Consiglio
dell'Unione europea

Bruxelles, 23 maggio 2022
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
in data:	23 maggio 2022
Destinatario:	Delegazioni
Oggetto:	Conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica - Conclusioni del Consiglio approvate dal Consiglio nella sessione del 23 maggio 2022

Si allegano per le delegazioni le conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, approvate dal Consiglio nella sessione del 23 maggio 2022.

ALLEGATO

Conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica

IL CONSIGLIO DELL'UNIONE EUROPEA,

RAMMENTANDO:

– le sue conclusioni sulla comunicazione congiunta del 25 giugno 2013 al Parlamento europeo e al Consiglio intitolata "Strategia dell'Unione europea per la cibersicurezza: un ciberspazio aperto e sicuro"[1],

– le sue conclusioni sul quadro strategico dell'UE in materia di ciberdifesa[2],

– le sue conclusioni sulla governance di internet[3],

– le sue conclusioni sulla diplomazia informatica[4],

– le sue conclusioni "Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza"[5],

– le sue conclusioni sulla comunicazione congiunta del 20 novembre 2017 al Parlamento europeo e al Consiglio: "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE"[6],

– le sue conclusioni su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica")[7],

– le sue conclusioni relative alla risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala[8],

– le sue conclusioni sugli orientamenti dell'UE per lo sviluppo delle capacità informatiche esterne[9],

– la decisione di esecuzione (UE) 2018/1993 del Consiglio, dell'11 dicembre 2018, relativa ai dispositivi integrati dell'UE per la risposta politica alle crisi[10],

---

1 Doc. 12109/13.
2 Doc. 15585/14.
3 Doc. 16200/14.
4 Doc. 6122/15 + COR 1.
5 Doc. 14540/16.
6 Doc. 14435/17 + COR 1.
7 Doc. 10474/17.
8 Doc. 10086/18.
9 Doc. 10496/18.

– le sue conclusioni sullo sviluppo di capacità e competenze in materia di cibersicurezza nell'UE[11],

– le sue conclusioni sull'importanza del 5G per l'economia europea e sulla necessità di attenuare i relativi rischi per la sicurezza[12],

– le sue conclusioni sul futuro di un'Europa altamente digitalizzata oltre il 2020: "Accrescere la competitività digitale ed economica e la coesione digitale in tutta l'Unione"[13],

– le sue conclusioni sugli sforzi complementari per rafforzare la resilienza e contrastare le minacce ibride[14],

– le sue conclusioni "Plasmare il futuro digitale dell'Europa"[15],

– le sue conclusioni sulla cibersicurezza dei dispositivi connessi[16],

– le sue conclusioni sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale[17],

– le sue conclusioni sulla sicurezza e la difesa[18],

– le sue conclusioni "Esplorare il potenziale dell'iniziativa concernente un'unità congiunta per il ciberspazio a integrazione della risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala"[19],

– 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[20],

---

10 GU L 320 del 17.12.2018, pag. 28.
11 Doc. 7737/19.
12 Doc. 14517/19.
13 Doc. 9596/19.
14 Doc. 14972/19.
15 Doc. 8711/20.
16 Doc. 13629/20.
17 Doc. 7290/21.
18 Doc. 8396/21.
19 Doc. 13048/21.
20 Doc. 7371/22.

1. SOTTOLINEA che negli ultimi anni si sono intensificati i comportamenti dolosi nel ciberspazio, provenienti da attori sia statali che non statali, ivi compresi un forte e costante aumento delle attività malevole che prendono di mira le infrastrutture critiche, le catene di approvvigionamento e la proprietà intellettuale dell'UE e degli Stati membri, l'accresciuto rischio di effetti di ricaduta, come anche un aumento degli attacchi ransomware contro le nostre imprese, le nostre organizzazioni e i nostri cittadini. OSSERVA che, con il ritorno della politica di potenza, alcuni paesi tentano sempre più di sfidare e minare l'ordine internazionale basato su regole nel ciberspazio, rendendo la dimensione informatica un settore sempre più conteso, così come avviene per l'alto mare, lo spazio aereo e lo spazio extra-atmosferico. RICONOSCE che gli attacchi informatici su larga scala o i tentativi di intrusione, interruzione o distruzione di reti e sistemi di informazione con effetti sistemici sono diventati più comuni, potrebbero compromettere la nostra sicurezza economica e avere ripercussioni sulle nostre istituzioni e sui nostri processi democratici, e dimostrano come taluni attori siano disposti a mettere a rischio la sicurezza e la stabilità internazionali. SOTTOLINEA che l'aggressione militare russa nei confronti dell'Ucraina ha dimostrato che le attività informatiche offensive possono essere parte integrante di strategie ibride che combinano intimidazione, destabilizzazione e perturbazioni economiche.

2. RIBADISCE che, a fronte degli attuali cambiamenti geopolitici, la forza della nostra Unione risiede nell'unità, nella solidarietà e nella determinazione e che l'attuazione della bussola strategica potenzierà l'autonomia strategica dell'UE e la sua capacità di lavorare con i partner per salvaguardare i suoi valori e interessi, anche nel settore informatico. SOTTOLINEA che un'UE più forte e più capace in materia di sicurezza e difesa apporterà un contributo positivo alla sicurezza globale e transatlantica ed è complementare alla NATO, che resta il fondamento della difesa collettiva per i suoi membri. RIBADISCE l'intenzione dell'UE di intensificare il sostegno all'ordine internazionale basato su regole, imperniato sulle Nazioni Unite.

3. In linea con le conclusioni del Consiglio sulla strategia dell'UE in materia di cibersicurezza e la bussola strategica, RIBADISCE la necessità di sviluppare la posizione dell'Unione in materia di deterrenza informatica migliorando la nostra capacità di prevenire gli attacchi informatici attraverso lo sviluppo e il potenziamento delle capacità, la formazione, le esercitazioni, un'accresciuta resilienza, e reagendo con fermezza agli attacchi informatici contro l'UE e i suoi Stati membri mediante l'utilizzo di tutti gli strumenti a disposizione dell'UE. Ciò include l'ulteriore dimostrazione della determinazione dell'UE a fornire risposte immediate e a lungo termine agli autori delle minacce che cercano di negarci l'accesso sicuro e aperto al ciberspazio e di incidere sui nostri interessi strategici, compresa la sicurezza dei nostri partner. In tale contesto, SOTTOLINEA che la posizione in materia di deterrenza informatica mira a combinare le varie iniziative che contribuiscono alle azioni dell'UE tese al consolidamento della pace e della stabilità nel ciberspazio e a favore di un ciberspazio aperto, libero, globale, stabile e sicuro, coordinando meglio al contempo le azioni a breve, medio e lungo termine per prevenire, scoraggiare, dissuadere e rispondere alle minacce e agli attacchi informatici e sfruttando le capacità informatiche. SOTTOLINEA che questi elementi dovrebbero essere incorporati nella posizione dell'UE in materia di deterrenza informatica, conformemente a cinque funzioni dell'UE nel settore informatico: rafforzare la nostra ciberresilienza e le nostre capacità di protezione; migliorare la gestione solidale e globale delle crisi; promuovere la nostra visione del ciberspazio; rafforzare la cooperazione con i paesi partner e le organizzazioni internazionali; prevenire gli attacchi informatici, difendersi da essi e rispondervi.

I. RAFFORZARE LA NOSTRA CIBERRESILIENZA E LE NOSTRE CAPACITÀ DI PROTEZIONE

4. RIBADISCE la necessità di accrescere il livello complessivo della cibersicurezza nell'UE, ATTENDE CON IMPAZIENZA la rapida adozione del progetto di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (NIS), del progetto di regolamento relativo alla resilienza operativa digitale per il settore finanziario (DORA), del progetto di direttiva sulla resilienza dei soggetti critici (CER) e PRENDE ATTO della proposta di regolamento che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione, al fine di promuovere un'Unione europea che protegga i suoi cittadini, i suoi servizi pubblici e le sue imprese nel ciberspazio. INCORAGGIA la Commissione a finalizzare l'adozione di proposte chiave tese a garantire che le infrastrutture, le tecnologie, i prodotti e i servizi digitali siano messi in sicurezza al fine di inviare un segnale chiaro relativamente alle ambizioni dell'UE in materia e di consentire il sostegno alle imprese affinché siano all'altezza delle sfide da affrontare. INVITA la Commissione a proporre requisiti comuni in materia di cibersicurezza per i dispositivi connessi e i processi e servizi associati mediante la normativa europea sulla ciberresilienza, che dovrebbe essere proposta dalla Commissione prima della fine del 2022, tenendo conto della necessità di un approccio orizzontale e olistico che copra l'intero ciclo di vita dei prodotti digitali, oltre che la normativa esistente, soprattutto nel settore della cibersicurezza.

5. INVITA le autorità competenti, quali l'organismo dei regolatori europei delle comunicazioni elettroniche (BEREC), l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) e il gruppo di cooperazione NIS (sicurezza delle reti e dell'informazione), insieme alla Commissione europea, a formulare, sulla base di una valutazione dei rischi, raccomandazioni rivolte agli Stati membri e alla Commissione europea con l'obiettivo di rafforzare la resilienza delle reti e infrastrutture di comunicazione nell'Unione europea, ivi compreso il proseguimento dell'attuazione del pacchetto di strumenti dell'UE per il 5G.

6. INVITA l'UE e gli Stati membri a intensificare gli sforzi tesi ad accrescere il livello complessivo della cibersicurezza, ad esempio agevolando l'emergere di fornitori di servizi di cibersicurezza affidabili, e SOTTOLINEA che incoraggiare lo sviluppo di tali fornitori dovrebbe essere prioritario per la politica industriale dell'UE nel settore della cibersicurezza. Al fine di resistere meglio agli attacchi informatici con potenziali effetti sistemici, nonché di contrastarli meglio, e sulla base degli insegnamenti tratti dalla gestione delle vulnerabilità connesse a SolarWinds, Microsoft Exchange e Log4J di Apache, INVITA la Commissione a proporre opzioni tese a incoraggiare l'emergere di un'industria di servizi di cibersicurezza affidabile, a rafforzare la cibersicurezza della catena di approvvigionamento delle TIC, ad affrontare i potenziali effetti delle vulnerabilità dei software per l'UE e gli Stati membri, anche in vista dell'imminente normativa europea sulla ciberresilienza, e a migliorare le capacità di individuazione delle minacce informatiche e di condivisione di informazioni al riguardo negli Stati membri e tra loro.

7. RIBADENDO che investire nell'innovazione e utilizzare meglio la tecnologia civile è fondamentale per rafforzare la nostra sovranità tecnologica, anche nel settore informatico, INVITA la Commissione a rendere rapidamente operativo il Centro europeo di competenza per la cibersicurezza al fine di sviluppare un ecosistema industriale, tecnologico e di ricerca europeo forte per il ciberspazio, SOTTOLINEA la necessità di dare impulso alla ricerca e all'innovazione, investire maggiormente nei settori civili e della difesa al fine di rafforzare la base industriale e tecnologica di difesa europea (EDTIB) e sviluppare le capacità informatiche dell'UE e dei suoi Stati membri, ivi comprese capacità di sostegno strategico. SOTTOLINEA l'importanza di utilizzare in modo intensivo le nuove tecnologie, in particolare la computazione quantistica, l'intelligenza artificiale e i big data, per conseguire vantaggi comparativi, anche in termini di operazioni di risposta agli attacchi informatici.

8. RICONOSCENDO che il potenziamento della nostra cibersicurezza è un modo per aumentare l'efficacia e la sicurezza dei nostri sforzi a terra, nell'aria, in mare e nello spazio extra-atmosferico, SOTTOLINEA l'importanza di integrare considerazioni in materia di cibersicurezza in tutte le politiche pubbliche dell'UE, compresa la legislazione settoriale che integra la direttiva NIS 2, e INVITA la Commissione a esaminare opzioni per rafforzare la cibersicurezza lungo l'intera catena di approvvigionamento della base industriale e tecnologica di difesa europea (EDTIB).

9. RICONOSCE che garantire risorse finanziarie e umane adeguate per la cibersicurezza e misure volte a creare un contesto favorevole alla competitività del settore privato è essenziale per sviluppare la posizione dell'UE in materia di deterrenza informatica e che la questione del finanziamento stabile e a lungo termine della cibersicurezza dovrebbe essere affrontata anche a livello dell'UE attraverso la progettazione e l'attuazione di un meccanismo orizzontale che combini molteplici fonti di finanziamento, compreso il costo delle risorse umane altamente qualificate. INVITA pertanto la Commissione a esaminare le opzioni per un siffatto meccanismo prima della fine del 2022, da discutere in seno ai pertinenti organi del Consiglio.

10. SOTTOLINEA la necessità di intensificare i nostri sforzi e di rafforzare la cooperazione in materia di lotta contro la criminalità informatica internazionale — in particolare contro i ransomware — attraverso il meccanismo EMPACT (piattaforma multidisciplinare europea di lotta alle minacce della criminalità), mediante scambi tra i settori responsabili della sicurezza informatica, delle attività di contrasto e delle attività diplomatiche, nonché rafforzando le capacità di contrasto in termini di indagini e azioni penali nei confronti della criminalità informatica. RIBADISCE il proprio impegno a informare il pubblico in merito alle minacce informatiche e alle misure adottate a livello nazionale e di UE contro tali minacce coinvolgendo la società civile, il settore privato e il mondo accademico, al fine di aumentare la consapevolezza e di promuovere un livello adeguato di protezione informatica e igiene informatica. SOTTOLINEA la necessità di concentrarsi sulle competenze e sulle capacità dei cittadini in materia di sicurezza informatica a livello dell'UE e degli Stati membri e di coinvolgere attivamente gli utenti nella loro protezione.

II. **MIGLIORARE LA GESTIONE SOLIDALE E GLOBALE DELLE CRISI**

11. Basandosi sulle esercitazioni annuali di cibersicurezza, su altre esercitazioni che comportano una dimensione informatica e sull'esercitazione EU CyCLES 2022, EVIDENZIA l'importanza di istituire un programma di esercitazioni periodiche intercomunitarie e multilivello in materia di cibersicurezza, al fine di testare e sviluppare la risposta interna ed esterna dell'UE agli incidenti di cibersicurezza su vasta scala, con la partecipazione del Consiglio, del SEAE, della Commissione e dei pertinenti portatori di interessi quali l'ENISA e il settore privato, che sarà articolato e contribuirà alla politica generale dell'UE in materia di esercitazioni. SOTTOLINEA l'importanza di sviluppare ulteriormente le esercitazioni Cyber Europe e Blue OLEx, combinando la risposta a diversi livelli. RICONOSCE la necessità di valutare e consolidare le esercitazioni esistenti e di esaminare la possibilità di ulteriori esercitazioni in segmenti specifici del settore informatico, in particolare un'esercitazione militare CERT e un'esercitazione incentrata sulla cooperazione tra istituzioni, organi e agenzie dell'UE in caso di crisi. RICONOSCE che la posizione dell'Unione in materia di deterrenza informatica rafforzerà la nostra capacità di prevenire gli attacchi informatici attraverso varie azioni, tra cui la formazione, e INVITA pertanto gli Stati membri a potenziare la cooperazione civile-militare nel campo della formazione e delle esercitazioni congiunte in questo settore.

12. SOTTOLINEA la necessità di testare e rafforzare ulteriormente la cooperazione operativa e la conoscenza situazionale comune tra gli Stati membri, anche attraverso reti consolidate quali la rete degli CSIRT e la rete delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe), al fine di migliorare la preparazione dell'UE ad affrontare incidenti di cibersicurezza su vasta scala. SOTTOLINEA l'importanza di lavorare allo sviluppo di un linguaggio comune, mirato alla discussione a livello politico, tra gli Stati membri e con le istituzioni, gli organi e le agenzie dell'UE al fine di contribuire a formulare una valutazione consolidata della gravità e dell'impatto dei pertinenti incidenti di cibersicurezza nonché dei possibili scenari evolutivi e, se del caso, delle esigenze che ne derivano. EVIDENZIA, a tale proposito, la necessità di migliorare la complementarità delle relazioni condivise di valutazione della situazione, comprese le relazioni della rete EU-CyCLONe sull'impatto e la gravità degli incidenti di cibersicurezza su vasta scala negli Stati membri dell'UE e le valutazioni delle minacce formulate dall'INTCEN nel quadro del pacchetto di strumenti della diplomazia informatica dell'UE. INVITA la Commissione, l'alto rappresentante e il gruppo di cooperazione NIS, in coordinamento con i pertinenti organismi e agenzie civili e militari e le pertinenti reti consolidate, compresa EU-CyCLONe, a effettuare entro la fine del 2022 una valutazione dei rischi e ad elaborare scenari di rischio in relazione alla cibersicurezza in una situazione di minaccia o di possibile attacco nei confronti di Stati membri o paesi partner e a presentarli agli organi competenti del Consiglio. SOTTOLINEA la necessità di una comunicazione pubblica adeguata e coordinata sulla risposta dell'UE agli incidenti di cibersicurezza su vasta scala.

13. In caso di incidente di cibersicurezza su vasta scala, SOTTOLINEA la necessità di rafforzare il coordinamento e, se opportuno — basandosi sui lavori e sui progressi compiuti dai gruppi di risposta rapida agli incidenti informatici nel quadro della PESCO e attingendo ai lavori della rete degli CSIRT e della rete EU-CyCLONe — la messa in comune volontaria delle capacità di risposta agli incidenti tra gli Stati membri. RICONOSCE che instaurare legami con il settore privato potrebbe amplificare le capacità pubbliche, in particolare in un contesto di carenza di competenze in tutta l'UE, e che l'individuazione e il coordinamento di partner privati potrebbe fare la differenza in caso di incidenti su vasta scala. Per prepararsi pienamente ad affrontare incidenti di cibersicurezza su vasta scala, INVITA la Commissione a presentare una proposta su un nuovo Fondo di risposta alle emergenze di cibersicurezza entro la fine del terzo trimestre del 2022.

14. In linea con la bussola strategica, RIBADISCE la necessità di investire nella nostra assistenza reciproca, conformemente all'articolo 42, paragrafo 7, del trattato sull'Unione europea, nonché nella solidarietà, conformemente all'articolo 222 del trattato sul funzionamento dell'Unione europea, in particolare attraverso esercitazioni frequenti. In tale contesto, SOTTOLINEA la necessità di continuare a lavorare alla fornitura e al coordinamento di sostegno bilaterale civile e/o militare — anche esplorando il possibile sostegno fornito dall'UE su esplicita richiesta degli Stati membri — e all'individuazione di misure di risposta adeguate, anche attraverso l'elaborazione di una strategia di comunicazione coordinata, nell'ambito dell'attuazione dell'articolo 42, paragrafo 7. OSSERVA che ciò dovrebbe includere anche l'esame dei collegamenti con gli attuali meccanismi di gestione delle crisi dell'UE e con il meccanismo di protezione civile dell'UE.

15. SOTTOLINEA che una posizione in materia di deterrenza informatica dell'UE richiederà una maggiore sicurezza delle comunicazioni. A tal fine, RIBADISCE gli orientamenti forniti a tale riguardo dalla bussola strategica e INVITA la Commissione e gli altri organi, istituzioni e agenzie pertinenti a effettuare entro la fine del 2022 una mappatura degli strumenti esistenti per la comunicazione sicura nel settore informatico, da discutere in seno ai pertinenti organi del Consiglio e con i pertinenti gruppi di cooperazione, quali la rete degli CSIRT e la rete EU-CyCLONe.

III. PROMUOVERE LA NOSTRA VISIONE DEL CIBERSPAZIO

16. RICORDA che l'approccio comune e globale dell'UE alla diplomazia informatica mira a contribuire a prevenire i conflitti, a ridurre le minacce alla cibersicurezza e a incrementare la stabilità nelle relazioni internazionali. In tale contesto RIBADISCE l'impegno dell'UE a favore della risoluzione pacifica delle controversie internazionali relative al ciberspazio e dell'applicazione del diritto internazionale — compresi il diritto internazionale dei diritti umani e il diritto internazionale umanitario — alle azioni degli Stati nel ciberspazio. SOTTOLINEA l'impegno dell'UE e dei suoi Stati membri ad agire conformemente alle norme volontarie e non vincolanti di comportamento responsabile degli Stati nel ciberspazio concordate da tutti gli Stati membri delle Nazioni Unite. PONE L'ACCENTO sull'importanza di un ciberspazio aperto, libero, globale, stabile e sicuro in cui i diritti umani, le libertà fondamentali e lo Stato di diritto siano pienamente applicati a sostegno del benessere sociale, della crescita economica, della prosperità e dell'integrità delle nostre società libere e democratiche e RIBADISCE l'impegno dell'UE e dei suoi Stati membri a continuare a promuovere tali valori e principi. Al fine di sviluppare canali per un dialogo costruttivo, franco e aperto con i principali portatori di interessi del ciberspazio, SOTTOLINEA l'importanza di rendere le questioni riguardanti il ciberspazio, compreso il pacchetto di strumenti della diplomazia informatica dell'UE, parte integrante dei negoziati di adesione all'Unione e dei dialoghi strategici e politici dell'UE con i partner e i concorrenti internazionali e, allo stesso tempo, INVITA l'alto rappresentante a rivedere gli attuali dialoghi bilaterali in materia di cibersicurezza nonché, se necessario, a proporre di avviare un'analoga cooperazione con altri paesi o pertinenti organizzazioni internazionali.

17. RICORDA l'importanza della cooperazione multilaterale, dal momento che anche gli altri portatori di interessi sono responsabili della cibersicurezza, in particolare per quanto riguarda l'attuazione delle raccomandazioni e decisioni adottate nei consessi internazionali e regionali. INVITA l'UE e i suoi Stati membri a promuovere ulteriormente il nostro modello di ciberspazio e di internet sulla base dell'approccio multipartecipativo e attraverso iniziative quali l'appello di Parigi a favore della fiducia e della sicurezza nel ciberspazio e la dichiarazione sul futuro di internet, sottolineando i vantaggi comuni della stabilità nel ciberspazio e attirando l'attenzione a livello globale sui pericoli di una visione di internet statocentrica e autoritaria, e INVITA l'UE e i suoi Stati membri a rafforzare ulteriormente la cooperazione con la comunità multipartecipativa, anche attraverso pertinenti progetti quali l'iniziativa dell'UE per la diplomazia informatica nel quadro dello strumento di politica estera dell'UE.

18. SI IMPEGNA a un dialogo costante nelle pertinenti organizzazioni internazionali, in particolare nei processi connessi al Primo e al Terzo Comitato delle Nazioni Unite, sottolineando nel contempo che nel ciberspazio e in relazione ad esso si applica, senza riserve, il diritto internazionale vigente. EVIDENZIA l'importanza di proseguire gli sforzi per sostenere e promuovere il quadro delle Nazioni Unite per il comportamento responsabile degli Stati e SOTTOLINEA che l'UE e i suoi Stati membri si adopereranno attivamente per rafforzarne l'attuazione, anche attraverso l'istituzione del programma d'azione per promuovere un comportamento responsabile degli Stati nel ciberspazio. SOTTOLINEA che l'UE e i suoi Stati membri parteciperanno attivamente ai negoziati per una futura convenzione delle Nazioni Unite che fungerà da strumento efficace per le autorità di contrasto e giudiziarie nella lotta globale contro la criminalità informatica, tenendo pienamente conto del quadro di strumenti internazionali e regionali esistente in questo ambito, in particolare la convenzione di Budapest sulla criminalità informatica. RILEVA l'importanza di continuare a sostenere lo sviluppo e la messa in opera di misure volte a rafforzare la fiducia (CBM) a livello regionale e internazionale e di continuare a incoraggiare l'uso delle CBM informatiche esistenti in seno all'OSCE, anche in tempi di tensioni internazionali.

19. RICORDA che l'adozione di un approccio proattivo basato sui diritti umani volto a garantire norme internazionali nei settori delle tecnologie emergenti e dell'architettura di base di internet, in linea con i valori e i principi democratici, è essenziale per garantire che internet rimanga globale, non frammentata e aperta, e SOSTIENE il principio secondo cui l'uso e lo sviluppo delle tecnologie devono avvenire nel rispetto dei diritti umani ed essere attenti alla riservatezza e il loro utilizzo deve essere legale, sicuro ed etico. INCORAGGIA l'alto rappresentante e la Commissione a sviluppare una visione strategica sulle questioni tecniche nel settore digitale che hanno ripercussioni sulla politica estera e che potrebbero avere un impatto sulla stabilità del ciberspazio e di internet in particolare, anche nelle pertinenti organizzazioni internazionali specializzate (Unione internazionale delle telecomunicazioni, ecc.).

IV. RAFFORZARE LA COOPERAZIONE CON I PAESI PARTNER E LE ORGANIZZAZIONI INTERNAZIONALI

20. SOTTOLINEA la necessità di collegare meglio la strategia dell'UE per lo sviluppo delle capacità informatiche con le norme delle Nazioni Unite in materia di comportamento responsabile degli Stati nel ciberspazio, anche sviluppando programmi mirati di cooperazione e di sviluppo delle capacità per sostenere i paesi terzi nei loro sforzi di attuazione e, di conseguenza, proseguendo e ampliando i nostri sforzi volti a promuovere il programma d'azione delle Nazioni Unite per promuovere un comportamento responsabile degli Stati nel ciberspazio. SOTTOLINEA l'importanza di integrare pienamente lo sviluppo delle capacità informatiche nell'offerta dell'UE in quanto garante della sicurezza, con un adeguato coordinamento degli sforzi tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'UE, e in particolare ACCOGLIE CON FAVORE la cooperazione tra gli Stati membri, nonché con i partner del settore pubblico e privato, segnatamente attraverso EU CyberNet (la rete dell'UE per lo sviluppo delle capacità informatiche) e il forum globale sulle competenze informatiche (Global Forum on Cyber Expertise, GFCE), al fine di garantire il coordinamento ed evitare duplicazioni.

INVITA l'alto rappresentante e la Commissione a istituire un *comitato per lo sviluppo delle capacità informatiche* entro il terzo trimestre del 2022 e a tenere scambi periodici in seno al gruppo orizzontale "Questioni riguardanti il ciberspazio". INVITA la Commissione e l'alto rappresentante a mobilitare ulteriormente lo strumento di vicinato, cooperazione allo sviluppo

e cooperazione internazionale (NDICI), lo strumento di assistenza preadesione (IPA III) e altri strumenti finanziari, quali lo strumento europeo per la pace (EPF) e la strategia "Global Gateway", per sostenere il rafforzamento della resilienza dei nostri partner, la loro capacità di individuare e affrontare le minacce informatiche e di indagare e perseguire la criminalità informatica, nonché lo sviluppo di progetti di cooperazione, anche in un contesto di crisi; in particolare, INCORAGGIA la cooperazione con i partner dei Balcani occidentali e del vicinato orientale e meridionale dell'UE e l'invio di esperti dell'UE e degli Stati membri per offrire sostegno in caso di crisi informatiche, tenendo conto dei mandati giuridici esistenti.

21. SOTTOLINEA la necessità di intensificare gli sforzi per sviluppare un approccio di sensibilizzazione dell'UE strutturato e aperto su come promuovere un'intesa comune globale dell'applicazione del diritto internazionale nel ciberspazio, del quadro delle Nazioni Unite per il comportamento responsabile degli Stati nel ciberspazio, compresa l'iniziativa per un programma d'azione per promuovere un comportamento responsabile degli Stati nel ciberspazio, nonché sulla posizione dell'UE e dei suoi Stati membri nel quadro dei negoziati in corso per una convenzione delle Nazioni Unite sulla criminalità informatica, e nell'ambito di tali sforzi CHIEDE all'alto rappresentante di presentare un piano di sensibilizzazione al Consiglio entro la fine del 2022. INCORAGGIA l'alto rappresentante e i servizi della Commissione ad avvalersi appieno e in modo sistematico delle 145 delegazioni e a sviluppare una collaborazione periodica e proficua tra queste ultime e le ambasciate degli Stati membri nei paesi terzi, sotto l'egida della prevista rete della diplomazia informatica dell'UE. INVITA l'alto rappresentante a istituire la rete della diplomazia informatica dell'UE entro il terzo trimestre del 2022, contribuendo allo scambio di informazioni, alle attività di formazione congiunte per il personale dell'UE e degli Stati membri, agli sforzi coerenti per lo sviluppo delle capacità e al rafforzamento dell'attuazione del quadro delle Nazioni Unite per il comportamento responsabile degli Stati nonché a misure volte a rafforzare la fiducia tra gli Stati.

22. SOTTOLINEA il suo impegno a cooperare maggiormente con le organizzazioni internazionali e i paesi partner per promuovere la comprensione condivisa del panorama delle minacce informatiche, sviluppare meccanismi di cooperazione e individuare in modo proattivo risposte diplomatiche cooperative. RICORDANDO i principali risultati della cooperazione UE-NATO nel settore della cibersicurezza nel quadro dell'attuazione delle dichiarazioni congiunte di Varsavia del 2016 e di Bruxelles del 2018, nel pieno rispetto dell'autonomia e delle procedure decisionali di entrambe le organizzazioni e sulla base dei principi di trasparenza, reciprocità e inclusività, SOTTOLINEA la necessità di rafforzare ulteriormente la cooperazione informatica con la NATO attraverso esercitazioni, condivisione di informazioni e scambi tra esperti, anche in materia di sviluppo delle capacità, creazione di capacità per i partner, missioni e operazioni, nonché di applicabilità del diritto internazionale e delle norme delle nazioni Unite in materia di comportamento responsabile degli Stati nel ciberspazio ed eventuali risposte coordinate alle attività informatiche malevole.

V. PREVENIRE GLI ATTACCHI INFORMATICI, DIFENDERSI DA ESSI E RISPONDERVI

23. RICONOSCE che il ciberspazio è diventato un'arena per la concorrenza geopolitica e RIBADISCE pertanto che l'UE deve essere in grado di rispondere in modo rapido e deciso agli attacchi informatici, come le attività informatiche malevole sostenute da Stati ai danni dell'UE e dei suoi Stati membri, e deve quindi rafforzare il pacchetto di strumenti della diplomazia informatica dell'UE e avvalersi appieno di tutti i suoi strumenti, compresi gli strumenti politici, economici, diplomatici, giuridici e di comunicazione strategica disponibili per prevenire, scoraggiare, dissuadere e rispondere alle attività informatiche malevole. SOTTOLINEA che gli attori ostili devono essere consapevoli del fatto che gli attacchi informatici contro gli Stati membri e le istituzioni dell'UE saranno individuati precocemente e tempestivamente e affrontati con tutte le politiche e tutti gli strumenti necessari. Basandosi in particolare sugli elementi della posizione in materia di deterrenza informatica, sugli insegnamenti tratti dall'attuazione del pacchetto di strumenti della diplomazia informatica sin dalla sua istituzione e sull'esercitazione Cyber (EU CyCLES), INVITA gli Stati membri e l'alto rappresentante, con il sostegno della Commissione, a lavorare a una versione riveduta delle linee guida di attuazione del pacchetto di strumenti della diplomazia informatica dell'UE entro la fine del primo trimestre del 2023, in particolare valutando ulteriori misure di risposta.

24. SOTTOLINEA la necessità di tenere scambi periodici sul panorama delle minacce informatiche negli organi e nei comitati competenti del Consiglio, dialogando inoltre periodicamente con il settore privato e attingendo alla valutazione dell'impatto e della gravità degli incidenti recenti, al fine di aumentare la consapevolezza e la preparazione generali per ulteriori applicazioni del pacchetto di strumenti della diplomazia informatica dell'UE e sviluppare ulteriori strumenti per sostenerne l'attuazione. Sebbene la sicurezza nazionale resti di esclusiva competenza di ciascuno Stato membro, PRENDE ATTO della necessità di rafforzare la condivisione di intelligence e di informazioni e la cooperazione tra gli Stati membri e con l'INTCEN al fine di poter condividere le informazioni di intelligence all'inizio del processo decisionale, anche sulla questione dell'attribuzione, e consentire in tal modo una risposta rapida, efficace e fondata alle attività informatiche malevole ai danni dell'UE e dei suoi partner. RIBADISCE l'importanza di rafforzare la capacità dell'INTCEN nel settore informatico, sulla base dei contributi volontari in materia di intelligence da parte degli Stati membri e senza pregiudicarne le competenze, e di esaminare la proposta relativa all'eventuale istituzione di un gruppo di lavoro di intelligence informatica degli Stati membri.

25. RICONOSCENDO che le dichiarazioni e le misure restrittive dell'UE adottate nel quadro del pacchetto di strumenti della diplomazia informatica dell'UE hanno inviato un forte messaggio per ribadire che le attività informatiche malevole che costituiscono una minaccia esterna per l'UE, i suoi Stati membri e i suoi partner sono inaccettabili e contribuiscono pertanto a prevenire, scoraggiare, dissuadere e rispondere alle attività informatiche malevole, RIBADISCE il suo impegno a ricorrere a tali misure al fine di ricordare gli obblighi che si applicano al ciberspazio a norma del diritto internazionale, compresa la Carta delle Nazioni Unite nella sua interezza, e a promuovere il quadro delle Nazioni Unite per il comportamento responsabile degli Stati nel ciberspazio, compreso l'obbligo di dovuta diligenza per tutti gli Stati di non consentire consapevolmente l'utilizzo del proprio territorio per atti illeciti a livello internazionale compiuti mediante l'uso delle TIC, al fine di sviluppare e promuovere ulteriormente la visione condivisa dell'UE sull'applicazione del diritto internazionale nel ciberspazio. Osservando che messaggi adeguati e rapidi attenuano i rischi di escalation e possono scoraggiare gli autori di attacchi che prendono di mira gli interessi europei, INVITA l'alto rappresentante a elaborare e presentare agli Stati membri una strategia di comunicazione coerente sull'uso del pacchetto di strumenti della diplomazia informatica dell'UE.

26. INCORAGGIA lo sviluppo di approcci e risposte graduali, mirati e duraturi alle attività informatiche malevoli, ricorrendo all'ampia gamma di strumenti forniti dal pacchetto di strumenti della diplomazia informatica dell'UE, compreso il regime delle sanzioni dell'UE contro gli attacchi informatici, e prevedendo misure supplementari. SOTTOLINEA la necessità di accrescere la possibilità di mobilitare, caso per caso, tutti gli strumenti disponibili, interni ed esterni, per prevenire, scoraggiare, dissuadere e rispondere agli attacchi informatici, attuandoli mediante un approccio rapido, efficace, graduale, mirato e duraturo basato su un impegno strategico a lungo termine. INVITA l'alto rappresentante, in cooperazione con la Commissione, a individuare possibili risposte comuni dell'UE agli attacchi informatici, comprese opzioni sanzionatorie, in tutti i settori, al fine di essere pronti, se necessario, ad agire rapidamente ed efficacemente, e a presentarle al Consiglio entro la fine del primo trimestre del 2023.

27. 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, eventualmente per sostenere altri Stati membri e l'UE. Ciascuno Stato membro è incoraggiato a rafforzare, se necessario, le proprie capacità di fornire e ricevere aiuto e assistenza. SOTTOLINEA che l'ulteriore sviluppo di tali capacità dovrebbe essere uno degli obiettivi principali della futura politica dell'UE in materia di ciberdifesa. 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 i pertinenti attori della ciberdifesa dell'UE e degli Stati membri e sviluppare le proprie capacità, conformemente ai rispettivi mandati. INVITA l'alto rappresentante, insieme alla Commissione, a integrare lo sviluppo di una posizione dell'UE in materia di deterrenza informatica presentando nel 2022 una proposta ambiziosa per una politica dell'UE in materia di ciberdifesa, la quale aprirà la strada all'ulteriore sviluppo, da parte del Consiglio, della posizione dell'UE in materia di deterrenza informatica.

28. SOTTOLINEA la necessità di aumentare l'interoperabilità e la condivisione di informazioni attraverso la cooperazione tra squadre di pronto intervento informatico militari (MilCERT). INVITA gli Stati membri a creare, sulla base dei lavori dell'AED, una rete MilCERT per sviluppare la cooperazione e agevolare lo scambio di informazioni — che contribuirebbe anche a promuovere il coordinamento con altre cibercomunità — nonché una rete di comandanti militari per la sicurezza informatica al fine di rafforzare la cooperazione strategica tra i comandi per la sicurezza informatica degli Stati membri dell'UE o altre autorità corrispondenti. L'istituzione di tali reti, insieme ai progetti informatici PESCO, contribuirebbe a rafforzare la ciberdifesa a livello dell'UE. Sottolinea l'importanza della cooperazione tra la rete MilCERT proposta e la rete civile (CSIRT) già esistente per migliorare la condivisione delle informazioni e la conoscenza situazionale.

29. Sulla base della visione e strategia militari dell'UE sul ciberspazio come dominio operativo e tenendo conto dell'elaborazione in corso del concetto militare sulla ciberdifesa per le operazioni e le missioni militari condotte dall'UE, RIBADISCE la necessità di integrare la dimensione informatica nella pianificazione e nello svolgimento delle missioni e operazioni PSDC, anche potenziandone le capacità informatiche, e SOTTOLINEA che ciò contribuirà a migliorare la conoscenza situazionale informatica a livello dell'UE.

30. In conclusione, OSSERVA che la posizione in materia di deterrenza informatica costituirà un passo avanti verso l'istituzione di una dottrina dell'UE in materia di azione nel ciberspazio, basata sul potenziamento della resilienza, delle capacità e delle opzioni di risposta, nonché su una posizione condivisa sull'applicazione del diritto internazionale nel ciberspazio. Il Consiglio FARÀ IL PUNTO sui progressi compiuti nell'attuazione delle presenti conclusioni nel 2023 al fine di garantire l'ulteriore sviluppo della posizione dell'UE in materia di deterrenza informatica.