Consiglio dell'Unione europea

Bruxelles, 23 giugno 2021
(OR. en)

10137/21

Fascicolo interistituzionale: 2021/0166(NLE)

CYBER 181	RECH 321
JAI 773	COMPET 510
JAIEX 79	IND 180
EJUSTICE 67	COTER 78
COSI 128	ENFOPOL 244
DATAPROTECT 173	COPS 249
COPEN 289	MI 501
TELECOM 272	IXIM 129
PROCIV 78	POLMIL 98
CSC 255	HYBRID 36
CIS 82	CSCI 95
RELEX 590	POLGEN 112

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	23 giugno 2021
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, segretario generale del Consiglio dell'Unione europea
n. doc. Comm.:	JOIN(2021) 14 final
Oggetto:	COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL CONSIGLIO Relazione sull'attuazione della strategia dell'UE in materia di cibersicurezza per il decennio digitale

Si trasmette in allegato, per le delegazioni, il documento JOIN(2021) 14 final.

All.: JOIN(2021) 14 final

COMMISSIONE
EUROPEA

ALTO RAPPRESENTANTE
DELL'UNIONE PER
GLI AFFARI ESTERI E
LA POLITICA DI SICUREZZA

Bruxelles, 23.6.2021
JOIN(2021) 14 final

2021/0166 (NLE)

COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL CONSIGLIO

Relazione sull'attuazione della strategia dell'UE in materia di cibersicurezza per il decennio digitale

COMUNICAZIONE CONGIUNTA AL PARLAMENTO EUROPEO E AL CONSIGLIO

Relazione sull'attuazione della strategia dell'UE in materia di cibersicurezza per il decennio digitale

I. Ciberresilienza, capacità operativa e apertura più essenziali che mai

La cibersicurezza è indispensabile per la realizzazione di una tecnologia più intelligente e più ecologica in un mondo post-pandemia. In generale è indispensabile per la sicurezza dell'UE ed è un pilastro dell'Unione della sicurezza. Lo sviluppo sociale, politico ed economico richiede una sovranità tecnologica e un ciberspazio globale, aperto e sicuro, fondato sullo Stato di diritto e sul rispetto dei diritti umani e delle libertà fondamentali. Questa è stata la premessa di base della comunicazione congiunta della Commissione e dell'alto rappresentante per gli affari esteri e la politica di sicurezza sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale, adottata il 16 dicembre 2020[1]. Tutte le entità critiche sono un potenziale bersaglio di attacchi informatici. Gli sviluppi negli ultimi sei mesi hanno corroborato l'accento posto dalla strategia sull'accelerazione delle riforme normative, gli investimenti e la risposta operativa collettiva.

I recenti attacchi informatici hanno dimostrato, in particolare, la maggiore pervasività delle attività di ransomware e spionaggio informatico e il loro crescente rischio per tutti i settori dell'economia e della società in generale. La portata degli incidenti occorsi è stata straordinaria: centinaia di migliaia di server colpiti negli attacchi a Microsoft Exchange; 18 000 organizzazioni potenzialmente raggiunte dalla campagna sferrata contro Orion di SolarWinds; i dati sensibili di centinaia di pazienti sottratti e i servizi sanitari bloccati nell'attacco ransomware al servizio sanitario irlandese; un'emergenza energetica e un massiccio furto di dati nell'attacco informatico sferrato al sistema di fatturazione di Colonial Pipeline e l'interruzione delle attività del maggior fornitore di carne di manzo al mondo[2]. Pur non essendo ancora chiarita pienamente la portata del danno, ciascuno di questi incidenti mette in luce le potenziali conseguenze profonde dello sfruttamento doloso delle vulnerabilità presenti nei prodotti, servizi, sistemi e reti delle tecnologie dell'informazione e della comunicazione. È prevedibile che tali attacchi informatici aumentino in termini di impatto e frequenza e compromettano la nostra sicurezza.

Per l'Unione europea è pertanto essenziale accelerare i progressi su tutti i fronti – legislativo, operativo, in termini di investimenti e diplomatico – come indicato nella strategia. Le proposte di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione ("la direttiva NIS 2")[3], di direttiva sulla resilienza dei soggetti critici[4] nonché di regolamento e di direttiva relativi

[1] Comunicazione congiunta al Parlamento europeo e al Consiglio, La strategia dell'UE in materia di cibersicurezza per il decennio digitale, JOIN (2020) 18.

[2] SolarWinds, una delle principali aziende statunitensi di tecnologie informatiche, nel 2020 è stata oggetto di un attacco informatico che si è diffuso anche ai suoi clienti e che è non è stato individuato per mesi, consentendo agli hacker di accedere a migliaia di società e uffici governativi che utilizzavano i prodotti della suite Orion, fra cui sei istituzioni, organi e organismi dell'UE. Dal gennaio 2021 sono stati scoperti svariati zero-day exploit in Microsoft Exchange Server a danno dei sistemi di posta elettronica in tutto il mondo. Nel mese di maggio il servizio sanitario nazionale irlandese è stato oggetto di un attacco che ha causato un impatto significativo sulla continuità del servizio. Colonial Pipeline, il maggior operatore statunitense di oleodotti, ha dovuto interrompere le attività il 7 maggio dopo aver scoperto che un attacco informatico aveva penetrato uno dei suoi principali sistemi informatici, mentre nel giugno 2021 JBS USA Holdings Inc., la filiale statunitense del maggior fornitore di carne al mondo in termini di fatturato, è stata oggetto di un attacco ransomware che ha causato gravi interruzioni delle attività.

[3] Proposta di direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148, COM(2020) 823.

alla resilienza operativa digitale[5] dovrebbero essere adottate quanto prima. In questo contesto è essenziale perseguire un approccio ambizioso, in particolare relativamente alle catene di approvvigionamento, tenuto conto di come le vulnerabilità dei recenti attacchi informatici fossero riconducibili ai fornitori di software, e adottare misure che garantiscano la resilienza delle amministrazioni pubbliche e la rapida segnalazione degli incidenti. L'esigenza di istituire una rete di centri operativi di sicurezza (o "SOC") per l'individuazione precoce di segnali di attacchi informatici è diventata più pressante che mai, come anche l'esigenza di sviluppare una risposta credibile, efficace e collettiva dell'UE, compreso a livello operativo, agli incidenti gravi tramite l'unità congiunta per il ciberspazio[6]. Dato l'aumento degli attacchi informatici condotti da attori statali o sponsorizzati dallo Stato, è necessario continuare a promuovere in seno alle Nazioni Unite un comportamento responsabile degli Stati, anche tramite dialoghi in materia di ciberspazio e scambi strutturati con organizzazioni regionali come l'Unione africana, il Forum regionale dell'ASEAN, l'Organizzazione degli Stati americani (OAS) e l'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE), insieme a un'azione diplomatica efficace in termini di prevenzione, dissuasione, deterrenza e risposta nei confronti di comportamenti dolosi nel ciberspazio. Di particolare importanza saranno la cooperazione con i paesi terzi che condividono gli stessi principi e le priorità dell'agenda transatlantica; in particolare dovrebbe essere ulteriormente esplorata la cooperazione UE-USA su aspetti specifici relativi alla cibersicurezza, anche rispetto allo scambio di informazioni e alla lotta al ransomware.

II. Panoramica dei primi sei mesi di attuazione

Una serie di azioni strategiche sono già a un livello avanzato.

II.1 Resilienza, sovranità tecnologica e leadership

In tutto il mondo, le catene di approvvigionamento e le infrastrutture critiche, inclusi gli ospedali che lottano contro la pandemia di COVID-19, sono attualmente a rischio costante di attacchi informatici. La Commissione sostiene i colegislatori per garantire una rapida adozione della proposta di riforma della direttiva NIS, che in particolare amplierà la copertura del settore sanitario, inclusi i laboratori di ricerca e la produzione di dispositivi medicali e farmaci critici, e le nuove attività del settore energetico, come la produzione di idrogeno, il teleriscaldamento, la produzione di energia elettrica e gli organismi centrali di stoccaggio petrolifero.

Il regolamento che istituisce il Centro europeo di competenza per la cibersicurezza e la rete dei centri nazionali di coordinamento è stato adottato il 20 maggio 2021[7]. Esso metterà in comune risorse provenienti dall'UE, dagli Stati membri e dall'industria per migliorare e rafforzare le capacità di cibersicurezza tecnologica e industriale, potenziando l'autonomia strategica aperta dell'UE e offrendo la possibilità di consolidare parte delle attività connesse con la cibersicurezza finanziate da Orizzonte Europa, dal programma Europa digitale e dal dispositivo per la ripresa e la resilienza, con flussi di finanziamento che ammontano in totale a 4,5 miliardi di EUR per i prossimi sei anni[8]. Ciò sosterrà lo sviluppo entro il 2023 di un ciberscudo dell'UE per l'individuazione precoce di attacchi informatici,

[4] Proposta di direttiva sulla resilienza dei soggetti critici, COM(2020) 829.
[5] Proposta di regolamento relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) N. 600/2014 e (UE) n. 909/2014, COM(2020) 595; proposta di direttiva che modifica le direttive 2006/43/CE, 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 e UE 2016/2341, COM(2020) 596.
[6] [Raccomandazione sull'unità congiunta per il ciberspazio].
[7] Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento.
[8] Il Centro europeo di competenza per la cibersicurezza svolgerà i propri compiti in particolare adottando decisioni relative ai fondi per la cibersicurezza provenienti dal programma Europa digitale, dal programma Orizzonte Europa e dagli Stati membri e gestendo tali fondi.

composto da una rete di centri operativi di sicurezza che possono essere pubblici o privati e che sfrutteranno strumenti basati sull'intelligenza artificiale. Svariati Stati membri hanno incluso lo sviluppo di tali centri nazionali nel quadro dei rispettivi piani per la ripresa e la resilienza. La Commissione integrerà questi sforzi stanziando fondi del programma Europa digitale e sostenendo il loro collegamento per fasi successive. I programmi finanziari sosterranno inoltre l'iniziativa EuroQCI per la costruzione di una infrastruttura di comunicazione quantistica sicura che comprenda l'intera UE[9], inclusi i territori d'oltremare, utilizzando la migliore combinazione di tecnologie terrestri e spaziali e una linea di bilancio specifica a sostegno della ciberresilienza nel settore sanitario.

Garantire la cibersicurezza del 5G è un processo continuo che accompagnerà il graduale dispiegamento del 5G e l'attuazione del pacchetto di strumenti dell'UE per il 5G[10]. La maggior parte degli Stati membri ha già – o avrà presto – predisposto quadri per imporre adeguate restrizioni ai fornitori di 5G. Il codice delle comunicazioni elettroniche comporta un rafforzamento degli obblighi a carico degli operatori di reti mobili e l'Agenzia dell'UE per la cibersicurezza (ENISA) sta preparando una proposta di sistema UE di certificazione della cibersicurezza delle reti 5G[11]. Alla luce delle nuove tendenze e degli sviluppi nella catena di approvvigionamento del 5G, le autorità degli Stati membri hanno deciso di avviare un'analisi approfondita delle implicazioni in materia di sicurezza delle soluzioni tecnologiche di rete interoperabili, aperte e disaggregate ("Open RAN") nell'ambito del pacchetto di strumenti dell'UE. Il risultato di tale lavoro contribuirà ulteriormente all'approccio concertato dell'UE alla sicurezza delle reti 5G.

Occorrono maggiori sforzi, in particolare tramite il piano d'azione per l'istruzione digitale dell'UE, per affrontare la massiccia carenza di competenze, che si prevede raggiungerà quasi due milioni di posti vacanti a livello globale nel settore della cibersicurezza entro il 2022 e 350 000 nella sola Europa, e la grave sottorappresentanza delle donne, le quali rappresentano solo l'11 % della forza lavoro nel settore della cibersicurezza a livello mondiale e ancor meno, ossia il 7 %, in Europa[12]. Altre iniziative politiche in corso includono il lavoro di preparazione per le future iniziative per la sicurezza dell'Internet delle cose e, sulle norme di Internet, lo sviluppo di un servizio di risoluzione del nome del dominio senza scopo di lucro ("DNS4EU").

II.2 Sviluppare capacità operative di prevenzione, dissuasione e risposta

Con l'aumento degli attacchi condotti da attori statali, sponsorizzati dallo Stato e criminali alle reti e ai sistemi di informazione e data la sempre maggiore dipendenza dalle basi di dati di informazioni sensibili, l'UE ha bisogno di maggiore interconnessione fra le cibercomunità. Queste devono rispondere in modo coerente agli aspetti civili, penali, diplomatici e di difesa degli attacchi informatici su vasta scala di cui sono stati vittime di recente molti settori economici sensibili. Sono pertanto necessari sforzi da parte di tutte le comunità per completare le quattro fasi delineate nella raccomandazione della Commissione sull'istituzione di un'unità congiunta per il ciberspazio, adottata contestualmente alla presente relazione, quale meccanismo per un ulteriore coordinamento e per colmare le lacune nella risposta dell'UE alle minacce informatiche[13]. Nella lotta contro la criminalità

[9] https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network.

[10] Relazione sull'impatto della raccomandazione della Commissione, del 26 marzo 2019, sulla cibersicurezza delle reti 5G, SWD(2020) 357 final, 16 dicembre 2020.

[11] La preparazione del sistema si basa sul sostegno del gruppo di cooperazione NIS ed è conforme all'articolo 48 del regolamento sulla cibersicurezza; regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013. https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-commission-requests-eu-cybersecurity-agency-develop-certification.

[12] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_it.

[13] [L'Unità congiunta per il ciberspazio consentirà una risposta coordinata alle crisi e agli incidenti informatici su vasta scala e la ripresa dagli stessi e aiuterà a garantire la mobilitazione di risorse per l'assistenza. Essa

informatica è stato raggiunto un accordo politico sul regolamento provvisorio contro gli abusi sessuali sui minori online, che sarà adottato a breve[14], e la nuova strategia della Commissione per la lotta alla criminalità organizzata[15] è incentrata sull'esigenza di dotare le forze di contrasto degli strumenti digitali di cui hanno bisogno. Nel febbraio 2020 la Commissione ha adottato anche un piano d'azione sulle sinergie tra l'industria civile, della difesa e dello spazio che individua un nuovo progetto faro per l'istituzione di un sistema di connettività sicuro globale dell'UE basato sulla tecnologia spaziale. Esso mira a "consentir[e] a tutti i cittadini europei di usufruire di connessioni ad alta velocità e fornir[e] un sistema di connettività resiliente che permetterà all'Europa di rimanere connessa in ogni circostanza"[16].

Da una prospettiva internazionale, in linea con le ambizioni fissate nel quadro della "bussola strategica" (Strategic Compass)[17], l'alto rappresentante sta attualmente preparando il riesame del quadro strategico dell'UE in materia di ciberdifesa che sarà presentato agli Stati membri nella seconda metà del 2021. L'alto rappresentante si è adoperato per migliorare la capacità dell'UE di prevenzione, dissuasione, deterrenza e risposta nei confronti di attività informatiche dolose, anche rafforzando la cooperazione internazionale. Il 17 maggio 2021 il Servizio europeo per l'azione esterna (SEAE) ha organizzato, in collaborazione con la presidenza portoghese e l'Istituto dell'Unione europea per gli studi sulla sicurezza (IUESS), un dibattito basato su scenari con gli Stati membri dell'UE e i partner internazionali per migliorare la reciproca comprensione dei rispettivi approcci diplomatici in termini di prevenzione, dissuasione, deterrenza e risposta nei confronti di attività informatiche dolose e al fine di individuare opportunità per rafforzare ulteriormente la cooperazione internazionale a tal fine[18]. Per rafforzare ulteriormente il pacchetto di strumenti della diplomazia informatica dell'UE, il SEAE sta raccogliendo gli insegnamenti tratti e può riesaminare gli orientamenti di attuazione del quadro relativo ad una risposta diplomatica comune dell'UE alle attività informatiche dolose.

Come annunciato nella strategia dell'UE in materia di cibersicurezza per il decennio digitale, la Commissione sta avviando uno studio per sviluppare strumenti di sensibilizzazione volti a migliorare la preparazione e la resilienza delle imprese dell'UE nei confronti dei furti di proprietà intellettuale favoriti dall'informatica[19]. La Commissione ha anche intensificato le azioni di applicazione in relazione alla direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione avviando ulteriori procedure d'infrazione nei confronti di svariati Stati membri nel giugno 2021[20]. La Commissione prenderà in considerazione ulteriori azioni, se del caso. Sarà altrettanto cruciale migliorare la disponibilità delle capacità di cibersicurezza nella forza lavoro dell'UE; il centro di competenza della cibersicurezza realizzerà azioni chiave in tal senso con lo scopo di migliorare le conoscenze e la capacità e di promuovere le competenze interdisciplinari da sviluppare nel settore della cibersicurezza.

II.3 Promuovere un ciberspazio globale e aperto

Il panorama delle minacce è aggravato dalle tensioni geopolitiche riguardanti la rete Internet globale e aperta e le tecnologie lungo l'intera catena di approvvigionamento. Le restrizioni di Internet e su

---

coinvolgerà esperti delle comunità della cibersicurezza per costruire una consapevolezza situazionale condivisa e garantire la necessaria preparazione. Coordinerà anche i meccanismi di assistenza su richiesta di uno o più Stati membri.]

[14] https://www.europarl.europa.eu/news/it/press-room/20210430IPR03213/provisional-agreement-on-temporary-rules-to-detect-and-remove-online-child-abuse.

[15] Strategia dell'UE per la lotta alla criminalità organizzata 2021-2025, COM(2021) 170 del 14.4.2021.

[16] COM (2021) 70 del 22.2.2021.

[17] Conclusioni del Consiglio sulla sicurezza e la difesa del 17 giugno 2020 (8910/20).

[18] https://eeas.europa.eu/headquarters/headquarters-homepage/98588/cyberspace-strengthening-cooperation-promoting-security-and-stability_it.

[19] COM(2020) 760 del 25.11.2020.

[20] Gli Stati membri in questione sono Austria, Belgio, Repubblica ceca, Estonia, Lussemburgo, Polonia e Svezia.

Internet, l'aumento di attività informatiche dolose e di quelle che colpiscono la sicurezza e l'integrità dei prodotti e dei servizi delle tecnologie dell'informazione e della comunicazione sono una minaccia per il ciberspazio globale e aperto, nonché per lo Stato di diritto, i diritti umani, le libertà fondamentali e i valori democratici. L'alto rappresentante, insieme con gli Stati membri, lavora pertanto al fine di promuovere un comportamento responsabile degli Stati nel ciberspazio, in particolare definendo, unitamente ad altri 53 copatrocinatori, un programma d'azione (PoA) volto a promuovere un comportamento responsabile degli Stati a livello delle Nazioni Unite, sulla base delle raccomandazioni della relazione approvata per consenso il 12 marzo 2021 dal gruppo di lavoro aperto sugli sviluppi nel settore delle tecnologie dell'informazione e delle telecomunicazioni nel contesto della sicurezza internazionale[21]. L'UE sta lavorando al rafforzamento e all'ampliamento delle relazioni con i paesi terzi, le organizzazioni internazionali e regionali e le comunità multipartecipative tramite i dialoghi in materia di ciberspazio, come definito nella strategia, con l'istituzione di una rete della diplomazia informatica dell'UE. Inoltre il comitato dell'UE per lo sviluppo delle capacità informatiche[22], che è in fase di creazione, consentirà alle istituzioni, agli organi e agli organismi dell'UE di coordinarsi e cooperare meglio in materia di sforzi per lo sviluppo delle capacità informatiche esterne dell'UE.

Nel contesto delle Nazioni Unite, il 26 maggio 2021 l'Assemblea generale ha adottato le modalità di lavoro del comitato ad hoc istituito con la risoluzione 74/247 sul "contrasto all'uso di tecnologie dell'informazione e della comunicazione a scopi criminali"[23]. Le modalità finali adottate comprendono elementi importanti per garantire procedure decisionali inclusive e una maggiore partecipazione della società civile nei lavori del comitato ad hoc. La prima sessione negoziale del processo che porterà a una nuova convenzione delle Nazioni Unite si terrà a New York nel gennaio 2022.

Durante la sessione plenaria del 28 maggio 2021 del comitato degli Stati parte della convenzione di "Budapest" del Consiglio d'Europa sulla criminalità informatica, gli Stati parte hanno concluso le discussioni e adottato un progetto di testo del secondo protocollo addizionale alla convenzione[24], che dovrebbe migliorare la cooperazione sulla criminalità informatica e le prove elettroniche nelle indagini penali. La Commissione ha preso parte a queste discussioni a nome dell'UE[25]. Ciò dovrebbe costituire una base per la conclusione formale dei negoziati nel corso della seconda metà del 2021 e per la successiva apertura alla firma del secondo protocollo addizionale all'inizio del 2022.

Insieme con i suoi partner, nel giugno 2021 l'UE ha reiterato la propria determinazione a lavorare insieme per far fronte all'urgente e sempre maggiore minaccia delle reti di ransomware criminali che rappresentano un rischio per i nostri cittadini e le nostre società, per portare avanti una comprensione comune di come il diritto internazionale vigente si applichi al ciberspazio e per promuovere questo approccio presso le Nazioni Unite e in altri consessi internazionali, esortando tutti gli Stati a individuare con urgenza le reti di ransomware criminali che operano dall'interno dei propri confini e a fare in modo che tali reti siano chiamate a rispondere delle loro azioni[26].

---

[21] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.
[22] https://www.eucybernet.eu/.
[23] https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html.
[24] https://rm.coe.int/0900001680a2aa42.
[25] Il secondo protocollo addizionale alla convenzione di Budapest sulla criminalità informatica include misure e salvaguardie per migliorare la cooperazione internazionale fra le autorità giudiziarie e di contrasto, nonché fra le autorità e i fornitori di servizi in altri paesi. La Commissione partecipa ai negoziati su tale protocollo a nome dell'UE; decisione del Consiglio del giugno 2019 (rif. 9116/19).
[26] Dichiarazione del vertice UE-USA, 15 giugno 2021; https://www.consilium.europa.eu/media/50443/eu-us-summit-joint-statement-15-june-final-final.pdf. Comunicato del vertice del G7 di Carbis Bay: Il nostro

II.4 La cibersicurezza nelle istituzioni, negli organi e negli organismi dell'UE

L'UE sta attualmente innalzando gli standard per la cibersicurezza e la sicurezza dell'informazione nelle istituzioni, negli organi e negli organismi dell'UE. La Commissione sta avviando le consultazioni dei portatori di interessi ed effettuando un'analisi comparativa delle attuali politiche al fine di adottare le proposte prima della fine del 2021.

III. Contesto della relazione

La Commissione e l'alto rappresentante hanno adottato la strategia dell'UE in materia di cibersicurezza il 16 dicembre 2020. Questa definisce le priorità e le azioni chiave per rafforzare la resilienza, l'autonomia, la leadership e la capacità operativa dell'Europa a fronte delle crescenti e complesse minacce alle sue reti e ai suoi sistemi di informazione e per promuovere un ciberspazio globale e aperto e i relativi partenariati internazionali. La Commissione e l'alto rappresentante si sono impegnati a monitorare i progressi compiuti nell'attuazione della strategia.

Il Consiglio europeo, nella sua dichiarazione del 26 febbraio 2021, ha invitato la Commissione e l'alto rappresentante a riferire in merito all'attuazione della strategia entro giugno 2021[27]. Il Consiglio, nelle conclusioni adottate il 9 marzo 2021, ha accolto con favore la strategia, sottolineando come la cibersicurezza fosse essenziale per costruire un'Europa resiliente, verde e digitale e ha incoraggiato la Commissione e l'alto rappresentante a definire un piano di attuazione dettagliato che stabilisse le priorità e il calendario delle azioni previste[28]. La strategia è all'esame delle commissioni competenti del Parlamento europeo, con una particolare attenzione accordata al rischio di regolamentazione frammentata e all'opportunità di rafforzare l'industria europea nel suo percorso di digitalizzazione[29]. Il 27 aprile il Comitato economico e sociale europeo ha adottato un parere che ha accolto con favore la strategia quale passo positivo verso la protezione dalle minacce informatiche globali e la salvaguardia della crescita economica[30].

La presente relazione risponde a tali sviluppi e in particolare all'invito del Consiglio europeo.

---

programma comune di azione globale per ricostruire meglio, 13 giugno 2021; https://www.consilium.europa.eu/media/50361/carbis-bay-g7-summit-communique.pdf.

[27] https://www.consilium.europa.eu/media/48625/2526-02-21-euco-statement-en.pdf.

[28] https://www.consilium.europa.eu/it/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/.

[29] (2021/2568(RSP)).

[30] https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/communication-cybersecurity-strategy.