Consiglio
dell'Unione europea

Bruxelles, 20 ottobre 2021
(OR. en)

13048/21

CYBER 263
JAI 1117
TELECOM 384
CSC 362
CIS 116
RELEX 874
ENFOPOL 370
COPS 373
COSI 190
HYBRID 62
CSCI 133
POLGEN 177
DATAPROTECT 244

RISULTATI DEI LAVORI

Origine:	Segretariato generale del Consiglio
in data:	19 ottobre 2021
Destinatario:	Delegazioni
n. doc. prec.:	12534/21
Oggetto:	Conclusioni del Consiglio – 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 – Conclusioni del Consiglio (19 ottobre 2021)

Si allegano per le delegazioni le conclusioni del Consiglio dal titolo "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", adottate dal Consiglio nella sessione del 19 ottobre 2021.

ALLEGATO

Conclusioni del Consiglio – 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

IL CONSIGLIO DELL'UNIONE EUROPEA,

RAMMENTANDO:

– le sue conclusioni sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale[1],

– le sue conclusioni relative alla risposta coordinata dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala[2],

– le sue conclusioni sulla diplomazia informatica[3],

– le sue conclusioni su un quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica")[4],

– le sue conclusioni sulla sicurezza e la difesa[5],

– il quadro strategico dell'UE in materia di ciberdifesa[6],

– le sue conclusioni dal titolo "Plasmare il futuro digitale dell'Europa"[7],

– 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,

---

1 Doc. 7290/21.
2 Doc. 10086/18.
3 Doc. 6122/15 + COR 1.
4 Doc. 10474/17.
5 Doc. 8396/21.
6 Doc. 15585/14.
7 Doc. 8711/20.

– le sue conclusioni sulla comunicazione congiunta al Parlamento europeo e al Consiglio: "Resilienza, deterrenza e difesa: verso una cibersicurezza forte per l'UE"[8],

– le sue conclusioni sullo sviluppo di capacità e competenze in materia di cibersicurezza nell'UE[9],

1. EVIDENZIA l'importanza della cibersicurezza per la costruzione di un'Europa resiliente, digitale e verde. SOTTOLINEA che la cibersicurezza è indispensabile per la prosperità e la sicurezza dell'UE e dei suoi Stati membri, dei suoi cittadini, delle sue imprese e delle sue istituzioni, nonché per difendere l'integrità delle nostre società libere e democratiche.

2. RICONOSCE il carattere transfrontaliero e intersettoriale di molte minacce alla cibersicurezza e i rischi e le potenziali implicazioni delle incessanti campagne segnate da attività informatiche dolose più incisive, sofisticate, mirate, complesse, persistenti e/o pervasive[10]. La pandemia di COVID-19 ha ulteriormente messo in luce le vulnerabilità delle nostre società e i possibili danni causati dagli incidenti di cibersicurezza su vasta scala all'economia, alla democrazia, ai servizi essenziali e alle infrastrutture critiche, in particolare nel settore sanitario. Ha inoltre esacerbato l'importanza della connettività e la dipendenza della società da sistemi informativi e di rete affidabili e sicuri. Infine, ha posto in evidenza la necessità di un'internet globale, aperta, libera, stabile e sicura, così come l'esigenza di fiducia nei prodotti, processi e servizi delle tecnologie dell'informazione e della comunicazione (TIC) e nella loro sicurezza, compresa la necessità di assicurare una catena di approvvigionamento resiliente.

---

8 Doc. 14435/17 + COR 1.
9 Doc. 7737/19.
10 Relazione 2020 dell'ENISA sul panorama delle minacce.

3. RIBADISCE l'importanza della ciberresilienza e dell'ulteriore sviluppo del quadro dell'UE per la gestione delle crisi di cibersicurezza[11] – con l'obiettivo di rispondere in modo efficiente e tempestivo a livello dell'UE agli incidenti e alle crisi di cibersicurezza su vasta scala – nonché della sua ulteriore integrazione nei meccanismi orizzontali e settoriali di risposta alle crisi dell'UE esistenti. SOTTOLINEA il ruolo del Consiglio e dei dispositivi integrati dell'UE per la risposta politica alle crisi (IPCR) nel garantire un coordinamento e una risposta tempestivi a livello politico dell'Unione alle crisi aventi un ampio impatto o rilevanza politica, che si verifichino all'interno o all'esterno dell'Unione. EVIDENZIA l'importanza di testare tali quadri e meccanismi in esercitazioni periodiche.

4. RICORDA che le attività a livello dell'UE per quanto riguarda gli incidenti e le crisi di cibersicurezza su vasta scala si svolgono nel rispetto dei principi di sussidiarietà, proporzionalità, complementarità, non duplicazione e riservatezza. RIBADISCE che agli Stati membri spetta la responsabilità primaria di rispondere agli incidenti e alle crisi di cibersicurezza su vasta scala che li colpiscono. RICORDA l'importanza del rispetto delle competenze degli Stati membri e la loro competenza esclusiva in materia di sicurezza nazionale, conformemente all'articolo 4, paragrafo 2, del trattato sull'Unione europea, compreso il settore della cibersicurezza.

5. RICORDA, nel contempo, l'importanza del rispetto delle competenze e dei mandati delle istituzioni, degli organi e delle agenzie dell'UE. L'alto rappresentante, la Commissione e altre istituzioni, altri organi e altre agenzie dell'UE svolgono altresì un ruolo essenziale, derivante dal diritto dell'Unione, anche a causa del possibile impatto degli incidenti e delle crisi di cibersicurezza su vasta scala sul mercato unico, così come sul funzionamento stesso delle istituzioni, degli organi e delle agenzie dell'UE.

[11] Doc. 10086/18.

6. SOTTOLINEA la necessità di evitare inutili duplicazioni e di cercare la complementarità e il valore aggiunto nell'ulteriore sviluppo del quadro dell'UE per la gestione delle crisi di cibersicurezza, nonché di garantire l'allineamento con i meccanismi, le iniziative, le reti, i processi e le procedure esistenti a livello nazionale ed europeo. EVIDENZIA l'importanza di razionalizzare i processi e le strutture esistenti per ridurre la complessità e, ai fini della coesione nell'Unione, migliorare l'accessibilità e la capacità di risposta a favore di coloro che necessitano di assistenza e solidarietà.

7. RICONOSCE l'applicabilità del diritto internazionale, compresa la Carta delle Nazioni Unite nella sua interezza, del diritto internazionale umanitario e del diritto internazionale dei diritti umani nel ciberspazio e PROMUOVE l'adesione alle norme, alle regole e ai principi volontari e non vincolanti di comportamento responsabile degli Stati nel ciberspazio, approvati da tutti gli Stati membri delle Nazioni Unite.

8. SI COMPIACE dei progressi compiuti negli ultimi anni in seno al Consiglio, in particolare in sede di gruppo orizzontale "Questioni riguardanti il ciberspazio" e di altri gruppi pertinenti del Consiglio, come anche dei progressi compiuti nella creazione di altre iniziative, reti e meccanismi di cooperazione e condivisione delle informazioni tra Stati membri, segnatamente il gruppo di cooperazione NIS e la rete di CSIRT, istituiti dalla direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016, la rete delle organizzazioni di collegamento per le crisi informatiche (CyCLONe), nonché altri progetti pertinenti connessi alla ciberdifesa e avviati nell'ambito della cooperazione strutturata permanente (PESCO)[12], la task force di azione congiunta contro la criminalità informatica (J-CAT), la rete giudiziaria europea per la criminalità informatica (EJCN), i contributi volontari degli Stati membri all'INTCEN e il coordinamento e la cooperazione nel contesto del pacchetto di strumenti della diplomazia informatica.

---

[12] In particolare, il progetto "gruppi di risposta rapida agli incidenti informatici e mutua assistenza in materia di cibersicurezza" coordinato dalla Lituania, il "Centro di coordinamento nel settore informatico e dell'informazione" coordinato dalla Germania, e la "piattaforma per la condivisione delle informazioni in materia di minaccia informatica e di risposta agli incidenti informatici" coordinata dalla Grecia.

9. RICORDA i quadri di cooperazione esistenti tra le istituzioni, gli organi e le agenzie dell'UE, quali la cooperazione strutturata tra l'ENISA e CERT-UE, nonché il memorandum d'intesa tra l'ENISA, l'Agenzia europea per la difesa (AED), il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol e CERT-UE. SOTTOLINEA l'importanza di proseguire la condivisione periodica delle informazioni con il Consiglio in merito agli ulteriori sviluppi in tali quadri di cooperazione.

10. EVIDENZIA l'importanza di rafforzare la cooperazione e la condivisione delle informazioni tra le varie cibercomunità all'interno dell'UE e dei suoi Stati membri a tutti i livelli necessari – tecnico, operativo e strategico/politico – e di collegare i meccanismi, le reti, le strutture, i processi e le procedure di gestione delle crisi esistenti laddove ciò sostenga e migliori la gestione di incidenti e crisi di cibersicurezza su vasta scala.

11. PRENDE ATTO dei progressi compiuti da un gruppo di Stati membri nella creazione di una capacità informatica operativa congiunta nel quadro della PESCO, i "gruppi di risposta rapida agli incidenti informatici", con l'obiettivo di approfondire la cooperazione volontaria nel settore informatico attraverso l'assistenza reciproca, anche nella risposta agli incidenti e alle crisi di cibersicurezza su vasta scala.

12. PRENDE ATTO dell'esperienza e della capacità di risposta 24 ore su 24 e 7 giorni su 7 della comunità delle autorità di contrasto nel settore della cooperazione operativa e dello scambio sicuro di informazioni per contrastare gli attacchi informatici transfrontalieri gravi, nel quadro del protocollo di risposta alle emergenze delle autorità di contrasto dell'UE.

13. PRENDE ATTO del proseguimento dell'attuazione del quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose ("pacchetto di strumenti della diplomazia informatica"). RICORDA che ogni Stato membro è libero di prendere la propria decisione sovrana in merito all'attribuzione di un'attività informatica dolosa, adottata caso per caso. RAMMENTA che le misure adottate nel quadro di una risposta diplomatica comune dell'UE alle attività informatiche dolose dovrebbero basarsi su una conoscenza situazionale condivisa concordata tra gli Stati membri. L'INTCEN svolge un ruolo centrale in quanto polo che fornisce all'UE conoscenza situazionale e una valutazione della minaccia in merito alle questioni informatiche, sulla base dei contributi volontari di intelligence da parte degli Stati membri e senza pregiudicarne le competenze.

14. RIBADISCE l'importanza dell'assistenza reciproca e della solidarietà, in linea con l'articolo 42, paragrafo 7, del trattato sull'Unione europea e con l'articolo 222 del trattato sul funzionamento dell'Unione europea, e INVITA a svolgere ulteriori esercitazioni con una dimensione cibernetica. RICORDA la necessità di riflettere sull'articolazione tra il quadro di gestione delle crisi di cibersicurezza dell'UE, il pacchetto di strumenti della diplomazia informatica e le disposizioni degli articoli summenzionati in caso di incidenti o crisi di cibersicurezza su vasta scala. RAMMENTA inoltre che gli obblighi degli Stati membri derivanti dall'articolo 42, paragrafo 7, del trattato sull'Unione europea non pregiudicano il carattere specifico della politica di sicurezza e di difesa di taluni Stati membri. RICORDA altresì che la NATO resta il fondamento della difesa collettiva per gli Stati che ne sono membri.

15. PRENDE ATTO della cooperazione tra l'UE e la NATO in materia di cibersicurezza e ciberdifesa, compresa la condivisione di informazioni tra CERT-UE e la capacità NATO di reazione a incidenti informatici (NCIRC), nel pieno rispetto dei principi di trasparenza, reciprocità e inclusività, nonché dell'autonomia decisionale di entrambe le organizzazioni.

16. RICONOSCE l'importanza della cooperazione, se del caso, con il settore privato in termini di esercizi di condivisione di informazioni, nonché della fornitura di competenze pertinenti, come pure di soluzioni e servizi affidabili, anche per quanto riguarda, ad esempio, il sostegno alla risposta agli incidenti e il rafforzamento della conoscenza situazionale tra le diverse cibercomunità.

17. RIMARCA l'importanza di canali di comunicazione sicuri per lo scambio di informazioni classificate e sensibili. SOTTOLINEA la necessità di compiere ulteriori progressi.

A tale riguardo, e tenuto conto di quanto precede,

18. PRENDE ATTO della raccomandazione della Commissione sull'istituzione di un'unità congiunta per il ciberspazio quale iniziativa da tenere in considerazione nell'ulteriore sviluppo del quadro dell'UE per la gestione delle crisi di cibersicurezza[13].

19. INVITA l'UE e i suoi Stati membri a proseguire i loro sforzi verso un quadro dell'UE per la gestione delle crisi di cibersicurezza che sia più completo ed efficace, muovendo dai meccanismi esistenti e dai progressi già realizzati, e a prendere in considerazione il potenziale dell'iniziativa concernente un'unità congiunta per il ciberspazio a integrazione di tali meccanismi adottando un approccio graduale. SOTTOLINEA che un processo incrementale, trasparente e inclusivo è essenziale per rafforzare la fiducia ed è pertanto fondamentale per l'ulteriore sviluppo di un quadro dell'UE per la gestione delle crisi di cibersicurezza. Tale processo dovrebbe rispettare i ruoli, le competenze e i mandati esistenti degli Stati membri e delle istituzioni, degli organi e delle agenzie dell'UE, nonché i principi enunciati nelle presenti conclusioni, tra cui proporzionalità, sussidiarietà, inclusività, complementarità, non duplicazione e riservatezza delle informazioni. SOTTOLINEA nel contempo che qualsiasi eventuale partecipazione o contributo degli Stati membri a un'eventuale unità congiunta per il ciberspazio riveste carattere volontario.

[13] C(2021) 4520 final (docc. 11155/21 e 11155/21 ADD1).

20. RIMARCA la necessità di stabilire metodi di lavoro e una governance adeguati, al fine di consentire il coinvolgimento e la partecipazione di tutti gli Stati membri alle deliberazioni e a processi decisionali efficaci sul quadro dell'UE per la gestione delle crisi di cibersicurezza, come pure al suo sviluppo, compresa l'eventuale iniziativa concernente un'unità congiunta per il ciberspazio. CHIEDE il rispetto delle prerogative del Consiglio a norma dei trattati e in virtù del principio di leale cooperazione.

21. SOTTOLINEA l'importanza di individuare e coinvolgere tutte le pertinenti cibercomunità all'interno dell'UE e dei suoi Stati membri, tenendo conto nel contempo dei loro diversi ruoli e responsabilità nei vari tipi di incidenti e crisi di cibersicurezza su vasta scala. SOTTOLINEA il ruolo determinante del Consiglio, in particolare attraverso il gruppo orizzontale "Questioni riguardanti il ciberspazio", in termini di definizione delle politiche e di coordinamento per quanto riguarda l'ulteriore sviluppo del quadro dell'UE per la gestione delle crisi di cibersicurezza. INVITA pertanto gli Stati membri, la Commissione, il servizio europeo per l'azione esterna (SEAE), l'INTCEN, CERT-UE, l'ENISA, Europol (EC3), Eurojust (EJCN), il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca, nonché i rappresentanti della rete di CSIRT, della rete CyCLONe, del gruppo di cooperazione NIS, dell'AED e dei pertinenti progetti PESCO, nonché altri eventuali portatori di interessi, a partecipare a tale processo. Potrebbe essere approfondita la possibilità di istituire un gruppo di lavoro, come proposto nella raccomandazione della Commissione, in cui sia garantita un'adeguata rappresentanza di tutti gli Stati membri e che agisca sotto la guida politica del Consiglio, che funga da forum temporaneo riunendo i rappresentanti di tutte le pertinenti cibercomunità negli Stati membri e all'interno dell'UE. Tale gruppo di lavoro dovrebbe riferire periodicamente in merito alle proprie attività e presentare eventuali suggerimenti al Consiglio per discussione, approvazione e ulteriori orientamenti. Si potrebbero stabilire inoltre altre forme di dialogo all'interno delle comunità e tra di esse, anche attraverso laboratori, seminari, esercitazioni e formazioni congiunte.

22. SOTTOLINEA il ruolo del Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e della rete dei centri nazionali di coordinamento in relazione all'eventuale unità congiunta per il ciberspazio, in particolare visto il ruolo che quest'ultima rivestirebbe nell'aumentare in modo sostanziale le capacità e le soluzioni tecnologiche, come pure le abilità e le competenze dell'Unione nel settore della cibersicurezza.

23. INVITA l'UE e i suoi Stati membri a impegnarsi per sviluppare ulteriormente il quadro dell'UE per la gestione delle crisi di cibersicurezza, anche esplorando il potenziale dell'iniziativa concernente un'unità congiunta per il ciberspazio, stabilendo e definendo il processo, comprese le tappe e il calendario, nonché chiarendo le finalità e i possibili ruoli e responsabilità. EVIDENZIA la necessità di consolidare in via prioritaria le reti e le interazioni esistenti all'interno di ciascuna comunità, nonché di realizzare una mappatura approfondita delle possibili lacune ed esigenze in termini di condivisione delle informazioni all'interno delle cibercomunità e tra di esse, come pure all'interno delle istituzioni, degli organi e delle agenzie europei e tra di essi, e successivamente di concordare possibili priorità e obiettivi primari di un'eventuale unità congiunta per il ciberspazio. Senza pregiudicare i risultati, SOTTOLINEA la necessità di concentrarsi sull'individuazione delle esigenze in termini di condivisione delle informazioni al fine di costruire una conoscenza situazionale comune tra tutte le comunità pertinenti. Nell'individuare le lacune e le esigenze in termini di condivisione delle informazioni, compreso l'eventuale ricorso a piattaforme virtuali, si dovrebbe continuare a prestare la dovuta attenzione a canali di comunicazione sicuri per lo scambio di informazioni classificate e sensibili, RIMARCANDO nel contempo l'importanza di utilizzare le infrastrutture già esistenti. L'introduzione di un approccio graduale è intesa a creare fiducia e a gettare le basi per eventuali ulteriori misure connesse al rafforzamento della preparazione e della cooperazione operativa. RICONOSCE che obiettivi diversi potrebbero giustificare soluzioni differenti e il coinvolgimento di insiemi diversi di rappresentanti delle pertinenti cibercomunità all'interno dell'UE e dei suoi Stati membri.

24. CHIEDE che nel corso dell'intero processo si proceda a un ulteriore esame della base giuridica per l'eventuale unità congiunta per il ciberspazio, compresa una valutazione dei compiti e dei ruoli rispetto a quelli assegnati all'ENISA nella raccomandazione alla luce dell'articolo 7 del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio del 17 aprile 2019. INVITA a proseguire la riflessione sui singoli elementi della raccomandazione sull'unità congiunta per il ciberspazio, anche per quanto riguarda l'idea dei gruppi di reazione rapida dell'UE per la cibersicurezza e il piano dell'UE di risposta agli incidenti e alle crisi di cibersicurezza. SOTTOLINEA che l'eventuale unità congiunta per il ciberspazio è tenuta a rispettare le competenze, i mandati e i poteri giuridici dei suoi eventuali futuri partecipanti.

25. INVITA l'UE e i suoi Stati membri a prendere in considerazione il potenziale dell'iniziativa concernente un'unità congiunta per il ciberspazio, anche dal punto di vista delle istituzioni, degli organi e delle agenzie dell'UE, al fine di integrare gli sforzi in corso a livello di Stati membri. ACCOGLIE CON FAVORE l'intenzione della Commissione di rafforzare la resilienza delle istituzioni, degli organi e delle agenzie dell'UE pertinenti attraverso la sua prossima proposta di regolamento recante norme comuni vincolanti in materia di cibersicurezza per le istituzioni, gli organi e le agenzie dell'UE.

26. In conclusione, RIBADISCE il suo impegno a rafforzare la ciberresilienza e a sviluppare ulteriormente il quadro dell'UE per la gestione delle crisi di cibersicurezza, SEGUIRÀ REGOLARMENTE i progressi e fornirà ulteriori orientamenti per integrare il quadro dell'UE per la gestione delle crisi di cibersicurezza.