



Documento di seduta

B9-0305/2021

2.6.2021

PROPOSTA DI RISOLUZIONE

presentata a seguito dell'interrogazione con richiesta di risposta orale
B9-0000/2021

a norma dell'articolo 136, paragrafo 5, del regolamento

sulla strategia dell'UE in materia di cibersecurity per il decennio digitale
(2021/2568(RSP))

Cristian-Silviu Buşoi

a nome della commissione per l'industria, la ricerca e l'energia

B9-0305/2021

Risoluzione del Parlamento europeo sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale (2021/2568(RSP))

Il Parlamento europeo,

- vista la comunicazione congiunta della Commissione e dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza, del 16 dicembre 2020, dal titolo "La strategia dell'UE in materia di cibersicurezza per il decennio digitale" (JOIN(2020)0018),
- vista la proposta di direttiva del Parlamento europeo e del Consiglio, presentata dalla Commissione il 16 dicembre 2020, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, che abroga la direttiva (UE) 2016/1148 (COM(2020)0823),
- vista la proposta di regolamento del Parlamento europeo e del Consiglio 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, presentata dalla Commissione il 24 settembre 2020 (COM(2020)0595),
- vista la proposta di regolamento del Parlamento europeo e del Consiglio che istituisce il Centro europeo di competenza industriale, tecnologica e di ricerca sulla cibersicurezza e la rete dei centri nazionali di coordinamento, presentata dalla Commissione il 12 settembre 2018 (COM(2018)0630),
- vista la comunicazione della Commissione, del 19 febbraio 2020, dal titolo "Plasmare il futuro digitale dell'Europa" (COM(2020)0067),
- visto il 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 (regolamento sulla cibersicurezza)¹,
- vista la direttiva 2014/53/UE del Parlamento europeo e del Consiglio, del 16 aprile 2014, concernente l'armonizzazione delle legislazioni degli Stati membri relative alla messa a disposizione sul mercato di apparecchiature radio e che abroga la direttiva 1999/5/CE²,
- vista la direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio, dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche³,
- visto il regolamento (UE) n. 1290/2013 del Parlamento europeo e del Consiglio, dell'11

¹ GUL 151 del 7.6.2019, pag. 15.

² GUL 153 del 22.5.2014, pag. 62.

³ GUL 321 del 17.12.2018, pag. 36.

dicembre 2013, che stabilisce le norme in materia di partecipazione e diffusione nell'ambito del programma quadro di ricerca e innovazione (2014-2020) – Orizzonte 2020 e che abroga il regolamento (CE) n. 1906/2006⁴,

- visto il regolamento (UE) n. 1291/2013 del Parlamento europeo e del Consiglio, dell'11 dicembre 2013, che istituisce il programma quadro di ricerca e innovazione (2014-2020) – Orizzonte 2020 e abroga la decisione n. 1982/2006/CE⁵,
 - visto il regolamento (UE) n. 2021/694 del Parlamento europeo e del Consiglio, del 29 aprile 2021, che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240⁶,
 - vista la direttiva 2010/40/UE del Parlamento europeo e del Consiglio, del 7 luglio 2010, sul quadro generale per la diffusione dei sistemi di trasporto intelligenti nel settore del trasporto stradale e nelle interfacce con altri modi di trasporto⁷,
 - vista la convenzione di Budapest sulla criminalità informatica, del 23 novembre 2001 (ETS n. 185),
 - vista la sua risoluzione del 16 dicembre 2020 su una nuova strategia per le PMI europee⁸,
 - vista la sua risoluzione del 25 marzo 2021 su una strategia europea per i dati⁹,
 - vista la sua risoluzione del 20 maggio 2021 sul tema "Plasmare il futuro digitale dell'Europa: eliminare gli ostacoli al funzionamento del mercato unico digitale e migliorare l'uso dell'IA per i consumatori europei"¹⁰,
 - vista la sua risoluzione del 21 gennaio 2021 sull'eliminazione del divario digitale di genere: la partecipazione delle donne all'economia digitale¹¹,
 - vista la sua risoluzione del 12 marzo 2019 sulle minacce per la sicurezza connesse all'aumento della presenza tecnologica cinese nell'Unione e sulla possibile azione a livello di Unione per ridurre tali minacce¹²,
 - vista l'interrogazione alla Commissione sulla strategia in materia di cibersicurezza per il decennio digitale (O-000037/2021 – B9-0000/2021),
 - visti l'articolo 136, paragrafo 5, e l'articolo 132, paragrafo 2, del suo regolamento,
- A. considerando che la trasformazione digitale è una priorità strategica fondamentale dell'Unione che è inevitabilmente associata a una maggiore esposizione alle minacce

⁴ GU L 347 del 20.12.2013, pag. 81.

⁵ GU L 347 del 20.12.2013, pag. 104.

⁶ GU L 166 del 11.5.2021, pag. 1.

⁷ GU L 207 del 6.8.2010, pag. 1.

⁸ Testi approvati, P9_TA(2020)0359.

⁹ Testi approvati, P9_TA(2021)0098.

¹⁰ Testi approvati, P9_TA(2021)0261.

¹¹ Testi approvati, P9_TA(2021)0026.

¹² Testi approvati, P8_TA(2019)0156.

informatiche;

- B. considerando che il numero dei dispositivi connessi, tra cui macchine, sensori, componenti industriali e reti che costituiscono l'internet degli oggetti (IoT), continua a crescere, e che si prevede che, entro il 2024, in tutto il mondo i dispositivi collegati all'IoT saranno 22,3 miliardi, il che aumenta l'esposizione agli attacchi informatici;
- C. considerando che il progresso tecnologico – come il calcolo quantistico – e le asimmetrie di accesso allo stesso potrebbero rappresentare un problema per il panorama della cibersicurezza;
- D. considerando che la crisi della COVID-19 ha ulteriormente evidenziato le vulnerabilità di alcuni settori critici, in particolare quello dell'assistenza sanitaria, e che le misure di telelavoro e di distanziamento sociale connesse a tale crisi hanno accresciuto la nostra dipendenza dalle tecnologie digitali e dalla connettività, mentre in tutta Europa stanno aumentando il numero e il livello di sofisticazione degli attacchi informatici e della cibercriminalità, compresi lo spionaggio e il sabotaggio, nonché l'accesso a sistemi, strutture e reti informatiche e la loro manipolazione mediante installazioni maligne e illegali;
- E. considerando che le minacce ibride, compreso il ricorso a campagne di disinformazione e ad attacchi informatici a infrastrutture, processi economici e istituzioni democratiche, stanno aumentando e stanno diventando un grave problema, sia nel mondo cibernetico che nel mondo fisico, e rischiano di incidere su processi democratici come le elezioni, le procedure legislative, l'applicazione della legge e la giustizia;
- F. considerando che vi è una dipendenza crescente dalla funzione centrale di internet e dai servizi internet essenziali per la comunicazione e l'hosting, le applicazioni e i dati, servizi per i quali la quota di mercato si sta progressivamente concentrando nelle mani di un numero sempre più ridotto di imprese;
- G. considerando che le capacità di attacchi distribuiti di negazione del servizio (DDoS) sono in aumento e che pertanto andrebbe rafforzata in parallelo la resilienza del nucleo di internet;
- H. considerando che la preparazione e la consapevolezza delle imprese, in particolare le PMI e le imprese individuali, in materia di cibersicurezza rimangono modeste, che mancano lavoratori qualificati (il deficit di manodopera è aumentato del 20 % dal 2015) e che i canali tradizionali di assunzione non soddisfano la domanda, anche per quanto riguarda le posizioni manageriali e interdisciplinari; che "quasi il 90 % della forza lavoro mondiale addetta alla cibersicurezza è costituito da uomini" e che "la persistente mancanza di diversità di genere restringe ulteriormente il serbatoio di talenti cui attingere"¹³;
- I. considerando che le capacità degli Stati membri in materia di cibersicurezza non sono omogenee e che la segnalazione degli incidenti e la condivisione delle informazioni tra di essi non sono né sistematiche né esaustive, mentre l'utilizzo dei centri di condivisione

¹³ Corte dei conti europea, *Le sfide insite in un'efficace politica dell'UE in materia di cibersicurezza*, documento di riflessione, marzo 2019.

e di analisi delle informazioni (ISAC) per lo scambio di informazioni tra i settori pubblico e privato non viene sfruttato come si potrebbe;

- J. considerando che non vi è accordo a livello UE sulla collaborazione in materia di intelligence informatica e sulla risposta collettiva agli attacchi informatici e ibridi; che per gli Stati membri presi singolarmente è molto difficile, dal punto di vista tecnico e geopolitico, adottare contromisure contro le minacce e gli attacchi informatici, in particolare quelli di natura ibrida;
- K. considerando che la condivisione transfrontaliera dei dati e la loro condivisione a livello mondiale sono importanti per la creazione di valore, a condizione che siano garantiti la tutela della vita privata e i diritti intellettuali e di proprietà; che l'applicazione delle leggi di paesi terzi in materia di dati potrebbe comportare un rischio in termini di cibersicurezza per i dati europei, poiché le imprese che operano in regioni diverse sono soggette a obblighi che si sovrappongono, a prescindere dall'ubicazione dei dati o dalla loro origine;
- L. considerando che quello della cibersicurezza è un mercato mondiale da 600 miliardi di EUR, che il suo valore dovrebbe crescere rapidamente e che l'Unione europea è un importatore netto di prodotti e soluzioni;
- M. considerando che vi è il rischio di una frammentazione del mercato unico a causa delle normative nazionali sulla cibersicurezza e della mancanza di una legislazione orizzontale sui requisiti essenziali di cibersicurezza per l'hardware e il software, tra cui le applicazioni e i prodotti connessi;
 - 1. accoglie con favore le iniziative delineate dalla Commissione nella comunicazione congiunta dal titolo "La strategia dell'UE in materia di cibersicurezza per il decennio digitale";
 - 2. chiede che venga promosso lo sviluppo, in tutto il territorio dell'Unione, di reti e sistemi di informazione, di infrastrutture e di una connettività che siano sicuri e affidabili;
 - 3. chiede che ci si ponga l'obiettivo che nell'Unione tutti i prodotti connessi a internet, compresi quelli destinati ai consumatori e a uso industriale, così come l'insieme delle catene di fornitura che li rendono disponibili, siano sicuri fin dalla progettazione, resilienti agli incidenti informatici e aggiornati rapidamente con delle patch qualora vengano scoperte vulnerabilità; valuta positivamente l'intenzione della Commissione di proporre norme orizzontali sui requisiti di cibersicurezza dei prodotti connessi e dei servizi associati e chiede che tali norme propongano l'armonizzazione delle legislazioni nazionali, al fine di evitare la frammentazione del mercato unico; chiede che si tenga conto della normativa in vigore (regolamento sulla cibersicurezza, nuovo quadro legislativo, regolamento sulla normazione) per evitare ambiguità e frammentazione;
 - 4. invita la Commissione a valutare la necessità di una proposta di regolamento orizzontale che introduca entro il 2023 requisiti di cibersicurezza per le applicazioni, il software, il software incorporato e i sistemi operativi, partendo dall'*acquis* dell'UE per i requisiti in materia di gestione dei rischi; sottolinea che le applicazioni, il software, il software incorporato e i sistemi operativi obsoleti (ossia che non ricevono più regolarmente patch e aggiornamenti di sicurezza) rappresentano una quota non trascurabile di tutti i

dispositivi connessi e costituiscono un rischio in termini di cibersecurity; invita la Commissione a includere questo aspetto nella sua proposta; suggerisce che la proposta includa l'obbligo per i produttori di comunicare in anticipo il periodo minimo in cui forniranno patch di sicurezza e aggiornamenti, così da permettere agli acquirenti di fare scelte informate; ritiene che i produttori debbano partecipare al programma per la divulgazione coordinata delle vulnerabilità (CVD) definito nella proposta di direttiva sulla sicurezza delle reti e dei sistemi informativi (direttiva NIS2);

5. sottolinea che la cibersecurity dovrebbe essere parte integrante della digitalizzazione; chiede pertanto che i progetti di digitalizzazione finanziati dall'Unione includano requisiti in materia di cibersecurity; valuta positivamente il sostegno alla ricerca e all'innovazione nel settore della cibersecurity, in particolare per quanto riguarda tecnologie dirompenti (come il calcolo quantistico e la crittografia quantistica) la cui comparsa potrebbe destabilizzare l'equilibrio internazionale; chiede inoltre che si prosegua l'attività di ricerca sugli algoritmi post-quantistici quali norma di sicurezza informatica;
6. ritiene che la digitalizzazione della nostra società implichi che tutti i settori sono interconnessi e che le debolezze di un settore possono essere di ostacolo anche in altri settori; insiste dunque sulla necessità che le politiche in materia di cibersecurity siano integrate nella strategia digitale dell'UE e nei finanziamenti dell'UE e siano coerenti e interoperabili in tutti i settori;
7. sollecita un uso coerente dei fondi europei per quanto riguarda la cibersecurity e la realizzazione delle relative infrastrutture; invita la Commissione e gli Stati membri a garantire che siano sfruttate le sinergie relative alla cibersecurity tra i diversi programmi, in particolare il programma Orizzonte Europa, il programma Europa digitale, il programma spaziale dell'UE, il dispositivo dell'UE per la ripresa e la resilienza, InvestEU e il meccanismo per collegare l'Europa, e a fare pieno uso del centro e della rete di competenza per la cibersecurity;
8. ricorda che l'infrastruttura di comunicazione è la pietra angolare di qualsiasi attività digitale e che garantirne la sicurezza è una priorità strategica per l'Unione; sostiene l'attuale sviluppo del sistema di certificazione della cibersecurity dell'UE per le reti 5G; accoglie con favore il pacchetto di strumenti dell'UE sulla cibersecurity del 5G e invita la Commissione, gli Stati membri e l'industria a continuare a impegnarsi per la creazione di reti di comunicazione sicure, comprese misure riguardanti l'intera catena di fornitura; invita la Commissione a evitare la dipendenza da un unico fornitore (*vendor lock-in*) e ad accrescere la sicurezza delle reti promuovendo iniziative che migliorino la virtualizzazione e la cloudificazione delle diversi componenti delle reti; chiede il rapido sviluppo delle prossime generazioni di tecnologie di comunicazione prevedendo quale principio fondamentale la cibersecurity fin dalla fase di progettazione e garantendo la protezione della vita privata e dei dati personali;
9. ribadisce l'importanza di istituire un nuovo e solido quadro di sicurezza per le infrastrutture critiche dell'UE al fine di salvaguardare gli interessi dell'UE in materia di sicurezza e sviluppare le capacità esistenti per rispondere adeguatamente ai rischi, alle minacce e all'evoluzione tecnologica;

10. invita la Commissione a elaborare disposizioni per garantire l'accessibilità, la disponibilità e l'integrità del nucleo pubblico di internet, e quindi la stabilità del cibernazio, in particolare per quanto riguarda l'accesso dell'UE al sistema root mondiale del DNS (sistema dei nomi di dominio); ritiene che tali disposizioni dovrebbero includere misure per la diversificazione dei fornitori onde attenuare l'attuale rischio di dipendenza dalle poche imprese che dominano il mercato; accoglie con favore la proposta di un sistema europeo dei nomi di dominio (DNS4EU) quale strumento per rafforzare la resilienza del nucleo di internet; invita la Commissione a valutare in che modo tale DNS4EU potrebbe avvalersi delle tecnologie, dei protocolli di sicurezza e delle conoscenze specialistiche più recenti in materia di minacce informatiche per offrire a tutti gli europei un sistema DNS rapido, sicuro e resiliente; ricorda che è necessario proteggere meglio il protocollo di instradamento BGP (*Border Gateway Protocol*) per prevenire dirottamenti del traffico internet; ricorda il proprio sostegno a favore di un modello multilaterale di governance di internet, nell'ambito del quale la cibersicurezza dovrebbe rappresentare uno dei temi centrali; sottolinea che l'Unione europea dovrebbe accelerare l'attuazione del protocollo IPv6; prende atto del modello "open source", che si è dimostrato efficiente ed efficace quale base del funzionamento di internet, e ne incoraggia pertanto l'uso;
11. riconosce la necessità di sviluppare la scienza forense in materia di cibersicurezza per combattere la criminalità, la criminalità informatica e gli attacchi informatici, compresi gli attacchi sponsorizzati da Stati, ma pone in guardia contro misure sproporzionate che mettono a repentaglio la sfera privata e la libertà di parola dei cittadini europei nell'utilizzo di internet; ricorda la necessità di concludere la revisione del secondo protocollo aggiuntivo alla convenzione di Budapest sulla criminalità informatica, che può migliorare la preparazione contro la criminalità informatica;
12. invita la Commissione e gli Stati membri a mettere in comune le loro risorse per rafforzare la resilienza strategica dell'Unione, ridurre la sua dipendenza dalle tecnologie estere e promuovere la sua posizione di leadership e la sua competitività nel campo della cibersicurezza in tutta la catena di fornitura digitale (compresi l'archiviazione e il trattamento dei dati nel *cloud*, le tecnologie dei processori, i circuiti integrati (chip), la connettività ultrasicura, il calcolo quantistico e la prossima generazione di reti);
13. ritiene che il progetto di un'infrastruttura di connettività ultra sicura sia uno strumento importante ai fini della sicurezza delle comunicazioni digitali sensibili; accoglie con favore l'annuncio dello sviluppo di un sistema globale di comunicazione satellitare sicura dell'UE che integra tecnologie di crittografia quantistica; ricorda che dovrebbero essere intrapresi sforzi costanti, in cooperazione con l'Agenzia dell'UE per il programma spaziale (EUSPA) e l'Agenzia spaziale europea (ESA), per garantire la sicurezza delle attività spaziali europee;
14. si rammarica del fatto che le pratiche di condivisione delle informazioni in relazione alle minacce e agli incidenti informatici non siano state recepite in maniera adeguata dal settore privato e da quello pubblico; invita la Commissione e gli Stati membri ad accrescere la fiducia e a ridurre gli ostacoli alla condivisione delle informazioni sulle minacce e gli attacchi informatici, a tutti i livelli; plaude agli sforzi compiuti da alcuni settori e invita a una collaborazione transettoriale, in quanto le vulnerabilità sono raramente specifiche a un determinato settore; sottolinea che gli Stati membri devono

unire le forze a livello europeo, al fine di condividere in modo efficiente le conoscenze più recenti di cui dispongono sui rischi per la cibersicurezza; incoraggia la costituzione di un gruppo di lavoro degli Stati membri sull'intelligence informatica al fine di promuovere la condivisione delle informazioni nell'UE e nello Spazio economico europeo, in particolare per prevenire attacchi informatici su vasta scala;

15. accoglie con favore la prevista creazione di un'unità congiunta per il ciber spazio che rafforzi la cooperazione tra gli organismi dell'UE e le autorità degli Stati membri responsabili di prevenire attacchi informatici, dissuadere da essi e rispondervi; invita la Commissione e gli Stati membri a potenziare ulteriormente la cooperazione nel campo della ciberdifesa e a sviluppare la ricerca su capacità di difesa all'avanguardia;
16. ricorda l'importanza del fattore umano nella strategia in materia di cibersicurezza; invita a continuare ad impegnarsi per fare opera di sensibilizzazione in materia di cibersicurezza, anche per quanto concerne l'igiene e l'alfabetizzazione informatiche;
17. sottolinea l'importanza di un quadro di sicurezza solido e coerente per proteggere dalle minacce informatiche il personale, i dati, le reti di comunicazione e i sistemi di informazione dell'UE nonché i processi decisionali, sulla base di norme esaustive, coerenti e omogenee e di una governance adeguata; chiede che siano rese disponibili risorse e capacità adeguate, anche nel contesto del rafforzamento del mandato della squadra di pronto intervento informatico dell'UE (CERT-UE) e in relazione alle discussioni in corso sulla definizione di norme comuni in materia di cibersicurezza vincolanti per tutte le istituzioni e tutti gli organi e le agenzie dell'Unione;
18. chiede un ricorso più ampio alla certificazione volontaria e alle norme in materia di cibersicurezza, poiché rappresentano importanti strumenti per migliorare il livello generale della cibersicurezza; valuta positivamente l'introduzione del quadro europeo di certificazione e il lavoro del gruppo europeo per la certificazione della cibersicurezza; invita l'ENISA e la Commissione, in sede di preparazione del sistema UE di certificazione della cibersicurezza per i servizi *cloud*, a valutare di rendere obbligatoria l'applicazione del diritto dell'Unione per il livello di garanzia "elevato";
19. sottolinea la necessità di soddisfare la domanda di manodopera nel settore della cibersicurezza colmando il deficit di competenze attraverso la prosecuzione degli sforzi in materia di istruzione e formazione; chiede che si presti particolare attenzione all'eliminazione del divario di genere esistente anche in questo settore;
20. riconosce la necessità di un migliore sostegno per le microimprese e le piccole e medie imprese, al fine di accrescere la loro comprensione di tutti i rischi per la sicurezza delle informazioni nonché delle opportunità per migliorare la loro cibersicurezza; invita l'ENISA e le autorità nazionali a sviluppare portali di autodiagnosi e guide alle migliori pratiche per le microimprese e le piccole e medie imprese; ricorda l'importanza della formazione e dell'accesso a finanziamenti dedicati per la sicurezza di queste entità;
21. incarica il suo Presidente di trasmettere la presente risoluzione alla Commissione e al Consiglio nonché ai governi e ai parlamenti degli Stati membri.