Parere del Comitato economico e sociale europeo sulla Comunicazione congiunta al Parlamento europeo e al Consiglio «La politica di ciberdifesa dell'UE»

(parere d'iniziativa)

(2023/C 293/04)

Relatore: **Anastasis YIAPANIS**

Correlatore: **Alberto MAZZOLA**

Decisione dell'Assemblea plenaria	20.9.2022
Base giuridica	Articolo 52, paragrafo 2, del Regolamento interno
	Parere d'iniziativa
Organo competente	Commissione consultiva per le trasformazioni industriali (CCMI)
Adozione in CCMI	27.3.2023
Adozione in sessione plenaria	14.6.2023
Sessione plenaria n.	579
Esito della votazione	
(favorevoli/contrari/astenuti)	208/1/2

1. **Conclusioni e raccomandazioni**

1.1. Il Comitato economico e sociale europeo (CESE) sostiene la politica dell'UE che viene proposta in materia di ciberdifesa, ma si sarebbe aspettato che nell'elaborazione di tali proposte venisse attribuito un ruolo di maggior rilievo alla società civile organizzata. Il Comitato trova difficile valutare a questo punto se le future iniziative delineate nella comunicazione congiunta saranno attuate e conseguiranno i risultati auspicati. Esorta le istituzioni dell'UE e gli Stati membri a dare priorità alle iniziative annunciate e a portarle avanti rapidamente.

1.2. Il CESE sottolinea la necessità di ulteriori misure per rafforzare la capacità dell'UE di individuare le minacce informatiche e chiede che i finanziamenti per la R&S siano destinati allo sviluppo di capacità europee d'avanguardia. La cooperazione tra il settore pubblico e quello privato è essenziale e non deve essere unidirezionale. Il CESE ritiene che il coordinamento dell'UE sia necessario per affrontare la frammentazione e garantire la cooperazione e gli investimenti congiunti tra gli Stati membri.

1.3. Il CESE è favorevole alla creazione del centro di coordinamento della ciberdifesa dell'UE e raccomanda agli Stati membri di impegnarsi a fornire una risposta rapida 24 ore su 24, 7 giorni su 7, di valutare la prontezza informatica e le prestazioni dei meccanismi di risposta alle crisi informatiche dell'UE, con particolare attenzione alle capacità militari e ai settori critici individuati dalla direttiva (EU) 2022/2555 del Parlamento europeo e del Consiglio (direttiva NIS 2) ([1]) riveduta sulla sicurezza delle reti e dei sistemi informativi . Il CESE è favorevole all'estensione del mandato del Centro europeo di competenza per la cibersicurezza (ECCC) per sostenere l'attività del Centro di coordinamento della ciberdifesa dell'UE.

1.4. Il CESE ritiene che per rafforzare l'autonomia strategica e la sovranità dell'Unione in materia di cibersicurezza occorra sviluppare, o adottare dal settore privato, una piattaforma dinamica di verifica in tempo reale e condivisione delle informazioni, al fine di individuare le attuali lacune nelle capacità esistenti. Essa inoltre può essere utilizzata per condividere le migliori pratiche, segnalare incidenti informatici e creare un elenco dell'UE di tutti i criminali informatici.

([1]) Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022,pag. 80).

1.5. Il CESE sottolinea la necessità di una migliore preparazione contro gli attacchi informatici, come quelli russi in Ucraina, diretti in particolare alle infrastrutture critiche. La cooperazione tra ecosistemi civili e militari è fondamentale per una gestione efficiente delle crisi, per l'interoperabilità e per evitare la duplicazione degli sforzi e degli investimenti, anche attraverso attacchi informatici simulati di prova.

1.6. Il CESE ritiene che gli investimenti nella ciberdifesa dovrebbero dare priorità alla protezione dei cittadini dell'UE e delle infrastrutture critiche, anche utilizzando fornitori di fiducia per l'acquisto di hardware e di software. Insiste sulla necessità di eseguire aggiornamenti tempestivi delle priorità e degli investimenti, che dovranno essere concordati dall'UE e dagli Stati membri, con la partecipazione dei pertinenti portatori di interessi privati.

1.7. L'UE deve mantenere e sviluppare le capacità necessarie per garantire la sicurezza dell'economia digitale, della società, della democrazia e delle tecnologie critiche e per fornire servizi fondamentali di cibersicurezza. Per garantire l'autonomia strategica dell'UE, è essenziale ridurre la dipendenza dai paesi terzi. Il CESE ritiene essenziale che l'UE adotti un approccio a medio termine nei confronti dell'autonomia nelle tecnologie chiave, e chiede con forza che gli impianti di ricerca e produzione siano creati da imprese con sede nell'UE, con un'adeguata politica industriale europea incentrata su un ecosistema informatico autonomo.

1.8. Le PMI dovrebbero ricevere un sostegno mirato e avere accesso a programmi di finanziamento che aumentano la loro resilienza agli attacchi informatici, nonché a opportunità di assistenza, formazione e istruzione sui rischi informatici e su come tutelarsi nei loro confronti. L'UE dovrebbe fornire un meccanismo di incentivazione che favorisca la progressiva familiarizzazione delle PMI e lo sviluppo di PMI innovative.

1.9. Il CESE sostiene il piano di istituire un'accademia delle competenze informatiche e chiede alla Commissione europea di coordinare e finanziare programmi di istruzione e formazione professionale su vasta scala che coinvolgano tutti gli Stati membri e mirino a creare una forza lavoro qualificata per tutte le agenzie e le organizzazioni coinvolte nella ciberdifesa, nonché per le reti civili private.

1.10. Il Comitato ritiene che la consapevolezza dei cittadini in merito alla cibersicurezza sia fondamentale per ridurre l'esposizione agli attacchi informatici e chiede programmi di istruzione in materia di cibersicurezza e programmi di formazione lungo tutto l'arco della vita che si concentrino sul miglioramento delle competenze e delle conoscenze informatiche. Il CESE è favorevole a integrare la cibersicurezza in tutte le future politiche pubbliche dell'UE e a informare il pubblico in merito alle minacce informatiche.

1.11. Il CESE ritiene che una forte cooperazione con gli alleati della NATO in ambito militare debba concentrarsi su un coordinamento e una reciprocità completi, su progetti congiunti di R&S&I, sulla condivisione delle migliori pratiche, su ampi programmi di formazione e simulazioni di attacchi informatici, con l'obiettivo principale di ampliare la capacità di risposta comune.

1.12. Il Comitato invita l'alto rappresentante a esaminare gli attuali dialoghi bilaterali in materia di ciberspazio e ad avviare ulteriori discussioni con altri paesi e con le pertinenti organizzazioni internazionali al fine di istituire un quadro mondiale per il rispetto del diritto internazionale nel ciberspazio, con un forte accento sulla reciprocità. Il Comitato ritiene che l'UE, grazie alla sua solida base nel campo delle libertà democratiche fondamentali, sia adatta ad assumere un ruolo guida nelle discussioni internazionali sul futuro della cibersicurezza, in particolare in seno alle Nazioni Unite.

1.13. L'UE dovrebbe adottare una posizione ferma contro qualsiasi sistema di punteggio sociale nei confronti dei cittadini. Il CESE chiarisce che una vera democrazia non può esistere senza una protezione efficace dei dati personali e ritiene che una gestione responsabile ed efficiente dei dati sia essenziale per trasformare l'iperconnettività in un vantaggio competitivo.

2. **Introduzione e osservazioni generali**

2.1. L'espansione digitale delle società comporta un gran numero di minacce alla cibersicurezza, generate dagli aggiornamenti tecnologici. Negli ultimi anni gli attacchi informatici sono aumentati in modo significativo in termini di numero e sofisticazione, compromettendo la sicurezza di enti sia pubblici che privati. Che si tratti di *ransomware*, *malware*, attacchi e-mail, violazioni dei dati, disinformazione, attacchi distribuiti di negazione del servizio (DDoS) o altre forme di attacco, tutti rappresentano una minaccia costante e continua per la sicurezza dell'UE nel suo complesso.

2.2. Il CESE accoglie con favore la comunicazione congiunta *Politica di ciberdifesa dell'UE* ([2]) e ritiene che occorra adesso agire con urgenza e in modo coordinato a livello dell'UE, coinvolgendo gli ecosistemi sia civili che militari del ciberspazio e garantendo un adeguato quadro di investimenti per le capacità di ciberdifesa. Tuttavia, il Comitato osserva che la comunicazione costituisce soltanto un'affermazione della volontà di agire e un elenco di future iniziative dell'UE che dovrebbero essere realizzate, e ritiene impossibile valutare se tali impegni futuri saranno effettivamente posti in essere, poiché i futuri negoziati tra i colegislatori incideranno naturalmente sul risultato finale del piano d'azione dell'UE per la cibersicurezza.

2.3. L'attacco russo contro la rete satellitare KA-SAT, che ha perturbato la comunicazione tra le forze militari ucraine, e il recente scandalo che ha coinvolto Éric Léandri, ingaggiato da alcune società del settore della difesa per svolgere attività di ciberspionaggio per loro conto, stanno ponendo la sicurezza informatica in cima all'elenco delle minacce alla sicurezza nell'UE. Sebbene il regolamento generale sulla protezione dei dati sia un solido atto legislativo dell'UE, in vigore da diversi anni, è chiaro che la crescente quantità di dati disponibili è vulnerabile e che il rischio che dei terzi oltrepassino il confine della legalità aumenta ogni giorno.

2.4. Data la natura transnazionale degli attacchi informatici, per ridurre l'attuale frammentazione e garantire che gli Stati membri siano pronti a cooperare e a investire congiuntamente è necessario il coordinamento dell'UE. Ciò è particolarmente importante per eventuali casi futuri in cui uno Stato membro sia preso di mira e tutti gli altri dovrebbero avere la possibilità di fornire un sostegno immediato.

3. **Intervenire insieme a rafforzamento della ciberdifesa**

3.1. Il Comitato prende atto delle ambiziose iniziative annunciate, volte a istituire un centro di coordinamento dell'UE in materia di ciberdifesa, sviluppare il progetto CyDef-X, creare squadre di pronto intervento informatico, preparare un'iniziativa di cibersolidarietà dell'UE ed esplorare lo sviluppo di regimi di certificazione di cibersicurezza per i prodotti, i servizi e i processi delle TIC. Il CESE raccomanda che tutti gli Stati membri si impegnino a essere in condizione di fornire una risposta rapida 24 ore al giorno e 7 giorni su 7, che il centro di coordinamento dell'UE sia coinvolto nella valutazione e nello sviluppo di relazioni periodiche sulla prontezza informatica degli Stati membri e sull'efficacia del meccanismo europeo di risposta alle crisi informatiche, concentrandosi sia sulle capacità militari che sui settori critici individuati dalla direttiva NIS 2. Ogni Stato membro dovrebbe disporre di specialisti con una formazione ad hoc per intervenire in caso di incidenti informatici, e dovrebbe verificare regolarmente la propria capacità di intervento in altri Stati membri.

3.2. Sebbene la comunicazione fornisca un lungo elenco di miglioramenti graduali, il CESE avrebbe auspicato una esplicita tabella di marcia per l'attuazione di tali iniziative, con una definizione chiara della governance e scadenze per la presentazione e l'adozione. Inoltre, il Comitato si sarebbe aspettato che alla società civile organizzata fosse attribuito un ruolo di maggior rilievo nell'elaborazione di queste proposte.

3.3. Il CESE ritiene che gli Stati membri debbano rafforzare la loro capacità interna di contrastare le minacce informatiche, impegnandosi nel contempo in progetti di cooperazione e condividendo informazioni e migliori pratiche con i loro omologhi di altri Stati membri. Urge investire nelle capacità di ciberdifesa e nella diffusione accelerata delle tecnologie ([3]) in tutti gli Stati membri, nonché nella preparazione comune per individuare gli attacchi informatici e riprendersi e difendersi da essi. Il CESE ritiene che per rafforzare l'autonomia dell'Unione in materia di cibersicurezza occorra sviluppare, o adottare dal settore privato, una piattaforma dinamica di verifica in tempo reale e condivisione delle informazioni, incentrata sull'individuazione delle attuali lacune nelle capacità.

3.4. Il CESE condivide l'opinione secondo cui, in questa fase, le operazioni militari nel ciberspazio dovrebbero rimanere di esclusiva competenza degli Stati membri; sostiene la cooperazione che è stata annunciata tra le squadre militari di pronto intervento informatico dell'UE (milCERT), i gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) e la squadra di pronto intervento informatico delle istituzioni, degli organi e delle agenzie dell'UE (CERT-UE).

3.5. La direttiva NIS 2 recentemente adottata e la direttiva sulla resilienza dei soggetti critici (CER) ([4]) hanno già introdotto obblighi nazionali e settoriali specifici per il quadro dell'UE in materia di ciberdifesa. Sono necessarie ulteriori azioni per migliorare la capacità di individuazione collettiva dell'UE, e il CESE chiede investimenti in R&S per sviluppare capacità europee all'avanguardia.

([2]) Comunicazione della Commissione *La politica di ciberdifesa dell'UE*

([3]) Come l'acceleratore per l'innovazione nel settore della difesa per il Nord Atlantico (DIANA) della NATO.

([4]) *Direttiva sulla resilienza dei soggetti critici*

4. **Mettere in sicurezza l'ecosistema di difesa dell'UE**

4.1. Il CESE è convinto che le complessità intrinseche e le sfide tecnologiche in rapida evoluzione abbiano trasformato l'ecosistema della difesa, e che la cibersicurezza sia diventata un tema comune sia per il settore militare che per quello civile, nonché per i cittadini dell'UE. La cooperazione tra gli ecosistemi civili e militari è ora più importante che mai e dovrebbe apportare benefici in termini di gestione più efficace delle crisi, nonché di continui progressi e interoperabilità, evitando la duplicazione o la moltiplicazione degli stessi sforzi e investimenti. Gli Stati membri dovrebbero essere pronti a condurre prove di stress nazionali per le infrastrutture critiche al fine di valutare e aumentare la resilienza ai futuri attacchi informatici.

4.2. Il CESE ritiene che gli investimenti nella ciberdifesa debbano essere destinati in via prioritaria alla protezione dei cittadini e delle infrastrutture critiche dell'UE. Dato il ritmo sostenuto della trasformazione digitale e la rapida evoluzione del panorama delle minacce, il Comitato esorta vivamente a concordare aggiornamenti tempestivi delle priorità e degli investimenti tra l'UE e gli Stati membri, consultando in modo approfondito le pertinenti parti in causa del settore privato. Spesso i dispositivi dell'Internet degli oggetti (IoT) non sono protetti altrettanto bene quanto i dispositivi tradizionali, e il CESE chiede di garantire un livello minimo di sicurezza attraverso le piattaforme di gestione integrata di accessi e identità (IDAM). Inoltre, poiché la certificazione è un metodo fondamentale per garantire un livello più elevato di sicurezza, il Comitato chiede che il nuovo approccio dell'UE in materia di certificazione ponga maggiormente l'accento sulla sicurezza dell'Internet degli oggetti.

4.3. L'UE deve rafforzare la resilienza agli attacchi informatici e creare una deterrenza informatica efficace. Le infrastrutture critiche devono essere protette da attacchi informatici di ogni tipo, anche da parte dei sistemi di difesa dell'UE. Il CESE ritiene che sia nell'interesse strategico dell'UE garantire che l'Unione mantenga e sviluppi le capacità essenziali per tutelare al proprio interno l'economia, la società e la democrazia digitali e realizzare una piena sovranità digitale come unico modo per proteggere le tecnologie critiche e per fornire servizi fondamentali ed efficaci di cibersicurezza. Ridurre la dipendenza da paesi terzi è essenziale anche per l'autonomia strategica dell'UE. Il CESE ritiene che le agenzie settoriali dell'UE (ENISA, AESA, ERA, EMA, ABE, ESA, HADEA ecc.) dovrebbero essere coinvolte nel processo e fornire orientamenti per lo sviluppo di sistemi di cibersicurezza.

4.4. La pandemia di COVID-19 ha accelerato la transizione digitale e ha trasformato il lavoro tradizionale in modalità ibrida e/o a distanza, creando nuove relazioni di lavoro e aspettative, nonché una nuova classe di nomadi digitali, che sono in aumento. Il CESE prende atto dei rapidi cambiamenti nel mercato del lavoro, che hanno portato all'adozione dell'architettura zero trust da parte delle imprese, attraverso soluzioni di gestione integrata di accessi e identità (*Identity Access Management*, IAM) e di gestione degli accessi privilegiati (*Privileged Access Management*, PAM). Il Comitato ritiene che questo tipo di gestione delle risorse delle imprese comporti nuove soluzioni legate alle minacce informatiche ed è dell'avviso che il settore privato debba essere sostenuto nel rafforzare il livello di sicurezza delle sue soluzioni digitali innovative.

4.5. Il CESE è piuttosto deluso dall'affermazione della Commissione secondo cui «In cooperazione con gli Stati membri potrebbe essere stabilito un piano di attuazione» e ritiene tale piano di attuazione obbligatorio. Ritiene che dovrebbe essere redatto congiuntamente con gli Stati membri e attuato al più presto. Il Comitato esprime preoccupazione per la posizione semplicistica adottata dalla Commissione ed esorta le istituzioni dell'UE e gli Stati membri ad agevolare un rapido avanzamento delle iniziative annunciate.

5. **Investire in capacità di ciberdifesa**

5.1. Poiché lo sviluppo tecnologico sta progredendo rapidamente, il ciberspazio è diventato il più recente campo di guerra, dopo la terraferma, il mare, l'aria e lo spazio. Ha inoltre generato grandi opportunità di criminalità per gli attori informatici malintenzionati, che vanno dagli hacker indipendenti ai criminali professionisti e persino a soggetti del settore pubblico.

5.2. Gli investimenti nelle attività di ricerca e sviluppo sono fondamentali e il CESE accoglie con favore i fondi ad hoc esistenti nell'ambito del programma Europa digitale, del Fondo europeo per la difesa, di Orizzonte Europa e dei programmi nazionali per la ripresa. Tuttavia, il Comitato auspica un maggior numero di progetti transnazionali incentrati sulla cooperazione e sull'interoperabilità tra i sistemi di ciberdifesa in tutti gli Stati membri, nonché maggiori sinergie tra gli strumenti di finanziamento, in particolare per le PMI innovative.

5.3. Il Comitato rileva che, come annunciato già nel 2020 nella strategia dell'UE per la cibersicurezza, il termine per la creazione dell'unità congiunta per il ciberspazio è quest'anno; attende notizie sul completamento del processo e sulla preparazione dell'UE a rispondere agli incidenti informatici su vasta scala. Il CESE si attende che essa migliorerà la conoscenza situazionale dell'UE e la capacità complessiva di risposta e ripresa.

5.4. Il CESE è favorevole all'estensione del mandato del Centro di competenza per la cibersicurezza (ECCC) per sostenere l'attività del Centro di coordinamento della ciberdifesa dell'UE. Inoltre, tale rete potrebbe sostenere la sovranità digitale europea sviluppando una base industriale competitiva europea per le capacità tecnologiche fondamentali, basata in parte sul lavoro sviluppato da partenariati contrattuali pubblico-privato (PPP). I PPP hanno dato prova di essere l'approccio più efficace per migliorare la cibersicurezza dell'intero ecosistema digitale, ma non possono essere unidirezionali: le istituzioni pubbliche devono condividere le loro informazioni con il settore privato.

5.5. Il CESE osserva che, per affrontare i futuri tentativi di pirateria informatica mediante computer quantistici, l'UE deve investire immediatamente in tecnologie all'avanguardia come la crittografia post-quantistica. Ritiene irrinunciabile che l'Europa punti in una prospettiva di medio termine all'autonomia, e chiede con insistenza che imprese con sede nell'UE sviluppino strutture di ricerca e di produzione. Il CESE ritiene importante aumentare le risorse dell'UE per la R&I digitale e sostenere gli investimenti degli operatori e dei fornitori nelle nuove funzionalità tecniche di sicurezza, anche in relazione a nuove tendenze come la realtà aumentata e il metaverso. In particolare, è essenziale costruire un'infrastruttura europea di cloud distribuito basata su norme europee riguardanti temi quali l'archiviazione e il trattamento dei dati ([5]).

5.6. Le PMI dovrebbero ricevere un'attenzione specifica e avere accesso a programmi di finanziamento che migliorino la loro preparazione agli attacchi informatici, nonché a programmi di assistenza, formazione e istruzione che le aiutino a comprendere i rischi informatici e le modalità per proteggersi. L'UE dovrebbe fornire un meccanismo di incentivazione che favorisca la progressiva familiarizzazione delle PMI.

5.7. La Commissione stima che l'attuale carenza di competenze in materia di cibersicurezza ammonti a mezzo milione di persone, e il CESE apprezza la proposta di creare un'accademia delle competenze informatiche. È evidente che gli sforzi a livello degli Stati membri non sono sufficienti a ridurre il divario di competenze, per cui il Comitato propone che, insieme al lancio della suddetta accademia, la Commissione utilizzi l'impulso impresso dall'Anno europeo delle competenze e coordini e finanzi programmi di formazione su vasta scala e programmi di istruzione e formazione professionale a livello dell'UE che coinvolgano tutti gli Stati membri e si concentrino sulla creazione di una forza lavoro qualificata per tutte le agenzie e gli organismi coinvolti nella ciberdifesa, nonché per le reti civili private. Occorre dedicare particolare attenzione alla formazione della forza lavoro, specie nei campi della scienza, della tecnologia, dell'ingegneria e della matematica (STEM).

5.8. Inoltre, il CESE ritiene essenziale sensibilizzare i cittadini in merito alla cibersicurezza al fine di ridurre l'esposizione agli attacchi informatici, e in particolare ai reati informatici di base che mirano alla popolazione in generale. Il Comitato chiede programmi di istruzione in materia di cibersicurezza e programmi di formazione sulla cibersicurezza lungo tutto l'arco della vita, incentrati sul miglioramento delle competenze informatiche e su un aumento della familiarità dei cittadini, specie giovani, con la cibersicurezza e del loro interesse per essa. Il CESE è favorevole a integrare le riflessioni sulla cibersicurezza in tutte le future politiche pubbliche dell'UE e a informare i cittadini in merito alle minacce informatiche, anche attraverso programmi di formazione gratuiti per la popolazione in generale, app gratuite per smartphone o annunci televisivi in prima serata. Parallelamente a queste azioni occorre promuovere un avanzamento culturale diffuso a tutti i livelli della società verso un approccio «orientato alla cibersicurezza».

5.9. Il CESE ritiene imprescindibile garantire valutazioni del profilo di rischio dei fornitori e applicare restrizioni pertinenti per quelli considerati ad alto rischio, comprese le esclusioni necessarie per risorse e applicazioni chiave definite critiche e sensibili nella valutazione coordinata del rischio a livello UE, nonché la certificazione di fornitori di fiducia di hardware e software.

6. **Partenariati per rispondere alle sfide comuni**

6.1. Il livello di preparazione ai futuri attacchi informatici varia notevolmente da uno Stato membro all'altro. Il CESE ritiene che il primo passo immediato sia la creazione di una piattaforma di comunicazione sulle migliori pratiche all'interno dell'UE, in cui gli Stati membri più avanzati in campo informatico possano condividere le loro conoscenze con gli altri paesi e facilitarne l'adozione immediata. Ciò contribuirebbe a migliorare la fiducia reciproca tra organismi nazionali. In secondo luogo, il Comitato ritiene che sia necessaria in tutta l'UE una maggiore cooperazione tra attori statali e non statali al fine di migliorare la cibersicurezza dei prodotti e dei servizi nel mercato interno. Il CESE propone inoltre di creare una piattaforma comune dell'UE per la segnalazione degli incidenti informatici, compresa una lista nera dell'UE di tutti gli attivisti nel campo della criminalità informatica.

([5]) Come l'iniziativa franco-tedesca Gaia-X.

6.2. Il CESE è del parere che una forte cooperazione con i nostri alleati della NATO nel settore militare debba concentrarsi non solo sullo sviluppo di capacità e sull'individuazione precoce, ma anche su progetti congiunti di ricerca, sviluppo e innovazione, sulla condivisione di buone pratiche e sugli scambi tra esperti, su ampi programmi di formazione e sulle simulazioni di attacchi informatici. L'obiettivo principale dovrebbe essere quello di ampliare la capacità di risposta comune e di creare sinergie per contrastare future minacce ibride, a seguito delle dichiarazioni congiunte di Varsavia del 2016 e di Bruxelles del 2018. La cooperazione tra l'UE e la NATO riserva ancora una serie di possibilità da sfruttare e i progressi immediati possono generare un autentico salto di qualità in termini di garanzia della sicurezza per i nostri cittadini e le nostre società.

6.3. Il Comitato ritiene che le discussioni a livello mondiale e con i nostri partner internazionali dovrebbero gettare le basi per promuovere un ciberspazio globale e aperto che tuteli i diritti umani, le libertà fondamentali e lo Stato di diritto e si concentri sullo sviluppo di norme internazionali vincolanti nei settori con un rapido sviluppo digitale. Il CESE raccomanda all'alto rappresentante di rivedere gli attuali dialoghi bilaterali in materia di ciberspazio e di avviare ulteriori negoziati con altri paesi e organizzazioni internazionali pertinenti al fine di promuovere un quadro globale per l'applicazione del diritto internazionale nel ciberspazio, basato su una rigorosa condizione di reciprocità.

6.4. Infine, il Comitato ritiene che l'UE sia nella posizione migliore per guidare i dibattiti internazionali sul futuro della cibersicurezza, in particolare nell'ambito delle discussioni delle Nazioni Unite, grazie alla solidità della sua fondazione sulle libertà democratiche fondamentali. L'UE deve inoltre impegnarsi nella lotta contro i regimi totalitari che monitorano i dati dei cittadini e violano i loro diritti e le loro libertà, e dovrebbe porsi fermamente contro qualsiasi tipo di sistema di punteggio sociale nei confronti dei cittadini. Il CESE afferma chiaramente che non può esistere una vera democrazia senza un'efficace protezione dei dati personali e ritiene che una gestione responsabile ed efficiente dei dati sia essenziale per trasformare l'iperconnettività in una risorsa.

Bruxelles, 14 giugno 2023

Il presidente
del Comitato economico e sociale europeo
Oliver RÖPKE