo trimestre del 2023. Il Consiglio invita inoltre gli Stati membri a dichiarare volontariamente le loro ambizioni e azioni in materia di ciberdifesa nel contesto della politica di ciberdifesa dell'UE e a fare pieno uso delle raccomandazioni e degli impegni volontari giuridicamente non vincolanti per accrescere i loro sforzi nazionali e multinazionali in materia di ciberdifesa volti a massimizzare l'impatto a livello dell'UE. Si invitano l'alto rappresentante, la Commissione e gli Stati membri a riferire e discutere con cadenza annuale in merito ai progressi compiuti nell'attuazione degli elementi della comunicazione congiunta e del relativo piano di attuazione a partire dal secondo trimestre del 2024.