Consiglio
dell'Unione europea

Bruxelles, 23 marzo 2021
(OR. en)

7290/21

CYBER 80
TELECOM 124
COPEN 144
CODEC 443
COPS 107
COSI 50
CSC 119
CSCI 45
IND 70
RECH 117
ESPACE 21

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
in data:	22 marzo 2021
Destinatario:	Delegazioni
Oggetto:	Conclusioni del Consiglio sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale - Conclusioni del Consiglio approvate dal Consiglio nella sessione del 22 marzo 2021

Si allegano per le delegazioni le conclusioni del Consiglio sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale, approvate dal Consiglio nella sessione del 22 marzo 2021.

ALLEGATO

Conclusioni del Consiglio sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale

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],

- sulla governance di internet[2],

- sulla comunicazione congiunta del 20 novembre 2017 al Parlamento europeo e al Consiglio: "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE"[3],

- sullo sviluppo di capacità e competenze in materia di cibersicurezza nell'UE[4],

- sull'importanza del 5G per l'economia europea e sulla necessità di attenuare i relativi rischi per la sicurezza[5],

- sul futuro di un'Europa altamente digitalizzata oltre il 2020: "Accrescere la competitività digitale ed economica e la coesione digitale in tutta l'Unione"[6],

- sugli sforzi complementari per rafforzare la resilienza e contrastare le minacce ibride[7],

- sul tema "Plasmare il futuro digitale dell'Europa"[8],

---

1 Doc. 12109/13.
2 Doc. 16200/14.
3 Doc. 14435/17 + COR 1.
4 Doc. 7737/19.
5 Doc. 14517/19.
6 Doc. 9596/19.
7 Doc. 14972/19.
8 Doc. 8711/20.

- sulla diplomazia digitale[9],

- sul rafforzamento della resilienza e il contrasto delle minacce ibride, compresa la disinformazione nel contesto della pandemia di COVID-19[10],

- sulla diplomazia informatica[11],

- sulla risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala[12],

- su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica")[13],

- sugli orientamenti dell'UE per lo sviluppo delle capacità informatiche esterne[14],

- su "Una ripresa che fa progredire la transizione verso un'industria europea più dinamica, resiliente e competitiva"[15],

- sulla cibersicurezza dei dispositivi connessi[16],

- sul tema "Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza"[17], nonché

- la risoluzione del Consiglio sulla crittografia - La sicurezza attraverso la crittografia e nonostante la crittografia[18] e

---

9 Doc. 12804/20.
10 Doc. 14064/20.
11 Doc. 6122/15 + COR 1.
12 Doc. 10086/18.
13 Doc. 10474/17.
14 Doc. 10496/18.
15 Doc. 13004/20.
16 Doc. 13629/20.
17 Doc. 14540/16.
18 Doc. 13084/1/20 REV 1.

- la dichiarazione degli Stati membri del 15 ottobre 2020 sulla costruzione del cloud di prossima generazione per le imprese e il settore pubblico nell'UE,

RICORDANDO le conclusioni del Consiglio europeo sulla COVID-19, sul mercato unico, sulla politica industriale, sul digitale e sulle relazioni esterne, del 1º e 2 ottobre 2020,[19] e quelle sulla disinformazione e le minacce ibride e su una nuova agenda strategica 2019-2024, del 20 giugno 2019[20],

RICORDANDO la Strategia globale per la politica estera e di sicurezza dell'Unione europea - Visione condivisa, azione comune: un'Europa più forte, del 28 giugno 2016,

RICORDANDO la comunicazione della Commissione europea "Plasmare il futuro digitale dell'Europa", del 19 dicembre 2020[21], e quella sulla strategia dell'UE per l'Unione della sicurezza, del 24 luglio 2020[22],

RICORDANDO la comunicazione congiunta della Commissione europea e dell'alto rappresentante su una nuova agenda UE-USA per il cambiamento globale, del 2 dicembre 2020[23],

1. SOTTOLINEA che la cibersicurezza è essenziale per costruire un'Europa resiliente, verde e digitale e ACCOGLIE CON FAVORE la comunicazione congiunta al Parlamento europeo e al Consiglio dal titolo "La strategia dell'UE in materia di cibersicurezza per il decennio digitale", che delinea il nuovo quadro relativo all'azione dell'UE nel settore che comprende "resilienza, sovranità tecnologica e leadership" e alle modalità con cui proteggere la sua popolazione, le sue imprese e le sue istituzioni dalle minacce e dagli incidenti informatici, rafforzando al contempo la fiducia delle persone e delle organizzazioni nella capacità dell'UE di promuovere sistemi informativi e di rete, infrastrutture e connettività sicuri e affidabili e di promuovere e proteggere un ciberspazio globale, aperto, libero, stabile e sicuro, fondato sui diritti umani, sulle libertà fondamentali, sulla democrazia e sullo Stato di diritto.

---

19 Doc. EUCO 13/20.
20 Doc. EUCO 9/19.
21 COM(2020) 67 final, 19.2.2020.
22 COM(2020) 605 final, 24.7.2020.
23 JOIN(2020) 22 final, 2.12.2020.

2. RICONOSCE che la pandemia di COVID-19 ha messo in primo piano nella nostra vita quotidiana la crescente necessità di fiducia negli strumenti e nei sistemi delle tecnologie dell'informazione e della comunicazione (TIC) e nella loro sicurezza. SOTTOLINEA che la cibersicurezza e un'internet globale e aperta sono fondamentali per il funzionamento della pubblica amministrazione e delle istituzioni a livello sia nazionale che dell'UE, nonché per la nostra società e per l'economia nel suo complesso.

3. PONE L'ACCENTO sulla necessità di una maggiore sensibilizzazione in merito alle questioni informatiche al livello decisionale politico e strategico, fornendo ai responsabili delle politiche conoscenze e informazioni pertinenti, e SOTTOLINEA l'esigenza di rafforzare la consapevolezza del grande pubblico e di promuovere l'igiene informatica.

4. CHIEDE di promuovere e tutelare i valori fondamentali dell'UE in materia di democrazia, Stato di diritto, diritti umani e libertà fondamentali, compresi il diritto alla libertà di espressione e d'informazione, il diritto alla libertà di riunione e di associazione e il diritto alla riservatezza nel ciberspazio. ACCOGLIE CON FAVORE, a tale riguardo, ulteriori sforzi costanti intesi a proteggere i difensori dei diritti umani e gli esponenti della società civile e del mondo accademico che si occupano di questioni quali la cibersicurezza, la riservatezza dei dati, la sorveglianza e la censura online fornendo ulteriori orientamenti pratici, promuovendo le migliori pratiche e intensificando gli sforzi dell'UE per prevenire le violazioni e gli abusi dei diritti umani e l'uso improprio delle tecnologie emergenti, in particolare mediante il ricorso a misure diplomatiche, ove necessario, e il controllo delle esportazioni di tali tecnologie. EVIDENZIA, in tale contesto, l'importanza del piano d'azione dell'UE per i diritti umani e la democrazia 2020-2024 e degli orientamenti dell'UE in materia di diritti umani per la libertà di espressione online e offline.

5. SOTTOLINEA che raggiungere l'autonomia strategica mantenendo nel contempo un'economia aperta è un obiettivo fondamentale dell'Unione per consentirle di autodeterminarsi in termini di percorso e interessi economici. Tale obiettivo implica anche il rafforzamento della capacità di compiere scelte autonome nel settore della cibersicurezza allo scopo di rafforzare la leadership digitale dell'UE e le sue capacità strategiche. RICORDA che ciò comprende l'individuazione e la riduzione delle dipendenze strategiche e l'aumento della resilienza negli ecosistemi industriali più sensibili e in settori specifici. SOTTOLINEA che a tal fine può rivelarsi necessario diversificare la produzione e le catene di approvvigionamento, favorire e attirare gli investimenti e la produzione in Europa, esplorare soluzioni alternative e modelli circolari e promuovere un'ampia cooperazione industriale tra gli Stati membri.

6. Tenendo presente la carenza di competenze digitali e in materia di cibersicurezza nella forza lavoro, SOTTOLINEA l'importanza di soddisfare la domanda di una forza lavoro qualificata nel settore del digitale e della cibersicurezza, in particolare sviluppando, trattenendo e attirando i migliori talenti, ad esempio attraverso l'istruzione e la formazione, per poter digitalizzare la nostra società in modo sicuro sotto il profilo informatico. INCORAGGIA l'aumento della partecipazione delle donne e delle ragazze all'istruzione nelle discipline STEM (scienza, tecnologia, ingegneria e matematica), come pure ad attività per il miglioramento del livello delle competenze e la riqualificazione delle occupazioni nel settore delle TIC per quanto riguarda le competenze digitali, in quanto ciò costituisce uno dei mezzi per colmare il divario digitale di genere.

7. 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 il proprio impegno a favore della risoluzione pacifica delle controversie internazionali relative al ciberspazio, come pure che tutti i suoi sforzi diplomatici dovrebbero, in via prioritaria, mirare a promuovere la sicurezza e la stabilità nel ciberspazio attraverso una maggiore cooperazione internazionale e a ridurre i rischi di errata percezione, escalation e conflitto che possono derivare da incidenti nell'ambito delle TIC, e SOSTIENE l'ulteriore sviluppo e la messa in opera di misure volte a rafforzare la fiducia (CBM) a livello regionale e internazionale. RIBADISCE l'appello dell'Assemblea generale delle Nazioni Unite, concordato per consenso, affinché gli Stati membri dell'ONU si ispirino alle raccomandazioni contenute nelle relazioni dell'UNGGE nel loro impiego delle TIC e RIAFFERMA l'applicazione del diritto internazionale, in particolare della Carta delle Nazioni Unite nella sua interezza, nel ciberspazio.

8. RIBADISCE che, al fine di definire in modo sostanziale le norme e gli standard internazionali nei settori delle tecnologie emergenti e delle infrastrutture tecniche e logiche essenziali per la disponibilità generale e l'integrità del nucleo pubblico di internet, assicurando che esse siano in linea con i valori universali e dell'UE e servendosi di un approccio multipartecipativo, è essenziale l'ulteriore sviluppo di norme e standard all'interno dell'Unione. Ciò garantirà che internet rimanga globale, aperta, libera, stabile e sicura, che l'impiego e lo sviluppo delle tecnologie digitali avvengano nel rispetto dei diritti umani e che il loro uso sia legale, sicuro ed etico. PRENDE ATTO della prossima strategia di normazione e SI IMPEGNA a condurre un'azione di sensibilizzazione proattiva e coordinata per promuovere la leadership e gli obiettivi dell'UE a livello internazionale, anche in seno a vari organismi internazionali di normazione e attraverso la cooperazione con partner che condividono le stesse idee, la società civile, il mondo accademico e il settore privato.

9. SOSTIENE FORTEMENTE il modello multipartecipativo per la governance di internet e la cibersicurezza e si impegna a rafforzare gli scambi regolari e strutturati con i portatori di interessi, compresi il settore privato, il mondo accademico e la società civile, nei consessi internazionali, anche nel contesto dell'appello di Parigi a favore della fiducia e della sicurezza nel ciberspazio. PROMUOVE un accesso a internet universale, egualitario e a prezzi contenuti che consenta di colmare i divari digitali e, in particolare, la responsabilizzazione delle donne e delle ragazze nonché delle persone che si trovano in situazioni di vulnerabilità o emarginazione, sia nell'elaborazione delle politiche che nell'uso di internet.

10. SOTTOLINEA la necessità di includere la cibersicurezza negli investimenti e nelle iniziative digitali dei prossimi anni e di contribuire progressivamente a creare condizioni di parità nella cibersicurezza e PRENDE ATTO del piano della Commissione per aumentare la spesa pubblica e mobilitare investimenti privati nel settore della cibersicurezza. EVIDENZIA l'importanza delle piccole e medie imprese (PMI) nell'ecosistema della cibersicurezza e RICONOSCE i pertinenti strumenti finanziari disponibili per sostenere misure fortemente incentrate sulla cibersicurezza all'interno della trasformazione digitale nel quadro finanziario pluriennale (QFP) 2021-2027, così come nel dispositivo per la ripresa e la resilienza.

11. ATTENDE CON INTERESSE la rapida attuazione del regolamento sul Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento, compresa la rapida istituzione e messa in funzione del Centro europeo di competenza sulla cibersicurezza a Bucarest. Una tempestiva adozione del suo programma contribuirà a massimizzare gli effetti degli investimenti intesi a rafforzare la leadership e l'autonomia strategica dell'Unione nel settore della cibersicurezza, sostenendo le capacità e le competenze tecnologiche, e ad aumentare la competitività globale dell'Unione con il contributo dell'industria e delle comunità accademiche in materia di cibersicurezza, comprese le PMI e i centri di ricerca, che trarranno vantaggio da una collaborazione più sistematica, inclusiva e strategica, tenendo conto della coesione dell'Unione e di tutti i suoi Stati membri.

12. PLAUDE ai lavori in corso condotti dall'ENISA, insieme agli Stati membri e alle parti interessate, per fornire all'UE sistemi di certificazione per i prodotti, i servizi e i processi TIC che dovrebbero contribuire a innalzare il livello complessivo della cibersicurezza all'interno del mercato unico digitale. In tale contesto, ATTENDE CON INTERESSE il programma di lavoro progressivo dell'Unione al fine di sviluppare sistemi di certificazione della cibersicurezza dell'UE nell'ambito del regolamento sulla cibersicurezza. RICONOSCE, a tale riguardo, il ruolo centrale dell'UE nello sviluppo di norme che siano in grado di dare forma al panorama della cibersicurezza e che contribuiscano a garantire una concorrenza leale all'interno dell'UE e su scala mondiale, promuovendo l'accesso al mercato e affrontando i rischi per la sicurezza, ma anche garantendo l'applicabilità del quadro legislativo dell'UE.

13. RIBADISCE l'importanza di valutare la necessità, nel lungo termine, di un atto legislativo orizzontale, che specifichi anche le condizioni necessarie per l'immissione sul mercato, per affrontare tutti gli aspetti attinenti alla cibersicurezza dei dispositivi connessi, quali la disponibilità, l'integrità e la riservatezza. ACCOGLIE CON FAVORE, a tale proposito, una discussione intesa a esaminare l'ambito di applicazione di tale normativa e i suoi collegamenti con il quadro di certificazione della cibersicurezza quale definito nel regolamento sulla cibersicurezza, al fine di aumentare il livello di sicurezza all'interno del mercato unico digitale. SOTTOLINEA che i requisiti di cibersicurezza dovrebbero essere definiti in linea con la pertinente legislazione dell'Unione, tra cui il regolamento sulla cibersicurezza, il nuovo quadro legislativo, il regolamento sulla normazione europea e un eventuale futuro atto legislativo orizzontale, al fine di evitare ambiguità e frammentazioni della legislazione.

14. RICONOSCE l'importanza di un approccio globale e orizzontale alla cibersicurezza nell'Unione, nel pieno rispetto delle competenze e delle esigenze degli Stati membri, nonché l'importanza del sostegno continuo all'assistenza tecnica e alla cooperazione per sviluppare la capacità degli Stati membri. Tenendo conto dell'evoluzione del panorama delle minacce informatiche, PRENDE ATTO della nuova proposta di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che si basa sulla direttiva NIS, e ribadisce il suo sostegno al rafforzamento e all'armonizzazione dei quadri nazionali di cibersicurezza e alla cooperazione continua tra gli Stati membri. SOTTOLINEA inoltre la necessità di allineare e articolare la legislazione settoriale in tale ambito.

15. PRENDE ATTO della proposta della Commissione di sostenere gli Stati membri nell'istituzione e nel rafforzamento dei centri operativi di sicurezza (SOC) al fine di creare una rete di SOC in tutta l'UE, per meglio monitorare e anticipare i segnali di attacchi alle reti. In tale contesto, ATTENDE i piani dettagliati della Commissione relativi alla rete dei SOC, nel rispetto delle competenze degli Stati membri. RICORDA le iniziative intraprese dagli Stati membri, con il sostegno dell'UE, per istituire CSIRT settoriali, nazionali e regionali e centri di condivisione e analisi delle informazioni (ISAC) nazionali o europei nell'ambito di una rete efficace di partenariati in materia di cibersicurezza nell'Unione. ATTENDE CON INTERESSE di esplorare il potenziale di questa rete per rafforzare i SOC, nonché la loro complementarità e il loro coordinamento con le reti e gli attori esistenti (in particolare la rete di CSIRT), al fine di promuovere una cultura di condivisione delle informazioni efficiente, sicura e affidabile. SOTTOLINEA che tale processo si baserà sul lavoro svolto nel contesto delle iniziative in materia di intelligenza artificiale e calcolo ad alte prestazioni e a opera dei poli europei dell'innovazione digitale.

16. PRENDE ATTO del possibile sviluppo di un sistema di connettività sicura, sulla base dell'infrastruttura europea di comunicazione quantistica (EuroQCI) e della comunicazione satellitare governativa dell'Unione europea (GOVSATCOM), e RICONOSCE che qualsiasi eventuale sviluppo futuro dovrebbe basarsi su un solido quadro di cibersicurezza e tenere conto dell'intera infrastruttura di comunicazione elettronica, come i sistemi di reti spaziali, terrestri e sottomarine.

17. ATTENDE CON INTERESSE le discussioni con la Commissione, l'ENISA, i due operatori dei server root DNS dell'UE e la comunità multipartecipativa, per valutare il ruolo dei due operatori nel garantire che internet resti globalmente accessibile senza frammentazioni. ACCOGLIE CON FAVORE le ulteriori discussioni sull'intenzione della Commissione di sviluppare un servizio europeo alternativo per l'accesso all'internet globale (iniziativa "DNS4EU"), basato su un modello trasparente, conforme alle più recenti norme e regole in materia di sicurezza, protezione dei dati e riservatezza fin dalla progettazione e per impostazione predefinita, al fine di contribuire ad aumentare la resilienza, mantenendo e rafforzando nel contempo la connettività internazionale di tutti gli Stati membri.

18. RICONOSCE la necessità di uno sforzo congiunto della Commissione e degli Stati membri per accelerare l'adozione di norme internet chiave tra cui l'IPv6 64 e di norme di sicurezza internet consolidate, in quanto fondamentali per aumentare il livello generale di sicurezza, resilienza, apertura e interoperabilità dell'internet globale, e rafforzare nel contempo la competitività dell'industria dell'UE, in particolare, degli operatori dell'infrastruttura di internet.

19. SOTTOLINEA l'importanza di un approccio coordinato nonché dello sviluppo e dell'attuazione di misure efficaci a livello nazionale per rafforzare la cibersicurezza delle reti 5G. SOSTIENE le prossime misure da adottare in materia di cibersicurezza delle reti 5G, presentate nell'appendice alla strategia dell'UE in materia di cibersicurezza e basate sui risultati della relazione sull'impatto della raccomandazione della Commissione sulla sicurezza delle reti 5G, ad esempio per quanto riguarda la definizione di un approccio globale e a lungo termine che tenga conto della catena del valore e dell'ecosistema del 5G nel complesso. Al fine di rafforzare ulteriormente l'approccio coordinato alla sicurezza delle reti 5G, ESORTA gli Stati membri, le istituzioni dell'UE e gli altri portatori di interessi pertinenti a proseguire i propri bilanci e aggiornamenti periodici, unitamente allo scambio di informazioni e migliori pratiche nell'ambito del flusso di lavoro specifico sulla cibersicurezza del 5G del gruppo di cooperazione NIS, e a riferire periodicamente al Consiglio in merito ai progressi compiuti. Pur sottolineando la responsabilità degli Stati membri per quanto riguarda la protezione della sicurezza nazionale, METTE IN RILIEVO il suo fermo impegno ad applicare le misure del pacchetto di strumenti dell'UE per il 5G e completarne rapidamente l'attuazione nonché a proseguire gli sforzi volti a garantire la sicurezza delle reti 5G e lo sviluppo delle future generazioni di reti. La stretta cooperazione tra gli Stati membri, la Commissione e l'ENISA in materia di sicurezza delle reti 5G potrebbe costituire un esempio per altre questioni nel settore della cibersicurezza, nel rispetto delle competenze degli Stati membri e dei principi di sussidiarietà e proporzionalità.

20. RICONOSCE l'importanza di integrare ulteriormente la cibersicurezza nei meccanismi di risposta alle crisi dell'UE e di sottoporre a prova tali meccanismi nelle esercitazioni pertinenti, e SOTTOLINEA l'importanza di rafforzare la cooperazione e la condivisione di informazioni tra le varie cibercomunità all'interno dell'UE nonché di collegare le iniziative, le strutture e le procedure esistenti (quali l'IPCR, la rete CSIRT, il gruppo di cooperazione NIS, la CyCLONe, il Centro europeo per la lotta alla criminalità informatica, l'INTCEN e altri organismi pertinenti dell'UE) in caso di minacce e incidenti informatici transfrontalieri su larga scala. TENENDO CONTO dei progressi già compiuti in questo settore, ATTENDE la proposta della Commissione relativa al processo, alle tappe e al calendario per la definizione dell'unità congiunta per il ciberspazio al fine di fornire valore aggiunto e una chiara focalizzazione nonché di razionalizzare il quadro di gestione delle crisi di cibersicurezza dell'UE, anche attraverso la preparazione, la conoscenza situazionale condivisa, un coordinamento rafforzato della risposta e delle esercitazioni, in modo trasparente e incrementale, evitando al contempo duplicazioni e sovrapposizioni e nel rispetto delle competenze degli Stati membri.

21. SOTTOLINEA al tempo stesso l'importanza di promuovere la cooperazione e lo scambio di informazioni tra gli attori pertinenti in materia di cibersicurezza e le autorità competenti nel settore della sicurezza e della giustizia penale, ad esempio le autorità giudiziarie e di contrasto, e la necessità di ampliare e migliorare la capacità di tali autorità di indagare e perseguire la criminalità informatica e di promuovere i negoziati internazionali e le norme dell'UE in materia di accesso transfrontaliero alle prove elettroniche. A prescindere dall'attuale contesto tecnologico, risulta fondamentale preservare i poteri delle autorità competenti nel settore della sicurezza e della giustizia penale attraverso un accesso legittimo che consenta loro lo svolgimento dei compiti secondo quanto prescritto e autorizzato dalla legge. Tali leggi che prevedono poteri esecutivi devono sempre rispettare pienamente il giusto processo e altre garanzie nonché i diritti fondamentali, in particolare il diritto al rispetto della vita privata e del carattere privato delle comunicazioni e il diritto alla protezione dei dati personali.

22. RIBADISCE il proprio sostegno allo sviluppo, all'attuazione e all'uso di una crittografia forte quale strumento necessario per proteggere i diritti fondamentali e la sicurezza digitale delle persone, dei governi, dell'industria e della società e RICONOSCE, al contempo, la necessità di garantire che le autorità competenti nel settore della sicurezza e della giustizia penale, quali le autorità di contrasto e giudiziarie, siano in grado di esercitare i loro legittimi poteri, sia online che offline, per proteggere le nostre società e i nostri cittadini. Le autorità competenti devono essere in grado di accedere ai dati in modo legittimo e mirato, nel pieno rispetto dei diritti fondamentali e delle pertinenti leggi in materia di protezione dei dati, preservando nel contempo la cibersicurezza. METTE IN RILIEVO che le azioni intraprese devono rispettare attentamente l'equilibrio tra tali interessi e i principi di necessità, proporzionalità e sussidiarietà.

23. SOSTIENE e PROMUOVE la convenzione di Budapest sulla criminalità informatica, e i lavori in corso sul secondo protocollo aggiuntivo a tale convenzione. Continua inoltre a partecipare a scambi multilaterali sulla criminalità informatica, anche nei processi connessi al Consiglio d'Europa, all'Ufficio delle Nazioni Unite contro la droga e il crimine (UNODC) e alla Commissione per la prevenzione del crimine e la giustizia penale, al fine di garantire una cooperazione internazionale rafforzata per contrastare la criminalità informatica; in tale ambito rientrano lo scambio di migliori pratiche e conoscenze tecniche, nonché il sostegno allo sviluppo di capacità, garantendo parallelamente il rispetto, la promozione e la protezione dei diritti umani e delle libertà fondamentali.

24. Sebbene la sicurezza nazionale rimanga di esclusiva competenza di ciascuno Stato membro, RICONOSCE 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 al lavoro dell'INTCEN quale polo per la conoscenza situazionale e le valutazioni della minaccia in merito alle questioni informatiche per l'UE nonché a esaminare la proposta relativa all'eventuale istituzione di un gruppo di lavoro di intelligence informatica degli Stati membri al fine di rafforzare la capacità specifica dell'INTCEN in questo settore, sulla base dei contributi volontari in materia di intelligence da parte degli Stati membri e senza pregiudicarne le competenze.

25. SOTTOLINEA l'importanza di un quadro di sicurezza solido e coerente per proteggere il personale, i dati, le reti di comunicazione e i sistemi di informazione e i processi decisionali dell'UE nella loro interezza sulla base di norme globali, coerenti e omogenee. In particolare, ciò dovrebbe avvenire stimolando la resilienza e migliorando la cultura della sicurezza dell'UE nei confronti delle minacce informatiche nonché rafforzando la sicurezza delle reti classificate e non classificate dell'UE, garantendo nel contempo una governance adeguata e la messa a disposizione di risorse e capacità sufficienti, anche nel contesto del consolidamento del mandato di CERT-UE. ACCOGLIE CON FAVORE, in tale contesto, le discussioni in corso in merito alla fissazione di norme comuni sulla sicurezza dell'informazione, che tengano in debita considerazione le regole di sicurezza del Consiglio per la protezione delle informazioni classificate UE, nonché alla definizione di norme comuni vincolanti sulla cibersicurezza per tutte le istituzioni, gli organismi e le agenzie dell'UE.

26. MUOVENDO dagli sforzi dell'UE in materia di diplomazia informatica, SI IMPEGNA ad aumentare l'efficacia e l'efficienza del pacchetto di strumenti della diplomazia informatica e ATTENDE CON INTERESSE che vengano approfondite le discussioni sul suo ambito di applicazione e sul suo utilizzo sulla base degli insegnamenti tratti finora dall'applicazione di tale strumento. Tali discussioni dovrebbero contribuire a promuovere la sicurezza a livello internazionale favorendo il dialogo e una visione condivisa delle questioni di cibersicurezza, rafforzando la prevenzione, la stabilità e la cooperazione e stimolando la fiducia e lo sviluppo di capacità e, ove necessario, applicando misure restrittive, al fine di prevenire, scoraggiare, dissuadere e rispondere ad attività informatiche dolose rivolte contro l'integrità e la sicurezza dell'UE e dei suoi Stati membri, contribuendo in tal modo alla sicurezza e alla stabilità internazionali e consolidando la posizione in materia di deterrenza informatica dell'UE, nel pieno rispetto delle competenze e delle prerogative nazionali. Segnatamente, si dovrebbe prestare particolare attenzione alla prevenzione e al contrasto degli attacchi informatici con effetti sistemici che potrebbero incidere sulle nostre catene di approvvigionamento e infrastrutture critiche e sui nostri servizi essenziali nonché sulle istituzioni e sui processi democratici e compromettere la nostra sicurezza economica, compresi i furti di proprietà intellettuale favoriti dall'informatica. Gli Stati membri e le istituzioni dell'UE dovrebbero inoltre proseguire la riflessione sull'articolazione tra il quadro di gestione delle crisi di cibersicurezza dell'UE, il pacchetto di strumenti della diplomazia informatica e le disposizioni dell'articolo 42, paragrafo 7, del TUE e dell'articolo 222 del TFUE, in particolare lavorando sulla base di scenari per definire una comprensione comune delle modalità pratiche di attuazione dell'articolo 42, paragrafo 7, del TUE.

27. RICONOSCE l'importanza di rafforzare la cooperazione con le organizzazioni internazionali e i paesi partner al fine di promuovere la comprensione condivisa del panorama delle minacce informatiche, sviluppare dialoghi e meccanismi di cooperazione, individuare, se del caso, risposte diplomatiche cooperative e migliorare lo scambio di informazioni, anche attraverso l'istruzione, la formazione e le esercitazioni. In particolare, SOTTOLINEA che un forte partenariato transatlantico nel settore della cibersicurezza contribuisce alla sicurezza, alla stabilità e alla prosperità comuni e PRENDE ATTO delle disposizioni sulla cooperazione in materia di cibersicurezza nell'ambito dell'accordo sugli scambi commerciali e la cooperazione UE-Regno Unito. 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, ribadisce l'importanza di una cooperazione rafforzata, sinergica e reciprocamente vantaggiosa attraverso l'istruzione, la formazione, le esercitazioni e una risposta coordinata alle attività informatiche dolose, nel pieno rispetto dell'autonomia e delle procedure decisionali di entrambe le organizzazioni, sulla base dei principi di trasparenza, reciprocità e inclusività.

28. Al fine di contribuire a un ciberspazio globale, aperto, libero, stabile e sicuro, che riveste un'importanza sempre maggiore per la prosperità, la crescita, la sicurezza, il benessere, la connettività e l'integrità costanti delle nostre società, SI IMPEGNA a un dialogo costante nei processi di definizione di norme nell'ambito delle organizzazioni internazionali, in particolare nei processi connessi al Primo Comitato delle Nazioni Unite, promuovendo e contribuendo al riconoscimento dell'applicazione del diritto internazionale nel ciberspazio nonché all'adesione alle norme, alle regole e ai principi del comportamento responsabile degli Stati nel ciberspazio, anche favorendo la rapida istituzione di un programma d'azione per promuovere un comportamento responsabile degli Stati nel ciberspazio (PoA) come seguito costruttivo, inclusivo e basato sul consenso ai lavori in corso sia del gruppo di lavoro aperto (OEWG) sia del gruppo di esperti governativi (UNGGE).

29. RICORDA il suo fermo impegno a favore di un multilateralismo efficace e di un ordine mondiale fondato su regole – con al centro le Nazioni Unite – e la sua determinazione a rafforzare la cooperazione e il coordinamento con le organizzazioni internazionali e regionali, segnatamente il sistema delle Nazioni Unite, la NATO, il Consiglio d'Europa, l'OSCE, l'OCSE, l'UA, l'OSA, l'ASEAN, l'ARF, il CCG e la Lega araba riguardo alle discussioni su questioni connesse al ciberspazio, nonché il proseguimento e l'ampliamento dei quadro dei dialoghi e delle consultazioni strutturati dell'UE in materia di cibersicurezza con i paesi terzi. SOTTOLINEA il suo sostegno attivo alle Nazioni Unite, in particolare in relazione all'Agenda 2030, compresi gli obiettivi di sviluppo sostenibile, e ACCOGLIE CON FAVORE la tabella di marcia per la cooperazione digitale e l'agenda per il disarmo del segretario generale delle Nazioni Unite, che promuovono la responsabilità e l'osservanza delle norme nel ciberspazio e contribuiscono alla prevenzione e alla risoluzione pacifica dei conflitti derivanti da attività dolose nel ciberspazio. ACCOGLIE CON FAVORE la proposta relativa all'istituzione, da parte dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, di una rete informale della diplomazia informatica dell'UE nell'ottica di sviluppare il coinvolgimento e le competenze sia dell'UE che degli Stati membri riguardo alle questioni internazionali riguardanti il ciberspazio, al fine di rafforzare le attività di sensibilizzazione coordinate.

30. ATTENDE CON INTERESSE la proposta di revisione del quadro strategico in materia di ciberdifesa, attesa a breve, e SI IMPEGNA a proseguire gli sforzi per rafforzare le dimensioni di cibersicurezza e ciberdifesa al fine di garantirne la piena integrazione nel più ampio settore della sicurezza e della difesa, in particolare nel contesto dei lavori sulla bussola strategica. RITIENE che le imminenti "visione e strategia militari dell'UE sul ciberspazio come dominio operativo" contribuiranno a promuovere tali discussioni. SI RALLEGRA dell'iniziativa dell'Agenzia europea per la difesa (AED) volta a promuovere la cooperazione tra le CERT militari e SOSTIENE gli sforzi compiuti per consolidare le sinergie civili-militari e il coordinamento in materia di ciberdifesa e cibersicurezza, compresi gli aspetti connessi allo spazio, anche attraverso i progetti specifici della PESCO.

31. ACCOGLIE CON FAVORE la proposta di elaborare un'agenda dell'UE per lo sviluppo delle capacità informatiche esterne, la proposta di creare un comitato dell'UE per lo sviluppo delle capacità informatiche, nonché l'istituzione e l'attuazione di EU CyberNet (la rete dell'UE per lo sviluppo delle capacità informatiche) al fine di aumentare la ciberresilienza e le capacità a livello mondiale. In tale contesto ACCOGLIE CON FAVORE la cooperazione con gli Stati membri, nonché con i partner del settore pubblico e privato, in particolare il forum globale sulle competenze informatiche (Global Forum on Cyber Expertise, GFCE) e altri organismi internazionali pertinenti, al fine di garantire il coordinamento ed evitare duplicazioni. In particolare, INCORAGGIA la cooperazione con i partner nei Balcani occidentali e nel vicinato orientale e meridionale dell'UE.

32. Al fine di garantire che tutti i paesi possano cogliere i vantaggi sociali, economici e politici di internet e dell'uso delle tecnologie, SI IMPEGNA ad assistere i paesi partner nell'affrontare la sfida crescente rappresentata dalle attività informatiche dolose, in particolare quelle che danneggiano lo sviluppo delle loro economie e società nonché l'integrità e la sicurezza dei sistemi democratici, anche in linea con gli sforzi profusi nell'ambito del piano d'azione per la democrazia europea.

33. Al fine di garantire lo sviluppo, l'attuazione e il monitoraggio delle proposte presentate nella strategia dell'UE in materia di cibersicurezza, e tenendo conto del carattere pluriennale di alcune iniziative, INCORAGGIA la Commissione e l'alto rappresentante per gli affari esteri e la politica di sicurezza a definire un piano di attuazione dettagliato che stabilisca le priorità e il calendario delle azioni previste. MONITORERÀ i progressi compiuti nell'attuazione delle presenti conclusioni mediante un piano d'azione che sarà periodicamente riesaminato e aggiornato dal Consiglio in stretta cooperazione con la Commissione europea e con l'alto rappresentante.