Parlamento europeo
2019-2024

Documento di seduta

A9-0426/2023

8.12.2023

***I
RELAZIONE

sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Commissione per l'industria, la ricerca e l'energia

Relatrice: Lina Gálvez Muñoz

Significato dei simboli utilizzati

*	Procedura di consultazione
***	Procedura di approvazione
***I	Procedura legislativa ordinaria (prima lettura)
***II	Procedura legislativa ordinaria (seconda lettura)
***III	Procedura legislativa ordinaria (terza lettura)

(La procedura indicata dipende dalla base giuridica proposta nel progetto di atto.)

Emendamenti a un progetto di atto

Emendamenti del Parlamento presentati su due colonne

Le soppressioni sono evidenziate in ***corsivo grassetto*** nella colonna di sinistra. Le sostituzioni sono evidenziate in ***corsivo grassetto*** nelle due colonne. Il testo nuovo è evidenziato in ***corsivo grassetto*** nella colonna di destra.

La prima e la seconda riga del blocco d'informazione di ogni emendamento identificano la parte di testo interessata del progetto di atto in esame. Se un emendamento verte su un atto esistente che il progetto di atto intende modificare, il blocco d'informazione comprende anche una terza e una quarta riga che identificano rispettivamente l'atto esistente e la disposizione interessata di quest'ultimo.

Emendamenti del Parlamento presentati in forma di testo consolidato

Le parti di testo nuove sono evidenziate in ***corsivo grassetto***. Le parti di testo soppresse sono indicate con il simbolo ▌ o sono barrate. Le sostituzioni sono segnalate evidenziando in ***corsivo grassetto*** il testo nuovo ed eliminando o barrando il testo sostituito.
A titolo di eccezione, le modifiche di carattere strettamente tecnico apportate dai servizi in vista dell'elaborazione del testo finale non sono evidenziate.

INDICE

Pagina

PROGETTO DI RISOLUZIONE LEGISLATIVA DEL PARLAMENTO EUROPEO

sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi (COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

(Procedura legislativa ordinaria: prima lettura)

Il Parlamento europeo,

– vista la proposta della Commissione al Parlamento europeo e al Consiglio (COM(2023)0209),

– visti l'articolo 294, paragrafo 2, l'articolo 173, paragrafo 3, e l'articolo 322, paragrafo 1, lettera a), del trattato sul funzionamento dell'Unione europea, a norma dei quali la proposta gli è stata presentata dalla Commissione (C9-0136/2023),

– visto l'articolo 294, paragrafo 3, del trattato sul funzionamento dell'Unione europea,

– visto il parere del Comitato economico e sociale europeo del 13 luglio 2023[1],

– visto l'articolo 59 del suo regolamento,

– visti i pareri della commissione per gli affari esteri e della commissione per i trasporti e il turismo,

– vista la relazione della commissione per l'industria, la ricerca e l'energia (A9-0426/2023),

1. adotta la posizione in prima lettura figurante in appresso;

2. approva la sua dichiarazione allegata alla presente risoluzione;

3. chiede alla Commissione di presentargli nuovamente la proposta qualora la sostituisca, la modifichi sostanzialmente o intenda modificarla sostanzialmente;

4. incarica la sua Presidente di trasmettere la posizione del Parlamento al Consiglio e alla Commissione nonché ai parlamenti nazionali.

[1] GU L 349 del 29.9.2023, pag. 167.

Emendamento 1

EMENDAMENTI DEL PARLAMENTO EUROPEO*

alla proposta della Commissione

2023/0109(COD)

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi*, e che modifica il Regolamento (UE) 2021/694*

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 173, paragrafo 3, e l'articolo 322, paragrafo 1, lettera a),

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere della Corte dei conti[2],

visto il parere del Comitato economico e sociale europeo[3],

visto il parere del Comitato delle regioni[4],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) L'utilizzo delle tecnologie dell'informazione e della comunicazione e la dipendenza dalle stesse sono diventati fondamentali***, ma nel contempo hanno introdotto potenziali vulnerabilità,*** in tutti i settori di attività economica ***e della democrazia***, dato che le pubbliche amministrazioni, le imprese e i cittadini dell'Unione sono più che mai interconnessi e interdipendenti a livello transettoriale e transfrontaliero.

---

* Emendamenti: il testo nuovo o modificato è evidenziato in grassetto corsivo e le soppressioni sono segnalate con il simbolo ▌.

2 GU C […] del […], pag. […].

3 GU C […] del […], pag. […].

4 GU C […] del […], pag. […].

(2) Attualmente si registra un incremento dell'entità, della frequenza e dell'impatto degli incidenti di cibersicurezza ***a livello dell'Unione e su scala mondiale, in termini di metodo e incidenza***, compresi gli attacchi alle catene di approvvigionamento con finalità di ciberspionaggio, di ransomware o di perturbazione, che rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi. In considerazione del rapido evolversi del panorama delle minacce, il rischio di possibili incidenti su vasta scala, che possono provocare interruzioni o danni significativi ***alle economie, alle democrazie e alle*** infrastrutture critiche ***in tutta l'Unione***, richiede una maggiore preparazione a tutti i livelli del quadro di cibersicurezza dell'Unione. Tale minaccia va oltre l'aggressione militare della Russia nei confronti dell'Ucraina ed è destinata a persistere, data la molteplicità di soggetti allineati con le autorità di governo ***e*** criminali ▌coinvolti nelle attuali tensioni geopolitiche. Tali incidenti possono ostacolare l'erogazione di servizi pubblici e lo svolgimento di attività economiche, anche in settori critici o altamente critici, generare consistenti perdite finanziarie, minare la fiducia degli utenti nonché causare gravi danni all'economia dell'Unione, e potrebbero persino avere conseguenze sulla salute o essere potenzialmente letali. Inoltre gli incidenti di cibersicurezza sono imprevedibili, in quanto spesso si verificano ed evolvono in periodi di tempo molto brevi, non sono circoscritti a una determinata zona geografica e si verificano simultaneamente o si diffondono istantaneamente in numerosi paesi. ***È pertanto necessaria una stretta e coordinata cooperazione tra il settore pubblico, il settore privato, il mondo accademico, la società civile e i media. Inoltre, la risposta dell'Unione deve essere coordinata con le istituzioni internazionali e con i partner internazionali di fiducia e che condividono gli stessi principi. I partner internazionali di fiducia e che condividono gli stessi principi sono i paesi che condividono i valori dell'Unione di democrazia, impegno a favore dei diritti umani, multilateralismo efficace e ordine basato su regole, in linea con i quadri e gli accordi di cooperazione internazionale. Per garantire la cooperazione con partner internazionali di fiducia e che condividono gli stessi principi e la protezione contro i rivali sistemici, i soggetti stabiliti in paesi terzi che non sono parti dell'AAP non dovrebbero essere autorizzati a partecipare agli appalti di cui al presente regolamento.***

(3) Occorre rafforzare la posizione competitiva del settore industriale e di quello dei servizi dell'Unione nell'ambito dell'economia digitalizzata e sostenerne la trasformazione digitale, consolidando il livello di cibersicurezza nel mercato unico digitale. Come raccomandato in tre diverse proposte della Conferenza sul futuro dell'Europa[5], è necessario accrescere la resilienza dei cittadini, delle imprese, ***in particolare le microimprese e le piccole e medie imprese (PMI), incluse le start-up,*** e dei soggetti che gestiscono infrastrutture critiche***, tra cui le autorità locali o regionali,*** contro le crescenti minacce alla cibersicurezza, che possono avere conseguenze devastanti a livello sociale ed economico. Occorre quindi investire in infrastrutture e servizi ***e creare capacità per sviluppare competenze in materia di cibersicurezza*** che permettano di velocizzare il rilevamento delle minacce e degli incidenti di cibersicurezza e di assicurare una risposta più rapida; inoltre gli Stati membri necessitano di assistenza per garantire una migliore preparazione e capacità di risposta più adeguate agli incidenti di cibersicurezza significativi e su vasta scala. L'Unione dovrebbe inoltre accrescere le sue capacità in questi settori, in particolare per quanto riguarda la raccolta e l'analisi di dati sulle minacce e sugli incidenti di cibersicurezza.

[5] https://futureu.europa.eu/it/?locale=it.

(3 bis) Gli attacchi informatici prendono spesso di mira i servizi pubblici e le infrastrutture locali, regionali o nazionali. Gli enti locali sono tra i bersagli più vulnerabili degli attacchi informatici per via della loro mancanza di risorse finanziarie e umane. È pertanto particolarmente importante che i decisori a livello locale siano consapevoli della necessità di aumentare la resilienza digitale, accrescere la loro capacità di ridurre l'impatto degli attacchi informatici e cogliere le opportunità offerte dal presente regolamento.

(4) L'Unione ha già adottato una serie di misure per ridurre le vulnerabilità e accrescere la resilienza delle infrastrutture e dei soggetti critici contro i rischi di cibersicurezza, in particolare la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[6], la raccomandazione (UE) 2017/1584 della Commissione[7], la direttiva 2013/40/UE del Parlamento europeo e del Consiglio[8] e il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[9]. Inoltre la raccomandazione del Consiglio su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche invita gli Stati membri ad adottare misure urgenti ed efficaci e a cooperare lealmente, efficacemente, in modo solidale e coordinato tra loro, con la Commissione e le altre autorità pubbliche competenti, nonché con i soggetti interessati, al fine di migliorare la resilienza delle infrastrutture critiche utilizzate per fornire servizi essenziali nel mercato interno.

(5) I crescenti rischi di cibersicurezza e un panorama di minacce globalmente complesso, con il chiaro rischio di rapida propagazione di incidenti informatici da uno Stato membro all'altro e da un paese terzo all'Unione, richiedono una solidarietà rafforzata a livello di Unione per migliorare il rilevamento delle minacce e degli incidenti di cibersicurezza, nonché la preparazione e la risposta agli stessi***, come pure la ripresa dai medesimi***. Nelle conclusioni del Consiglio su una posizione dell'UE in materia di deterrenza informatica[10] gli Stati membri hanno inoltre invitato la Commissione a presentare una proposta su un nuovo Fondo di risposta alle emergenze di cibersicurezza.

(6) La comunicazione congiunta sulla politica di ciberdifesa dell'UE[11], adottata il 10 novembre 2022, ha annunciato un'iniziativa dell'UE per la cibersolidarietà con gli obiettivi seguenti: rafforzare le capacità comuni dell'UE in materia di rilevamento, conoscenza situazionale e risposta, promuovendo la realizzazione di ***una rete*** unionale

---

6 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 (GU L 333 del 27.12.2022).

7 Raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (GU L 239 del 19.9.2017, pag. 36).

8 Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio (GU L 218 del 14.8.2013, pag. 8).

9 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") (GU L 151 del 7.6.2019, pag. 15).

10 Conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, approvate dal Consiglio nella sessione del 23 maggio 2022 (9364/22).

11 Comunicazione congiunta al Parlamento europeo e al Consiglio – La politica di ciberdifesa dell'UE (JOIN(2022) 49 final).

dei centri operativi di sicurezza ("SOC"), sostenere la costituzione graduale di una forza di riserva per la cibersicurezza a livello di UE, con servizi prestati da operatori privati di fiducia, e le prove presso soggetti critici al fine di rilevare potenziali vulnerabilità basate sulle valutazioni del rischio effettuate a livello UE.

(7) Occorre rafforzare il rilevamento e la conoscenza situazionale delle minacce e degli incidenti informatici in tutta l'Unione e intensificare la solidarietà migliorando la preparazione e le capacità degli Stati membri e dell'Unione di ***prevenire gli*** incidenti di cibersicurezza significativi e su vasta scala ***e di rispondere agli stessi***. Di conseguenza si dovrebbe realizzare ***una rete*** paneuropea di SOC (ciberscudo europeo) per sviluppare e potenziare capacità comuni in materia di rilevamento e conoscenza situazionale, ***rafforzando le capacità dell'Unione di rilevamento delle minacce e di condivisione delle informazioni,*** creare un meccanismo per le emergenze di cibersicurezza al fine di sostenere gli Stati membri nella preparazione e nella risposta agli incidenti di cibersicurezza significativi e su vasta scala e nella ripresa immediata dagli stessi, e istituire un meccanismo di riesame degli incidenti di cibersicurezza per riesaminare e valutare specifici incidenti significativi o su vasta scala. La realizzazione di tali azioni non pregiudica gli articoli 107 e 108 del trattato sul funzionamento dell'Unione europea ("TFUE").

(8) Per conseguire questi obiettivi occorre inoltre modificare il regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio[12] in alcuni settori. In particolare il presente regolamento dovrebbe modificare il regolamento (UE) 2021/694 aggiungendo nuovi obiettivi operativi relativi al ciberscudo europeo e al meccanismo per le emergenze di cibersicurezza nell'ambito dell'obiettivo specifico 3 del programma Europa digitale, che mira a garantire la resilienza, l'integrità e l'affidabilità del mercato unico digitale, a rafforzare le capacità di monitoraggio delle minacce e degli attacchi informatici e di risposta agli stessi, nonché a rafforzare la cooperazione transfrontaliera in materia di cibersicurezza. È opportuno stabilire le condizioni specifiche in base alle quali può essere concesso il sostegno finanziario per queste azioni e definire i meccanismi di governance e di coordinamento necessari per raggiungere gli obiettivi previsti. Altre modifiche del regolamento (UE) 2021/694 dovrebbero includere descrizioni delle azioni proposte nell'ambito dei nuovi obiettivi operativi, nonché indicatori misurabili per monitorare l'attuazione di questi ultimi.

(9) Il finanziamento delle azioni ai sensi del presente regolamento dovrebbe essere previsto dal regolamento (UE) 2021/694, che dovrebbe rimanere l'atto di base pertinente per le azioni di cui all'obiettivo specifico 3 del programma Europa digitale. Le condizioni specifiche di partecipazione riguardanti ciascuna azione saranno indicate nei programmi di lavoro pertinenti, in linea con le disposizioni applicabili del regolamento (UE) 2021/694.

(9 bis) Alla luce degli sviluppi geopolitici e del crescente panorama delle minacce informatiche, e al fine di garantire la continuità e l'ulteriore sviluppo delle misure stabilite nel presente regolamento dopo il 2027, in particolare il ciberscudo europeo e il meccanismo per le emergenze di cibersicurezza, è necessario prevedere una linea di bilancio specifica nel quadro finanziario pluriennale per il periodo 2028-2034. Gli Stati membri dovrebbero cercare di impegnarsi a sostenere tutte le misure

[12] Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio, del 29 aprile 2021, che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240 (GU L 166 dell'11.5.2021, pag. 1).

necessarie per ridurre le minacce e gli incidenti informatici in tutta l'Unione e rafforzare la solidarietà.

(10) Al presente regolamento si applicano le regole finanziarie orizzontali adottate dal Parlamento europeo e dal Consiglio in base all'articolo 322 TFUE. Tali regole sono stabilite nel regolamento ***(UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio***[13], definiscono in particolare le modalità relative alla formazione e all'esecuzione del bilancio dell'Unione e organizzano il controllo della responsabilità degli agenti finanziari. Le regole adottate in base all'articolo 322 TFUE comprendono anche un regime generale di condizionalità per la protezione del bilancio dell'Unione istituito dal regolamento (UE, Euratom) 2020/2092 del Parlamento europeo e del Consiglio[14].

(11) Ai fini di una sana gestione finanziaria è opportuno stabilire norme specifiche in materia di riporto degli stanziamenti d'impegno e di pagamento inutilizzati. Pur rispettando il principio secondo cui il bilancio dell'Unione è fissato annualmente, il presente regolamento dovrebbe, in considerazione della natura imprevedibile, eccezionale e specifica del panorama della cibersicurezza, prevedere la possibilità di riportare i fondi inutilizzati oltre a quelli stabiliti nel regolamento ***(UE, Euratom) 2018/1046***, massimizzando così la capacità del meccanismo per le emergenze di cibersicurezza di sostenere gli Stati membri nel contrastare efficacemente le minacce informatiche.

(11 bis) Il meccanismo per le emergenze di cibersicurezza e la riserva dell'UE per la cibersicurezza istituiti dal presente regolamento sono iniziative nuove che non erano previste nella definizione del quadro finanziario pluriennale per il periodo 2021-2027, e il finanziamento di tali iniziative dovrebbe limitare il più possibile la riduzione dei finanziamenti per altre priorità del programma Europa digitale. L'importo delle risorse finanziarie destinate alla riserva dell'UE per la cibersicurezza dovrebbe pertanto essere ridotto ed essere ricavato principalmente dai margini non assegnati nell'ambito dei massimali del quadro finanziario pluriennale, o mobilitato attraverso gli strumenti speciali non tematici del quadro finanziario pluriennale. Gli stanziamenti o le riassegnazioni di fondi a partire dai programmi esistenti dovrebbero essere limitati al minimo indispensabile, al fine di proteggere detti programmi, in particolare Erasmus+, da un impatto negativo e garantire che si possano conseguire gli obiettivi prefissati.

(12) Al fine di rendere più efficaci la prevenzione e la valutazione delle minacce e degli incidenti informatici, nonché la risposta agli stessi ***e la ripresa da essi***, occorre sviluppare una conoscenza più completa delle minacce alle risorse e alle infrastrutture critiche sul territorio dell'Unione, compresa la loro distribuzione geografica, l'interconnessione e gli effetti potenziali in caso di attacchi informatici contro tali infrastrutture. ***Un approccio proattivo all'individuazione, all'attenuazione e alla***

---

13 ***Regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio, del 18 luglio 2018, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione, che modifica i regolamenti (UE) n. 1296/2013, (UE) n. 1301/2013, (UE) n. 1303/2013, (UE) n. 1304/2013, (UE) n. 1309/2013, (UE) n. 1316/2013, (UE) n. 223/2014, (UE) n. 283/2014 e la decisione n. 541/2014/UE e abroga il regolamento (UE, Euratom) n. 966/2012 (GU L 193 del 30.7.2018, pag. 1, ELI: http://data.europa.eu/eli/reg/2018/1046/oj).***

14 ***Regolamento (UE, Euratom) 2020/2092 del Parlamento europeo e del Consiglio, del 16 dicembre 2020, relativo a un regime generale di condizionalità per la protezione del bilancio dell'Unione (GU L 433I del 22.12.2020, pag. 1, ELI: http://data.europa.eu/eli/reg/2020/2092/oj).***

prevenzione delle potenziali minacce informatiche comprende lo sviluppo di capacità di rilevamento avanzate necessarie per bloccare le minacce persistenti avanzate. L'intelligence delle minacce è costituita da informazioni raccolte, analizzate e interpretate per comprendere le minacce e i rischi potenziali. Analizzando e correlando grandi quantità di dati, scopre modelli, tendenze e indicatori di compromissione che possono rivelare attività malevole o vulnerabilità. Dovrebbe essere realizzata ***una rete*** di SOC dell'Unione su vasta scala ("ciberscudo europeo"), comprendente diverse piattaforme transfrontaliere interoperanti, ciascuna composta da diversi SOC nazionali. Tale infrastruttura dovrebbe essere al servizio degli interessi e delle esigenze di cibersicurezza nazionali e dell'Unione, sfruttando tecnologie all'avanguardia per strumenti di analisi e di raccolta di dati avanzati, migliorando le capacità di rilevamento e di gestione delle minacce informatiche e permettendo una conoscenza situazionale in tempo reale. ***Un SOC nazionale fa riferimento a una capacità centralizzata responsabile della raccolta continua di informazioni di intelligence delle minacce e del miglioramento della posizione in materia di deterrenza informatica dei soggetti rientranti nella giurisdizione nazionale attraverso la prevenzione, il rilevamento e l'analisi delle minacce alla cibersicurezza.*** Dovrebbe inoltre servire a incrementare le capacità di rilevamento delle minacce e degli incidenti di cibersicurezza e quindi a integrare e sostenere i soggetti e le reti dell'Unione responsabili della gestione delle crisi nell'UE, in particolare la rete europea delle organizzazioni di collegamento per le crisi informatiche ("EU-CyCLONe"), come definita nella direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[15].

(13) ***Per partecipare al ciberscudo europeo,*** ogni Stato membro dovrebbe designare un organismo pubblico a livello nazionale, incaricato di coordinare le attività di rilevamento delle minacce informatiche in tale Stato membro. ***Gli Stati membri sono incoraggiati a integrare la capacità del SOC nazionale nella loro struttura e governance informatica esistente per evitare di creare ulteriori livelli di governance e per allineare il presente regolamento agli atti legislativi in vigore, in particolare la direttiva (UE) 2022/2555.*** Questi SOC nazionali dovrebbero fungere da punto di riferimento e porta di accesso a livello nazionale per la partecipazione ***di soggetti pubblici e privati, in particolare i rispettivi SOC nazionali,*** al ciberscudo europeo e garantire che le informazioni sulle minacce informatiche provenienti da soggetti pubblici e privati siano condivise e raccolte a livello nazionale in modo efficace e semplificato. ***I SOC nazionali dovrebbero rafforzare la cooperazione e la condivisione delle informazioni tra soggetti pubblici e privati al fine di abbattere i silos di comunicazione attualmente esistenti. Così facendo, essi possono sostenere la creazione di modelli di scambio di dati e dovrebbero facilitare e incoraggiare la condivisione delle informazioni in un ambiente sicuro e di fiducia. Una cooperazione stretta e coordinata tra soggetti pubblici e privati è fondamentale per rafforzare la resilienza dell'Unione nel campo della cibersicurezza.***

(14) Nell'ambito del ciberscudo europeo è opportuno istituire diversi centri operativi di cibersicurezza transfrontalieri ("SOC transfrontalieri") che, a loro volta, dovrebbero riunire i SOC nazionali di almeno tre Stati membri, in modo da sfruttare appieno i

[15] 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).

vantaggi derivanti dal rilevamento delle minacce transfrontaliere e dalla gestione e condivisione delle informazioni. L'obiettivo generale dei SOC transfrontalieri dovrebbe essere quello di rafforzare le capacità di analisi, prevenzione e rilevamento delle minacce alla cibersicurezza e di favorire l'elaborazione di analisi di alta qualità sulle minacce alla cibersicurezza***, anche tramite la raccolta e la condivisione di dati e informazioni su possibili atti di pirateria informatica, minacce ed exploit malevoli di nuova creazione che non sono ancora stati utilizzati in un ciberincidente, nonché lavori di analisi***, in particolare mediante la condivisione di dati provenienti da varie fonti, pubbliche o private, nonché tramite la condivisione e l'uso congiunto di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi e prevenzione in un contesto ***sicuro e*** di fiducia**, *con il sostegno dell'ENISA, in questioni relative alla cooperazione operativa tra gli Stati membri.*** Tali SOC dovrebbero ***agevolare e incoraggiare la condivisione di informazioni in un contesto sicuro e di fiducia e*** garantire nuove capacità aggiuntive, basandosi sui SOC e sui gruppi di intervento per la sicurezza informatica in caso di incidente ("CSIRT") esistenti nonché su altri soggetti pertinenti e integrandoli.

(15) A livello nazionale, il monitoraggio, il rilevamento e l'analisi delle minacce informatiche sono solitamente garantiti dai SOC di soggetti pubblici e privati, in combinazione con i CSIRT. Questi ultimi inoltre scambiano informazioni nel contesto della rete di CSIRT, conformemente a quanto disposto dalla direttiva (UE) 2022/2555. I SOC transfrontalieri dovrebbero costituire una nuova capacità ***integrata nell'infrastruttura di cibersicurezza esistente, specialmente nella*** rete di CSIRT, mettendo in comune e condividendo i dati sulle minacce alla cibersicurezza provenienti da soggetti pubblici e privati***, in particolare dai relativi SOC***, accrescendo il valore di tali dati mediante l'analisi di esperti, infrastrutture acquisite congiuntamente e strumenti all'avanguardia, e contribuendo ***alla*** sovranità tecnologica***, all'autonomia strategica, alla competitività e alla resilienza dell'Unione, nonché allo sviluppo di un ecosistema di cibersicurezza significativo, anche in collaborazione con partner internazionali di fiducia e che condividono gli stessi principi***. .

(16) I SOC transfrontalieri dovrebbero fungere da punto centrale in grado di consentire un'ampia condivisione di dati pertinenti e di analisi delle minacce informatiche e permettere la diffusione di informazioni sulle minacce tra più soggetti di diversa natura (ad esempio, squadre di pronto intervento informatico ("CERT"), CSIRT, centri di analisi e condivisione delle informazioni ("ISAC"), operatori di infrastrutture critiche) ***per facilitare l'abbattimento dei silos di comunicazione attualmente esistenti. Così facendo, i SOC transfrontalieri potrebbero anche sostenere la creazione di modelli di scambio di dati in tutta l'Unione.*** Le informazioni scambiate tra i partecipanti a un SOC transfrontaliero potrebbero includere dati provenienti da reti e sensori, feed di analisi delle minacce, indicatori di compromissione e informazioni contestualizzate su incidenti, minacce e vulnerabilità***, anche tramite la raccolta e la condivisione di dati e informazioni su possibili atti di pirateria informatica, minacce ed exploit malevoli di nuova creazione che non sono ancora stati utilizzati in un ciberincidente, nonché lavori di analisi***. I SOC transfrontalieri dovrebbero inoltre stipulare accordi di cooperazione con altri SOC transfrontalieri.

(17) La condivisione della conoscenza situazionale tra le autorità competenti è un prerequisito indispensabile per la preparazione e il coordinamento a livello dell'Unione in caso di incidenti di cibersicurezza significativi e su vasta scala. La direttiva

(UE) 2022/2555 istituisce EU-CyCLONe al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala e di garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione. La raccomandazione (UE) 2017/1584 relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala definisce il ruolo di tutti i soggetti interessati. La direttiva (UE) 2022/2555 ricorda altresì le responsabilità della Commissione nell'ambito del meccanismo unionale di protezione civile ("UCPM") istituito dalla decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio[16], nonché la sua responsabilità per quanto riguarda la fornitura di relazioni analitiche per i dispositivi integrati per la risposta politica alle crisi ("IPCR") ai sensi della decisione di esecuzione (UE) 2018/1993 ***del Consiglio***[17]. Pertanto, nelle situazioni in cui ottengono informazioni relative a un incidente di cibersicurezza potenziale o in corso su vasta scala, i SOC transfrontalieri dovrebbero fornire informazioni pertinenti a EU-CyCLONe, alla rete di CSIRT e alla Commissione***, conformemente alla direttiva (UE) 2022/2555***. In particolare, a seconda della situazione, le informazioni da condividere potrebbero includere informazioni tecniche, informazioni sulla natura e sulle motivazioni dell'autore di un attacco informatico o di un potenziale autore nonché informazioni non tecniche di livello superiore su un incidente di cibersicurezza potenziale o in corso su vasta scala. In questo contesto è opportuno prestare la dovuta attenzione al principio della necessità di conoscere e alla natura potenzialmente sensibile delle informazioni condivise.

(18) I soggetti che partecipano al ciberscudo europeo dovrebbero garantire un elevato livello di interoperabilità tra di loro, che riguardi anche, a seconda dei casi, il formato dei dati, la tassonomia e gli strumenti di gestione e di analisi dei dati, nonché prevedere canali di comunicazione sicuri, un livello minimo di sicurezza del livello applicazioni, un quadro operativo della conoscenza situazionale e indicatori. L'adozione di una tassonomia comune e la definizione di un modello per le relazioni sulla situazione al fine di descrivere la causa tecnica e le ripercussioni degli incidenti di cibersicurezza dovrebbero tenere conto dei lavori in corso in materia di notifica degli incidenti nel contesto dell'attuazione della direttiva (UE) 2022/2555.

(19) Per consentire lo scambio di dati sulle minacce alla cibersicurezza provenienti da varie fonti, su vasta scala, in un contesto ***sicuro e*** di fiducia, i soggetti che partecipano al ciberscudo europeo dovrebbero essere dotati di strumenti, apparecchiature e infrastrutture all'avanguardia e altamente sicuri ***nonché di personale qualificato***. Ciò dovrebbe consentire di migliorare le capacità collettive di rilevamento e di avvertire tempestivamente le autorità e i soggetti competenti, in particolare utilizzando le più recenti tecnologie di intelligenza artificiale e di analisi dei dati.

(20) Mediante la raccolta, la condivisione e lo scambio di dati, il ciberscudo europeo dovrebbe rafforzare la sovranità tecnologica***, l'autonomia strategica, la competitività e la resilienza dell'Unione, nonché un ecosistema di cibersicurezza significativo dell'Unione.*** La condivisione di dati selezionati di alta qualità dovrebbe inoltre

---

16 ***Decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio, del 17 dicembre 2013, su un meccanismo unionale di protezione civile (Testo rilevante ai fini del SEE) (***GU L 347 del 20.12.2013, pag. 924, ***ELI:*** http://data.europa.eu/eli/dec/2013/1313/oj***).***

17 ***Decisione di esecuzione (UE) 2018/1993 del Consiglio, dell'11 dicembre 2018, relativa ai dispositivi integrati dell'UE per la risposta politica alle crisi (GU L 320 del 17.12.2018, pag. 28, ELI: http://data.europa.eu/eli/dec_impl/2018/1993/oj).***

contribuire allo sviluppo di tecnologie avanzate di intelligenza artificiale e di analisi dei dati***. L'intelligenza artificiale è più efficace se abbinata all'analisi umana. Pertanto, una forza lavoro qualificata rimane essenziale per la condivisione di dati di alta qualità.*** La condivisione di dati selezionati di alta qualità dovrebbe essere facilitata dal collegamento del ciberscudo europeo con l'infrastruttura paneuropea di calcolo ad alte prestazioni istituita dal regolamento (UE) 2021/1173 del Consiglio[18].

(21) Sebbene il ciberscudo europeo sia un progetto civile, la comunità della ciberdifesa potrebbe trarre beneficio dalle maggiori capacità di rilevamento e di conoscenza situazionale sviluppate nel settore civile per la protezione delle infrastrutture critiche. I SOC transfrontalieri, con il sostegno della Commissione e del Centro europeo di competenza per la cibersicurezza ("ECCC"), e in collaborazione con l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza (l'"alto rappresentante"), dovrebbero gradualmente mettere a punto norme e protocolli specifici ***in materia di condizioni di accesso e di garanzie*** per consentire la cooperazione con la comunità di ciberdifesa, anche per quanto riguarda le indagini e le condizioni di sicurezza***, nel rispetto del carattere civile delle istituzioni e della destinazione dei finanziamenti, utilizzando pertanto i fondi a disposizione della comunità di difesa***. Lo sviluppo del ciberscudo europeo dovrebbe essere accompagnato da una riflessione che consenta la futura collaborazione con le reti e le piattaforme responsabili della condivisione delle informazioni nella comunità di ciberdifesa, in stretta collaborazione con l'alto rappresentante ***e nel pieno rispetto dei diritti e delle libertà***.

(22) La condivisione delle informazioni tra i partecipanti al ciberscudo europeo dovrebbe essere conforme alle prescrizioni giuridiche esistenti e in particolare al diritto nazionale e dell'Unione in materia di protezione dei dati, nonché alle norme dell'Unione sulla concorrenza che disciplinano lo scambio di informazioni. Il destinatario delle informazioni dovrebbe attuare, nella misura in cui il trattamento dei dati personali sia necessario, misure tecniche e organizzative a salvaguardia dei diritti e delle libertà degli interessati, distruggere i dati non appena non sono più necessari per la finalità dichiarata e comunicarne la distruzione all'organismo che li ha resi disponibili.

(23) Fatto salvo l'articolo 346 TFUE, lo scambio di informazioni riservate ai sensi ***del diritto*** dell'Unione o ***nazionale*** dovrebbe essere limitato alle informazioni pertinenti e commisurate a tale scopo, tutelare la riservatezza di dette informazioni e proteggere la sicurezza e gli interessi commerciali dei soggetti interessati, nel pieno rispetto dei segreti commerciali e aziendali.

(24) Alla luce dell'aumento dei rischi e del numero di incidenti informatici che colpiscono gli Stati membri, occorre istituire uno strumento di sostegno alle crisi per migliorare la resilienza dell'Unione agli incidenti di cibersicurezza significativi e su vasta scala e integrare le azioni degli Stati membri mediante un sostegno finanziario di emergenza per la preparazione, la risposta e il ripristino immediato dei servizi essenziali. Tale strumento dovrebbe consentire una rapida ***ed efficace*** mobilitazione dell'assistenza in circostanze definite e nel rispetto di condizioni ben precise, e permettere un monitoraggio e una valutazione accurati delle modalità di utilizzo delle risorse. Sebbene agli Stati membri spetti la responsabilità primaria della prevenzione degli incidenti e

[18] Regolamento (UE) 2021/1173 del Consiglio, del 13 luglio 2021, relativo all'istituzione dell'impresa comune per il calcolo ad alte prestazioni europeo e che abroga il regolamento (UE) 2018/1488 (GU L 256 del 19.7.2021, pag. 3, ***ELI: http://data.europa.eu/eli/reg/2021/1173/oj***).

delle crisi di cibersicurezza, nonché della preparazione e della risposta agli stessi, il meccanismo per le emergenze di cibersicurezza promuove la solidarietà tra gli Stati membri conformemente all'articolo 3, paragrafo 3, del trattato sull'Unione europea ("TUE").

(25) Il meccanismo per le emergenze di cibersicurezza dovrebbe fornire un sostegno agli Stati membri, integrando le loro misure e le loro risorse nonché altre opzioni di sostegno esistenti in caso di risposta agli incidenti di cibersicurezza significativi e su vasta scala e di ripresa immediata dagli stessi, come i servizi forniti dall'Agenzia dell'Unione europea per la cibersicurezza ("ENISA") conformemente al suo mandato, la risposta coordinata e l'assistenza della rete di CSIRT, il sostegno a strategie di attenuazione offerto da EU-CyCLONe, nonché l'assistenza reciproca tra gli Stati membri, anche nel contesto dell'articolo 42, paragrafo 7, TUE, i gruppi di risposta rapida agli incidenti informatici della PESCO[19] e i gruppi di risposta rapida alle minacce ibride. Tale meccanismo dovrebbe rispondere alla necessità di garantire la disponibilità di mezzi specializzati per sostenere la preparazione e la risposta agli incidenti di cibersicurezza in tutta l'Unione e nei paesi terzi.

(26) Il presente strumento non pregiudica le procedure e i quadri di coordinamento della risposta alle crisi a livello dell'Unione, in particolare l'UCPM[20], gli IPCR[21] e la direttiva (UE) 2022/2555, e può contribuire alle azioni attuate nel contesto dell'articolo 42, paragrafo 7, TUE o nelle situazioni definite nell'articolo 222 TFUE oppure integrare tali azioni. L'utilizzo del presente strumento dovrebbe inoltre essere coordinato, laddove opportuno, con l'attuazione delle misure del pacchetto di strumenti della diplomazia informatica.

(27) L'assistenza fornita ai sensi del presente regolamento dovrebbe sostenere e integrare le azioni intraprese dagli Stati membri a livello nazionale. A tal fine occorre garantire una stretta collaborazione e consultazione tra la Commissione***, l'ENISA*** e lo Stato membro interessato. Nel richiedere un sostegno nell'ambito del meccanismo per le emergenze di cibersicurezza, lo Stato membro dovrebbe fornire informazioni pertinenti che ne giustifichino la necessità.

(28) Secondo quanto disposto dalla direttiva (UE) 2022/2555 gli Stati membri sono tenuti a designare o istituire una o più autorità di gestione delle crisi informatiche e a garantire che tali autorità dispongano di risorse adeguate per svolgere i loro compiti in modo efficace ed efficiente. La direttiva impone inoltre gli Stati membri di individuare le capacità, le risorse e le procedure da poter impiegare in caso di crisi, nonché di adottare un piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala, in cui siano definiti gli obiettivi e le modalità di gestione degli stessi. Gli Stati membri sono altresì tenuti a istituire uno o più CSIRT che siano incaricati di gestire gli incidenti, secondo un processo ben definito, e che si occupino almeno dei settori, dei sottosettori e dei tipi di soggetti che rientrano nell'ambito di applicazione di tale direttiva, nonché a garantire che i CSIRT dispongano di risorse adeguate per svolgere efficacemente i

---

19 Decisione (PESC) 2017/2315 del Consiglio, dell'11 dicembre 2017, che istituisce la cooperazione strutturata permanente (PESCO) e fissa l'elenco degli Stati membri partecipanti.

20 Decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio, del 17 dicembre 2013, su un meccanismo unionale di protezione civile (GU L 347 del 20.12.2013, pag. 924).

21 Dispositivi integrati per la risposta politica alle crisi (IPCR) e conformemente alla raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala.

rispettivi compiti. Il presente regolamento non pregiudica il ruolo della Commissione di garantire il rispetto da parte degli Stati membri degli obblighi previsti dalla direttiva (UE) 2022/2555. Il meccanismo per le emergenze di cibersicurezza dovrebbe fornire assistenza per azioni volte a rafforzare la preparazione e azioni di risposta agli incidenti intese ad attenuare l'impatto di incidenti di cibersicurezza significativi e su vasta scala, al fine di sostenere la ripresa immediata e/o il ripristino del funzionamento di servizi essenziali.

(29) Nell'ambito delle azioni di preparazione, al fine di promuovere un approccio coerente e rafforzare la sicurezza in tutta l'Unione e nel suo mercato interno, è opportuno fornire un sostegno per verificare e valutare in modo coordinato il livello di cibersicurezza dei soggetti che operano nei settori altamente critici individuati ai sensi della direttiva (UE) 2022/2555. A tal fine la Commissione, con il sostegno dell'ENISA e in collaborazione con il gruppo di cooperazione NIS istituito dalla direttiva (UE) 2022/2555, dovrebbe individuare periodicamente i settori o i sottosettori pertinenti idonei a ricevere un sostegno finanziario per lo svolgimento di una verifica coordinata a livello dell'Unione. I settori o i sottosettori dovrebbero essere selezionati dall'allegato I della direttiva (UE) 2022/2555 ("Settori ad alta criticità"). Gli esercizi di verifica coordinata dovrebbero basarsi su scenari di rischio e metodologie comuni. La selezione dei settori e l'elaborazione degli scenari di rischio dovrebbero tenere conto delle valutazioni del rischio e degli scenari di rischio pertinenti a livello dell'Unione, compresa la necessità di evitare duplicazioni, come la valutazione del rischio e gli scenari di rischio previsti nelle conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, di cui devono occuparsi la Commissione, l'alto rappresentante e il gruppo di cooperazione NIS, in coordinamento con i pertinenti organismi e agenzie civili e militari e le pertinenti reti consolidate, compresa EU-CyCLONe. Dovrebbero inoltre essere prese in considerazione la valutazione del rischio delle reti e delle infrastrutture di comunicazione richiesta dall'invito ministeriale congiunto di Nevers e condotta dal gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA, e in collaborazione con l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC), le valutazioni coordinate del rischio da condurre ai sensi dell'articolo 22 della direttiva (UE) 2022/2555 e i test di resilienza operativa digitale previsti dal regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio[22]. La selezione dei settori dovrebbe inoltre tenere conto della raccomandazione del Consiglio su un approccio coordinato a livello di Unione per rafforzare la resilienza delle infrastrutture critiche.

(30) Il meccanismo per le emergenze di cibersicurezza dovrebbe inoltre offrire sostegno ad altre azioni di preparazione e sostenere la preparazione in altri settori non interessati dalla verifica coordinata dei soggetti che operano in settori altamente critici. Tali azioni potrebbero includere vari tipi di attività di preparazione nazionali.

(31) Il meccanismo per le emergenze di cibersicurezza dovrebbe inoltre sostenere azioni di risposta agli incidenti volte ad attenuare l'impatto di incidenti di cibersicurezza significativi e su vasta scala, al fine di favorire la ripresa immediata o ripristinare il funzionamento di servizi essenziali. Ove opportuno, dovrebbe integrare l'UCPM per

[22] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, 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, (UE) n. 909/2014 e (UE) 2016/1011.

garantire un approccio globale di risposta all'impatto esercitato dagli incidenti informatici sui cittadini.

(32) Il meccanismo per le emergenze di cibersicurezza dovrebbe sostenere l'assistenza fornita dagli Stati membri a uno Stato membro in cui si sia verificato un incidente di cibersicurezza significativo o su vasta scala, anche mediante la rete di CSIRT di cui all'articolo 15 della direttiva (UE) 2022/2555. Gli Stati membri che forniscono assistenza dovrebbero essere autorizzati a presentare richieste di copertura dei costi relativi all'invio di squadre di esperti nel quadro dell'assistenza reciproca. I costi ammissibili potrebbero includere le spese di viaggio e di alloggio nonché l'indennità giornaliera degli esperti di cibersicurezza.

(33) È opportuno istituire gradualmente una riserva per la cibersicurezza a livello di Unione, costituita da servizi erogati da fornitori privati di servizi di sicurezza gestiti a sostegno di azioni di risposta e di ripresa immediata in caso di incidenti di cibersicurezza significativi o su vasta scala. La riserva dell'UE per la cibersicurezza dovrebbe garantire la disponibilità e la prontezza dei servizi, ***rafforzando nel contempo la resilienza dell'Unione, inclusa la partecipazione dei fornitori europei di servizi di sicurezza gestiti che sono PMI e garantendo la creazione di un ecosistema di cibersicurezza, in particolare le microimprese e le PMI, comprese le start-up, attraverso investimenti nella ricerca e nell'innovazione (R&I) per sviluppare tecnologie all'avanguardia, come quelle relative al cloud e all'intelligenza artificiale***. ***I fornitori di fiducia, comprese le PMI, dovrebbero essere in grado di collaborare tra loro al fine di soddisfare i criteri di cui sopra***. I servizi della riserva dell'UE per la cibersicurezza dovrebbero servire a sostenere le autorità nazionali nel fornire assistenza ai soggetti colpiti che operano in settori critici o altamente critici, a integrazione delle azioni da esse svolte a livello nazionale. ***Pertanto, la riserva per la cibersicurezza dovrebbe incentivare gli investimenti nella ricerca e nell'innovazione per promuovere lo sviluppo di tali tecnologie. Ove opportuno, potrebbero essere condotti esercizi comuni con i fornitori di fiducia e i potenziali utenti della riserva per la cibersicurezza al fine di garantire il funzionamento efficiente della riserva stessa.*** Nel richiedere il sostegno della riserva dell'UE per la cibersicurezza, gli Stati membri dovrebbero specificare il sostegno fornito al soggetto interessato a livello nazionale, che è opportuno prendere in considerazione nella valutazione della richiesta dello Stato membro. I servizi di tale riserva possono inoltre servire a sostenere le istituzioni, gli organi e gli organismi dell'Unione, in condizioni analoghe. ***La Commissione dovrebbe garantire il coinvolgimento degli Stati membri e scambi approfonditi con gli stessi al fine di evitare duplicazioni con iniziative analoghe, anche nell'ambito dell'Organizzazione del trattato del Nord Atlantico (NATO).***

(34) Ai fini della selezione di fornitori di servizi privati per la prestazione di servizi nel contesto della riserva dell'UE per la cibersicurezza, occorre stabilire una serie di criteri minimi da includere nel corrispondente bando di gara, in modo da garantire che siano soddisfatte le esigenze delle autorità e dei soggetti degli Stati membri che operano in settori critici o altamente critici. ***Dovrebbe essere incoraggiata la partecipazione dei fornitori più piccoli, attivi a livello regionale e locale.***

(35) Al fine di sostenere l'istituzione della riserva dell'UE per la cibersicurezza, la Commissione potrebbe valutare la possibilità di chiedere all'ENISA di preparare una proposta di sistema di certificazione ai sensi del regolamento (UE) 2019/881 per i servizi di sicurezza gestiti nei settori che rientrano nel meccanismo per le emergenze di

cibersicurezza. ***Al fine di svolgere i compiti aggiuntivi derivanti da questa disposizione, l'ENISA dovrebbe ricevere finanziamenti aggiuntivi adeguati.***

(36) Al fine di sostenere gli obiettivi del presente regolamento di promuovere la condivisione della conoscenza situazionale, rafforzare la resilienza dell'Unione e consentire una risposta efficace agli incidenti di cibersicurezza significativi e su vasta scala, EU-CyCLONe, la rete di CSIRT o la Commissione dovrebbero essere in grado di chiedere all'ENISA di riesaminare e valutare le minacce, le vulnerabilità e le azioni di attenuazione in relazione a uno specifico incidente di cibersicurezza significativo o su vasta scala. Dopo il completamento del riesame e della valutazione di un incidente, l'ENISA dovrebbe preparare una relazione di riesame dell'incidente, in collaborazione con i pertinenti portatori di interessi, compresi i rappresentanti del settore privato, degli Stati membri, della Commissione e di altre istituzioni, organi e organismi dell'UE pertinenti. Per quanto riguarda il settore privato, l'ENISA sta attualmente predisponendo canali per lo scambio di informazioni con fornitori specializzati, compresi i fornitori di soluzioni di sicurezza gestite e i venditori, al fine di contribuire alla realizzazione della sua missione, che consiste nel raggiungere un elevato livello comune di cibersicurezza in tutta l'Unione. Basandosi sulla collaborazione con i portatori di interessi, compreso il settore privato, la relazione di riesame riguardante incidenti specifici dovrebbe mirare a valutare le cause, gli impatti e le misure di attenuazione di un incidente una volta verificatosi. È opportuno prestare particolare attenzione ai contributi e agli insegnamenti condivisi dai fornitori di servizi di sicurezza gestiti che soddisfano le condizioni di massima integrità professionale, imparzialità e competenza tecnica necessaria come disposto dal presente regolamento. La relazione dovrebbe essere presentata a EU-CyCLONe, alla rete di CSIRT e alla Commissione per essere integrata nelle rispettive attività. Se l'incidente riguarda un paese terzo, la Commissione condividerà inoltre la relazione con l'alto rappresentante.

(37) Tenendo conto della natura imprevedibile degli attacchi di cibersicurezza e del fatto che spesso non sono circoscritti a un'area geografica specifica e presentano un elevato rischio di propagazione, il rafforzamento della resilienza dei paesi limitrofi e della loro capacità di rispondere efficacemente agli incidenti di cibersicurezza significativi e su vasta scala contribuisce alla protezione dell'Unione nel suo complesso. I paesi terzi associati al programma Europa digitale possono quindi essere sostenuti dalla riserva dell'UE per la cibersicurezza, laddove ciò sia previsto dal rispettivo accordo di associazione al programma Europa digitale. Il finanziamento per i paesi terzi associati dovrebbe essere sostenuto dall'Unione nel quadro dei partenariati e degli strumenti di finanziamento pertinenti per tali paesi. Il sostegno dovrebbe riguardare servizi nell'ambito della risposta e della ripresa immediata in caso di incidenti di cibersicurezza significativi o su vasta scala. Le condizioni stabilite per la riserva dell'UE per la cibersicurezza e per i fornitori di fiducia nel presente regolamento dovrebbero essere applicate quando è fornito sostegno ai paesi terzi associati al programma Europa digitale.

(37 bis) I paesi terzi potrebbero accedere alle risorse e al sostegno previsti dal presente regolamento, utilizzando il sostegno per la risposta agli incidenti fornito dalla riserva dell'UE per la cibersicurezza. Inoltre, ai fini della fornitura di servizi specifici nell'ambito della riserva dell'UE per la cibersicurezza potrebbero occorrere fornitori di servizi di risposta agli incidenti di paesi terzi, compresi paesi terzi associati al programma Europa digitale o altri paesi partner internazionali e membri della NATO.

In deroga al regolamento (UE, Euratom) 2018/1046, al fine di rafforzare la sovranità tecnologica dell'Unione, la sua autonomia strategica aperta, competitività e resilienza e salvaguardarne le risorse strategiche, gli interessi o la sicurezza, non dovrebbero essere autorizzati a partecipare soggetti stabiliti in paesi terzi che non sono parti dell'AAP e che non sono stati sottoposti a controllo ai sensi del regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio[23] e, se necessario, a misure di mitigazione, tenendo conto degli obiettivi stabiliti nel presente regolamento. La dimensione esterna del presente regolamento dovrebbe essere in linea con le disposizioni stabilite nell'accordo di associazione nell'ambito del programma Europa digitale. La partecipazione dei paesi terzi dovrebbe essere soggetta al controllo pubblico, con il coinvolgimento dei poteri legislativi, per garantire che i cittadini possano partecipare al processo.

(38) Al fine di garantire condizioni uniformi di attuazione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione per specificare le condizioni dell'interoperabilità tra i SOC transfrontalieri; determinare le modalità procedurali per la condivisione delle informazioni relative a un incidente di cibersicurezza su vasta scala, potenziale o in corso, tra i SOC transfrontalieri e i soggetti dell'Unione; stabilire i requisiti tecnici al fine di garantire la sicurezza del ciberscudo europeo; specificare i tipi e il numero di servizi di risposta richiesti per la riserva dell'UE per la cibersicurezza; e specificare ulteriormente le modalità dettagliate di assegnazione dei servizi di sostegno della riserva dell'UE per la cibersicurezza. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio*.

---

* ***Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione (GU L 55 del 28.2.2011, pag. 13, ELI: http://data.europa.eu/eli/reg/2011/182/oj).***

(38 bis) Per attuare efficacemente il ciberscudo europeo e il meccanismo per le emergenze di cibersicurezza è fondamentale disporre di personale qualificato, in grado di fornire i pertinenti servizi di cibersicurezza in modo affidabile e secondo gli standard più elevati. Pertanto, è preoccupante che l'Unione si trovi ad affrontare, da un lato, un divario di talenti caratterizzato da una carenza di professionisti qualificati e, dall'altro, un panorama delle minacce in rapida evoluzione, come riconosciuto nella comunicazione della Commissione del 18 aprile 2023 sull'Accademia per le competenze in materia di cibersicurezza. È importante colmare tale divario di talenti rafforzando la cooperazione e il coordinamento tra i diversi portatori di interessi, compresi il settore privato, il mondo accademico, gli Stati membri, la Commissione e l'ENISA, al fine di aumentare e creare sinergie, in tutti i territori, per gli investimenti nell'istruzione e nella formazione, lo sviluppo di partenariati pubblico-privati, il sostegno a iniziative di ricerca e innovazione, lo sviluppo e il riconoscimento reciproco

---

23 Regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio, del 19 marzo 2019, che istituisce un quadro per il controllo degli investimenti esteri diretti nell'Unione (GU L 79I del 21.3.2019, pag. 1), ELI: http://data.europa.eu/eli/reg/2019/452/oj.

di norme comuni e la certificazione delle competenze in materia di cibersicurezza, anche attraverso il quadro europeo delle competenze in materia di cibersicurezza. Ciò dovrebbe agevolare anche la mobilità dei professionisti della cibersicurezza all'interno dell'Unione. Il presente regolamento dovrebbe mirare a promuovere una forza lavoro più diversificata nel settore della cibersicurezza. Tutte le misure volte ad aumentare le competenze in materia di cibersicurezza richiedono garanzie per evitare una "fuga di cervelli" e un rischio per la mobilità dei lavoratori.

(38 ter) ***È necessario rafforzare le abilità e le competenze specialistiche, interdisciplinari e generali in tutta l'Unione, con particolare attenzione alle donne, in quanto il divario di genere persiste nel settore della cibersicurezza, nel quale le donne rappresentano il 20 % della presenza media mondiale. Le donne devono essere presenti e coinvolte nella progettazione del futuro digitale e della sua governance.***

(38 quater) ***Il rafforzamento della ricerca e dell'innovazione (R&I) nel campo della cibersicurezza è destinato ad aumentare la resilienza e l'autonomia strategica aperta dell'Unione. Analogamente, è importante creare sinergie con i programmi di R&I e con gli strumenti e le istituzioni esistenti, nonché rafforzare la cooperazione e il coordinamento tra le diverse parti interessate, tra cui il settore privato, la società civile, il mondo accademico, gli Stati membri, la Commissione e l'ENISA;***

(38 quinquies) ***Il presente regolamento dovrebbe contribuire all'impegno della dichiarazione europea sui diritti e i principi digitali per il decennio digitale per proteggere gli interessi delle nostre democrazie, dei nostri cittadini, delle nostre imprese e delle nostre istituzioni pubbliche dai rischi di cibersicurezza e dalla criminalità informatica, comprese le violazioni dei dati e il furto o la manipolazione dell'identità. L'applicazione del presente regolamento dovrebbe inoltre contribuire a migliorare l'attuazione di altre normative, ad esempio in materia di intelligenza artificiale, riservatezza dei dati e regolamentazione dei dati in termini di cibersicurezza e ciberresilienza.***

(38 sexies) ***Una maggiore cultura della cibersicurezza, che consideri la sicurezza, compresa quella dell'ambiente digitale, come un bene pubblico, sarà fondamentale per l'efficace attuazione del presente regolamento. Pertanto, l'elaborazione di misure volte a includere e accrescere la consapevolezza dei cittadini dovrebbe essere un ulteriore strumento per garantire la salvaguardia delle nostre democrazie e dei nostri valori fondamentali.***

(38 septies) ***Al fine di integrare determinati elementi non essenziali del presente regolamento, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 TFUE per specificare le condizioni di interoperabilità tra i SOC transfrontalieri, stabilire le modalità procedurali per la condivisione delle informazioni tra i SOC transfrontalieri, da un lato, e EU-CyCLONe, la rete di CSIRT e la Commissione, dall'altro, specificare i tipi e il numero di servizi di risposta richiesti per la riserva dell'UE per la cibersicurezza e specificare ulteriormente le modalità dettagliate di assegnazione dei servizi di sostegno della riserva dell'UE per la cibersicurezza. È di particolare importanza che durante i lavori preparatori la Commissione svolga adeguate consultazioni, anche a livello di esperti, nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016*. In particolare, al fine di garantire la parità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio ricevono tutti i documenti contemporaneamente agli esperti degli Stati membri, e i loro esperti hanno***

sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione incaricati della preparazione di tali atti delegati.

****GU L 123 del 12.5.2016, pag. 1, ELI: http://data.europa.eu/eli/agree_interinstit/2016/512/oj.***

(39) ***Gli obiettivi*** del presente regolamento***, vale a dire rafforzare le capacità dell'Unione in materia di prevenzione, rilevamento, risposta e ripresa in caso di minacce informatiche e istituire un quadro generale che permetta di decompartimentare la comunicazione, non possono essere conseguiti in misura sufficiente dagli Stati membri, ma possono essere conseguiti*** meglio a livello di Unione. L'Unione può quindi intervenire in base ai principi di sussidiarietà e proporzionalità sanciti dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per il conseguimento di tale obiettivo ***in ottemperanza al principio di proporzionalità enunciato nello stesso articolo***,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

Capo I

OBIETTIVI GENERALI, OGGETTO E DEFINIZIONI

Articolo 1

Oggetto e finalità

1. Il presente regolamento stabilisce misure volte a rafforzare le capacità dell'Unione in materia di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi, in particolare mediante:

a) la realizzazione di ***una rete*** paneuropea di centri operativi di sicurezza ("ciberscudo europeo") per sviluppare e potenziare capacità comuni in materia di rilevamento e conoscenza situazionale;

b) la creazione di un meccanismo per le emergenze di cibersicurezza al fine di sostenere gli Stati membri nella preparazione e nella risposta agli incidenti di cibersicurezza significativi e su vasta scala e nella ripresa immediata dagli stessi;

c) l'istituzione di un meccanismo europeo di riesame degli incidenti di cibersicurezza finalizzato al riesame e alla valutazione di incidenti significativi o su vasta scala.

2. Il presente regolamento persegue l'obiettivo di rafforzare la solidarietà a livello dell'Unione mediante gli obiettivi specifici seguenti:

a) migliorare il rilevamento e la conoscenza situazionale comuni dell'Unione in materia di minacce e incidenti informatici, consentendo così ***di sostenere la capacità industriale***

dell'Unione e degli Stati membri nel settore della sicurezza informatica e di rafforzare la posizione competitiva dell'industria, ***in particolare delle microimprese, delle PMI, comprese le startup,*** e dei settori dei servizi nell'Unione nell'ambito dell'economia digitale e di contribuire alla sovranità tecnologica dell'Unione***, alla sua autonomia strategica aperta, alla competitività e alla resilienza in tale settore, rafforzando l'ecosistema della sicurezza informatica al fine di garantire forti capacità dell'Unione, anche in cooperazione con i partner internazionali***;

b) rafforzare la preparazione dei soggetti che operano in settori critici e altamente critici in tutta l'Unione e potenziare la solidarietà sviluppando capacità di risposta comuni contro gli incidenti di cibersicurezza significativi o su vasta scala, permettendo inoltre ai paesi terzi associati al programma Europa digitale di accedere al sostegno offerto dall'Unione per la risposta agli incidenti di cibersicurezza;

c) accrescere la resilienza dell'Unione e contribuire a una risposta efficace, riesaminando e valutando gli incidenti significativi o su vasta scala, traendone anche insegnamenti e, se del caso, formulando raccomandazioni.

c bis) sviluppare, in modo coordinato, capacità, know-how e competenze della forza lavoro, al fine di garantire la cibersicurezza e creare sinergie con l'Accademia per le competenze in materia di cibersicurezza.

3. Il presente regolamento lascia impregiudicata la responsabilità primaria degli Stati membri in materia di sicurezza nazionale, sicurezza pubblica e prevenzione, indagine, accertamento e perseguimento dei reati.

Articolo 2

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

-1 bis) "centro operativo per la sicurezza nazionale" o "SOC nazionale": una capacità nazionale centralizzata che raccoglie e analizza continuamente informazioni di intelligence sulle minacce informatiche e migliora la posizione in materia di cibersicurezza in conformità dell'articolo 4;

1) **"centro operativo di sicurezza transfrontaliero" *o* "SOC transfrontaliero"**: una piattaforma multinazionale che riunisce in una struttura di rete coordinata i SOC nazionali ***in conformità dell'articolo 5***;

2) **"organismo pubblico"**: ***organismi*** di diritto pubblico ***quali definiti*** all'articolo 2, paragrafo 1, punto 4), della direttiva 2014/24/UE del Parlamento europeo e del Consiglio[24];

3) **"consorzio ospitante"**: un consorzio composto da Stati partecipanti, rappresentati da SOC nazionali, ***in conformità dell'articolo 5***;

[24] Direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65).

4) **"soggetto"**: un soggetto quale definito all'articolo 6, punto 38), della direttiva (UE) 2022/2555;

4 bis) "soggetto critico", un soggetto critico quale definito all'articolo 2, punto 1, della direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio[25];

5) **"soggetti che operano in settori critici o altamente critici"**: ***i*** soggetti ***nei settori*** elencati negli allegati I e II della direttiva (UE) 2022/2555;

5 bis) "gestione degli incidenti": la gestione degli incidenti quale definita all'articolo 6, punto 8), della direttiva (UE) 2022/2555;

5 ter) "rischio": un rischio quale definito all'articolo 6, punto 9), della direttiva (UE) 2022/2555;

(6) **"minaccia informatica"**: una minaccia informatica quale definita all'articolo 2, punto 8), del regolamento (UE) 2019/881;

6 bis) "minaccia informatica significativa": una minaccia informatica quale definita all'articolo 6, punto 11, della direttiva (UE) 2022/2555;

(7) **"incidente di cibersicurezza significativo"**: un incidente di cibersicurezza che soddisfa i criteri stabiliti all'articolo 23, paragrafo 3, della direttiva (UE) 2022/2555;

(8) **"incidente di cibersicurezza su vasta scala"**: un incidente quale definito all'articolo 6, punto 7), della direttiva (UE) 2022/2555;

(9) **"preparazione"**: stato di prontezza e capacità in grado di garantire una risposta rapida ed efficace a un incidente di cibersicurezza significativo o su vasta scala, ottenuto a seguito di azioni di valutazione e monitoraggio del rischio intraprese in anticipo;

(10) **"risposta"**: azione intrapresa nel caso di un incidente di cibersicurezza significativo o su vasta scala, oppure durante o dopo tale incidente, per far fronte alle conseguenze negative immediate e a breve termine da esso generate;

10 bis) "prestatore di servizi di sicurezza gestiti": un prestatore di servizi di pagamento quale definito all'articolo 6, punto 40, della direttiva (UE) 2022/2555;

11) **"fornitori di fiducia *di servizi di sicurezza gestiti*"**: fornitori di servizi di sicurezza gestiti selezionati ***per essere inclusi nella riserva dell'UE per la cibersicurezza*** in conformità dell'articolo 16 del presente regolamento.

---

25 Direttiva (UE) 2022/2557 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio ***(GU L 333 del 27.12.2022, p. 164, ELI: http://data.europa.eu/eli/dir/2022/2557/oj).***

Capo II

IL CIBERSCUDO EUROPEO

Articolo 3

Istituzione del ciberscudo europeo

1. È istituita ***una rete*** di centri operativi di sicurezza ("ciberscudo europeo") volta a sviluppare capacità avanzate che permettano all'Unione di rilevare, analizzare ed elaborare dati sulle minacce e prevenire gli incidenti informatici nell'Unione. Tale infrastruttura è composta da centri operativi di sicurezza nazionali ("SOC nazionali") e transfrontalieri ("SOC transfrontalieri").

Le azioni di attuazione del ciberscudo europeo sono sostenute da finanziamenti del programma Europa digitale e attuate in conformità del regolamento (UE) 2021/694 e in particolare dell'obiettivo specifico 3.

2. Il ciberscudo europeo ha le funzioni seguenti:

a) mettere in comune e condividere, attraverso i SOC transfrontalieri, i dati sulle minacce e sugli incidenti informatici provenienti da varie fonti ***e, se del caso, a scambiare informazioni con la rete CSIRT***;

b) produrre analisi sulle minacce informatiche e informazioni di alta qualità e fruibili mediante l'uso di strumenti all'avanguardia, in particolare l'intelligenza artificiale e le tecnologie di analisi dei dati;

c) contribuire a una migliore protezione e risposta alle minacce informatiche***, anche fornendo raccomandazioni concrete ai soggetti***;

d) contribuire a un più rapido rilevamento delle minacce informatiche e alla conoscenza situazionale in tutta l'Unione;

e) fornire servizi e attività per la comunità di cibersicurezza nell'Unione, compreso il contributo allo sviluppo di strumenti avanzati di intelligenza artificiale e di analisi dei dati.

È messo a punto in collaborazione con l'infrastruttura paneuropea di calcolo ad alte prestazioni istituita ai sensi del regolamento (UE) 2021/1173.

Articolo 4

Centri operativi di sicurezza nazionali

1. Per ***poter*** partecipare al ciberscudo europeo, ogni Stato membro designa almeno un SOC nazionale. Il SOC nazionale è ***una capacità nazionale centralizzata all'interno di*** un organismo pubblico. ***Ove possibile, i SOC nazionali sono integrati nei CSIRT o in altre infrastrutture e governance di cibersicurezza esistenti.***

Il SOC ha la capacità di fungere da punto di riferimento e da porta di accesso ad altre organizzazioni pubbliche e private a livello nazionale***, in particolare ai rispettivi SOC nazionali,*** per la raccolta e l'analisi di informazioni sulle minacce e sugli incidenti di cibersicurezza ***e, se del caso, per lo scambio di tali informazioni con membri della rete CSIRT di tale Stato membro,*** e per contribuire a un SOC transfrontaliero. È dotato di tecnologie all'avanguardia in grado di ***prevenire,*** rilevare, aggregare e analizzare dati relativi alle minacce e agli incidenti di cibersicurezza.

Un SOC nazionale o un CSIRT può richiedere dati raccolti mediante telemetria, sensori o registrazioni dei propri soggetti critici nazionali ai fornitori di servizi di sicurezza gestiti che forniscono un servizio al soggetto critico. Tali dati sono condivisi conformemente al diritto dell'Unione in materia di protezione dei dati e al solo scopo di sostenere il SOC nazionale o il CSIRT nel rilevare e prevenire le minacce e gli incidenti di cibersicurezza.

2. A seguito di un invito a manifestare interesse, i SOC nazionali ***possono essere*** selezionati dal Centro europeo di competenza per la cibersicurezza ("ECCC") per partecipare con quest'ultimo a un appalto congiunto di strumenti e infrastrutture. L'ECCC può attribuire sovvenzioni ai SOC nazionali selezionati per finanziare il funzionamento di tali strumenti e infrastrutture. Il contributo finanziario dell'Unione copre fino al 50 % dei costi di acquisizione degli strumenti e delle infrastrutture e fino al 50 % dei costi operativi, mentre i costi restanti devono essere coperti dallo Stato membro. Prima di avviare la procedura di acquisizione degli strumenti e delle infrastrutture, l'ECCC e il SOC nazionale concludono una convezione di accoglienza e di utilizzo che disciplina l'uso degli strumenti e delle infrastrutture.

3. Un SOC nazionale, selezionato ai sensi del paragrafo 2, si impegna a candidarsi per partecipare a un SOC transfrontaliero entro due anni dalla data di acquisizione degli strumenti e delle infrastrutture o, se precedente, dalla data in cui riceve la sovvenzione. Se non partecipa a un SOC transfrontaliero entro tale termine, un SOC nazionale non può beneficiare dell'ulteriore sostegno dell'Unione ai sensi del presente regolamento.

Articolo 5

Centri operativi di sicurezza transfrontalieri

1. Un consorzio ospitante composto da almeno tre Stati membri, rappresentati da SOC nazionali, impegnati a collaborare per coordinare le loro attività di rilevamento e di monitoraggio delle minacce informatiche, è ammesso a partecipare alle azioni volte all'istituzione di un SOC transfrontaliero. ***Un SOC tranfrontaliero è progettato in modo da individuare e analizzare le minacce alla cibersicurezza, impedire gli incidenti e sostenere l'elaborazione di analisi di alta qualità, in particolare mediante lo scambio di dati provenienti da varie fonti, pubbliche e private, nonché tramite la condivisione di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi e capacità di protezione in un contesto di fiducia e sicuro.***

2. A seguito di un invito a manifestare interesse, un consorzio ospitante può essere selezionato dall'ECCC per partecipare con quest'ultimo a un appalto congiunto di strumenti e infrastrutture. L'ECCC può attribuire al consorzio ospitante una sovvenzione per finanziare il funzionamento degli strumenti e delle infrastrutture. Il contributo finanziario dell'Unione copre fino al 75 % dei costi di acquisizione degli strumenti e delle infrastrutture e fino al 50 % dei costi operativi, mentre i costi restanti devono essere coperti dal consorzio ospitante. Prima di avviare la procedura di acquisizione degli strumenti e delle infrastrutture, l'ECCC e il consorzio ospitante concludono una convezione di accoglienza e di utilizzo che disciplina l'uso degli strumenti e delle infrastrutture.

2a. In deroga all'articolo 176 del regolamento (UE, Euratom) 2018/1046, i soggetti stabiliti in paesi terzi che non sono parti dell'AAP non partecipano all'aggiudicazione congiunta di strumenti e infrastrutture.

3. I membri del consorzio ospitante stipulano un accordo di consorzio scritto che definisce le disposizioni interne per l'attuazione della convezione di accoglienza e di utilizzo.

4. Un SOC transfrontaliero è rappresentato a fini legali da un SOC nazionale che funge da SOC coordinatore, o dal consorzio ospitante se quest'ultimo ha personalità giuridica. Il SOC coordinatore è responsabile del rispetto delle prescrizioni della convezione di accoglienza e di utilizzo e del presente regolamento.

Articolo 6

Cooperazione e condivisione di informazioni tra SOC transfrontalieri e al loro interno

1. I membri di un consorzio ospitante scambiano tra loro, all'interno del SOC transfrontaliero, informazioni pertinenti, comprese informazioni relative a minacce informatiche, quasi incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli autori delle minacce, allarmi di cibersicurezza e raccomandazioni relative alla configurazione degli strumenti di cibersicurezza per rilevare gli attacchi informatici, laddove tale condivisione di informazioni:

a) ***migliori lo scambio di informazioni sulle minacce informatiche tra SOC nazionali e transfrontalieri e ISAC del settore allo scopo di prevenire, rilevare o attenuare gli incidenti;***

b) accresca il livello di cibersicurezza, in particolare sensibilizzando in merito alle minacce informatiche, limitando o inibendo la capacità di diffusione di tali minacce e sostenendo una serie di capacità di difesa, la risoluzione e la divulgazione delle vulnerabilità, tecniche di rilevamento, contenimento e prevenzione delle minacce, strategie di attenuazione o fasi di risposta e ripresa, oppure promuovendo la ricerca collaborativa sulle minacce tra soggetti pubblici e privati.

2. L'accordo di consorzio scritto di cui all'articolo 5, paragrafo 3, stabilisce:

a) l'impegno a condividere ***i*** dati ***significativi*** di cui al paragrafo 1 e le condizioni di scambio di tali informazioni;

b) un quadro di governance che incentivi la condivisione delle informazioni da parte di tutti i partecipanti;

c) obiettivi per contribuire allo sviluppo di strumenti avanzati di intelligenza artificiale e di analisi dei dati.

3. Per incoraggiare lo scambio di informazioni tra SOC transfrontalieri ***e gli ISAC del settore***, ***i SOC frontalieri*** garantiscono un elevato livello di interoperabilità tra di loro ***e, ove possibile, con gli ISAC del settore***. Per facilitare l'interoperabilità tra i SOC transfrontalieri ***e gli ISAC del settore, le norme e i protocolli di condivisione delle informazioni possono essere armonizzati con le norme internazionali e le migliori pratiche del settore***. ***È altresì incoraggiato l'appalto congiunto di infrastrutture, servizi e strumenti informatici. Inoltre,*** previa consultazione dell'ECCC ***e dell'ENISA, alla Commissione è conferito il potere di adottare, entro il ... [sei mesi dalla data di entrata in vigore del presente regolamento], atti delegati in conformità dell'articolo 20 bis per integrare il presente regolamento, specificando*** le condizioni di tale interoperabilità ***in stretto coordinamento con i SOC transfrontalieri e sulla base di norme internazionali e delle migliori pratiche del settore.***

4. I SOC transfrontalieri stipulano accordi di cooperazione tra di loro ***e, se del caso, con gli ISAC del settore***, specificando i principi di condivisione delle informazioni ***e di interoperabilità*** tra le piattaforme transfrontaliere, ***tenendo conto dei meccanismi di condivisione delle informazioni pertinenti già esistenti previsti dalla direttiva (UE) 2022/2555***. ***Se del caso, i SOC transfrontalieri concludono accordi di cooperazione con gli ISAC del settore. Nel contesto di un incidente di cibersicurezza su vasta scala, potenziale o in corso, i meccanismi di condivisione delle informazioni sono conformi alle pertinenti disposizioni della direttiva (UE) 2022/2555.***

Articolo 7

Cooperazione e condivisione di informazioni con la rete di CSIRT

1. Quando i SOC transfrontalieri ottengono informazioni relative a un incidente di cibersicurezza su vasta scala, potenziale o in corso***, ai fini di una condivisa capacità di analisi della situazione, il SOC coordinatore*** fornisce senza indebito ritardo le informazioni pertinenti al ***suo CSIRT o alla sua autorità competente, che ne darà notifica a*** EU-CyCLONe, alla rete di CSIRT e alla Commissione ***e a ENISA***, in considerazione dei rispettivi ruoli ***e procedimenti*** di gestione delle crisi conformemente alla direttiva (UE) 2022/2555. ***Il presente paragrafo non impone ulteriori obblighi ai soggetti pubblici o privati di comunicare un incidente di***

cibersicurezza su vasta scala potenziale o in corso ai fini dell'adempimento degli obblighi di cui alla direttiva (UE) 2022/2555.

2. ***Alla*** Commissione ***è conferito il potere di adottare atti delegati conformemente all'articolo 20 bis, previa consultazione della rete CSIRT, al fine di integrare il presente regolamento determinando*** le modalità procedurali per la condivisione delle informazioni di cui al paragrafo 1 ***del presente articolo e in conformità della direttiva (UE) 2022/2555***.

Articolo 8

Sicurezza

1. Gli Stati membri che partecipano al ciberscudo europeo garantiscono un elevato livello di sicurezza ***e riservatezza*** dei dati e di sicurezza fisica dell'infrastruttura del ciberscudo europeo e assicurano che l'infrastruttura sia adeguatamente gestita e controllata, in modo da proteggerla dalle minacce e da garantire la sua sicurezza e quella dei sistemi, compresa quella dei dati scambiati attraverso l'infrastruttura.

2. Gli Stati membri che partecipano al ciberscudo europeo garantiscono che la condivisione di informazioni nell'ambito del ciberscudo europeo con soggetti che non sono organismi pubblici degli Stati membri non influisca negativamente sugli interessi di sicurezza dell'Unione.

3. La Commissione può adottare atti di esecuzione che stabiliscono i requisiti tecnici che gli Stati membri devono rispettare per adempiere gli obblighi di cui ai paragrafi 1 e 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2, del presente regolamento. ***Essi sono conformi alle direttive (UE) 2022/2555 e (UE) 2022/2557. Nei suoi atti di esecuzione***, la Commissione, sostenuta dall'alto rappresentante, tiene conto delle pertinenti norme di sicurezza a livello di difesa, al fine di facilitare la cooperazione con i soggetti militari.

Capo III

MECCANISMO PER LE EMERGENZE DI CIBERSICUREZZA

Articolo 9

Istituzione del meccanismo per le emergenze di cibersicurezza

1. È istituito un meccanismo per le emergenze di cibersicurezza al fine di migliorare la resilienza dell'Unione alle minacce gravi alla cibersicurezza e, in uno spirito di solidarietà, prepararsi all'impatto a breve termine degli incidenti di cibersicurezza significativi e su vasta scala nonché attenuare tale impatto (il "meccanismo").

2. Le azioni di attuazione del meccanismo ▌sono sostenute da finanziamenti a titolo del programma Europa digitale e attuate in conformità del regolamento (UE) 2021/694 e in particolare dell'obiettivo specifico 3.

Articolo 10

Tipi di azioni

1. Il meccanismo sostiene i tipi di azioni seguenti:

a) azioni di preparazione, compresa la verifica coordinata della preparazione dei soggetti che operano in settori altamente critici in tutta l'Unione;

b) azioni di risposta, a sostegno della risposta agli incidenti di cibersicurezza significativi e su vasta scala e della ripresa immediata dagli stessi, che devono essere condotte da fornitori di fiducia ***di servizi di sicurezza gestiti*** che partecipano alla riserva dell'UE per la cibersicurezza istituita ai sensi dell'articolo 12;

c) azioni di assistenza reciproca mediante le quali le autorità nazionali di uno Stato membro forniscono assistenza a un altro Stato membro, in particolare come previsto dall'articolo 11, paragrafo 3, lettera f), della direttiva (UE) 2022/2555.

1 bis. A seguito dell'attivazione del meccanismo, la Commissione, con cadenza annuale, valuta e pubblica una relazione sul funzionamento sia positivo che negativo del meccanismo, compresa l'eventuale necessità di ulteriori requisiti di cooperazione o formazione.

Articolo 11

Verifica coordinata della preparazione dei soggetti

1. Al fine di sostenere la verifica coordinata della preparazione dei soggetti di cui all'articolo 10, paragrafo 1, lettera a), in tutta l'Unione, previa consultazione con il gruppo di cooperazione NIS e l'ENISA, la Commissione individua i settori o i sottosettori interessati, a partire dai settori ad alta criticità di cui all'allegato I della direttiva (UE) 2022/2555, i cui soggetti possono essere sottoposti alla verifica coordinata della preparazione, tenendo conto delle valutazioni coordinate del rischio e dei test di resilienza esistenti e pianificati ***conformemente alle disposizioni stabilite per i tipi di soggetti nei settori ad alta criticità di cui all'allegato I della direttiva (UE) 2022/2555***.

2. Il gruppo di cooperazione NIS, in collaborazione con la Commissione, l'ENISA, l'alto rappresentante ***e i soggetti che sono sottoposti a verifica coordinata della preparazione conformemente al paragrafo 1***, elabora scenari di rischio e metodologie comuni per gli esercizi di verifica coordinata ***della preparazione, che sfociano in un piano di lavoro concertato***. ***I soggetti sottoposti a verifica coordinata della preparazione elaborano e attuano un piano di bonifica che esegue le raccomandazioni risultanti dalle verifiche della preparazione.***

Il gruppo di cooperazione NIS può orientare la definizione delle priorità dei settori o sottosettori per gli esercizi di verifica coordinata della preparazione.

Articolo 12

Istituzione della riserva dell'UE per la cibersicurezza

1. È istituita una riserva dell'UE per la cibersicurezza al fine di assistere gli utenti di cui al paragrafo 3 nella risposta o nella fornitura di sostegno per la risposta agli incidenti di cibersicurezza significativi o su vasta scala e nella ripresa immediata da tali incidenti.

Se risulta evidente che i servizi appaltati non possono essere pienamente utilizzati al fine di fornire sostegno nel rispondere a incidenti significativi o su vasta scala, tali servizi possono essere convertiti, in via eccezionale, in esercitazioni o formazioni per affrontare gli incidenti e forniti agli utenti su richiesta dall'amministrazione aggiudicatrice.

2. La riserva dell'UE per la cibersicurezza consiste in servizi di risposta agli incidenti erogati da fornitori di fiducia ***di servizi di sicurezza gestiti*** selezionati in base ai criteri di cui all'articolo 16. La riserva ***dell'UE per la cibersicurezza*** include servizi preimpegnati. I servizi sono realizzabili in tutti gli Stati membri ***e rafforzano la sovranità tecnologica dell'Unione, la sua autonomia strategica aperta, la competitività e la resilienza nel settore della cibersicurezza, anche promuovendo l'innovazione nel mercato unico digitale in tutta l'Unione***.

3. Tra gli utenti che usufruiscono dei servizi della riserva dell'UE per la cibersicurezza figurano:

a) le autorità di gestione delle crisi informatiche e i CSIRT degli Stati membri di cui rispettivamente all'articolo 9, paragrafi 1 e 2, e all'articolo 10 della direttiva (UE) 2022/2555;

b) le istituzioni e gli organi e organismi dell'Unione***, di cui all'articolo 3, paragrafo 1, del regolamento (UE) .../2023 del Parlamento europeo e del Consiglio[26] e CERT-UE***;

4. Gli utenti di cui al paragrafo 3, lettera a), utilizzano i servizi della riserva dell'UE per la cibersicurezza al fine di rispondere o sostenere la risposta agli incidenti significativi o su vasta scala che colpiscono soggetti che operano in settori critici o altamente critici e sostenere la ripresa immediata da tali incidenti.

5. La Commissione ha la responsabilità generale dell'attuazione della riserva dell'UE per la cibersicurezza. La Commissione determina le priorità e l'evoluzione della riserva dell'UE per la cibersicurezza ***in collaborazione con il gruppo di coordinamento NIS2 e*** in linea con i requisiti degli utenti di cui al paragrafo 3, ne supervisiona l'attuazione e assicura la complementarità, la coerenza, le sinergie e i collegamenti con altre azioni di sostegno ai sensi del presente regolamento, nonché con altre azioni e programmi dell'Unione.

6. La Commissione ***affida*** il funzionamento e l'amministrazione della riserva dell'UE per la cibersicurezza, in tutto o in parte, all'ENISA, mediante accordi di contributo.

7. Al fine di sostenere la Commissione nell'istituzione della riserva dell'UE per la cibersicurezza, l'ENISA prepara una mappatura dei servizi necessari***, comprensiva delle competenze e delle capacità necessarie alla forza lavoro impegnata nel settore della cibersicurezza,*** previa consultazione con gli Stati membri e la Commissione ***e, se del caso, con i fornitori di servizi di sicurezza gestiti e altri rappresentanti del settore della cibersicurezza***. L'ENISA prepara inoltre una mappatura analoga, previa consultazione con la Commissione***, fornitori di servizi di sicurezza gestiti e, se del caso, altri rappresentanti del settore della cibersicurezza***, per individuare le esigenze dei paesi terzi ammissibili al sostegno della riserva

[26] ***Regolamento (UE) .../2023 che stabilisce misure per un livello comune elevato di cibersicurezza nelle istituzioni, negli organi e negli organismi dell'Unione (GU C del ..., pag. ..., ELI: ...).***

dell'UE per la cibersicurezza ai sensi dell'articolo 17. La Commissione, ove opportuno, consulta l'alto rappresentante ***e informa il Consiglio in merito alle esigenze dei paesi terzi***.

8. ***Alla*** Commissione ***è conferito il potere di adottare*** atti ***delegati conformemente all'articolo 20 bis al fine di integrare il presente regolamento specificando*** i tipi e il numero di servizi di risposta richiesti per la riserva dell'UE per la cibersicurezza. ▌..

Articolo 13

Richieste di sostegno della riserva dell'UE per la cibersicurezza

1. Gli utenti di cui all'articolo 12, paragrafo 3, possono richiedere servizi della riserva dell'UE per la cibersicurezza a sostegno della risposta agli incidenti di cibersicurezza significativi o su vasta scala e della ripresa immediata dagli stessi.

2. Per ricevere il sostegno della riserva dell'UE per la cibersicurezza, gli utenti di cui all'articolo 12, paragrafo 3, adottano misure per attenuare gli effetti dell'incidente per il quale è richiesto il sostegno, compresa la fornitura di assistenza tecnica diretta e di altre risorse volte a sostenere la risposta all'incidente e gli sforzi di ripresa immediata.

3. Le richieste di sostegno da parte degli utenti di cui all'articolo 12, paragrafo 3, lettera a), del presente regolamento sono trasmesse alla Commissione e all'ENISA tramite il punto di contatto unico designato o istituito dallo Stato membro in conformità dell'articolo 8, paragrafo 3, della direttiva (UE) 2022/2555.

4. Gli Stati membri informano la rete di CSIRT e, se del caso, EU-CyCLONe in merito alle loro richieste di sostegno nella risposta agli incidenti e nella ripresa immediata ai sensi del presente articolo.

5. Le richieste di sostegno nella risposta agli incidenti e nella ripresa immediata includono:

a) adeguate informazioni sul soggetto interessato e sugli impatti potenziali dell'incidente nonché sull'uso previsto del sostegno richiesto, compresa un'indicazione delle esigenze stimate;

b) informazioni sulle misure adottate per attenuare l'impatto dell'incidente per il quale è richiesto il sostegno, di cui al paragrafo 2;

c) informazioni su altre forme di sostegno disponibili per il soggetto interessato, compresi gli accordi contrattuali in essere per servizi di risposta agli incidenti e di ripresa immediata, nonché i contratti assicurativi potenzialmente in grado di coprire il tipo di incidente in questione.

6. L'ENISA, in collaborazione con la Commissione e il gruppo di cooperazione NIS, elabora un modello per facilitare la presentazione di richieste di sostegno della riserva dell'UE per la cibersicurezza.

7. ***Alla*** Commissione ***è conferito il potere di adottare*** atti ***delegati conformemente all'articolo 20 bis al fine di integrare il presente regolamento specificando*** ulteriormente le modalità dettagliate di assegnazione dei servizi di sostegno della riserva dell'UE per la cibersicurezza. ▌

Articolo 14

Attuazione del sostegno della riserva dell'UE per la cibersicurezza

1. Le richieste di sostegno della riserva dell'UE per la cibersicurezza sono valutate dalla Commissione, con il supporto dell'ENISA o come definito negli accordi di contributo ai sensi dell'articolo 12, paragrafo 6, e senza ***indebito*** ritardo ***e in ogni caso entro 24 ore*** è trasmessa una risposta agli utenti di cui all'articolo 12, paragrafo 3.

2. Per definire l'ordine di priorità delle richieste, in caso di più richieste concomitanti, si tiene conto dei criteri seguenti, ove opportuno:

a) la gravità dell'incidente di cibersicurezza;

b) il tipo di soggetto interessato, dando maggiore priorità agli incidenti che colpiscono soggetti essenziali, quali definiti all'articolo 3, paragrafo 1, della direttiva (UE) 2022/2555;

c) l'impatto potenziale sugli Stati membri o sugli utenti interessati;

d) la portata e la natura potenzialmente transfrontaliera dell'incidente e il rischio di propagazione ad altri Stati membri o utenti;

e) le misure adottate dall'utente per sostenere la risposta e gli sforzi di ripresa immediata, di cui all'articolo 13, paragrafo 2, e all'articolo 13, paragrafo 5, lettera b).

3. I servizi della riserva dell'UE per la cibersicurezza sono forniti in conformità di accordi specifici stipulati tra il fornitore di servizi e l'utente a cui viene fornito il sostegno nell'ambito della riserva dell'UE per la cibersicurezza. Tali accordi includono condizioni di responsabilità ***e qualsiasi altra disposizione che le parti dell'accordo ritengano necessaria per la fornitura del rispettivo servizio***.

4. Gli accordi di cui al paragrafo 3 ***sono*** basati su modelli preparati dall'ENISA, previa consultazione degli Stati membri ***e, ove opportuno, di altri utenti della riserva dell'UE per la cibersicurezza***.

5. La Commissione e l'ENISA non si assumono alcuna responsabilità contrattuale per i danni causati a terzi dai servizi forniti nel quadro dell'attuazione della riserva dell'UE per la cibersicurezza, ***salvo nei casi di negligenza grave nella valutazione dell'applicazione del fornitore di servizi, o nel caso in cui la Commissione o l'ENISA siano utenti della riserva dell'UE per la cibersicurezza ai sensi dell'articolo 14, paragrafo 3***.

6. Entro un mese dalla fine dell'azione di sostegno, gli utenti forniscono alla Commissione, all'ENISA***, alla rete di CSIRT e, ove opportuno, a EU-CyCLONe*** una relazione sintetica sul servizio fornito, sui risultati ottenuti e sugli insegnamenti tratti. Quando l'utente proviene da un paese terzo, come indicato nell'articolo 17, tale relazione è condivisa con l'alto rappresentante. ***La relazione rispetta il diritto nazionale e dell'Unione in materia di protezione delle informazioni sensibili o classificate.***

7. La Commissione riferisce ***periodicamente e almeno due volte all'anno*** al gruppo di cooperazione NIS in merito alle modalità di impiego e ai risultati del sostegno. ***La relazione tutela la riservatezza delle informazioni, conformemente al diritto nazionale e dell'Unione in materia di protezione delle informazioni sensibili o classificate.***

Articolo 15

Coordinamento con i meccanismi di gestione delle crisi

1. Nei casi in cui gli incidenti di cibersicurezza significativi o su vasta scala siano causati da catastrofi, quali definite nella decisione n. 1313/2013/UE[27], o vi diano luogo, il sostegno previsto dal presente regolamento per rispondere a tali incidenti integra le azioni di cui alla decisione n. 1313/2013/UE senza pregiudicare quest'ultima.

2. Nel caso di un incidente di cibersicurezza transfrontaliero su vasta scala che comporti il ricorso a dispositivi integrati per la risposta politica alle crisi (IPCR), il sostegno previsto dal presente regolamento per rispondere a tale incidente è gestito in conformità dei protocolli e delle procedure pertinenti nell'ambito di tali dispositivi.

3. In consultazione con l'alto rappresentante, il sostegno nell'ambito del meccanismo per le emergenze di cibersicurezza può integrare l'assistenza fornita nel contesto della politica estera e di sicurezza comune e della politica di sicurezza e di difesa comune, anche mediante i gruppi di risposta rapida agli incidenti informatici. Tale sostegno può inoltre integrare l'assistenza fornita da uno Stato membro a un altro Stato membro, o contribuirvi, nel contesto dell'articolo 42, paragrafo 7, ***TUE***.

4. Il sostegno nell'ambito del meccanismo per le emergenze di cibersicurezza può far parte della risposta congiunta dell'Unione e degli Stati membri nelle situazioni di cui all'articolo 222 ***TFUE***.

Articolo 16

Fornitori di fiducia

1. Nelle procedure di appalto per l'istituzione della riserva dell'UE per la cibersicurezza, l'amministrazione aggiudicatrice agisce in conformità dei principi stabiliti nel regolamento (UE, Euratom) 2018/1046 e conformemente ai principi seguenti:

a) garantire che la riserva dell'UE per la cibersicurezza includa servizi che possano essere realizzabili in tutti gli Stati membri, tenendo conto in particolare dei requisiti nazionali per la fornitura di tali servizi, compresa la certificazione o l'accreditamento;

b) garantire la protezione degli interessi essenziali di sicurezza dell'Unione e dei suoi Stati membri;

c) garantire che la riserva dell'UE per la cibersicurezza apporti valore aggiunto dell'UE, contribuendo agli obiettivi di cui all'articolo 3 del regolamento (UE) 2021/694, tra cui la promozione dello sviluppo delle competenze in materia di cibersicurezza nell'UE ***e del conseguimento dell'equilibrio di genere nel settore, nonché il rafforzamento della sovranità tecnologica, dell'autonomia strategica aperta, della competitività e della resilienza dell'Unione***.

2. Al momento dell'appalto di servizi per la riserva dell'UE per la cibersicurezza, l'amministrazione aggiudicatrice include nei documenti di gara i criteri di selezione seguenti:

[27] Decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio, del 17 dicembre 2013, su un meccanismo unionale di protezione civile (GU L 347 del 20.12.2013, pag. 924).

a) il fornitore dimostra che il suo personale è dotato della massima integrità professionale, indipendenza e responsabilità, nonché della competenza tecnica necessaria per svolgere le attività nel suo campo specifico, e garantisce la permanenza/continuità delle competenze e delle risorse tecniche necessarie;

b) il fornitore, le sue filiali e i suoi subappaltatori dispongono di un quadro di protezione delle informazioni sensibili relative al servizio, in particolare delle prove, dei risultati e delle relazioni, che sia conforme alle norme di sicurezza dell'Unione sulla protezione delle informazioni classificate dell'UE;

c) il fornitore dimostra, tramite prove sufficienti, che la sua struttura di governo è trasparente, non suscettibile di compromettere la sua imparzialità e la qualità dei servizi prestati o di causare conflitti di interesse;

d) il fornitore è in possesso di un nulla osta di sicurezza adeguato, almeno per il personale destinato alla realizzazione del servizio;

e) il fornitore dispone del livello di sicurezza pertinente per i suoi sistemi informatici;

f) il fornitore è dotato dell'attrezzatura tecnica hardware e software ***aggiornata*** necessaria a supportare il servizio richiesto ***e, se del caso, è conforme al regolamento (UE) .../... del Parlamento europeo e del Consiglio[28] (2022/0272(COD))***;

g) il fornitore è in grado di dimostrare di avere esperienza nella fornitura di servizi analoghi alle autorità nazionali competenti o ai soggetti che operano in settori critici o altamente critici;

h) il fornitore è in grado di prestare il servizio in tempi brevi nello Stato membro o negli Stati membri in cui ciò è possibile;

i) il fornitore è in grado di prestare il servizio nella lingua locale dello Stato membro o degli Stati membri in cui ciò è possibile***, o in una delle lingue di lavoro delle istituzioni dell'Unione***;

j) una volta posto in essere un sistema ***europeo*** di certificazione ***della cibersicurezza*** per il servizio di sicurezza gestito a norma del regolamento (UE) 2019/881, il fornitore è certificato conformemente a tale sistema ***entro un termine di due anni dalla relativa adozione;***

j bis) il fornitore è in grado di prestare il servizio in modo indipendente e non nell'ambito di un pacchetto, salvaguardando così la possibilità per l'utente di passare a un altro fornitore di servizi;

j ter) ai fini dell'articolo 12, paragrafo 1, il fornitore include nella proposta di gara la possibilità di convertire i servizi di risposta agli incidenti non utilizzati in esercitazioni o corsi di formazione;

j quater) il fornitore è stabilito e dispone di proprie strutture di gestione esecutiva nell'Unione, in un paese associato o in un paese terzo che è parte dell'accordo sugli appalti pubblici nell'ambito dell'Organizzazione mondiale del commercio (AAP);

j quinquies) il fornitore non è soggetto al controllo di un paese terzo non associato o di un soggetto di un paese terzo non associato che non è parte dell'AAP o, in alternativa,

---

28 ***Regolamento (UE) …/… del Parlamento europeo e del Consiglio del … (GU L ... del …, pag. …, ELI: ...).***

tale soggetto è stato sottoposto a un controllo ai sensi del regolamento (UE) 2019/452 e, se necessario, a misure di mitigazione, tenendo conto degli obiettivi di cui al presente regolamento.

Articolo 17

Sostegno ai paesi terzi

1. I paesi terzi possono richiedere il sostegno della riserva dell'UE per la cibersicurezza nei casi in cui è previsto dagli accordi di associazione conclusi in relazione alla loro partecipazione al programma Europa digitale.

2. Il sostegno della riserva dell'UE per la cibersicurezza è conforme al presente regolamento e rispetta le condizioni specifiche stabilite negli accordi di associazione di cui al paragrafo 1.

3. Tra gli utenti dei paesi terzi associati che possono essere destinatari dei servizi della riserva dell'UE per la cibersicurezza rientrano le autorità competenti come i CSIRT e le autorità di gestione delle crisi informatiche.

4. Ogni paese terzo ammissibile al sostegno della riserva dell'UE per la cibersicurezza designa un'autorità che funga da punto di contatto unico ai fini del presente regolamento.

5. Prima di ricevere il sostegno della riserva dell'UE per la cibersicurezza, i paesi terzi forniscono alla Commissione e all'alto rappresentante informazioni sulle loro capacità di resilienza informatica e di gestione del rischio, tra cui almeno le informazioni sulle misure nazionali adottate per prepararsi agli incidenti di cibersicurezza significativi o su vasta scala, nonché informazioni sui soggetti nazionali responsabili, compresi i CSIRT o soggetti equivalenti, sulle loro capacità e sulle risorse loro assegnate. Qualora riguardino gli Stati membri, le disposizioni degli articoli 13 e 14 del presente regolamento si applicano ai paesi terzi come indicato nel paragrafo 1.

6. La Commissione ***dà notifica al Consiglio senza indebito ritardo e*** si coordina con l'alto rappresentante in merito alle richieste ricevute e all'attuazione del sostegno concesso ai paesi terzi dalla riserva dell'UE per la cibersicurezza.

Capo IV

MECCANISMO DI RIESAME DEGLI INCIDENTI DI CIBERSICUREZZA

Articolo 18

Meccanismo di riesame degli incidenti di cibersicurezza

1. Su richiesta della Commissione, di EU-CyCLONe o della rete di CSIRT, l'ENISA riesamina e valuta le minacce, le vulnerabilità e le azioni di attenuazione in relazione a uno specifico incidente di cibersicurezza significativo o su vasta scala. Al termine del riesame e della valutazione di un incidente, l'ENISA presenta una relazione di riesame dell'incidente alla rete di CSIRT, a EU-CyCLONe e alla Commissione per sostenerli nello svolgimento dei loro compiti, in particolare alla luce di quelli stabiliti negli articoli 15 e 16 della direttiva (UE)

2022/2555. Laddove opportuno, la Commissione condivide la relazione con l'alto rappresentante.

2. Per preparare la relazione di riesame dell'incidente di cui al paragrafo 1, l'ENISA collabora con tutti i portatori di interessi, compresi i rappresentanti degli Stati membri, della Commissione, di altre istituzioni e di altri organi e organismi pertinenti dell'UE, dei fornitori di servizi di sicurezza gestiti ***nei SOC nazionali e transfrontalieri*** e degli utenti di servizi di cibersicurezza***, e ne raccoglie i riscontri, integrati da garanzie e da un monitoraggio idonei ad assicurare che gli insegnamenti tratti e le migliori pratiche individuate siano sostenute dai soggetti del settore dei servizi di cibersicurezza***. Ove opportuno, l'ENISA collabora anche con i soggetti interessati da incidenti di cibersicurezza significativi o su vasta scala. A sostegno del riesame l'ENISA può anche consultare altri tipi di portatori di interessi. I rappresentanti consultati dichiarano eventuali potenziali conflitti di interessi.

3. La relazione comprende un riesame e un'analisi dello specifico incidente di cibersicurezza significativo o su vasta scala, nonché delle cause principali, delle vulnerabilità e degli insegnamenti tratti. La relazione tutela la riservatezza delle informazioni, conformemente al diritto nazionale o dell'Unione in materia di protezione delle informazioni sensibili o classificate. ***Essa non include dettagli sulle vulnerabilità sfruttate attivamente che rimangono non risolte.***

3 bis. La relazione di cui al paragrafo 1 del presente articolo illustra gli insegnamenti tratti dalle valutazioni inter pares effettuate a norma dell'articolo 19 della direttiva (UE) 2022/2555.

4. Ove opportuno, la relazione formula raccomandazioni***, anche destinate a tutti i portatori di interessi,*** per migliorare la posizione dell'Unione in materia di deterrenza informatica.

5. Ove possibile una versione della relazione è resa disponibile al pubblico. Tale versione contiene solo informazioni pubbliche.

Capo V

DISPOSIZIONI FINALI

Articolo 19

Modifiche del regolamento (UE) 2021/694

Il regolamento (UE) 2021/694 è così modificato:

1) l'articolo 6 è così modificato:

a) il paragrafo 1 è così modificato:

i) è inserita la seguente lettera a bis):

"a bis) sostenere lo sviluppo di un ciberscudo europeo, compresi l'elaborazione, la realizzazione e il funzionamento di piattaforme SOC nazionali e transfrontaliere che contribuiscano alla conoscenza situazionale nell'Unione e al potenziamento delle capacità di analisi delle minacce informatiche dell'Unione;";

ii) è aggiunta la seguente lettera g):

istituire e gestire un meccanismo per le emergenze di cibersicurezza inteso a sostenere gli Stati membri nella preparazione agli incidenti di cibersicurezza significativi e nella risposta agli stessi, a integrazione delle risorse e delle capacità nazionali e di altre forme di sostegno disponibili a livello di Unione, compresa l'istituzione di una riserva dell'UE per la cibersicurezza.";

b) il paragrafo 2 è sostituito dal seguente:

"2. Le azioni nell'ambito dell'obiettivo specifico 3 sono attuate principalmente mediante il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento in conformità del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio*, fatta eccezione per le azioni di attuazione della riserva dell'UE per la cibersicurezza, che sono attuate dalla Commissione e dall'ENISA.";

---

* 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 (GU L 202 dell'8.6.2021, pag. 1***,*** ***ELI:*** ***http://data.europa.eu/eli/reg/2021/887/oj***).

(2) l'articolo 9 è così modificato:

a) al paragrafo 2, le lettere b), c) e d) sono sostituite dalle seguenti:

"b) 1 776 956 000 EUR per l'obiettivo specifico 2 – Intelligenza artificiale;

c) ***1 620 566 000*** EUR per l'obiettivo specifico 3 – Cibersicurezza e fiducia;

d) ***500 347 000*** EUR per l'obiettivo specifico 4 – Competenze digitali avanzate;";

a bis) è inserito il seguente nuovo paragrafo 2 bis:

"(2 bis) L'importo di cui al paragrafo 2, lettera c), è utilizzato primariamente per conseguire gli obiettivi operativi di cui all'articolo 6, paragrafo 1, lettere da a) a f), del programma.";

a ter) è inserito il seguente nuovo paragrafo 2 ter:

"(2 ter) L'importo destinato all'istituzione e all'attuazione della riserva dell'UE per la cibersicurezza non supera i 27 milioni di EUR per la durata prevista del regolamento che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e

risposta agli stessi.";

b) è aggiunto il seguente paragrafo 8:

"8. In deroga all'articolo 12, paragrafo 4, del regolamento (UE, Euratom) 2018/1046, gli stanziamenti d'impegno e di pagamento non utilizzati per le azioni ***nel contesto dell'attuazione della riserva dell'UE per la cibersicurezza*** che perseguono gli obiettivi di cui all'articolo 6, paragrafo 1, lettera g), del presente regolamento sono riportati di diritto e possono essere impegnati e pagati fino al 31 dicembre dell'esercizio successivo.

La Commissione comunica al Parlamento e al Consiglio gli stanziamenti riportati a norma dell'articolo 12, paragrafo 6, del regolamento (UE, Euratom) 2018/1046.";

(3) all'articolo 14, il paragrafo 2 è sostituito dal seguente:

"2. Il Programma può concedere finanziamenti in tutte le forme previste dal regolamento ***(UE, Euratom) 2018/1046***, anche, in particolare, sotto forma di appalti, quale forma principale, o di sovvenzioni e premi.

Qualora, per il conseguimento di uno degli obiettivi di un'azione, siano necessarie gare di appalto per acquisire beni e servizi innovativi, le sovvenzioni possono essere concesse unicamente a beneficiari che sono amministrazioni aggiudicatrici o enti aggiudicatori ai sensi delle direttive 2014/24/UE [27] e 2014/25/UE [28] del Parlamento europeo e del Consiglio.

Qualora la fornitura di beni o servizi innovativi non ancora disponibili su larga scala commerciale sia necessaria per il conseguimento degli obiettivi di un'azione, l'amministrazione aggiudicatrice o l'ente aggiudicatore può autorizzare l'aggiudicazione di contratti multipli nell'ambito della stessa procedura di appalto.

Per motivi di pubblica sicurezza debitamente giustificati, l'amministrazione aggiudicatrice o l'ente aggiudicatore può imporre come condizione che il luogo di esecuzione del contratto sia situato nel territorio dell'Unione.

Nell'attuazione delle procedure di appalto per la riserva dell'UE per la cibersicurezza istituita dall'articolo 12 del regolamento (UE) 2023/**…**, la Commissione e l'ENISA possono fungere da centrale di committenza per condurre una procedura di appalto per conto o a nome di paesi terzi associati al Programma, in linea con l'articolo 10. La Commissione e l'ENISA possono anche agire in veste di grossisti, comprando, immagazzinando e rivendendo o donando forniture e servizi, comprese le locazioni, per tali paesi terzi. In deroga all'articolo 169, paragrafo 3, del regolamento (UE) **…/…** [rifusione del RF], la richiesta di un singolo paese terzo è sufficiente per conferire alla Commissione o all'ENISA il mandato di agire.

Nell'attuazione delle procedure di appalto per la riserva dell'UE per la cibersicurezza istituita dall'articolo 12 del regolamento (UE) 2023/**…**, la Commissione e l'ENISA possono fungere da centrale di committenza per condurre una procedura di appalto per conto o a nome di istituzioni, organi e organismi dell'Unione. La Commissione e

l'ENISA possono anche agire in veste di grossisti, comprando, immagazzinando e rivendendo o donando forniture e servizi, comprese le locazioni, per le istituzioni, gli organi e gli organismi dell'Unione. In deroga all'articolo 169, paragrafo 3, del regolamento (UE) **…/…** [rifusione del RF], la richiesta di un singolo paese terzo è sufficiente per conferire alla Commissione o all'ENISA il mandato di agire.

Il Programma può inoltre concedere finanziamenti sotto forma di strumenti finanziari nell'ambito di operazioni di finanziamento misto. ";

(4) è aggiunto l'articolo 16 bis seguente:

"***Articolo 16 bis***

Nel caso di azioni volte ad attuare il ciberscudo europeo stabilito dall'articolo 3 del regolamento (UE) 2023/XX, le norme applicabili sono quelle sancite agli articoli 4 e 5 del regolamento (UE) 2023/**…**. In caso di contrasto tra le disposizioni del presente regolamento e gli articoli 4 e 5 del regolamento (UE) 2023/**…**, prevalgono questi ultimi e si applicano a tali azioni specifiche.";

(5) l'articolo 19 è sostituito dal seguente:

"Le sovvenzioni nell'ambito del Programma sono attribuite e gestite conformemente al titolo VIII del regolamento ***(UE, Euratom) 2018/1046*** e possono coprire fino al 100 % dei costi ammissibili, fatto salvo il principio di cofinanziamento stabilito all'articolo 190 del regolamento ***(UE, Euratom) 2018/1046***. Tali sovvenzioni devono essere concesse e gestite conformemente a ciascun obiettivo specifico.

Il sostegno erogato sotto forma di sovvenzioni può essere concesso direttamente dall'ECCC, senza invito a presentare proposte, ai SOC nazionali di cui all'articolo 4 del regolamento ***(UE) .../...*** e al consorzio ospitante di cui all'articolo 5 del regolamento ***(UE) .../...***, in conformità dell'articolo 195, primo comma, lettera d), del regolamento ***(UE, Euratom) 2018/1046***.

Il sostegno erogato sotto forma di sovvenzioni per il meccanismo per le emergenze di cibersicurezza di cui all'articolo 10 del regolamento ***(UE) .../...*** può essere concesso direttamente dall'ECCC agli Stati membri senza invito a presentare proposte, in conformità dell'articolo 195, primo comma, lettera d), del regolamento ***(UE, Euratom) 2018/1046***.

Per le azioni specificate nell'articolo 10, paragrafo 1, lettera c), del regolamento ***(UE) .../...***, l'ECCC informa la Commissione e l'ENISA sulle richieste di sovvenzioni dirette degli Stati membri senza invito a presentare proposte.

A sostegno dell'assistenza reciproca per la risposta a un incidente di cibersicurezza significativo o su vasta scala, come definito all'articolo 10, lettera c), del regolamento ***(UE) .../...***, e in conformità dell'articolo 193, paragrafo 2, secondo comma, lettera a), del regolamento ***(UE, Euratom) 2018/1046***, in casi debitamente giustificati i costi possono

essere considerati ammissibili anche se sono stati sostenuti prima della presentazione della domanda di sovvenzione.";

(6) gli allegati I e II del regolamento (UE) 2021/694 sono modificati conformemente all'allegato del presente regolamento.

Articolo 19 bis
Risorse supplementari per l'ENISA

L'ENISA riceve risorse supplementari per svolgere i compiti aggiuntivi conferitile dal presente regolamento. Tale sostegno supplementare, anche finanziario, non pregiudica il conseguimento degli obiettivi di altri programmi dell'Unione, in particolare del programma Europa digitale.

Articolo 20

Valutazione *e riesame*

1. Entro [***due*** anni dalla data di applicazione del presente regolamento] ***e successivamente ogni due anni***, la Commissione ***effettua una valutazione del funzionamento delle misure stabilire nel presente regolamento e*** trasmette al Parlamento europeo e al Consiglio una relazione ▌.

2. La valutazione verte in particolare sui seguenti elementi:

a) l'uso e il valore aggiunto dei SOC transfrontalieri e la misura in cui contribuiscono ad accelerare il rilevamento delle minacce informatiche, la risposta alle stesse e la conoscenza situazionale; la partecipazione attiva dei SOC nazionali al ciberscudo europeo, compreso il numero di SOC nazionali e transfrontalieri istituiti e la misura in cui ha contribuito all'elaborazione e allo scambio di informazioni di alta qualità e fruibili nonché di analisi sulle minacce informatiche; il numero e i costi delle infrastrutture o degli strumenti di cibersicurezza, o di entrambi, acquisiti congiuntamente; il numero di accordi di cooperazione conclusi tra i SOC transfrontalieri e i CERT del settore; il numero di incidenti segnalati alla rete CSIRT e le relative conseguenze sull'attività della rete CSIRT;

b) i risultati sia positivi che negativi del meccanismo per le emergenze di cibersicurezza, compresa l'eventuale necessità di definire ulteriori requisiti in materia di cooperazione o formazione;

c) il contributo del presente regolamento al rafforzamento della resilienza e della sovranità strategica aperta dell'Unione, al miglioramento della competitività dei settori industriali interessati, delle microimprese e delle PMI, comprese le start-up, nonché allo sviluppo delle competenze in materia di cibersicurezza nell'Unione;

d) l'uso e il valore aggiunto della riserva dell'UE per la cibersicurezza, compreso il numero di fornitori di servizi di sicurezza di fiducia che fanno parte di tale riserva; il numero, la tipologia, i costi e l'impatto delle azioni intraprese a sostegno della risposta agli incidenti di cibersicurezza, nonché i relativi utenti e fornitori; il tempo medio per il riconoscimento da parte della Commissione, per il dispiegamento e la risposta della riserva dell'UE per la cibersicurezza, nonché per la ripresa dell'utente dagli incidenti; l'eventuale estensione dell'ambito di applicazione della riserva dell'UE per la cibersicurezza ai servizi di preparazione agli incidenti o alle esercitazioni comuni con i fornitori di servizi di sicurezza gestiti di fiducia e i potenziali utenti della riserva dell'UE per la cibersicurezza, al fine di garantire il funzionamento efficiente di tale riserva ove necessario;

e) il contributo del presente regolamento allo sviluppo e al miglioramento delle capacità e delle competenze della forza lavoro nel settore della cibersicurezza, necessari per rafforzare la capacità dell'Unione di rilevare e prevenire le minacce e gli incidenti di cibersicurezza, di rispondervi e di riprendersi dagli stessi;

f) il contributo del presente regolamento alla diffusione e allo sviluppo di tecnologie all'avanguardia nell'Unione.

3. Sulla base delle relazioni di cui al paragrafo 1, la Commissione, se del caso, presenta una proposta legislativa al Parlamento europeo e al Consiglio al fine di modificare il presente regolamento.

Articolo 20 bis

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

2. Il potere di adottare atti delegati di cui all'articolo 6, paragrafo 3, all'articolo 7, paragrafo 2, all'articolo 12, paragrafo 8, e all'articolo 13, paragrafo 7, è conferito alla Commissione per un periodo di ... anni a decorrere dal ... [data di entrata in vigore dell'atto legislativo di base o qualsiasi altra data fissata dai colegislatori]. La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi prima della scadenza del periodo

di ... anni. La delega di potere è tacitamente prorogata per periodi di identica durata, a meno che il Parlamento europeo o il Consiglio non si oppongano a tale proroga al più tardi tre mesi prima della scadenza di ciascun periodo.

3. La delega di potere di cui all'articolo 6, paragrafo 3, all'articolo 7, paragrafo 2, all'articolo 12, paragrafo 8, e all'articolo 13, paragrafo 7, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella Gazzetta ufficiale dell'Unione europea o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

4. Prima dell'adozione dell'atto delegato la Commissione consulta gli esperti designati da ciascuno Stato membro nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016.

5. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

6. L'atto delegato adottato a norma dell'articolo 6, paragrafo 3, dell'articolo 7, paragrafo 2, dell'articolo 12, paragrafo 8, e dell'articolo 13, paragrafo 7, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di [due mesi] su iniziativa del Parlamento europeo o del Consiglio.

Articolo 21

Procedura di comitato

1. La Commissione è assistita dal comitato di coordinamento del programma Europa digitale istituito dal regolamento (UE) 2021/694. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.
2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

Articolo 22

Entrata in vigore

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Strasburgo, il

Per il Parlamento europeo	*Per il Consiglio*
La presidente	*La presidente*

ALLEGATO

Il regolamento (UE) 2021/694 è così modificato:

(1) nell'allegato I, la sezione "Obiettivo specifico 3 - Cibersicurezza e fiducia" è sostituita dalla seguente:

"Obiettivo specifico 3 — Cibersicurezza e fiducia

Il Programma incentiva il rafforzamento, lo sviluppo e l'acquisizione di capacità essenziali volte a rendere sicure l'economia digitale, la società e la democrazia dell'Unione rafforzandone il potenziale industriale e la competitività in ambito di cibersicurezza, oltre a migliorare le capacità sia del settore privato sia del settore pubblico di proteggere i cittadini e le imprese dalle minacce informatiche, anche attraverso il sostegno all'attuazione della direttiva (UE) 2016/1148.

Le azioni iniziali e, laddove opportuno, le azioni successive del presente obiettivo comprendono:

1. il coinvestimento con gli Stati membri in attrezzature avanzate per la cibersicurezza, in infrastrutture e know-how, essenziali per proteggere le infrastrutture fondamentali e il mercato unico digitale nel suo complesso. Tale coinvestimento potrebbe comprendere investimenti in impianti quantistici e risorse di dati per la cibersicurezza e la conoscenza situazionale nel ciberspazio, compresi i SOC nazionali e i SOC transfrontalieri che costituiscono il ciberscudo europeo, e in altri strumenti da mettere a disposizione del settore pubblico e di quello privato in tutta Europa;

2. l'ampliamento delle capacità tecnologiche esistenti e la messa in rete dei centri di

competenza negli Stati membri, in modo tale che tali capacità rispondano alle esigenze del settore pubblico e dell'industria, anche per quanto riguarda prodotti e servizi che rafforzano la cibersicurezza e la fiducia all'interno del mercato unico digitale;

3. la garanzia di un'ampia implementazione di soluzioni di cibersicurezza e fiducia efficaci e all'avanguardia in tutti gli Stati membri. Tale implementazione comprende il rafforzamento della sicurezza dei prodotti dalla progettazione alla commercializzazione;

4. il sostegno volto a colmare le lacune di competenze in materia di cibersicurezza, ***prestando particolare attenzione al conseguimento dell'equilibrio di genere,*** ad esempio, allineando i programmi relativi a tali competenze, adattandoli alle esigenze settoriali specifiche***, compresa un'attenzione interdisciplinare e generale,*** e favorendo l'accesso a corsi di formazione mirati e specializzati ***per consentire a tutte le persone in tutti i territori, senza pregiudizi, di beneficiare delle opportunità offerte dal presente regolamento.***

5. la promozione della solidarietà tra gli Stati membri nella preparazione e nella risposta agli incidenti di cibersicurezza significativi tramite l'introduzione di servizi di cibersicurezza a livello transfrontaliero, tra cui il sostegno all'assistenza reciproca tra le autorità pubbliche e l'istituzione di una riserva di fornitori di ***servizi di sicurezza gestiti*** di fiducia a livello dell'Unione.";

(2) nell'allegato II la sezione "Obiettivo specifico 3 - Cibersicurezza e fiducia" è sostituita dalla seguente:

"Obiettivo specifico 3 — Cibersicurezza e fiducia

3.1. Numero di infrastrutture o strumenti di cibersicurezza, o di entrambi, acquisiti congiuntamente ***nell'ambito del ciberscudo europeo***

3.2. Numero di utenti e comunità di utenti che hanno accesso a strutture di cibersicurezza europee

3.3. Numero***, tipologia, costi e impatto delle*** azioni ***intraprese*** a sostegno della preparazione e della risposta agli incidenti di cibersicurezza nell'ambito del meccanismo per le emergenze di cibersicurezza ▌. ***La misura in cui le raccomandazioni delle prove di preparazione sono state attuate e applicate dall'utente, nonché il tempo medio per il riconoscimento da parte della Commissione, per la risposta della riserva dell'UE per la cibersicurezza nonché per la ripresa dell'utente dagli incidenti."***

MOTIVAZIONE

CONTESTO

La cibersicurezza è e dovrebbe essere al centro delle nostre democrazie. Le minacce alla cibersicurezza sono legate alla diffusione dell'insicurezza tra la popolazione e le imprese, nonché all'aumento della disinformazione, che mina i principi democratici fondamentali per il rispetto dei diritti umani. Per prevenire tutto ciò, un ambiente digitale sicuro e soggetto al controllo pubblico è fondamentale per le nostre democrazie.

Gli attacchi informatici nell'UE stanno crescendo sia in termini di metodi che di impatto. Inoltre, secondo la relazione 2022 dell'ENISA sul panorama delle minacce[1], l'attacco russo all'Ucraina ha innescato profondi cambiamenti, anche prima dell'invasione, dando il via a una nuova era per i **cyberware**. Le priorità individuate nel corso di questo conflitto informatico sono la necessità di **creare capacità** per **programmi** e progetti **multilaterali** e la necessità di **sviluppare rapidamente** le competenze. Per essere più resilienti, è urgente una risposta comune europea, basata su una più forte cooperazione a livello europeo oltre a quella nazionale.

Una maggiore cultura della cibersicurezza, che consideri la sicurezza, compresa quella dell'ambiente digitale, come un bene pubblico, sarà fondamentale per l'efficace attuazione del regolamento in esame.

Inoltre, gli attacchi informatici sono spesso diretti ai **servizi pubblici** e alle infrastrutture **locali, regionali o nazionali** (ad esempio il settore sanitario, che rimane un bersaglio primario degli attacchi informatici[2]). I dati evidenziano inoltre che le **autorità locali**, a fronte della mancanza di risorse finanziarie e umane, sono tra i bersagli più vulnerabili e che è particolarmente importante sensibilizzare i leader a livello locale per aumentare la resilienza digitale[3]. Gli attacchi colpiscono principalmente e direttamente i cittadini e mettono quindi a repentaglio le nostre democrazie, anche attraverso campagne di disinformazione. Il senso di insicurezza che queste situazioni possono instillare nella popolazione può portare a preferenze politiche improntate a un impegno radicale per la sicurezza a scapito del rispetto dei diritti fondamentali. Ma è vero anche il contrario: la sicurezza è una componente essenziale delle nostre democrazie, compatibile con tutti gli altri diritti e ad essi necessaria.

Inoltre, anche **le aziende e le PMI** dell'UE sono vittime della criminalità informatica e, con il crescente ricorso alla sfera digitale per condurre le imprese, la cibersicurezza desta sempre più preoccupazioni. Le PMI sono le meno preparate, in quanto dispongono di minori risorse per proteggersi e sono meno consapevoli di poter essere vittime di tali attacchi.

Si prevede che questi attacchi continueranno e aumenteranno in futuro, soprattutto in

---

[1] ENISA "Threat Landscape 2022" (Panorama delle minacce 2022), ottobre 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport

[2] ENISA, "Threat Landscape: Health Sector" (Panorama delle minacce: il settore sanitario), luglio 2023. https://www.enisa.europa.eu/publications/health-threat-landscape/@@download/fullReport

[3] Comitato europeo delle regioni, "Digital Resilience" (Resilienza digitale), 2023. https://cor.europa.eu/en/engage/studies/Documents/Digital%20resilience.pdf

situazioni di instabilità politica e, più in particolare, in contesti di guerra. Con l'avanzare della transizione digitale, la resilienza digitale diventa sempre più importante per la nostra vita quotidiana e per l'**autonomia strategica aperta dell'UE**.

PROPOSTA DELLA RELATRICE

La relatrice ritiene che l'UE debba essere meglio preparata per il futuro e si compiace di questo urgente atto legislativo volto a mettere in comune risorse, informazioni e conoscenze per garantire la solidarietà tra gli Stati membri, far crescere la capacità industriale nell'UE, **sviluppare in modo coordinato competenze e capacità** che garantiscano la cibersicurezza, essere più resiliente agli attacchi futuri e proteggere le nostre democrazie da un approccio individualistico alle esigenze di sicurezza. È inoltre importante tutelare l'integrità dei nostri processi elettorali. Questo atto legislativo è un impegno essenziale per conseguire l'obiettivo di un'**autonomia strategica aperta**.

Per questi motivi, l'UE ha bisogno di una **governance** forte e **coordinata** e di una cooperazione strutturata con il settore privato per promuovere lo sviluppo dell'industria informatica europea. Oltre alla collaborazione con partner internazionali che condividono gli stessi principi, è auspicabile collaborare con altri paesi che non hanno le stesse capacità e che potrebbero aver bisogno di aiuto in caso di attacchi informatici. Il regolamento dell'UE sulla cibersolidarietà deve definire bene la sua governance e non sovrapporsi a iniziative e normative già esistenti, come la direttiva NIS 2.

La proposta si basa in modo significativo sullo scambio di informazioni su base volontaria tra gli Stati membri. Per tale motivo, la relatrice propone di rafforzare le garanzie per creare fiducia tra gli Stati membri al fine di aumentare la loro partecipazione e cooperazione, ad esempio per quanto riguarda le acquisizioni congiunte di infrastrutture e il coinvolgimento dei poteri legislativi, onde assicurare la fiducia dei cittadini e le **garanzie democratiche**.

In secondo luogo, propone di **garantire il bilancio** dei prossimi QFP per questa iniziativa, anche con l'impegno degli Stati membri, al fine di garantire la continuità delle attività sviluppate nell'ambito del regolamento dell'UE sulla cibersolidarietà oltre il 2027.

In terzo luogo, la relatrice propone di migliorare la **struttura di governance**, di definire chiaramente la governance e di allinearla alla legislazione esistente.

La relatrice propone inoltre un migliore **coordinamento** tra i diversi organismi degli Stati membri responsabili della cibersicurezza per offrire uno scudo informatico comune. Suggerisce altresì di aumentare il contributo dell'ENISA al coordinamento e all'interazione tra i diversi attori delle comunità nazionali.

Quanto alla **nuova riserva per la cibersicurezza**, la relatrice ritiene che abbia il potenziale di sviluppare le capacità industriali nell'Unione, anche per le PMI, con investimenti nella ricerca e nell'innovazione (R&I) per mettere a punto tecnologie all'avanguardia, come le tecnologie cloud e di intelligenza artificiale. Inoltre, la relatrice propone di mantenere la partecipazione dell'industria, di migliorare i criteri e la fiducia nella sua partecipazione (ad esempio associando la partecipazione a un'impresa nazionale o locale) chiarendo i criteri e la definizione di **sovranità tecnologica** e garantendo un equilibrio tra gli attori UE e non UE. Propone inoltre di

applicare un **sistema di certificazione** ai fornitori privati nell'ambito del **meccanismo per le emergenze di cibersicurezza**, al fine di instaurare partenariati affidabili e a lungo termine.

Per quanto riguarda il **meccanismo di revisione degli incidenti**, la relatrice propone di rafforzare il ruolo dell'ENISA e del settore privato nei SOC, con le giuste garanzie e il giusto monitoraggio, per accertare che gli insegnamenti tratti siano fatti propri anche dagli attori del settore. La relatrice suggerisce inoltre di tener conto degli insegnamenti tratti dalle revisioni tra pari, come indicato nella direttiva NIS 2, e di aumentare i finanziamenti dell'ENISA tesi a garantire un'applicazione efficace della legislazione e una protezione adeguata per far fronte alle minacce alla cibersicurezza.

La proposta in esame ha per definizione una forte **dimensione esterna**, sia perché i paesi terzi possono accedere alle risorse e al sostegno previsti dal regolamento dell'UE sulla cibersolidarietà, utilizzando il sostegno alla risposta agli incidenti fornito dalla riserva dell'UE per la cibersicurezza, sia perché tale riserva necessita di attori del settore privato di paesi terzi. Anche la dimensione esterna dovrebbe essere soggetta al controllo pubblico, cui i poteri legislativi contribuiranno per garantire la partecipazione dei cittadini al processo. La cibersicurezza dovrebbe essere considerata un bene pubblico.

Un altro elemento chiave della proposta in esame è lo sviluppo delle capacità e delle competenze, che non si limita all'investimento nello sviluppo di conoscenze, ma prevede l'investimento nell'accesso di tutti i cittadini alle opportunità di formazione per queste competenze. La relatrice propone di rafforzare il legame con l'**Accademia dell'UE per le competenze in materia di cibersicurezza**, che intende colmare il divario di talenti in tale settore riunendo iniziative pubbliche e private e fornendo formazione e certificazione ai cittadini. Il rafforzamento richiede garanzie per evitare una "fuga di cervelli" e non costituirebbe un rischio per la mobilità dei lavoratori.

La relatrice propone inoltre l'adozione di investimenti e misure attive per sviluppare le competenze in questo settore, considerando che il 2023 è l'Anno europeo delle competenze, e per aumentare la consapevolezza dei cittadini. Le misure dovranno essere concepite in modo da non creare squilibri tra gli Stati membri, dato che l'elevata domanda di manodopera e l'alto livello dei salari nel settore possono produrre una forma di fuga di cervelli verso posizioni meglio retribuite.

Per questi motivi, la relatrice propone di rafforzare le abilità e le competenze specialistiche, interdisciplinari e generali in tutta l'UE, con particolare attenzione alle donne, in quanto il divario di genere persiste nel settore della cibersicurezza, nel quale le donne rappresentano il 20 % della presenza media mondiale[4]. Le donne devono essere presenti e coinvolte nella progettazione del futuro digitale e della sua governance.

La relatrice intende inoltre rafforzare il triangolo tra i centri di competenza nazionali, il Centro europeo di competenza per la cibersicurezza (ECCC) e l'ENISA nello sviluppo di

[4] Risoluzione del Parlamento europeo del 10 giugno 2021 sulla promozione della parità tra donne e uomini in materia di istruzione e occupazione nel campo della scienza, della tecnologia, dell'ingegneria e della matematica (STEM) (2019/2164(INI)) https://www.europarl.europa.eu/doceo/document/TA-9-2021-0296_IT.html.

abilità e competenze. È altresì necessario rafforzare il ruolo dell'**industria** nello **sviluppo delle competenze** e creare partenariati con il **mondo accademico** e gli attori della società civile, contando con l'esperienza, le conoscenze e le specializzazioni regionali e le alleanze con i paesi terzi, al fine di aumentare gli scambi e garantire un approccio globale a sostegno di cittadini, imprese e istituzioni.

La relatrice propone inoltre di condividere la cooperazione in materia di talenti e di misurazione dei danni umani causati dagli attacchi informatici (ad esempio, l'impatto di un attacco ransomware al settore sanitario).

Raccomanda misure volte a includere e accrescere la consapevolezza dei cittadini, senza allarmismi, come ulteriore strumento per garantire la salvaguardia delle nostre democrazie e dei nostri valori fondamentali, così come una maggiore **cultura della cibersicurezza**, che consideri la sicurezza, compresa quella dell'ambiente digitale, come un bene pubblico. In questo modo potremo garantire un modello di democrazia digitale, contrapposto a un modello di autoritarismo digitale, all'insegna della trasparenza, della democrazia e con la certezza che lo sviluppo di una legislazione ex ante può portare.

La relatrice è inoltre del parere che il rafforzamento della **R&I** nel campo della cibersicurezza aumenterà la resilienza e l'autonomia strategica aperta dell'UE. Occorre parimenti garantire sinergie con i programmi di ricerca e innovazione con gli strumenti e le istituzioni esistenti, nonché rafforzare il triangolo della conoscenza per colmare il divario di competenze in tutta l'Unione.

Tale legislazione aumenterà anche la resilienza dell'UE e dei suoi Stati membri, non solo direttamente attraverso le leggi in materia di cibersicurezza e ciberresilienza, ma anche con l'impatto che può avere sullo sviluppo esponenziale dell'intelligenza artificiale e con l'impatto che la regolamentazione dei dati e della riservatezza dei dati può avere sulla cibersicurezza.

Contribuirà inoltre a rispettare l'impegno della **dichiarazione europea sui diritti e i principi digitali per il decennio digitale** per proteggere gli interessi dei cittadini, delle imprese e delle istituzioni pubbliche dai rischi di cibersicurezza e dalla criminalità informatica, comprese le violazioni dei dati e il furto o la manipolazione dell'identità.

Alla luce di quanto precede, la relatrice ritiene che la proposta, compresi lo scudo europeo per la cibersicurezza e il meccanismo per le emergenze di cibersicurezza, dovrebbe essere operativa il più rapidamente possibile, al fine di disporre di un quadro generale ed evitare compartimenti stagni, dato che il ciberspazio non ha frontiere.

ALLEGATO: ENTITÀ O PERSONE
DA CUI LA RELATRICE HA RICEVUTO CONTRIBUTI

Conformemente all'allegato I, articolo 8, del regolamento, la relatrice dichiara di aver ricevuto, nel corso dell'elaborazione della relazione, fino alla sua approvazione in commissione, contributi dalle seguenti entità o persone:

Entità e/o persona
CorwdStrike
CyberPeace institute
Microsoft Corporation
Romanian National Cyber Security Directorate
ENISA
Centro Criptológico Nacional
Permanent Representation of Spain
Trellix
Palo Alto Networks Inc
Committee of the regions rapporteur

L'elenco che precede è compilato sotto l'esclusiva responsabilità della relatrice.

27.10.2023

PARERE DELLA COMMISSIONE PER GLI AFFARI ESTERI

destinato alla commissione per l'industria, la ricerca e l'energia

sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi
(COM(2023)0209) – C9-0136/2023 – 2023/0109(COD))

Relatore per parere: Dragoş Tudorache

Emendamento 1

Proposta di regolamento
Considerando 1

Testo della Commissione	*Emendamento*
(1) L'utilizzo delle tecnologie dell'informazione e della comunicazione e la dipendenza dalle stesse sono diventati fondamentali in tutti i settori di attività economica, dato che le pubbliche amministrazioni, le imprese e i cittadini dell'Unione sono più che mai interconnessi e interdipendenti a livello transettoriale e transfrontaliero.	(1) L'utilizzo delle tecnologie dell'informazione e della comunicazione e la dipendenza dalle stesse sono diventati fondamentali in tutti i settori di attività economica ***e militare***, dato che le pubbliche amministrazioni, le imprese e i cittadini dell'Unione***, come pure i soggetti del settore militare e della difesa,*** sono più che mai interconnessi e interdipendenti a livello transettoriale e transfrontaliero.

Emendamento 2

Proposta di regolamento
Considerando 2

Testo della Commissione	*Emendamento*
(2) Attualmente si registra un incremento dell'entità, della frequenza e dell'impatto degli incidenti di cibersicurezza, compresi gli attacchi alle	(2) Attualmente si registra un incremento dell'entità, della frequenza e dell'impatto degli incidenti di cibersicurezza, compresi gli attacchi alle

catene di approvvigionamento con finalità di ciberspionaggio, di ransomware o di perturbazione, che rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi. In considerazione del rapido evolversi del panorama delle minacce, il rischio di possibili incidenti su vasta scala, che possono provocare interruzioni o danni significativi a infrastrutture critiche, richiede una maggiore preparazione a tutti i livelli del quadro di cibersicurezza dell'Unione. ***Tale minaccia va*** oltre l'aggressione militare della Russia nei confronti dell'Ucraina ***ed è destinata*** a persistere, data la molteplicità di soggetti allineati con le autorità di governo, criminali e hacktivisti coinvolti nelle attuali tensioni geopolitiche. Tali incidenti possono ostacolare l'erogazione di servizi pubblici e lo svolgimento di attività economiche, anche in settori critici o altamente critici, generare consistenti perdite finanziarie, minare la fiducia degli utenti nonché causare gravi danni all'economia dell'Unione, e potrebbero persino avere conseguenze sulla salute o essere potenzialmente letali. Inoltre gli incidenti di cibersicurezza sono imprevedibili, in quanto spesso si verificano ed evolvono in periodi di tempo molto brevi, non sono circoscritti a una determinata zona geografica e si verificano simultaneamente o si diffondono istantaneamente in numerosi paesi.

catene di approvvigionamento con finalità di ciberspionaggio, di ransomware o di perturbazione, che rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi. In considerazione del rapido evolversi del panorama delle minacce, il rischio di possibili incidenti su vasta scala, che possono provocare interruzioni o danni significativi a infrastrutture critiche, richiede una maggiore preparazione a tutti i livelli del quadro di cibersicurezza dell'Unione. ***La gravità di queste minacce è diventata ancora più rilevante a causa del ritorno della guerra sul nostro continente. Tali minacce vanno*** oltre l'aggressione militare della Russia nei confronti dell'Ucraina ***e sono destinate*** a persistere, data la molteplicità di soggetti allineati con le autorità di governo, criminali e hacktivisti coinvolti nelle attuali tensioni geopolitiche. Tali incidenti possono ostacolare l'erogazione di servizi pubblici e lo svolgimento di attività economiche, anche in settori critici o altamente critici, generare consistenti perdite finanziarie, minare la fiducia degli utenti nonché causare gravi danni all'economia ***e alla sicurezza*** dell'Unione, e potrebbero persino avere conseguenze sulla salute o essere potenzialmente letali ***attraverso l'eventuale compromissione degli impianti connessi alla sicurezza locale o nazionale***. Inoltre gli incidenti di cibersicurezza sono imprevedibili, in quanto spesso si verificano ed evolvono in periodi di tempo molto brevi, non sono circoscritti a una determinata zona geografica e si verificano simultaneamente o si diffondono istantaneamente in numerosi paesi. ***La cibersicurezza è importante per proteggere i nostri valori europei e garantisce il funzionamento delle nostre democrazie proteggendo le nostre infrastrutture elettorali e le nostre procedure democratiche da qualsiasi ingerenza straniera.***

Emendamento 3

Proposta di regolamento
Considerando 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	(2 bis) La cibersicurezza è fondamentale per mantenere la nostra Unione al sicuro e impedire che soggetti malintenzionati, statali e non statali, compromettano la nostra democrazia, la nostra economia e la nostra sicurezza. È necessario prevenire la formazione di un panorama frammentato, in quanto tale situazione non rappresenterebbe un approccio adeguato, in particolare di fronte alla sfida di un futuro attacco informatico su larga scala rivolto in contemporanea a diversi Stati membri o infrastrutture critiche transnazionali. È dunque necessario un organismo dell'Unione che funga da piattaforma di coordinamento per tutti gli strumenti, i fondi e i meccanismi esistenti e futuri in materia di cibersicurezza.

Emendamento 4

Proposta di regolamento
Considerando 3

Testo della Commissione	*Emendamento*
(3) Occorre rafforzare la posizione competitiva del settore industriale e di quello dei servizi dell'Unione nell'ambito dell'economia digitalizzata e sostenerne la trasformazione digitale, consolidando il livello di cibersicurezza nel mercato unico digitale. Come raccomandato in tre diverse proposte della Conferenza sul futuro dell'Europa[16], è necessario accrescere la resilienza dei cittadini, delle imprese e dei soggetti che gestiscono infrastrutture critiche contro le crescenti minacce alla cibersicurezza, che possono avere conseguenze devastanti a livello sociale ed	(3) Occorre rafforzare la posizione competitiva del settore industriale e di quello dei servizi dell'Unione nell'ambito dell'economia digitalizzata e sostenerne la trasformazione digitale, consolidando il livello di cibersicurezza nel mercato unico digitale. Come raccomandato in tre diverse proposte della Conferenza sul futuro dell'Europa[16], è necessario accrescere la resilienza dei cittadini, delle imprese e dei soggetti che gestiscono infrastrutture critiche contro le crescenti minacce alla cibersicurezza, che possono avere conseguenze devastanti a livello sociale ed

economico. Occorre quindi investire in infrastrutture e servizi che permettano di velocizzare il rilevamento delle minacce e degli incidenti di cibersicurezza e di assicurare una risposta più rapida; inoltre gli Stati membri necessitano di assistenza per garantire una migliore preparazione e capacità di risposta più adeguate agli incidenti di cibersicurezza significativi e su vasta scala. L'Unione dovrebbe inoltre accrescere le sue capacità in questi settori, in particolare per quanto riguarda la raccolta e l'analisi di dati sulle minacce e sugli incidenti di cibersicurezza.

[16] https://futureu.europa.eu/it/

economico. Occorre quindi investire in infrastrutture e servizi che permettano di velocizzare il rilevamento delle minacce e degli incidenti di cibersicurezza e di assicurare una risposta più rapida; inoltre gli Stati membri necessitano di assistenza per garantire una migliore preparazione e capacità di risposta più adeguate agli incidenti di cibersicurezza significativi e su vasta scala. L'Unione dovrebbe inoltre accrescere le sue capacità in questi settori, in particolare per quanto riguarda la raccolta e l'analisi di dati sulle minacce e sugli incidenti di cibersicurezza***, come pure la sua abilità di reagire in modo proattivo e risoluto a tali minacce e incidenti***.

[16] https://futureu.europa.eu/it/

Emendamento 5

Proposta di regolamento
Considerando 4

Testo della Commissione	*Emendamento*
(4) L'Unione ha già adottato una serie di misure per ridurre le vulnerabilità e accrescere la resilienza delle infrastrutture e dei soggetti critici contro i rischi di cibersicurezza, in particolare la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[17], la raccomandazione (UE) 2017/1584 della Commissione[18], la direttiva 2013/40/UE del Parlamento europeo e del Consiglio[19] e il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[20]. Inoltre la raccomandazione del Consiglio su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche invita gli Stati membri ad adottare misure urgenti ed efficaci e a cooperare lealmente, efficacemente, in modo solidale e coordinato tra loro, con la Commissione e le altre autorità pubbliche competenti,	(4) L'Unione ha già adottato una serie di misure per ridurre le vulnerabilità e accrescere la resilienza delle infrastrutture e dei soggetti critici contro i rischi di cibersicurezza, in particolare la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[17], la raccomandazione (UE) 2017/1584 della Commissione[18], la direttiva 2013/40/UE del Parlamento europeo e del Consiglio[19] e il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[20]. Inoltre la raccomandazione del Consiglio su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche invita gli Stati membri ad adottare misure urgenti ed efficaci e a cooperare lealmente, efficacemente ***e proattivamente***, in modo solidale e coordinato tra loro, con la Commissione e le altre autorità pubbliche

nonché con i soggetti interessati, al fine di migliorare la resilienza delle infrastrutture critiche utilizzate per fornire servizi essenziali nel mercato interno.

competenti, nonché con i soggetti interessati, al fine di migliorare la resilienza delle infrastrutture critiche utilizzate per fornire servizi essenziali nel mercato interno. ***Inoltre, nel 2022 marzo l'Unione ha approvato e lanciato la bussola strategica per la sicurezza e la difesa, incentrata tra l'altro sul rafforzamento della cibersicurezza e sul potenziamento della cooperazione internazionale con gli alleati e i partner democratici che condividono gli stessi principi, in particolare in questo settore. La cibersicurezza è stata inoltre un punto focale della terza dichiarazione congiunta sulla cooperazione UE-NATO, adottata di recente nel gennaio 2023. In particolare, la relazione finale di valutazione della task force UE-NATO raccomandava di sfruttare appieno le sinergie tra l'UE e la NATO[1], compreso lo scambio di migliori pratiche tra gli attori civili e militari per quanto concerne l'attuazione delle pertinenti politiche e normative in materia di cibersicurezza.***

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_it

---

[17] 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 (GU L 333 del 27.12.2022).

[18] Raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (GU L 239 del 19.9.2017, pag. 36).

[19] Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi

[17] 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 (GU L 333 del 27.12.2022).

[18] Raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (GU L 239 del 19.9.2017, pag. 36).

[19] Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi

di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio (GU L 218 del 14.8.2013, pag. 8).

[20] 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") (GU L 151 del 7.6.2019, pag. 15).

di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio (GU L 218 del 14.8.2013, pag. 8).

[20] 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") (GU L 151 del 7.6.2019, pag. 15).

Emendamento 6

Proposta di regolamento
Considerando 6

Testo della Commissione	*Emendamento*
(6) La comunicazione congiunta sulla politica di ciberdifesa dell'UE[22], adottata il 10 novembre 2022, ha annunciato un'iniziativa dell'UE per la cibersolidarietà con gli obiettivi seguenti: rafforzare le capacità comuni dell'UE in materia di rilevamento, conoscenza situazionale e risposta, promuovendo la realizzazione di un'infrastruttura unionale dei centri operativi di sicurezza ("SOC"), sostenere la costituzione graduale di una forza di riserva per la cibersicurezza a livello di UE, con servizi prestati da operatori privati di fiducia, e le prove presso soggetti critici al fine di rilevare potenziali vulnerabilità basate sulle valutazioni del rischio effettuate a livello UE.	(6) La comunicazione congiunta sulla politica di ciberdifesa dell'UE[22], adottata il 10 novembre 2022, ha annunciato un'iniziativa dell'UE per la cibersolidarietà con gli obiettivi seguenti: rafforzare le capacità comuni dell'UE in materia di rilevamento, conoscenza situazionale e risposta, promuovendo la realizzazione di un'infrastruttura unionale dei centri operativi di sicurezza ("SOC"), sostenere la costituzione graduale di una forza di riserva per la cibersicurezza a livello di UE, con servizi prestati da operatori privati di fiducia, e le prove presso soggetti critici al fine di rilevare potenziali vulnerabilità basate sulle valutazioni del rischio effettuate a livello UE. ***Inoltre, anche la rapida evoluzione del panorama delle minacce informatiche e la rapidità dello sviluppo tecnologico dimostrano la necessità di rafforzare il coordinamento e la cooperazione civile-militare, come sottolineato dal Consiglio nelle sue conclusioni sulla politica dell'UE in***

	materia di ciberdifesa[1].
	[1] Conclusioni del Consiglio sulla politica di ciberdifesa dell'UE, approvate dal Consiglio nella sessione del 22 maggio 2023 (9618/23).
[22] Comunicazione congiunta al Parlamento europeo e al Consiglio – La politica di ciberdifesa dell'UE (JOIN(2022) 49 final).	[22] Comunicazione congiunta al Parlamento europeo e al Consiglio – La politica di ciberdifesa dell'UE (JOIN(2022) 49 final).

Emendamento 7

Proposta di regolamento
Considerando 6 bis (nuovo)

Testo della Commissione	*Emendamento*
	(6 bis) Data la mancanza di una linea netta di demarcazione fra le questioni civili e militari e la natura di duplice uso degli strumenti e delle tecnologie cibernetiche, è necessario un approccio globale e olistico allo spazio digitale. Nel caso di un incidente e di una crisi di cibersicurezza su vasta scala che coinvolgano più di uno Stato membro, è opportuno stabilire un'adeguata gestione e governance delle crisi. Tali strutture dovrebbero organizzare lo scambio di informazioni, il coordinamento e la cooperazione con le strutture di sicurezza esterna e di gestione militare delle crisi dell'Unione e gli organismi degli Stati membri incaricati della sicurezza e della difesa (la comunità di ciberdifesa). Ciò dovrebbe applicarsi anche alle operazioni e alle missioni di politica di sicurezza e di difesa comune condotte dall'Unione per assicurare la pace e la stabilità nel suo vicinato e oltre.

Emendamento 8

Proposta di regolamento
Considerando 7

Testo della Commissione	*Emendamento*
(7) Occorre rafforzare il rilevamento e la conoscenza situazionale delle minacce e degli incidenti informatici in tutta l'Unione e intensificare la solidarietà migliorando la preparazione e le capacità degli Stati membri e dell'Unione di rispondere agli incidenti di cibersicurezza significativi e su vasta scala. Di conseguenza si dovrebbe realizzare un'infrastruttura paneuropea di SOC (ciberscudo europeo) per sviluppare e potenziare capacità comuni in materia di rilevamento e conoscenza situazionale, creare un meccanismo per le emergenze di cibersicurezza al fine di sostenere gli Stati membri nella preparazione e nella risposta agli incidenti di cibersicurezza significativi e su vasta scala e nella ripresa immediata dagli stessi, e istituire un meccanismo di riesame degli incidenti di cibersicurezza per riesaminare e valutare specifici incidenti significativi o su vasta scala. La realizzazione di tali azioni non pregiudica gli articoli 107 e 108 del trattato sul funzionamento dell'Unione europea ("TFUE").	(7) Occorre rafforzare il rilevamento e la conoscenza situazionale delle minacce e degli incidenti informatici in tutta l'Unione e intensificare la solidarietà migliorando la preparazione e le capacità degli Stati membri e dell'Unione di rispondere agli incidenti di cibersicurezza significativi e su vasta scala. Di conseguenza si dovrebbe realizzare un'infrastruttura paneuropea di SOC (ciberscudo europeo) per sviluppare e potenziare capacità comuni in materia di rilevamento e conoscenza situazionale, creare un meccanismo per le emergenze di cibersicurezza al fine di sostenere gli Stati membri nella preparazione e nella risposta agli incidenti di cibersicurezza significativi e su vasta scala e nella ripresa immediata dagli stessi***, compresi gli incidenti che riguardano più di uno Stato membro, istituire, ove possibile e necessario, un meccanismo per le emergenze di cibersicurezza che dovrebbe organizzare la condivisione di informazioni e la cooperazione con le autorità di difesa degli Stati membri con il sostegno delle istituzioni, degli organi e degli organismi dell'UE (la comunità di ciberdifesa dell'UE)***, e istituire un meccanismo di riesame degli incidenti di cibersicurezza per riesaminare e valutare specifici incidenti significativi o su vasta scala. ***Tali nuove strutture dovrebbero inoltre sostenere le operazioni e le missioni PSDC dell'UE.*** La realizzazione di tali azioni non pregiudica gli articoli 107 e 108 del trattato sul funzionamento dell'Unione europea ("TFUE").

Emendamento 9

Proposta di regolamento
Considerando 11

Testo della Commissione	*Emendamento*
(11) Ai fini di una sana gestione finanziaria è opportuno stabilire norme specifiche in materia di riporto degli stanziamenti d'impegno e di pagamento inutilizzati. Pur rispettando il principio secondo cui il bilancio dell'Unione è fissato annualmente, il presente regolamento dovrebbe, in considerazione della natura imprevedibile, eccezionale e specifica del panorama della cibersicurezza, prevedere la possibilità di riportare i fondi inutilizzati oltre a quelli stabiliti nel regolamento finanziario, massimizzando così la capacità del meccanismo per le emergenze di cibersicurezza di sostenere gli Stati membri nel contrastare efficacemente le minacce informatiche.	(11) Ai fini di una sana gestione finanziaria è opportuno stabilire norme specifiche in materia di riporto degli stanziamenti d'impegno e di pagamento inutilizzati. Pur rispettando il principio secondo cui il bilancio dell'Unione è fissato annualmente, il presente regolamento dovrebbe, in considerazione della natura imprevedibile, eccezionale e specifica del panorama della cibersicurezza, prevedere la possibilità di riportare i fondi inutilizzati oltre a quelli stabiliti nel regolamento finanziario, massimizzando così la capacità del meccanismo per le emergenze di cibersicurezza di sostenere gli Stati membri nel contrastare efficacemente le minacce informatiche. ***Tali norme specifiche consentirebbero inoltre un sostegno finanziario a più lungo termine per gli appalti congiunti di strumenti e infrastrutture ultrasicuri di prossima generazione, al fine di migliorare le capacità collettive di rilevamento mediante l'utilizzo dell'intelligenza artificiale (IA) e dell'analisi dei dati più recenti.***

Emendamento 10

Proposta di regolamento
Considerando 13

Testo della Commissione	*Emendamento*
(13) Ogni Stato membro dovrebbe designare un organismo pubblico a livello nazionale, incaricato di coordinare le attività di rilevamento delle minacce informatiche in tale Stato membro. Questi SOC nazionali dovrebbero fungere da punto di riferimento e porta di accesso a livello nazionale per la partecipazione al ciberscudo europeo e garantire che le informazioni sulle minacce informatiche provenienti da soggetti pubblici e privati	(13) Ogni Stato membro dovrebbe designare un organismo pubblico a livello nazionale, incaricato di coordinare le attività di rilevamento delle minacce informatiche in tale Stato membro. Questi SOC nazionali dovrebbero fungere da punto di riferimento e porta di accesso a livello nazionale per la partecipazione al ciberscudo europeo e garantire che le informazioni sulle minacce informatiche provenienti da soggetti pubblici e privati

siano condivise e raccolte a livello nazionale in modo efficace e semplificato.

siano condivise e raccolte a livello nazionale in modo efficace e semplificato. ***Ove possibile e necessario, i SOC dovrebbero altresì consentire la partecipazione di soggetti del settore della difesa, istituendo un "pilastro della difesa" in termini di governance e di tipo di informazioni condivise, come stabilito nella comunicazione congiunta sulla politica di ciberdifesa dell'UE[1] e sostenuto dall'alto rappresentante.***

[1] Comunicazione congiunta al Parlamento europeo e al Consiglio – La politica di ciberdifesa dell'UE (JOIN(2022) 49 final).

Emendamento 11

Proposta di regolamento
Considerando 14

Testo della Commissione	*Emendamento*
(14) Nell'ambito del ciberscudo europeo è opportuno istituire diversi centri operativi di cibersicurezza transfrontalieri ("SOC transfrontalieri") che, a loro volta, dovrebbero riunire i SOC nazionali di almeno tre Stati membri, in modo da sfruttare appieno i vantaggi derivanti dal rilevamento delle minacce transfrontaliere e dalla gestione e condivisione delle informazioni. L'obiettivo generale dei SOC transfrontalieri dovrebbe essere quello di rafforzare le capacità di analisi, prevenzione e rilevamento delle minacce alla cibersicurezza e di favorire l'elaborazione di analisi di alta qualità sulle minacce alla cibersicurezza, in particolare mediante la condivisione di dati provenienti da varie fonti, pubbliche o private, nonché tramite la condivisione e l'uso congiunto di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi e prevenzione in un contesto di fiducia. Tali SOC dovrebbero garantire nuove capacità aggiuntive,	(14) Nell'ambito del ciberscudo europeo è opportuno istituire diversi centri operativi di cibersicurezza transfrontalieri ("SOC transfrontalieri") che, a loro volta, dovrebbero riunire i SOC nazionali di almeno tre Stati membri***, compreso un "pilastro della difesa"***, in modo da sfruttare appieno i vantaggi derivanti dal rilevamento delle minacce transfrontaliere e dalla gestione e condivisione delle informazioni. L'obiettivo generale dei SOC transfrontalieri dovrebbe essere quello di rafforzare le capacità di analisi, prevenzione e rilevamento delle minacce alla cibersicurezza e di favorire l'elaborazione di analisi di alta qualità sulle minacce alla cibersicurezza, in particolare mediante la condivisione di dati provenienti da varie fonti, pubbliche o private ***e, ove possibile e necessario, militari***, ***con orientamenti sufficienti per lo scambio di informazioni,*** nonché tramite la condivisione e l'uso congiunto di strumenti all'avanguardia e lo sviluppo

basandosi sui SOC e sui gruppi di intervento per la sicurezza informatica in caso di incidente ("CSIRT") esistenti nonché su altri soggetti pertinenti e integrandoli.

congiunto di capacità di rilevamento, analisi e prevenzione in un contesto di fiducia. Tali SOC dovrebbero garantire nuove capacità aggiuntive, basandosi sui SOC e sui gruppi di intervento per la sicurezza informatica in caso di incidente ("CSIRT") esistenti nonché su altri soggetti pertinenti e integrandoli.

Emendamento 12

Proposta di regolamento
Considerando 15

Testo della Commissione	*Emendamento*
(15) A livello nazionale, il monitoraggio, il rilevamento e l'analisi delle minacce informatiche sono solitamente garantiti dai SOC di soggetti pubblici e privati, in combinazione con i CSIRT. Questi ultimi inoltre scambiano informazioni nel contesto della rete di CSIRT, conformemente a quanto disposto dalla direttiva (UE) 2022/2555. I SOC transfrontalieri dovrebbero costituire una nuova capacità complementare alla rete di CSIRT, mettendo in comune e condividendo i dati sulle minacce alla cibersicurezza provenienti da soggetti pubblici e privati, accrescendo il valore di tali dati mediante l'analisi di esperti, infrastrutture acquisite congiuntamente e strumenti all'avanguardia, e contribuendo allo sviluppo delle capacità e della ***sovranità tecnologica*** dell'Unione.	(15) A livello nazionale, il monitoraggio, il rilevamento e l'analisi delle minacce informatiche sono solitamente garantiti dai SOC di soggetti pubblici e privati, in combinazione con i CSIRT. Questi ultimi inoltre scambiano informazioni nel contesto della rete di CSIRT, conformemente a quanto disposto dalla direttiva (UE) 2022/2555. I SOC transfrontalieri dovrebbero costituire una nuova capacità complementare alla rete di CSIRT, mettendo in comune e condividendo i dati sulle minacce alla cibersicurezza provenienti da soggetti pubblici e privati, accrescendo il valore di tali dati mediante l'analisi di esperti, infrastrutture acquisite congiuntamente e strumenti all'avanguardia, e contribuendo allo sviluppo delle capacità e della ***resilienza*** dell'Unione.

Emendamento 13

Proposta di regolamento
Considerando 16

Testo della Commissione	*Emendamento*
(16) I SOC transfrontalieri dovrebbero fungere da punto centrale in grado di consentire un'ampia condivisione di dati	(16) I SOC transfrontalieri dovrebbero fungere da punto centrale in grado di consentire un'ampia condivisione di dati

pertinenti e di analisi delle minacce informatiche e permettere la diffusione di informazioni sulle minacce tra più soggetti di diversa natura (ad esempio, squadre di pronto intervento informatico ("CERT"), CSIRT, centri di analisi e condivisione delle informazioni ("ISAC"), operatori di infrastrutture critiche). Le informazioni scambiate tra i partecipanti a un SOC transfrontaliero potrebbero includere dati provenienti da reti e sensori, feed di analisi delle minacce, indicatori di compromissione e informazioni contestualizzate su incidenti, minacce e vulnerabilità. I SOC transfrontalieri dovrebbero inoltre stipulare accordi di cooperazione con altri SOC transfrontalieri.

pertinenti e di analisi delle minacce informatiche e permettere la diffusione di informazioni sulle minacce tra più soggetti di diversa natura (ad esempio, squadre di pronto intervento informatico ("CERT"), CSIRT, centri di analisi e condivisione delle informazioni ("ISAC"), operatori di infrastrutture critiche***, come pure la comunità di ciberdifesa***). Le informazioni scambiate tra i partecipanti a un SOC transfrontaliero potrebbero includere dati provenienti da reti e sensori, feed di analisi delle minacce, indicatori di compromissione e informazioni contestualizzate su incidenti, minacce e vulnerabilità. I SOC transfrontalieri dovrebbero inoltre stipulare accordi di cooperazione con altri SOC transfrontalieri ***e, una volta istituita, con una rete operativa per le squadre militari di pronto intervento informatico "milCERTs" (MICNET)***.

Emendamento 14

Proposta di regolamento
Considerando 17

Testo della Commissione	*Emendamento*
(17) La condivisione della conoscenza situazionale tra le autorità competenti è un prerequisito indispensabile per la preparazione e il coordinamento a livello dell'Unione in caso di incidenti di cibersicurezza significativi e su vasta scala. La direttiva (UE) 2022/2555 istituisce EU-CyCLONe al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala e di garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione. La raccomandazione (UE) 2017/1584 relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala definisce il ruolo di tutti i soggetti	(17) La condivisione della conoscenza situazionale tra le autorità competenti è un prerequisito indispensabile per la preparazione e il coordinamento a livello dell'Unione in caso di incidenti di cibersicurezza significativi e su vasta scala. La direttiva (UE) 2022/2555 istituisce EU-CyCLONe al fine di sostenere la gestione coordinata a livello operativo degli incidenti e delle crisi di cibersicurezza su vasta scala e di garantire il regolare scambio di informazioni pertinenti tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione. La raccomandazione (UE) 2017/1584 relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala definisce il ruolo di tutti i soggetti

interessati. La direttiva (UE) 2022/2555 ricorda altresì le responsabilità della Commissione nell'ambito del meccanismo unionale di protezione civile ("UCPM") istituito dalla decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio, nonché la sua responsabilità per quanto riguarda la fornitura di relazioni analitiche per i dispositivi integrati per la risposta politica alle crisi ("IPCR") ai sensi della decisione di esecuzione (UE) 2018/1993. Pertanto, nelle situazioni in cui ottengono informazioni relative a un incidente di cibersicurezza potenziale o in corso su vasta scala, i SOC transfrontalieri dovrebbero fornire informazioni pertinenti a EU-CyCLONe, alla rete di CSIRT e alla Commissione. In particolare, a seconda della situazione, le informazioni da condividere potrebbero includere informazioni tecniche, informazioni sulla natura e sulle motivazioni dell'autore di un attacco informatico o di un potenziale autore nonché informazioni non tecniche di livello superiore su un incidente di cibersicurezza potenziale o in corso su vasta scala. In questo contesto è opportuno prestare la dovuta attenzione al principio della necessità di conoscere e alla natura potenzialmente sensibile delle informazioni condivise.

interessati. La direttiva (UE) 2022/2555 ricorda altresì le responsabilità della Commissione nell'ambito del meccanismo unionale di protezione civile ("UCPM") istituito dalla decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio, nonché la sua responsabilità per quanto riguarda la fornitura di relazioni analitiche per i dispositivi integrati per la risposta politica alle crisi ("IPCR") ai sensi della decisione di esecuzione (UE) 2018/1993. Pertanto, nelle situazioni in cui ottengono informazioni relative a un incidente di cibersicurezza potenziale o in corso su vasta scala, i SOC transfrontalieri dovrebbero fornire informazioni pertinenti a EU-CyCLONe, alla rete di CSIRT***, alla comunità di ciberdifesa*** e alla Commissione. In particolare, a seconda della situazione, le informazioni da condividere potrebbero includere informazioni tecniche, informazioni sulla natura e sulle motivazioni dell'autore di un attacco informatico o di un potenziale autore nonché informazioni non tecniche di livello superiore su un incidente di cibersicurezza potenziale o in corso su vasta scala. In questo contesto è opportuno prestare la dovuta attenzione al principio della necessità di conoscere e alla natura potenzialmente sensibile delle informazioni condivise.

Emendamento 15

Proposta di regolamento
Considerando 19

Testo della Commissione	*Emendamento*
(19) Per consentire lo scambio di dati sulle minacce alla cibersicurezza provenienti da varie fonti, su vasta scala, in un contesto di fiducia, i soggetti che partecipano al ciberscudo europeo dovrebbero essere dotati di strumenti, apparecchiature e infrastrutture all'avanguardia e altamente sicuri. Ciò	(19) Per consentire lo scambio di dati sulle minacce alla cibersicurezza provenienti da varie fonti, su vasta scala, in un contesto di fiducia, i soggetti che partecipano al ciberscudo europeo dovrebbero essere dotati di strumenti, apparecchiature e infrastrutture all'avanguardia e altamente sicuri***, esclusi i***

dovrebbe consentire di migliorare le capacità collettive di rilevamento e di avvertire tempestivamente le autorità e i soggetti competenti, in particolare utilizzando le più recenti tecnologie di intelligenza artificiale e di analisi dei dati.	***fornitori ad alto rischio di prodotti critici con elementi digitali***. Ciò dovrebbe consentire di migliorare le capacità collettive di rilevamento e di avvertire tempestivamente le autorità e i soggetti competenti, in particolare utilizzando le più recenti tecnologie di intelligenza artificiale e di analisi dei dati. ***L'utilizzo dell'intelligenza artificiale dovrebbe essere sottoposto a una sorveglianza umana ed è opportuno garantire per chi esercita tale funzione un livello sufficiente di alfabetizzazione nell'ambito dell'IA, nonché il sostegno e l'autorità necessari.***

Emendamento 16

Proposta di regolamento
Considerando 19 bis (nuovo)

Testo della Commissione	*Emendamento*
	(19 bis) In conformità al regolamento [XX/XXXX (regolamento sulla resilienza informatica)], i soggetti che partecipano al ciberscudo europeo dovrebbero soddisfare anche i requisiti stabiliti nel presente regolamento per tutti i prodotti con elementi digitali. Alla luce dei crescenti rischi derivanti dalle dipendenze economiche, è necessario ridurre al minimo l'esposizione a fornitori ad alto rischio di prodotti critici mediante un quadro strategico comune per la sicurezza economica dell'UE. La dipendenza da fornitori ad alto rischio di prodotti critici con elementi digitali comporta un rischio strategico che dovrebbe essere affrontato a livello dell'Unione, in particolare se un paese è impegnato in spionaggio economico o coercizione economica e se la sua legislazione impone l'accesso arbitrario a qualsiasi tipo di operazioni o dati aziendali, in particolare quando i prodotti critici sono destinati a essere usati dai soggetti essenziali di cui alla direttiva

(UE) 2022/2555.

Emendamento 17

Proposta di regolamento
Considerando 20

Testo della Commissione	*Emendamento*
(20) Mediante la raccolta, la condivisione e lo scambio di dati, il ciberscudo europeo dovrebbe rafforzare la sovranità tecnologica dell'Unione. La condivisione di dati selezionati di alta qualità dovrebbe inoltre contribuire allo sviluppo di tecnologie avanzate di intelligenza artificiale e di analisi dei dati e dovrebbe essere facilitata dal collegamento del ciberscudo europeo con l'infrastruttura paneuropea di calcolo ad alte prestazioni istituita dal regolamento (UE) 2021/1173 del Consiglio[25].	(20) Mediante la raccolta, la condivisione e lo scambio di dati, il ciberscudo europeo dovrebbe rafforzare la sovranità tecnologica***, l'autonomia strategica, la competitività e la resilienza*** dell'Unione. La condivisione di dati selezionati di alta qualità dovrebbe inoltre contribuire allo sviluppo di tecnologie avanzate di intelligenza artificiale e di analisi dei dati e dovrebbe essere facilitata dal collegamento del ciberscudo europeo con l'infrastruttura paneuropea di calcolo ad alte prestazioni istituita dal regolamento (UE) 2021/1173 del Consiglio[25].
[25] Regolamento (UE) 2021/1173 del Consiglio, del 13 luglio 2021, relativo all'istituzione dell'impresa comune per il calcolo ad alte prestazioni europeo e che abroga il regolamento (UE) 2018/1488 (GU L 256 del 19.7.2021, pag. 3).	[25] Regolamento (UE) 2021/1173 del Consiglio, del 13 luglio 2021, relativo all'istituzione dell'impresa comune per il calcolo ad alte prestazioni europeo e che abroga il regolamento (UE) 2018/1488 (GU L 256 del 19.7.2021, pag. 3).

Emendamento 18

Proposta di regolamento
Considerando 25

Testo della Commissione	*Emendamento*
(25) Il meccanismo per le emergenze di cibersicurezza dovrebbe fornire un sostegno agli Stati membri, integrando le loro misure e le loro risorse nonché altre opzioni di sostegno esistenti in caso di risposta agli incidenti di cibersicurezza significativi e su vasta scala e di ripresa immediata dagli stessi, come i servizi	(25) Il meccanismo per le emergenze di cibersicurezza dovrebbe fornire un sostegno agli Stati membri, integrando le loro misure e le loro risorse nonché altre opzioni di sostegno esistenti in caso di risposta agli incidenti di cibersicurezza significativi e su vasta scala e di ripresa immediata dagli stessi, come i servizi

forniti dall'Agenzia dell'Unione europea per la cibersicurezza ("ENISA") conformemente al suo mandato, la risposta coordinata e l'assistenza della rete di CSIRT, il sostegno a strategie di attenuazione offerto da EU-CyCLONe, nonché l'assistenza reciproca tra gli Stati membri, anche nel contesto dell'articolo 42, paragrafo 7, TUE, i gruppi di risposta rapida agli incidenti informatici della PESCO***[26]*** e i gruppi di risposta rapida alle minacce ibride. Tale meccanismo dovrebbe rispondere alla necessità di garantire la disponibilità di mezzi specializzati per sostenere la preparazione e la risposta agli incidenti di cibersicurezza in tutta l'Unione e nei paesi terzi.

---

[26] Decisione (PESC) 2017/2315 del Consiglio, dell'11 dicembre 2017, che istituisce la cooperazione strutturata permanente (PESCO) e fissa l'elenco degli Stati membri partecipanti.

forniti dall'Agenzia dell'Unione europea per la cibersicurezza ("ENISA") conformemente al suo mandato, la risposta coordinata e l'assistenza della rete di CSIRT, il sostegno a strategie di attenuazione offerto da EU-CyCLONe, nonché l'assistenza reciproca tra gli Stati membri, anche nel contesto dell'articolo 42, paragrafo 7, TUE, i gruppi di risposta rapida agli incidenti informatici della PESCO***[1], il nuovo centro di coordinamento nel settore informatico e dell'informazione (CIDCC) e il centro di coordinamento della ciberdifesa dell'UE (EUCDCC) che dovrebbe succedergli,*** e i gruppi di risposta rapida alle minacce ibride. Tale meccanismo dovrebbe rispondere alla necessità di garantire la disponibilità di mezzi specializzati per sostenere la preparazione e la risposta agli incidenti di cibersicurezza in tutta l'Unione e nei paesi terzi***, in particolare nei paesi candidati all'adesione all'UE che sono allineati con la politica estera e di sicurezza comune e con la politica di sicurezza e di difesa comune dell'Unione, sostenendoli nel potenziamento delle loro capacità informatiche e rafforzando la cooperazione transfrontaliera e regionale in materia di cibersicurezza tra tali paesi candidati***.

[1] Decisione (PESC) 2017/2315 del Consiglio, dell'11 dicembre 2017, che istituisce la cooperazione strutturata permanente (PESCO) e fissa l'elenco degli Stati membri partecipanti.

---

[26] Decisione (PESC) 2017/2315 del Consiglio, dell'11 dicembre 2017, che istituisce la cooperazione strutturata permanente (PESCO) e fissa l'elenco degli Stati membri partecipanti.

Emendamento 19

Proposta di regolamento
Considerando 26

Testo della Commissione	*Emendamento*
(26) Il presente strumento non pregiudica le procedure e i quadri di coordinamento della risposta alle crisi a livello dell'Unione, in particolare l'UCPM[27], gli IPCR[28] e la direttiva (UE) 2022/2555, e può contribuire alle azioni attuate nel contesto dell'articolo 42, paragrafo 7, TUE o nelle situazioni definite nell'articolo 222 TFUE oppure integrare tali azioni. L'utilizzo del presente strumento dovrebbe inoltre essere coordinato***, laddove opportuno,*** con l'attuazione delle misure del pacchetto di strumenti della diplomazia informatica.	(26) Il presente strumento non pregiudica le procedure e i quadri di coordinamento della risposta alle crisi a livello dell'Unione, in particolare l'UCPM[27], gli IPCR[28] e la direttiva (UE) 2022/2555, e può contribuire alle azioni attuate nel contesto dell'articolo 42, paragrafo 7, TUE o nelle situazioni definite nell'articolo 222 TFUE oppure integrare tali azioni. L'utilizzo del presente strumento dovrebbe inoltre essere coordinato con l'attuazione delle misure del pacchetto di strumenti della diplomazia informatica***, migliorando la cooperazione a livello strategico, operativo e tecnico tra la comunità di ciberdifesa e altre comunità informatiche, in particolare al fine di rafforzare le capacità nei confronti delle minacce alla cibersicurezza provenienti dall'esterno dell'Unione, comprese le misure restrittive, che possono essere utilizzate per prevenire attività informatiche malevoli e per rispondervi***.
[27] Decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio, del 17 dicembre 2013, su un meccanismo unionale di protezione civile (GU L 347 del 20.12.2013, pag. 924).	[27] Decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio, del 17 dicembre 2013, su un meccanismo unionale di protezione civile (GU L 347 del 20.12.2013, pag. 924).
[28] Dispositivi integrati per la risposta politica alle crisi (IPCR) e conformemente alla raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala.	[28] Dispositivi integrati per la risposta politica alle crisi (IPCR) e conformemente alla raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala.

Emendamento 20

Proposta di regolamento
Considerando 28

Testo della Commissione	*Emendamento*
(28) Secondo quanto disposto dalla direttiva (UE) 2022/2555 gli Stati membri sono tenuti a designare o istituire una o più autorità di gestione delle crisi informatiche e a garantire che tali autorità dispongano di risorse adeguate per svolgere i loro compiti in modo efficace ed efficiente. La direttiva impone inoltre gli Stati membri di individuare le capacità, le risorse e le procedure da poter impiegare in caso di crisi, nonché di adottare un piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala, in cui siano definiti gli obiettivi e le modalità di gestione degli stessi. Gli Stati membri sono altresì tenuti a istituire uno o più CSIRT che siano incaricati di gestire gli incidenti, secondo un processo ben definito, e che si occupino almeno dei settori, dei sottosettori e dei tipi di soggetti che rientrano nell'ambito di applicazione di tale direttiva, nonché a garantire che i CSIRT dispongano di risorse adeguate per svolgere efficacemente i rispettivi compiti. Il presente regolamento non pregiudica il ruolo della Commissione di garantire il rispetto da parte degli Stati membri degli obblighi previsti dalla direttiva (UE) 2022/2555. Il meccanismo per le emergenze di cibersicurezza dovrebbe fornire assistenza per azioni volte a rafforzare la preparazione e azioni di risposta agli incidenti intese ad attenuare l'impatto di incidenti di cibersicurezza significativi e su vasta scala, al fine di sostenere la ripresa immediata e/o il ripristino del funzionamento di servizi essenziali.	(28) Secondo quanto disposto dalla direttiva (UE) 2022/2555 gli Stati membri sono tenuti a designare o istituire una o più autorità di gestione delle crisi informatiche e a garantire che tali autorità dispongano di risorse adeguate per svolgere i loro compiti in modo efficace ed efficiente. La direttiva impone inoltre gli Stati membri di individuare le capacità, le risorse e le procedure da poter impiegare in caso di crisi, nonché di adottare un piano nazionale di risposta agli incidenti e alle crisi di cibersicurezza su vasta scala, in cui siano definiti gli obiettivi e le modalità di gestione degli stessi. Gli Stati membri sono altresì tenuti a istituire uno o più CSIRT che siano incaricati di gestire gli incidenti, secondo un processo ben definito, e che si occupino almeno dei settori, dei sottosettori e dei tipi di soggetti che rientrano nell'ambito di applicazione di tale direttiva, nonché a garantire che i CSIRT dispongano di risorse adeguate per svolgere efficacemente i rispettivi compiti. Il presente regolamento non pregiudica il ruolo della Commissione di garantire il rispetto da parte degli Stati membri degli obblighi previsti dalla direttiva (UE) 2022/2555. Il meccanismo per le emergenze di cibersicurezza dovrebbe fornire assistenza per azioni volte a rafforzare la preparazione e azioni di risposta agli incidenti intese ad attenuare l'impatto di incidenti di cibersicurezza significativi e su vasta scala, al fine di sostenere la ripresa immediata e/o il ripristino del funzionamento di servizi essenziali***, sfruttando adeguatamente l'intera gamma di opzioni difensive a disposizione delle comunità civile e militare***.

Emendamento 21

Proposta di regolamento
Considerando 29

Testo della Commissione	*Emendamento*
(29) Nell'ambito delle azioni di preparazione, al fine di promuovere un approccio coerente e rafforzare la sicurezza in tutta l'Unione e nel suo mercato interno, è opportuno fornire un sostegno per verificare e valutare in modo coordinato il livello di cibersicurezza dei soggetti che operano nei settori altamente critici individuati ai sensi della direttiva (UE) 2022/2555. A tal fine la Commissione, con il sostegno dell'ENISA e in collaborazione con il gruppo di cooperazione NIS istituito dalla direttiva (UE) 2022/2555, dovrebbe individuare periodicamente i settori o i sottosettori pertinenti idonei a ricevere un sostegno finanziario per lo svolgimento di una verifica coordinata a livello dell'Unione. ***I*** settori o ***i*** sottosettori dovrebbero essere selezionati dall'allegato I della direttiva (UE) 2022/2555 ("Settori ad alta criticità"). Gli esercizi di verifica coordinata dovrebbero basarsi su scenari di rischio e metodologie comuni. La selezione dei settori e l'elaborazione degli scenari di rischio dovrebbero tenere conto delle valutazioni del rischio e degli scenari di rischio pertinenti a livello dell'Unione, compresa la necessità di evitare duplicazioni, come la valutazione del rischio e gli scenari di rischio previsti nelle conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, di cui devono occuparsi la Commissione, l'alto rappresentante e il gruppo di cooperazione NIS, in coordinamento con i pertinenti organismi e agenzie civili e militari e le pertinenti reti consolidate, compresa EU-CyCLONe. Dovrebbero inoltre essere prese in considerazione la valutazione del rischio delle reti e delle infrastrutture di comunicazione richiesta dall'invito	(29) Nell'ambito delle azioni di preparazione, al fine di promuovere un approccio coerente e rafforzare la sicurezza in tutta l'Unione e nel suo mercato interno, è opportuno fornire un sostegno per verificare e valutare in modo coordinato il livello di cibersicurezza dei soggetti che operano nei settori altamente critici individuati ai sensi della direttiva (UE) 2022/2555. A tal fine la Commissione, con il sostegno dell'ENISA e in collaborazione con il gruppo di cooperazione NIS istituito dalla direttiva (UE) 2022/2555, dovrebbe individuare periodicamente i settori o i sottosettori pertinenti idonei a ricevere un sostegno finanziario per lo svolgimento di una verifica coordinata a livello dell'Unione. ***Ove opportuno, dovrebbe essere associato anche il servizio europeo per l'azione esterna (SEAE), in particolare attraverso il Centro di intelligence dell'UE (INTCEN) e la sua cellula per l'analisi delle minacce ibride, con il sostegno della direzione "Intelligence" dello Stato maggiore dell'Unione europea (EUMS) nell'ambito della capacità unica di analisi dell'intelligence (SIAC), al fine di fornire valutazioni aggiornate e contribuire in tal modo all'individuazione dei*** settori o sottosettori ***che*** dovrebbero essere selezionati dall'allegato I della direttiva (UE) 2022/2555 ("settori ad alta criticità"). Gli esercizi di verifica coordinata dovrebbero basarsi su scenari di rischio e metodologie comuni. ***Tali esercitazioni dovrebbero anche svolgere un ruolo importante per migliorare la cooperazione tra soggetti civili e militari. Nell'organizzare le esercitazioni, la Commissione, il SEAE e l'ENISA dovrebbero pertanto valutare in modo***

ministeriale congiunto di Nevers e condotta dal gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA, e in collaborazione con l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC), le valutazioni coordinate del rischio da condurre ai sensi dell'articolo 22 della direttiva (UE) 2022/2555 e i test di resilienza operativa digitale previsti dal regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio***[29]***. La selezione dei settori dovrebbe inoltre tenere conto della raccomandazione del Consiglio su un approccio coordinato a livello di Unione per rafforzare la resilienza delle infrastrutture critiche.

sistematico di includere partecipanti da altre cibercomunità, come l'Agenzia europea per la difesa (AED) e altri soggetti pertinenti. La selezione dei settori e l'elaborazione degli scenari di rischio dovrebbero tenere conto delle valutazioni del rischio e degli scenari di rischio pertinenti a livello dell'Unione, compresa la necessità di evitare duplicazioni, come la valutazione del rischio e gli scenari di rischio previsti nelle conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, di cui devono occuparsi la Commissione, l'alto rappresentante e il gruppo di cooperazione NIS, in coordinamento con i pertinenti organismi e agenzie civili e militari e le pertinenti reti consolidate, compresa EU-CyCLONe. Dovrebbero inoltre essere prese in considerazione la valutazione del rischio delle reti e delle infrastrutture di comunicazione richiesta dall'invito ministeriale congiunto di Nevers e condotta dal gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA, e in collaborazione con l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC), le valutazioni coordinate del rischio da condurre ai sensi dell'articolo 22 della direttiva (UE) 2022/2555 e i test di resilienza operativa digitale previsti dal regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio***[1]***. La selezione dei settori dovrebbe inoltre tenere conto della raccomandazione del Consiglio su un approccio coordinato a livello di Unione per rafforzare la resilienza delle infrastrutture critiche.

[1] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, 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, (UE) n. 909/2014 e (UE) 2016/1011.

[29] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, 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, (UE) n. 909/2014 e (UE) 2016/1011.

[29] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, 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, (UE) n. 909/2014 e (UE) 2016/1011.

Emendamento 22

Proposta di regolamento
Considerando 32

Testo della Commissione	*Emendamento*
(32) Il meccanismo per le emergenze di cibersicurezza dovrebbe sostenere l'assistenza fornita dagli Stati membri a uno Stato membro in cui si sia verificato un incidente di cibersicurezza significativo o su vasta scala, anche mediante la rete di CSIRT di cui all'articolo 15 della direttiva (UE) 2022/2555. Gli Stati membri che forniscono assistenza dovrebbero essere autorizzati a presentare richieste di copertura dei costi relativi all'invio di squadre di esperti nel quadro dell'assistenza reciproca. I costi ammissibili potrebbero includere le spese di viaggio e di alloggio nonché l'indennità giornaliera degli esperti di cibersicurezza.	(32) Il meccanismo per le emergenze di cibersicurezza dovrebbe sostenere l'assistenza fornita dagli Stati membri a uno Stato membro in cui si sia verificato un incidente di cibersicurezza significativo o su vasta scala, anche mediante la rete di CSIRT di cui all'articolo 15 della direttiva (UE) 2022/2555. Gli Stati membri che forniscono assistenza dovrebbero essere autorizzati a presentare richieste di copertura dei costi relativi all'invio di squadre di esperti nel quadro dell'assistenza reciproca***, garantendo un coordinamento efficiente tra i pertinenti programmi e strumenti dell'UE, compresi lo strumento europeo per la pace (EPF), la PESC e l'NDICI, nell'ambito dell'assistenza a paesi terzi, in particolare all'Ucraina e alla Moldova***. I costi ammissibili potrebbero includere le spese di viaggio e di alloggio nonché l'indennità giornaliera degli esperti di cibersicurezza.

Emendamento 23

Proposta di regolamento
Considerando 33

Testo della Commissione	*Emendamento*
(33) È opportuno istituire gradualmente una riserva per la cibersicurezza a livello di Unione, costituita da servizi erogati da fornitori privati di servizi di sicurezza gestiti a sostegno di azioni di risposta e di ripresa immediata in caso di incidenti di cibersicurezza significativi o su vasta scala. La riserva dell'UE per la cibersicurezza dovrebbe garantire la disponibilità e la prontezza dei servizi. I servizi della riserva dell'UE per la cibersicurezza dovrebbero servire a sostenere le autorità nazionali nel fornire assistenza ai soggetti colpiti che operano in settori critici o altamente critici, a integrazione delle azioni da esse svolte a livello nazionale. Nel richiedere il sostegno della riserva dell'UE per la cibersicurezza, gli Stati membri dovrebbero specificare il sostegno fornito al soggetto interessato a livello nazionale, che è opportuno prendere in considerazione nella valutazione della richiesta dello Stato membro. I servizi di tale riserva possono inoltre servire a sostenere le istituzioni, gli organi e gli organismi dell'Unione, in condizioni analoghe.	(33) È opportuno istituire gradualmente una riserva per la cibersicurezza a livello di Unione, costituita da servizi erogati da fornitori privati di servizi di sicurezza gestiti a sostegno di azioni di risposta e di ripresa immediata in caso di incidenti di cibersicurezza significativi o su vasta scala. La riserva dell'UE per la cibersicurezza dovrebbe garantire la disponibilità e la prontezza dei servizi. I servizi della riserva dell'UE per la cibersicurezza dovrebbero servire a sostenere le autorità nazionali nel fornire assistenza ai soggetti colpiti che operano in settori critici o altamente critici, a integrazione delle azioni da esse svolte a livello nazionale. Nel richiedere il sostegno della riserva dell'UE per la cibersicurezza, gli Stati membri dovrebbero specificare il sostegno fornito al soggetto interessato a livello nazionale, che è opportuno prendere in considerazione nella valutazione della richiesta dello Stato membro. I servizi di tale riserva possono inoltre servire a sostenere le istituzioni, gli organi e gli organismi dell'Unione***, comprese le missioni PSDC***, in condizioni analoghe.

Emendamento 24

Proposta di regolamento
Considerando 34

Testo della Commissione	*Emendamento*
(34) Ai fini della selezione di fornitori di servizi privati per la prestazione di servizi nel contesto della riserva dell'UE per la cibersicurezza, occorre stabilire una serie di criteri minimi da includere nel corrispondente bando di gara, in modo da garantire che siano soddisfatte le esigenze delle autorità e dei soggetti degli Stati membri che operano in settori critici o altamente critici.	(34) Ai fini della selezione di fornitori di servizi privati per la prestazione di servizi nel contesto della riserva dell'UE per la cibersicurezza, occorre stabilire una serie di criteri minimi da includere nel corrispondente bando di gara, in modo da garantire che siano soddisfatte le esigenze delle autorità e dei soggetti degli Stati membri che operano in settori critici o altamente critici***, tenendo conto inoltre dei rischi associati alla partecipazione di***

fornitori da paesi concorrenti strategici, il che potrebbe comportare rischi per la sicurezza economica, nonché implicazioni per la sicurezza strategica dell'Unione.

Emendamento 25

Proposta di regolamento
Considerando 36

Testo della Commissione	*Emendamento*
(36) Al fine di sostenere gli obiettivi del presente regolamento di promuovere la condivisione della conoscenza situazionale, rafforzare la resilienza dell'Unione e consentire una risposta efficace agli incidenti di cibersicurezza significativi e su vasta scala, EU-CyCLONe, la rete di CSIRT o la Commissione dovrebbero essere in grado di chiedere all'ENISA di riesaminare e valutare le minacce, le vulnerabilità e le azioni di attenuazione in relazione a uno specifico incidente di cibersicurezza significativo o su vasta scala. Dopo il completamento del riesame e della valutazione di un incidente, l'ENISA dovrebbe preparare una relazione di riesame dell'incidente, in collaborazione con i pertinenti portatori di interessi, compresi i rappresentanti del settore privato, degli Stati membri, della Commissione e di altre istituzioni, organi e organismi dell'UE pertinenti. Per quanto riguarda il settore privato, l'ENISA sta attualmente predisponendo canali per lo scambio di informazioni con fornitori specializzati, compresi i fornitori di soluzioni di sicurezza gestite e i venditori, al fine di contribuire alla realizzazione della sua missione, che consiste nel raggiungere un elevato livello comune di cibersicurezza in tutta l'Unione. Basandosi sulla collaborazione con i portatori di interessi, compreso il settore privato, la relazione di riesame riguardante incidenti specifici dovrebbe mirare a valutare le cause, gli impatti e le misure di	(36) Al fine di sostenere gli obiettivi del presente regolamento di promuovere la condivisione della conoscenza situazionale, rafforzare la resilienza dell'Unione e consentire una risposta efficace agli incidenti di cibersicurezza significativi e su vasta scala, EU-CyCLONe, la rete di CSIRT o la Commissione dovrebbero essere in grado di chiedere all'ENISA di riesaminare e valutare le minacce, le vulnerabilità e le azioni di attenuazione in relazione a uno specifico incidente di cibersicurezza significativo o su vasta scala. ***In vista dello sviluppo di un sistema di connettività sicuro, basato sull'infrastruttura europea di comunicazione quantistica (EuroQCI) e sulla comunicazione satellitare governativa dell'Unione europea (GOVSATCOM), in particolare l'attuazione di GALILEO GNSS per gli utenti della difesa, ogni possibile sviluppo futuro dovrebbe tenere conto dell'avvento dell'"iperguerra", che unisce la velocità e la sofisticatezza del calcolo quantistico a sistemi militari altamente autonomi.*** Dopo il completamento del riesame e della valutazione di un incidente, l'ENISA dovrebbe preparare una relazione di riesame dell'incidente, in collaborazione con i pertinenti portatori di interessi, compresi i rappresentanti del settore privato, degli Stati membri, della Commissione e di altre istituzioni, organi e organismi dell'UE pertinenti. Per quanto riguarda il settore privato, l'ENISA sta

attenuazione di un incidente una volta verificatosi. È opportuno prestare particolare attenzione ai contributi e agli insegnamenti condivisi dai fornitori di servizi di sicurezza gestiti che soddisfano le condizioni di massima integrità professionale, imparzialità e competenza tecnica necessaria come disposto dal presente regolamento. La relazione dovrebbe essere presentata a EU-CyCLONe, alla rete di CSIRT e alla Commissione per essere integrata nelle rispettive attività. Se l'incidente riguarda un paese terzo, la Commissione condividerà inoltre la relazione con l'alto rappresentante.

attualmente predisponendo canali per lo scambio di informazioni con fornitori specializzati, compresi i fornitori di soluzioni di sicurezza gestite e i venditori, al fine di contribuire alla realizzazione della sua missione, che consiste nel raggiungere un elevato livello comune di cibersicurezza in tutta l'Unione. Basandosi sulla collaborazione con i portatori di interessi, compreso il settore privato, la relazione di riesame riguardante incidenti specifici dovrebbe mirare a valutare le cause, gli impatti e le misure di attenuazione di un incidente una volta verificatosi. È opportuno prestare particolare attenzione ai contributi e agli insegnamenti condivisi dai fornitori di servizi di sicurezza gestiti che soddisfano le condizioni di massima integrità professionale, imparzialità e competenza tecnica necessaria come disposto dal presente regolamento. La relazione dovrebbe essere presentata a EU-CyCLONe, alla rete di CSIRT e alla Commissione per essere integrata nelle rispettive attività. Se l'incidente riguarda un paese terzo, la Commissione condividerà inoltre la relazione con l'alto rappresentante***, il SEAE e qualsiasi missione PSDC nel paese interessato dall'incidente attraverso le rispettive sedi centrali***.

Emendamento 26

Proposta di regolamento
Considerando 37

Testo della Commissione	*Emendamento*
(37) Tenendo conto della natura imprevedibile degli attacchi di cibersicurezza e del fatto che spesso non sono circoscritti a un'area geografica specifica e presentano un elevato rischio di propagazione, il rafforzamento della resilienza dei paesi limitrofi e della loro capacità di rispondere efficacemente agli	(37) Tenendo conto della natura imprevedibile degli attacchi di cibersicurezza e del fatto che spesso non sono circoscritti a un'area geografica specifica e presentano un elevato rischio di propagazione, il rafforzamento della resilienza dei paesi limitrofi***, in particolare dell'Ucraina e della Moldova,*** e della loro

incidenti di cibersicurezza significativi e su vasta scala contribuisce alla protezione dell'Unione nel suo complesso. I paesi terzi associati al programma Europa digitale ***possono*** quindi essere sostenuti dalla riserva dell'UE per la cibersicurezza***, laddove ciò sia previsto dal rispettivo accordo di associazione al programma Europa digitale***. Il finanziamento per i paesi terzi associati dovrebbe essere sostenuto dall'Unione nel quadro dei partenariati e degli strumenti di finanziamento pertinenti per tali paesi. Il sostegno dovrebbe riguardare servizi nell'ambito della risposta e della ripresa immediata in caso di incidenti di cibersicurezza significativi o su vasta scala. Le condizioni stabilite per la riserva dell'UE per la cibersicurezza e per i fornitori di fiducia nel presente regolamento dovrebbero essere applicate quando è fornito sostegno ai paesi terzi associati al programma Europa digitale.	capacità di rispondere efficacemente agli incidenti di cibersicurezza significativi e su vasta scala contribuisce alla protezione dell'Unione nel suo complesso. I paesi terzi associati al programma Europa digitale ***dovrebbero*** quindi essere sostenuti dalla riserva dell'UE per la cibersicurezza***. Il sostegno dovrebbe applicarsi anche ai paesi terzi in cui sia schierata una missione PSDC con un mandato specifico per rafforzare la resilienza alle minacce ibride, comprese le minacce informatiche, o in cui sia stata adottata una misura di assistenza nell'ambito dell'EPF per rafforzare la resilienza informatica del paese***. Il finanziamento per i paesi terzi associati dovrebbe essere sostenuto dall'Unione nel quadro dei partenariati e degli strumenti di finanziamento pertinenti per tali paesi. Il sostegno dovrebbe riguardare servizi nell'ambito della risposta e della ripresa immediata in caso di incidenti di cibersicurezza significativi o su vasta scala. Le condizioni stabilite per la riserva dell'UE per la cibersicurezza e per i fornitori di fiducia nel presente regolamento dovrebbero essere applicate quando è fornito sostegno ai paesi terzi associati al programma Europa digitale.

Emendamento 27

Proposta di regolamento
Articolo 1 – paragrafo 1 – lettera c

Testo della Commissione	*Emendamento*
c) l'istituzione di un meccanismo europeo di riesame degli incidenti di cibersicurezza finalizzato al riesame e alla valutazione di incidenti significativi o su vasta scala.	c) l'istituzione di un meccanismo europeo di riesame degli incidenti di cibersicurezza finalizzato al riesame e alla valutazione di incidenti ***o di minacce*** significativi o su vasta scala.

Emendamento 28

Proposta di regolamento
Articolo 1 – paragrafo 2 – lettera a

Testo della Commissione	*Emendamento*
a) migliorare il rilevamento e la conoscenza situazionale comuni dell'Unione in materia di minacce e incidenti informatici, consentendo così di rafforzare la posizione competitiva dei settori dell'industria e dei servizi nell'Unione nell'ambito dell'economia digitale e di contribuire alla ***sovranità*** tecnologica dell'Unione nel settore della cibersicurezza;	a) migliorare il rilevamento e la conoscenza situazionale comuni dell'Unione in materia di minacce e incidenti informatici, consentendo così di rafforzare la posizione competitiva dei settori dell'industria e dei servizi nell'Unione nell'ambito dell'economia digitale e di contribuire alla ***resilienza*** tecnologica dell'Unione nel settore della cibersicurezza;

Emendamento 29

Proposta di regolamento
Articolo 1 – paragrafo 2 – lettera b

Testo della Commissione	*Emendamento*
b) rafforzare la preparazione dei soggetti che operano in settori critici e altamente critici in tutta l'Unione e potenziare la solidarietà sviluppando capacità di risposta comuni contro gli incidenti di cibersicurezza significativi o su vasta scala, permettendo inoltre ai paesi terzi associati al programma Europa digitale di accedere al sostegno offerto dall'Unione per la risposta agli incidenti di cibersicurezza;	b) rafforzare la preparazione dei soggetti che operano in settori critici e altamente critici in tutta l'Unione e potenziare la solidarietà sviluppando capacità di risposta comuni contro gli incidenti di cibersicurezza significativi o su vasta scala, permettendo inoltre ai paesi terzi associati al programma Europa digitale ***o ai paesi terzi candidati che non ledono gli interessi di sicurezza e di difesa dell'Unione e dei suoi Stati membri, quali stabiliti nel quadro della PESC a norma del titolo V TUE,*** di accedere al sostegno offerto dall'Unione per la risposta agli incidenti di cibersicurezza; ***Gli Stati membri dovrebbero prendere in considerazione un programma attivo di ciberdifesa quale parte integrante della loro strategia nazionale per la cibersicurezza che includa regolari esercizi di formazione congiunti tra Stati membri e organizzazioni internazionali. Tale programma dovrebbe fornire una***

capacità sincronizzata e in tempo reale per individuare, rilevare, analizzare e mitigare le minacce;

Emendamento 30

Proposta di regolamento
Articolo 1 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. ridurre i rischi sistemici di cibersicurezza posti dalla dipendenza da apparecchiature critiche provenienti da paesi che lederebbero gli interessi di sicurezza e di difesa dell'Unione e dei suoi Stati membri, quali stabiliti nel quadro della PESC a norma del titolo V TUE.

Emendamento 31

Proposta di regolamento
Articolo 2 – punto 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	"comunità della ciberdifesa": le autorità di difesa degli Stati membri, sostenute dalle istituzioni, dagli organi e dagli organismi dell'UE, come stabilito nella comunicazione congiunta sulla politica di ciberdifesa dell'UE[1];
	[1] Comunicazione congiunta al Parlamento europeo e al Consiglio – La politica di ciberdifesa dell'UE (JOIN(2022) 49 final).

Emendamento 32

Proposta di regolamento
Articolo 3 – paragrafo 2 – comma 1 – lettera b bis (nuova)

Testo della Commissione	*Emendamento*
	b bis) contribuire a modernizzare l'intero

	sistema di ciberdifesa, migliorando la qualità delle capacità di ciberdifesa attraverso la diffusione di sistemi di IA, nonché ad accelerare lo scambio di informazioni tra i SOC nazionali e i SOC transfrontalieri;

Emendamento 33

Proposta di regolamento
Articolo 3 – paragrafo 2 – comma 1 – lettera d bis (nuova)

Testo della Commissione	*Emendamento*
	d bis) riesaminare e valutare le tecnologie e le attrezzature critiche per la cibersicurezza impiegate dai SOC in risposta agli incidenti di cibersicurezza per i rischi sistemici derivanti dal controllo di fornitori ad alto rischio da parte di paesi che lederebbero gli interessi di sicurezza e di difesa dell'Unione e dei suoi Stati membri stabiliti nel quadro della PESC a norma del titolo V TUE.

Emendamento 34

Proposta di regolamento
Articolo 1 – paragrafo 1 – comma 2

Testo della Commissione	*Emendamento*
Il SOC ha la capacità di fungere da punto di riferimento e da porta di accesso ad altre organizzazioni pubbliche e private a livello nazionale per la raccolta e l'analisi di informazioni sulle minacce e sugli incidenti di cibersicurezza e per contribuire a un SOC transfrontaliero. È dotato di tecnologie all'avanguardia in grado di rilevare, aggregare e analizzare dati relativi alle minacce e agli incidenti di cibersicurezza.	Il SOC ha la capacità di fungere da punto di riferimento e da porta di accesso ad altre organizzazioni pubbliche e private***, e ove necessario militari,*** a livello nazionale per la raccolta e l'analisi di informazioni sulle minacce e sugli incidenti di cibersicurezza e per contribuire a un SOC transfrontaliero. È dotato di tecnologie all'avanguardia in grado di rilevare, aggregare e analizzare dati relativi alle minacce e agli incidenti di cibersicurezza.

Emendamento 35

Proposta di regolamento
Articolo 4 – paragrafo 2

Testo della Commissione	*Emendamento*
2. A seguito di un invito a manifestare interesse, i SOC nazionali sono selezionati dal Centro europeo di competenza per la cibersicurezza ("ECCC") per partecipare con quest'ultimo a un appalto congiunto di strumenti e infrastrutture. L'ECCC può attribuire sovvenzioni ai SOC nazionali selezionati per finanziare il funzionamento di tali strumenti e infrastrutture. Il contributo finanziario dell'Unione copre fino al 50 % dei costi di acquisizione degli strumenti e delle infrastrutture e fino al 50 % dei costi operativi, mentre i costi restanti devono essere coperti dallo Stato membro. Prima di avviare la procedura di acquisizione degli strumenti e delle infrastrutture, l'ECCC e il SOC nazionale concludono una convezione di accoglienza e di utilizzo che disciplina l'uso degli strumenti e delle infrastrutture.	2. A seguito di un invito a manifestare interesse, i SOC nazionali sono selezionati dal Centro europeo di competenza per la cibersicurezza ("ECCC") per partecipare con quest'ultimo a un appalto congiunto di strumenti e infrastrutture. L'ECCC può attribuire sovvenzioni ai SOC nazionali selezionati per finanziare il funzionamento di tali strumenti e infrastrutture***, rigorosamente a condizione che tali strumenti e infrastrutture siano forniti da fornitori di fiducia a norma dell'articolo 16***. Il contributo finanziario dell'Unione copre fino al 50 % dei costi di acquisizione degli strumenti e delle infrastrutture e fino al 50 % dei costi operativi, mentre i costi restanti devono essere coperti dallo Stato membro. Prima di avviare la procedura di acquisizione degli strumenti e delle infrastrutture, l'ECCC e il SOC nazionale concludono una convezione di accoglienza e di utilizzo che disciplina l'uso degli strumenti e delle infrastrutture.

Emendamento 36

Proposta di regolamento
Articolo 5 – paragrafo 2

Testo della Commissione	*Emendamento*
2. A seguito di un invito a manifestare interesse, un consorzio ospitante è selezionato dall'ECCC per partecipare con quest'ultimo a un appalto congiunto di strumenti e infrastrutture. L'ECCC può attribuire al consorzio ospitante una sovvenzione per finanziare il funzionamento degli strumenti e delle infrastrutture. Il contributo finanziario dell'Unione copre fino al 75 % dei costi di	2. A seguito di un invito a manifestare interesse, un consorzio ospitante è selezionato dall'ECCC per partecipare con quest'ultimo a un appalto congiunto di strumenti e infrastrutture. L'ECCC può attribuire al consorzio ospitante una sovvenzione per finanziare il funzionamento degli strumenti e delle infrastrutture***, rigorosamente a condizione che questi ultimi siano forniti da fornitori***

acquisizione degli strumenti e delle infrastrutture e fino al 50 % dei costi operativi, mentre i costi restanti devono essere coperti dal consorzio ospitante. Prima di avviare la procedura di acquisizione degli strumenti e delle infrastrutture, l'ECCC e il consorzio ospitante concludono una convezione di accoglienza e di utilizzo che disciplina l'uso degli strumenti e delle infrastrutture.	***di fiducia a norma dell'articolo 16***. Il contributo finanziario dell'Unione copre fino al 75 % dei costi di acquisizione degli strumenti e delle infrastrutture e fino al 50 % dei costi operativi, mentre i costi restanti devono essere coperti dal consorzio ospitante. Prima di avviare la procedura di acquisizione degli strumenti e delle infrastrutture, l'ECCC e il consorzio ospitante concludono una convezione di accoglienza e di utilizzo che disciplina l'uso degli strumenti e delle infrastrutture.

Emendamento 37

Proposta di regolamento
Articolo 5 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. Qualsiasi infrastruttura o fornitore originario di un paese terzo ad alto rischio è automaticamente escluso.

Emendamento 38

Proposta di regolamento
Articolo 6 – paragrafo 1 – lettera b bis (nuova)

Testo della Commissione	*Emendamento*
	b bis) sostenga direttamente il rafforzamento delle capacità militari e di difesa dei membri partecipanti o prevenga una minaccia diretta e imminente alla loro sicurezza. Poiché lo sfruttamento delle vulnerabilità nel settore della difesa può causare perturbazioni e danni significativi, la cibersicurezza del settore della difesa richiede misure speciali per garantire la sicurezza delle catene di approvvigionamento, in particolare dei soggetti a un livello inferiore della catena stessa che non richiedono l'accesso a informazioni classificate, ma che potrebbero comportare gravi rischi per l'intero settore. Occorre prestare

	particolare attenzione all'impatto che qualsiasi violazione potrebbe avere e alla minaccia di qualsiasi potenziale manipolazione dei dati di rete che potrebbe rendere inutili le capacità di difesa essenziali o addirittura aggirare i loro sistemi operativi rendendoli vulnerabili al dirottamento.

Emendamento 39

Proposta di regolamento
Articolo 6 – paragrafo 1 – lettera b ter (nuova)

Testo della Commissione	*Emendamento*
	b ter) sostenga il rafforzamento delle capacità di difesa dei membri partecipanti o prevenga una minaccia diretta e imminente alla loro sicurezza, garantendo la sicurezza delle catene di approvvigionamento, in particolare dei soggetti a livello inferiore della catena stessa che non richiedono l'accesso a informazioni classificate, ma che potrebbero comportare gravi rischi per l'intero settore.

Emendamento 40

Proposta di regolamento
Articolo 7 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Quando ottengono informazioni relative a un incidente di cibersicurezza su vasta scala, potenziale o in corso, i SOC transfrontalieri forniscono senza indebito ritardo le informazioni pertinenti a EU-CyCLONe, alla rete di CSIRT e alla Commissione, in considerazione dei rispettivi ruoli di gestione delle crisi conformemente alla direttiva (UE) 2022/2555.	1. Quando ottengono informazioni relative a un incidente di cibersicurezza su vasta scala, potenziale o in corso, i SOC transfrontalieri forniscono senza indebito ritardo le informazioni pertinenti a EU-CyCLONe, alla rete di CSIRT e alla Commissione, ***compresi l'alto rappresentante e il SEAE se l'incidente riguarda un paese terzo,*** in considerazione dei rispettivi ruoli di gestione delle crisi conformemente alla direttiva (UE)

2022/2555.

Emendamento 41

Proposta di regolamento
Articolo 8 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Gli Stati membri che partecipano al ciberscudo europeo garantiscono un elevato livello di sicurezza dei dati e di sicurezza fisica dell'infrastruttura del ciberscudo europeo e assicurano che l'infrastruttura sia adeguatamente gestita e controllata, in modo da proteggerla dalle minacce e da garantire la sua sicurezza e quella dei sistemi, ***compresa quella*** dei dati scambiati attraverso l'infrastruttura.	1. Gli Stati membri che partecipano al ciberscudo europeo garantiscono un elevato livello di sicurezza dei dati e di sicurezza fisica dell'infrastruttura del ciberscudo europeo e assicurano che l'infrastruttura sia adeguatamente gestita e controllata, in modo da proteggerla dalle minacce e da garantire la sua sicurezza e quella dei sistemi, ***riducendo i rischi e promuovendo il vantaggio tecnologico dell'UE nei settori critici, comprese misure volte a limitare o escludere i fornitori ad alto rischio, nonché da proteggere la sicurezza*** dei dati scambiati attraverso l'infrastruttura.

Emendamento 42

Proposta di regolamento
Articolo 8 – paragrafo 2

Testo della Commissione	*Emendamento*
2. Gli Stati membri che partecipano al ciberscudo europeo garantiscono che la condivisione di informazioni nell'ambito del ciberscudo europeo con soggetti che non sono organismi pubblici degli Stati membri non influisca negativamente sugli interessi di sicurezza dell'Unione.	2. Gli Stati membri che partecipano al ciberscudo europeo garantiscono che la condivisione di informazioni nell'ambito del ciberscudo europeo con soggetti che non sono organismi pubblici degli Stati membri non influisca negativamente sugli interessi di sicurezza dell'Unione ***e che qualsiasi condivisione di informazioni con fornitori ad alto rischio abbia una portata limitata e non pregiudichi la sicurezza e gli interessi strategici dell'Unione***.

Emendamento 43

Proposta di regolamento
Articolo 8 – paragrafo 3

Testo della Commissione	*Emendamento*
3. La Commissione può adottare atti di esecuzione che stabiliscono i requisiti tecnici che gli Stati membri devono rispettare per adempiere gli obblighi di cui ai paragrafi 1 e 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2, del presente regolamento. Nel fare ciò, la Commissione, sostenuta dall'alto rappresentante, tiene conto delle pertinenti norme di sicurezza a livello di difesa, al fine di facilitare la cooperazione con i soggetti militari.	3. La Commissione può adottare atti di esecuzione che stabiliscono i requisiti tecnici che gli Stati membri devono rispettare per adempiere gli obblighi di cui ai paragrafi 1 e 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2, del presente regolamento. Nel fare ciò, la Commissione, sostenuta dall'alto rappresentante, tiene conto delle pertinenti norme di sicurezza a livello di difesa, al fine di facilitare la cooperazione con i soggetti militari***, sfruttando adeguatamente l'intera gamma di opzioni difensive a disposizione delle comunità civile e militare per la sicurezza e la difesa dell'UE in senso lato, e ne informa il Parlamento europeo***.

Emendamento 44

Proposta di regolamento
Articolo 9 – paragrafo 2

Testo della Commissione	*Emendamento*
2. Le azioni di attuazione del meccanismo per le emergenze di cibersicurezza sono sostenute da finanziamenti a titolo del programma Europa digitale e attuate in conformità del regolamento (UE) 2021/694 e in particolare dell'obiettivo specifico 3**.**	2. Le azioni di attuazione del meccanismo per le emergenze di cibersicurezza sono sostenute da finanziamenti a titolo del programma Europa digitale e attuate in conformità del regolamento (UE) 2021/694 e in particolare dell'obiettivo specifico 3 ***nonché a titolo dello strumento europeo per la pace (EPF) quando riguardano misure di assistenza a paesi terzi, in particolare l'Ucraina e la Moldova;***

Emendamento 45

Proposta di regolamento
Articolo 10 – paragrafo 1 – lettera a

Testo della Commissione	*Emendamento*
a) azioni di preparazione, compresa la verifica coordinata della preparazione dei soggetti che operano in settori altamente critici in tutta l'Unione;	a) azioni di preparazione, compresa la verifica coordinata della preparazione dei soggetti che operano in settori altamente critici***, come le infrastrutture pubbliche, le infrastrutture elettorali, i trasporti, la sanità, la finanza, le telecomunicazioni, l'approvvigionamento e la sicurezza alimentari,*** in tutta l'Unione;

Emendamento 46

Proposta di regolamento
Articolo 1 – paragrafo 1 – lettera c

Testo della Commissione	*Emendamento*
c) azioni di assistenza reciproca mediante le quali le autorità nazionali di uno Stato membro forniscono assistenza a un altro Stato membro, in particolare come previsto dall'articolo 11, paragrafo 3, lettera f), della direttiva (UE) 2022/2555**.**	c) azioni di assistenza reciproca mediante le quali le autorità nazionali di uno Stato membro forniscono assistenza a un altro Stato membro, in particolare come previsto dall'articolo 11, paragrafo 3, lettera f), della direttiva (UE) 2022/2555***, e nel contesto dell'articolo 42, paragrafo 7, TUE e dell'articolo 222 TFUE;***

Emendamento 47

Proposta di regolamento
Articolo 10 – paragrafo 1 – lettera c bis (nuova)

Testo della Commissione	*Emendamento*
	c bis) sostituzione ed eliminazione graduale delle attrezzature critiche provenienti da fornitori ad alto rischio, i quali potrebbero ledere gli interessi di sicurezza e di difesa dell'Unione e dei suoi Stati membri stabiliti nel quadro della PESC a norma del titolo V TUE.

Emendamento 48

Proposta di regolamento
Articolo 11 – paragrafo 2

Testo della Commissione	*Emendamento*
2. Il gruppo di cooperazione NIS, in collaborazione con la Commissione, l'ENISA ***e*** l'alto rappresentante, elabora scenari di rischio e metodologie comuni per gli esercizi di verifica coordinata.	2. Il gruppo di cooperazione NIS, in collaborazione con la Commissione, l'ENISA***,*** l'alto rappresentante***, il SEAE e, se del caso, con l'AED***, elabora scenari di rischio e metodologie comuni per gli esercizi di verifica coordinata.

Emendamento 49

Proposta di regolamento
Articolo 12 – paragrafo 2

Testo della Commissione	*Emendamento*
2. La riserva dell'UE per la cibersicurezza consiste in servizi di risposta agli incidenti erogati da fornitori di fiducia selezionati in base ai criteri di cui all'articolo 16. La riserva include servizi preimpegnati. I servizi sono realizzabili in tutti gli Stati membri.	2. La riserva dell'UE per la cibersicurezza consiste in servizi di risposta agli incidenti erogati da fornitori di fiducia selezionati in base ai criteri di cui all'articolo 16. La riserva include servizi preimpegnati. I servizi sono realizzabili in tutti gli Stati membri ***e in tutti i paesi terzi che soddisfano i requisiti applicabili del presente regolamento***.

Emendamento 50

Proposta di regolamento
Articolo 12 – paragrafo 3 – lettera b

Testo della Commissione	*Emendamento*
b) le istituzioni e gli organi e organismi dell'Unione.	b) le istituzioni e gli organi e organismi dell'Unione***, comprese le missioni PSDC***.

Emendamento 51

Proposta di regolamento
Articolo 12 – paragrafo 4

Testo della Commissione	*Emendamento*
4. Gli utenti di cui al paragrafo 3, lettera a), utilizzano i servizi della riserva dell'UE per la cibersicurezza al fine di rispondere o sostenere la risposta agli incidenti significativi o su vasta scala che colpiscono soggetti che operano in settori critici o altamente critici e sostenere la ripresa immediata da tali incidenti.	4. Gli utenti di cui al paragrafo 3, lettera a), utilizzano i servizi della riserva dell'UE per la cibersicurezza al fine di rispondere o sostenere la risposta agli incidenti significativi o su vasta scala che colpiscono soggetti che operano in settori critici o altamente critici e sostenere la ripresa immediata da tali incidenti***, come le infrastrutture pubbliche, le infrastrutture elettorali, i trasporti, la sanità, la finanza, le telecomunicazioni, l'approvvigionamento e la sicurezza alimentari***.

Emendamento 52

Proposta di regolamento
Articolo 12 – paragrafo 5

Testo della Commissione	*Emendamento*
5. La Commissione ha la responsabilità generale dell'attuazione della riserva dell'UE per la cibersicurezza. La Commissione determina le priorità e l'evoluzione della riserva dell'UE per la cibersicurezza, in linea con i requisiti degli utenti di cui al paragrafo 3, ne supervisiona l'attuazione e assicura la complementarità, la coerenza, le sinergie e i collegamenti con altre azioni di sostegno ai sensi del presente regolamento, nonché con altre azioni ***e*** programmi dell'Unione.	5. La Commissione ha la responsabilità generale dell'attuazione della riserva dell'UE per la cibersicurezza. La Commissione determina le priorità e l'evoluzione della riserva dell'UE per la cibersicurezza, in linea con i requisiti degli utenti di cui al paragrafo 3, ne supervisiona l'attuazione e assicura la complementarità, la coerenza, le sinergie e i collegamenti con altre azioni di sostegno ai sensi del presente regolamento, nonché con altre azioni***, altri*** programmi ***e altri obiettivi*** dell'Unione***, in particolare l'obiettivo strategico di ridurre le dipendenze da fornitori ad alto rischio, i quali potrebbero ledere gli interessi di sicurezza e di difesa dell'Unione e dei suoi Stati membri stabiliti nel quadro della PESC a norma del titolo V TUE***.

Emendamento 53

Proposta di regolamento
Articolo 12 – paragrafo 7

Testo della Commissione	*Emendamento*
7. Al fine di sostenere la Commissione nell'istituzione della riserva dell'UE per la cibersicurezza, l'ENISA prepara una mappatura dei servizi necessari, previa consultazione con gli Stati membri e la Commissione. L'ENISA prepara inoltre una mappatura analoga, previa consultazione con la Commissione, per individuare le esigenze dei paesi terzi ammissibili al sostegno della riserva dell'UE per la cibersicurezza ai sensi dell'articolo 17. La Commissione, ove opportuno, consulta l'alto rappresentante.	7. Al fine di sostenere la Commissione nell'istituzione della riserva dell'UE per la cibersicurezza, l'ENISA prepara una mappatura dei servizi necessari, previa consultazione con gli Stati membri e la Commissione. L'ENISA prepara inoltre una mappatura analoga, previa consultazione con la Commissione, per individuare***, con il sostegno del SEAE,*** le esigenze dei paesi terzi ammissibili al sostegno della riserva dell'UE per la cibersicurezza ai sensi dell'articolo 17. La Commissione, ove opportuno, consulta l'alto rappresentante.

Emendamento 54

Proposta di regolamento
Articolo 14 – paragrafo 2 – lettera a bis (nuova)

Testo della Commissione	*Emendamento*
	a bis) l'impatto dell'incidente sulla sicurezza e la difesa dell'Unione;

Emendamento 55

Proposta di regolamento
Articolo 15 – paragrafo 3

Testo della Commissione	*Emendamento*
3. In consultazione con l'alto rappresentante, il sostegno nell'ambito del meccanismo per le emergenze di cibersicurezza può integrare l'assistenza fornita nel contesto della politica estera e di sicurezza comune e della politica di sicurezza e di difesa comune, anche mediante i gruppi di risposta rapida agli	3. In consultazione con l'alto rappresentante, il sostegno nell'ambito del meccanismo per le emergenze di cibersicurezza può integrare l'assistenza fornita nel contesto della politica estera e di sicurezza comune e della politica di sicurezza e di difesa comune, anche mediante i gruppi di risposta rapida agli

incidenti informatici. Tale sostegno può inoltre integrare l'assistenza fornita da uno Stato membro a un altro Stato membro, o contribuirvi, nel contesto dell'articolo 42, paragrafo 7, del trattato sull'Unione europea.	incidenti informatici ***(CRRT), al fine di sostenere meglio gli Stati membri dell'Unione, le missioni e le operazioni PSDC e i paesi terzi allineati alla politica estera e di sicurezza comune e alla politica di sicurezza e di difesa comune dell'UE, in particolare l'Ucraina e la Moldova, nei loro sforzi di sviluppo delle capacità di ciberdifesa***. Tale sostegno può inoltre integrare l'assistenza fornita da uno Stato membro a un altro Stato membro, o contribuirvi, nel contesto dell'articolo 42, paragrafo 7, del trattato sull'Unione europea.

Emendamento 56

Proposta di regolamento
Articolo 16 – paragrafo 2 – lettera a bis (nuova)

Testo della Commissione	*Emendamento*
	a bis) il fornitore dimostra che le sue strutture decisionali e gestionali sono scevre da qualsiasi influenza indebita da parte di governi di Stati, la quale potrebbe ledere gli interessi di sicurezza e di difesa dell'Unione e dei suoi Stati membri stabiliti nel quadro della PESC a norma del titolo V TUE;

Emendamento 57

Proposta di regolamento
Articolo 16 – paragrafo 2 – lettera f

Testo della Commissione	*Emendamento*
f) il fornitore è dotato dell'attrezzatura tecnica hardware e software necessaria a supportare il servizio richiesto;	f) il fornitore è dotato dell'attrezzatura tecnica hardware e software necessaria a supportare il servizio richiesto ***e soddisfa i requisiti di cui all'articolo X del regolamento XX/XXXX (regolamento sulla resilienza informatica)***;

Emendamento 58

Proposta di regolamento
Articolo 16 – paragrafo 2 – lettera j bis (nuova)

Testo della Commissione	*Emendamento*
	j bis) non è ammissibile alcun fornitore originario di un paese terzo ad alto rischio.

Emendamento 59

Proposta di regolamento
Articolo 16 – paragrafo 2 – lettera j ter (nuova)

Testo della Commissione	*Emendamento*
	j ter) il fornitore opera, ove possibile, in stretta cooperazione con le pertinenti PMI;

Emendamento 60

Proposta di regolamento
Articolo 17 – paragrafo 1

Testo della Commissione	*Emendamento*
1. I paesi terzi possono richiedere il sostegno della riserva dell'UE per la cibersicurezza nei casi in cui è previsto dagli accordi di associazione conclusi in relazione alla loro partecipazione al programma Europa digitale.	1. I paesi terzi possono richiedere il sostegno della riserva dell'UE per la cibersicurezza***:***
	a) nei casi in cui è previsto dagli accordi di associazione conclusi in relazione alla loro partecipazione al programma Europa digitale***;***
	b) qualora in tali paesi terzi sia schierata una missione PSDC con un mandato specifico per rafforzare la resilienza alle minacce ibride, comprese le minacce informatiche, o sia stata adottata una misura di assistenza dell'EPF per rafforzare la ciberresilienza del paese.

Emendamento 61

Proposta di regolamento
Articolo 17 – paragrafo 2

Testo della Commissione	*Emendamento*
2. Il sostegno della riserva dell'UE per la cibersicurezza è conforme al presente regolamento e rispetta le condizioni specifiche stabilite negli accordi di associazione di cui al paragrafo 1.	2. Il sostegno della riserva dell'UE per la cibersicurezza è conforme al presente regolamento e rispetta le condizioni specifiche stabilite negli accordi di associazione di cui al paragrafo 1***, tranne che per i paesi terzi cui si applicano le disposizioni di cui al paragrafo 1, lettera b)***.

Emendamento 62

Proposta di regolamento
Articolo 18 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Su richiesta della Commissione, di EU-CyCLONe o della rete di CSIRT, l'ENISA riesamina e valuta le minacce, le vulnerabilità e le azioni di attenuazione in relazione a uno specifico incidente di cibersicurezza significativo o su vasta scala. Al termine del riesame e della valutazione di un incidente, l'ENISA presenta una relazione di riesame dell'incidente alla rete di CSIRT, a EU-CyCLONe e alla Commissione per sostenerli nello svolgimento dei loro compiti, in particolare alla luce di quelli stabiliti negli articoli 15 e 16 della direttiva (UE) 2022/2555. Laddove opportuno, la Commissione condivide la relazione con l'alto rappresentante.	1. Su richiesta della Commissione, di EU-CyCLONe o della rete di CSIRT, l'ENISA riesamina e valuta le minacce, le vulnerabilità e le azioni di attenuazione in relazione a uno specifico incidente di cibersicurezza significativo o su vasta scala. Al termine del riesame e della valutazione di un incidente, l'ENISA presenta una relazione di riesame dell'incidente alla rete di CSIRT, a EU-CyCLONe e alla Commissione per sostenerli nello svolgimento dei loro compiti, in particolare alla luce di quelli stabiliti negli articoli 15 e 16 della direttiva (UE) 2022/2555. Laddove opportuno, ***in particolare se l'incidente riguarda un paese terzo,*** la Commissione condivide la relazione con l'alto rappresentante ***e il SEAE***.

Emendamento 63

Proposta di regolamento
Articolo 18 – paragrafo 3 bis (nuovo)

Testo della Commissione	*Emendamento*
	3 bis. La relazione è trasmessa al Parlamento europeo conformemente al diritto dell'Unione o nazionale in materia di protezione delle informazioni sensibili classificate.

Emendamento 64

Proposta di regolamento
Articolo 19 – punto 1 – lettera a – punto 1
Regolamento (UE) 2021/694
Articolo 6 – paragrafo 1

Testo della Commissione	*Emendamento*
a bis) sostenere lo sviluppo di un ciberscudo europeo, compresi l'elaborazione, la realizzazione e il funzionamento di piattaforme SOC nazionali e transfrontaliere che contribuiscano alla conoscenza situazionale nell'Unione e al potenziamento delle capacità di analisi delle minacce informatiche dell'Unione;	a bis) sostenere lo sviluppo di un ciberscudo europeo, compresi l'elaborazione, la realizzazione e il funzionamento di piattaforme SOC nazionali e transfrontaliere che contribuiscano alla conoscenza situazionale nell'Unione, al potenziamento delle capacità di analisi delle minacce informatiche dell'Unione***, nonché alla riduzione della dipendenza dell'Unione da fornitori ad altro rischio di apparecchiature o componenti critici per la cibersicurezza, i quali potrebbero ledere gli interessi di sicurezza e di difesa dell'Unione e dei suoi Stati membri stabiliti nel quadro della PESC a norma del titolo V TUE***;

Emendamento 65

Proposta di regolamento
Articolo 20

Testo della Commissione	*Emendamento*
Entro [***quattro*** anni dalla data di applicazione del presente regolamento], la	Entro [***tre*** anni dalla data di applicazione del presente regolamento ***e***

Commissione trasmette al Parlamento europeo e al Consiglio una relazione di valutazione e sul riesame del presente regolamento.	***successivamente ogni due anni***], la Commissione trasmette al Parlamento europeo e al Consiglio una relazione di valutazione e sul riesame del presente regolamento.

PROCEDURA DELLA COMMISSIONE COMPETENTE PER PARERE

Titolo	Istituzione di misure intese a rafforzare la solidarietà e la capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi
Riferimenti	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Commissione competente per il merito Annuncio in Aula	ITRE 1.6.2023
Parere espresso da Annuncio in Aula	AFET 1.6.2023
Relatore(trice) per parere Nomina	Dragoş Tudorache 16.6.2023
Esame in commissione	18.9.2023
Approvazione	24.10.2023
Esito della votazione finale	+: 39 –: 4 0: 0
Membri titolari presenti al momento della votazione finale	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Supplenti presenti al momento della votazione finale	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

VOTAZIONE FINALE PER APPELLO NOMINALE
IN SEDE DI COMMISSIONE COMPETENTE PER PARERE

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kyrtsos, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	-
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Mick Wallace

0	0

Significato dei simboli utilizzati:
+ : favorevoli
- : contrari
0 : astenuti

25.10.2023

PARERE DELLA COMMISSIONE PER I TRASPORTI E IL TURISMO

destinato alla commissione per l'industria, la ricerca e l'energia

sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Relatore per parere: Gheorghe Falcă

BREVE MOTIVAZIONE

Le organizzazioni che subiscono attacchi informatici, anche nel settore dei trasporti, raramente li denunciano, in quanto tendono a considerarli "cattiva pubblicità". Ciò vale in particolare per le aziende del settore privato. La maggior parte delle organizzazioni preferisce affrontare la questione internamente e spesso è l'autore dell'attacco a renderlo pubblico. Nell'UE, la buona notizia è che, con l'entrata in vigore della direttiva (UE) 2022/2555 sulla sicurezza delle reti (nota come "direttiva NIS 2"), gli obblighi di segnalazione degli incidenti saranno armonizzati in tutti gli Stati membri. Questi ultimi hanno tempo fino a ottobre 2024 per recepire la direttiva nell'ordinamento nazionale. Di conseguenza, è probabile che la natura e l'entità del problema saranno meglio comprese nei prossimi anni.

Di recente l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) ha pubblicato una relazione1 contenente informazioni sulle minacce alla cibersicurezza nel settore dei trasporti. Nella relazione si sottolinea che i criminali informatici sono stati responsabili di oltre la metà (55 %) degli incidenti rilevati nel periodo di riferimento 2022 e che la finalità principale di tali attacchi era il guadagno economico. Dalla relazione emerge inoltre che la maggior parte degli attacchi informatici nel settore dei trasporti prende di mira i sistemi informatici, causando perturbazioni operative.

Per quanto riguarda la preparazione e la risposta agli incidenti di cibersicurezza, il sostegno a livello di Unione e la solidarietà tra gli Stati membri sono attualmente limitati. Nelle conclusioni del maggio 2022 il Consiglio ha evidenziato la necessità di affrontare queste lacune, invitando la Commissione a presentare una proposta su un nuovo **Fondo di risposta alle emergenze di**

[1] "Understanding Cyber Threats in Transport" (Comprendere le minacce informatiche nel settore dei trasporti), ENISA, pubblicata il 21 marzo 2023.

cibersicurezza[2].

La proposta di regolamento in esame attua la **strategia dell'UE in materia di cibersicurezza** adottata nel dicembre 2020, che annunciava la creazione di un **ciberscudo europeo** per il rafforzamento delle capacità di rilevamento delle minacce informatiche e di condivisione delle informazioni nell'Unione europea tramite una federazione di centri operativi di sicurezza (SOC) nazionali e transfrontalieri. Le azioni del regolamento saranno sostenute da **finanziamenti nel quadro dell'obiettivo strategico "Cibersicurezza" del programma Europa digitale**.

Il bilancio totale comprende un aumento di 100 milioni di EUR che, secondo la proposta di regolamento, saranno riassegnati da altri obiettivi strategici del programma Europa digitale. In questo modo il nuovo importo totale disponibile per le azioni in materia di cibersicurezza nell'ambito del programma Europa digitale sarà pari a 842,8 milioni di EUR.

Una parte dei 100 milioni di EUR aggiuntivi rafforzerà il bilancio gestito dal Centro europeo di competenza per la cibersicurezza (ECCC) per l'attuazione di azioni riguardanti i SOC e la preparazione nell'ambito dei loro programmi di lavoro. Il finanziamento aggiuntivo servirà inoltre a sostenere l'istituzione della riserva dell'UE per la cibersicurezza. Integrando il bilancio già previsto per azioni analoghe nel quadro del programma di lavoro principale e del programma di lavoro sulla cibersicurezza del programma Europa digitale per il periodo 2023-2027, tale finanziamento potrebbe portare l'importo totale per il 2023-2027 a 551 milioni, mentre 115 milioni sono già stati stanziati per progetti pilota per il periodo 2021-2022. Includendo i contributi degli Stati membri, il bilancio complessivo potrebbe ammontare a 1,109 miliardi di EUR.

[2] Conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, 23 maggio 2022 (9364/22).

Posizione del relatore

Il relatore accoglie con favore la nuova proposta e ritiene che apporterà benefici significativi alle varie parti interessate. Il relatore sottolinea la necessità di comprendere più a fondo le esigenze e i requisiti in materia di cibersicurezza nel settore dei trasporti e di garantire ai soggetti critici di tale settore l'accesso a finanziamenti adeguati per la preparazione e la risposta agli incidenti nonché la risoluzione degli stessi.

Il relatore sostiene il kit di strumenti per la cibersicurezza nel settore dei trasporti, che mira a contribuire al rafforzamento della consapevolezza in materia di rischi informatici e di igiene informatica, prestando particolare attenzione al settore dei trasporti. Il kit tiene conto delle infrastrutture di trasporto critiche e della mobilità militare, soprattutto nel contesto della guerra in Ucraina. Si rivolge alle imprese di trasporto di tutte le dimensioni e di tutti i settori di attività, in particolare, ma non solo, a:

- vettori aerei, gestori aeroportuali, aeroporti centrali, centri di gestione e di controllo del traffico aereo, l'Agenzia dell'Unione europea per la sicurezza aerea ed Eurocontrol;
- gestori dell'infrastruttura, imprese ferroviarie e il sistema europeo di gestione del traffico ferroviario (ERTMS);
- compagnie di navigazione per il trasporto per vie d'acqua interne, marittimo e costiero di passeggeri e merci, organi di gestione dei porti, compresi i relativi impianti portuali, enti che gestiscono opere e attrezzature all'interno dei porti e gestori di servizi di assistenza al traffico marittimo;
- autorità stradali responsabili del controllo della gestione del traffico e gestori di sistemi di trasporto intelligenti;
- nonché servizi postali e di corriere.

Il relatore ritiene che l'entità del bilancio per il funzionamento del **Fondo di risposta alle emergenze di cibersicurezza** ne determinerà il successo. Pertanto, dovrebbe essere sufficiente a sostenere gli Stati membri nella **preparazione** e nella **risposta** agli incidenti di cibersicurezza significativi e su vasta scala e nella **ripresa** dagli stessi. Il sostegno per la risposta agli incidenti deve essere reso disponibile anche alle istituzioni, agli organi e agli organismi dell'Unione.

Il **ciberscudo europeo** migliorerà le capacità di rilevamento delle minacce informatiche degli Stati membri. Il **meccanismo per le emergenze di cibersicurezza** integrerà le azioni degli Stati membri mediante un sostegno di emergenza per la preparazione, la risposta e la ripresa immediata/il ripristino del funzionamento dei servizi essenziali.

EMENDAMENTI

La commissione per i trasporti e il turismo invita la commissione per l'industria, la ricerca e l'energia, competente per il merito, a prendere in considerazione quanto segue:

Emendamento 1

Proposta di regolamento
Considerando 2

Testo della Commissione	*Emendamento*
(2) Attualmente si registra un incremento dell'entità, della frequenza e dell'impatto degli incidenti di cibersicurezza, compresi gli attacchi alle catene di approvvigionamento con finalità di ciberspionaggio, di ransomware o di perturbazione, che rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi. In considerazione del rapido evolversi del panorama delle minacce, il rischio di possibili incidenti su vasta scala, che possono provocare interruzioni o danni significativi a infrastrutture critiche, richiede una maggiore preparazione a tutti i livelli del quadro di cibersicurezza dell'Unione. Tale minaccia va oltre l'aggressione militare della Russia nei confronti dell'Ucraina ed è destinata a persistere, data la molteplicità di soggetti allineati con le autorità di governo, criminali e hacktivisti coinvolti nelle attuali tensioni geopolitiche. Tali incidenti possono ostacolare l'erogazione di servizi pubblici e lo svolgimento di attività economiche, anche in settori critici o altamente critici, generare consistenti perdite finanziarie, minare la fiducia degli utenti nonché causare gravi danni all'economia dell'Unione, e potrebbero persino avere conseguenze sulla salute o essere potenzialmente letali. Inoltre gli incidenti di cibersicurezza sono imprevedibili, in quanto spesso si verificano ed evolvono in periodi di tempo molto brevi, non sono circoscritti a una determinata zona geografica e si verificano	(2) Attualmente si registra un incremento dell'entità, della frequenza e dell'impatto degli incidenti di cibersicurezza, compresi gli attacchi alle catene di approvvigionamento con finalità di ciberspionaggio, di ransomware o di perturbazione, che rappresentano una grave minaccia per il funzionamento delle reti e dei sistemi informativi***, nonché per le infrastrutture informatiche e fisiche critiche***. In considerazione del rapido evolversi del panorama delle minacce, il rischio di possibili incidenti su vasta scala, che possono provocare interruzioni o danni significativi a infrastrutture critiche, richiede una maggiore preparazione a tutti i livelli del quadro di cibersicurezza dell'Unione. Tale minaccia va oltre l'aggressione militare della Russia nei confronti dell'Ucraina ed è destinata a persistere, data la molteplicità di soggetti allineati con le autorità di governo, criminali e hacktivisti coinvolti nelle attuali tensioni geopolitiche. Tali incidenti possono ostacolare l'erogazione di servizi pubblici ***e di trasporti pubblici e privati*** e lo svolgimento di attività economiche, anche in settori critici o altamente critici, generare consistenti perdite finanziarie, minare la fiducia degli utenti nonché causare gravi danni all'economia dell'Unione ***nonché alla mobilità all'interno dell'Unione***, e potrebbero persino avere conseguenze sulla salute o essere potenzialmente letali. Inoltre gli incidenti di cibersicurezza sono

simultaneamente o si diffondono istantaneamente in numerosi paesi.	imprevedibili, in quanto spesso si verificano ed evolvono in periodi di tempo molto brevi, non sono circoscritti a una determinata zona geografica e si verificano simultaneamente o si diffondono istantaneamente in numerosi paesi.

Emendamento 2

Proposta di regolamento
Considerando 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	(2 bis) Il settore dei trasporti è interessato da una minaccia di cibersicurezza sempre più grave rappresentata da attori sponsorizzati dallo Stato, criminali informatici e hacktivisti che prendono di mira le autorità, gli operatori, i produttori, i fornitori e i prestatori di servizi nei settori del trasporto aereo, marittimo, ferroviario e stradale. L'Agenzia dell'Unione europea per la cibersicurezza (ENISA) ha rilevato un aumento del 25 % del numero medio mensile di incidenti segnalati ai danni del settore dei trasporti nel 2022, rispetto ai livelli del 2021. La maggior parte degli attacchi contro il settore dei trasporti ha come bersaglio i sistemi informatici, con conseguenti possibili perturbazioni operative[3 bis].
	[3 bis] ENISA (2023), "Threat Landscape: Transport Sector" (Panorama delle minacce: il settore dei trasporti), pag. 7 e pag. 17.

Emendamento 3

Proposta di regolamento
Considerando 2 ter (nuovo)

Testo della Commissione	*Emendamento*
	(2 ter) L'invasione non provocata

dell'Ucraina da parte della Russia ha determinato un aumento significativo degli incidenti di cibersicurezza, compresi gli attacchi informatici distribuiti di negazione del servizio (DDoS), che hanno preso di mira il settore dei trasporti nell'UE e nelle aree limitrofe, in particolare aeroporti, linee ferroviarie e autorità di trasporto[3 ter]. È molto probabile che gli attacchi continuino ad aumentare.

[3 ter] ENISA (2023), "Threat Landscape: Transport Sector" (Panorama delle minacce: il settore dei trasporti), pag. 9.

Emendamento 4

Proposta di regolamento
Considerando 2 quater (nuovo)

Testo della Commissione	*Emendamento*
	(2 quater) Gli attacchi informatici prendono di mira le autorità e gli organismi di tutti i sottosettori dei trasporti, colpendo le imprese ferroviarie, i gestori delle infrastrutture e gli operatori portuali. Per quanto riguarda il settore stradale, sono divenuti bersagli i costruttori di apparecchiature originali (OEM), i fornitori e i prestatori di servizi, oltre agli operatori del trasporto pubblico. Nel settore del trasporto aereo, i principali obiettivi sono stati le compagnie aeree e gli operatori aeroportuali, seguiti dai prestatori di servizi, dagli operatori del trasporto di superficie e dalla catena di approvvigionamento[3 quater].

[3 quater] ENISA (2023), "Threat Landscape: Transport Sector" (Panorama delle minacce: il settore dei trasporti), pag. 17.

Emendamento 5

Proposta di regolamento
Considerando 3

Testo della Commissione	*Emendamento*
(3) Occorre rafforzare la posizione competitiva del settore industriale e di quello dei servizi dell'Unione nell'ambito dell'economia digitalizzata e sostenerne la trasformazione digitale, consolidando il livello di cibersicurezza nel mercato unico digitale. Come raccomandato in tre diverse proposte della Conferenza sul futuro dell'Europa[4], è necessario accrescere la resilienza dei cittadini, delle imprese e dei soggetti che gestiscono infrastrutture critiche contro le crescenti minacce alla cibersicurezza, che possono avere conseguenze devastanti a livello sociale ed economico. Occorre quindi investire in infrastrutture e servizi che permettano di velocizzare il rilevamento delle minacce e degli incidenti di cibersicurezza e di assicurare una risposta più rapida; inoltre gli Stati membri necessitano di assistenza per garantire una migliore preparazione e capacità di risposta più adeguate agli incidenti di cibersicurezza significativi e su vasta scala. L'Unione dovrebbe inoltre accrescere le sue capacità in questi settori, in particolare per quanto riguarda la raccolta e l'analisi di dati sulle minacce e sugli incidenti di cibersicurezza.	(3) Occorre rafforzare la posizione competitiva del settore industriale e di quello dei servizi dell'Unione nell'ambito dell'economia digitalizzata e sostenerne la trasformazione digitale, consolidando il livello di cibersicurezza nel mercato unico digitale. Come raccomandato in tre diverse proposte della Conferenza sul futuro dell'Europa[4], è necessario accrescere la resilienza dei cittadini, delle imprese***, degli operatori di trasporto*** e dei soggetti che gestiscono infrastrutture critiche contro le crescenti minacce alla cibersicurezza, che possono avere conseguenze devastanti a livello sociale ed economico. Occorre quindi investire in infrastrutture e servizi che permettano di velocizzare il rilevamento delle minacce e degli incidenti di cibersicurezza e di assicurare una risposta più rapida; inoltre gli Stati membri necessitano di assistenza per garantire una migliore preparazione e capacità di risposta più adeguate agli incidenti di cibersicurezza significativi e su vasta scala. L'Unione dovrebbe inoltre accrescere le sue capacità in questi settori, in particolare per quanto riguarda la raccolta e l'analisi di dati sulle minacce e sugli incidenti di cibersicurezza***, nonché sullo stato e sull'evoluzione del mercato del lavoro della cibersicurezza, in quanto svolge un ruolo determinante nella fornitura dei necessari servizi di rilevamento e risposta***.
[4] https://futureu.europa.eu/en/	[4] https://futureu.europa.eu/en/

Emendamento 6

Proposta di regolamento
Considerando 4

Testo della Commissione	*Emendamento*
(4) L'Unione ha già adottato una serie di misure per ridurre le vulnerabilità e accrescere la resilienza delle infrastrutture e dei soggetti critici contro i rischi di cibersicurezza, in particolare la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[5], la raccomandazione (UE) 2017/1584 della Commissione[6], la direttiva 2013/40/UE del Parlamento europeo e del Consiglio[7] e il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[8]. Inoltre la raccomandazione del Consiglio su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche invita gli Stati membri ad adottare misure urgenti ed efficaci e a cooperare lealmente, efficacemente, in modo solidale e coordinato tra loro, con la Commissione e le altre autorità pubbliche competenti, nonché con i soggetti interessati, al fine di migliorare la resilienza delle infrastrutture critiche utilizzate per fornire servizi essenziali nel mercato interno.	(4) L'Unione ha già adottato una serie di misure per ridurre le vulnerabilità e accrescere la resilienza delle infrastrutture e dei soggetti critici contro i rischi di cibersicurezza, in particolare la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[5], la raccomandazione (UE) 2017/1584 della Commissione[6], la direttiva 2013/40/UE del Parlamento europeo e del Consiglio[7] e il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[8]***, nonché la proposta di regolamento sugli orientamenti per lo sviluppo della rete transeuropea dei trasporti e la proposta di regolamento relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (legge sulla ciberresilienza)***. Inoltre la raccomandazione del Consiglio su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche invita gli Stati membri ad adottare misure urgenti ed efficaci e a cooperare lealmente, efficacemente, in modo solidale e coordinato tra loro, con la Commissione e le altre autorità pubbliche competenti, nonché con i soggetti interessati, al fine di migliorare la resilienza delle infrastrutture critiche utilizzate per fornire servizi essenziali nel mercato interno.
[5] 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 (GU L 333 del 27.12.2022).	[5] 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 (GU L 333 del 27.12.2022).
[6] Raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (GU L 239 del 19.9.2017,	[6] Raccomandazione (UE) 2017/1584 della Commissione, del 13 settembre 2017, relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala (GU L 239 del 19.9.2017,

pag. 36).

[7] Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio (GU L 218 del 14.8.2013, pag. 8).

[8] 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") (GU L 151 del 7.6.2019, pag. 15).

pag. 36).

[7] Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio (GU L 218 del 14.8.2013, pag. 8).

[8] 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") (GU L 151 del 7.6.2019, pag. 15).

Emendamento 7

Proposta di regolamento
Considerando 4 bis (nuovo)

Testo della Commissione	*Emendamento*
	(4 bis) Pur accogliendo con favore il kit di strumenti della Commissione europea per la cibersicurezza nel settore dei trasporti[8 bis], che contiene informazioni di base sulle minacce che possono interessare le organizzazioni del settore dei trasporti (diffusione di malware, attacchi di negazione del servizio, accesso non autorizzato e furto, manipolazione del software) ed elenca buone pratiche di attenuazione, gli operatori di trasporto dovrebbero ricevere una formazione adeguata in materia di cibersicurezza ed essere dotati di strumenti adeguati per prevenire le minacce informatiche. Il bilancio dell'Unione dovrebbe inoltre coprire il sostegno, ad esempio la formazione, fornito dall'ENISA per consentire l'efficace attuazione, da parte degli operatori di trasporto, delle migliori pratiche di attenuazione incluse nel kit di

strumenti.

[8 bis] ENISA (marzo 2023), "Threat Landscape: Health Sector" (Panorama delle minacce: il settore sanitario).

[8 ter] Commissione europea (2021), Kit di strumenti per la cibersicurezza nel settore dei trasporti, disponibile all'indirizzo https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_it

Emendamento 8

Proposta di regolamento
Considerando 4 bis (nuovo)

Testo della Commissione	*Emendamento*
	(4 bis) Un approccio coordinato a livello dell'Unione per rafforzare la preparazione e la resilienza delle infrastrutture critiche, quali le infrastrutture di trasporto, si basa sullo sviluppo delle capacità degli Stati membri. Come riconosciuto nella recente comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo "Colmare il divario di talenti nel settore della cibersicurezza per rafforzare la competitività, la crescita e la resilienza dell'UE"[8 bis], la sicurezza dell'Unione non può essere garantita senza il bene più prezioso dell'UE: la sua popolazione.

[8 bis] Comunicazione della Commissione al Parlamento europeo e al Consiglio dal titolo "Colmare il divario di talenti nel settore della cibersicurezza per rafforzare la competitività, la crescita e la resilienza dell'UE ("Accademia per le competenze in materia di cibersicurezza"), COM(2023)0207 final.

Emendamento 9

Proposta di regolamento
Considerando 12

Testo della Commissione	*Emendamento*
(12) Al fine di rendere più efficaci la prevenzione e la valutazione delle minacce e degli incidenti informatici, nonché la risposta agli stessi, occorre sviluppare una conoscenza più completa delle minacce alle risorse e alle infrastrutture critiche sul territorio dell'Unione, compresa la loro distribuzione geografica, l'interconnessione e gli effetti potenziali in caso di attacchi informatici contro tali infrastrutture. Dovrebbe essere realizzata un'infrastruttura di SOC dell'Unione su vasta scala ("ciberscudo europeo"), comprendente diverse piattaforme transfrontaliere interoperanti, ciascuna composta da diversi SOC nazionali. Tale infrastruttura dovrebbe essere al servizio degli interessi e delle esigenze di cibersicurezza nazionali e dell'Unione, sfruttando tecnologie all'avanguardia per strumenti di analisi e di raccolta di dati avanzati, migliorando le capacità di rilevamento e di gestione delle minacce informatiche e permettendo una conoscenza situazionale in tempo reale. Dovrebbe inoltre servire a incrementare le capacità di rilevamento delle minacce e degli incidenti di cibersicurezza e quindi a integrare e sostenere i soggetti e le reti dell'Unione responsabili della gestione delle crisi nell'UE, in particolare la rete europea delle organizzazioni di collegamento per le crisi informatiche ("EU-CyCLONe"), come definita nella direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[12].	(12) Al fine di rendere più efficaci la prevenzione e la valutazione delle minacce e degli incidenti informatici, nonché la risposta agli stessi, occorre sviluppare una conoscenza più completa delle minacce alle risorse e alle infrastrutture critiche sul territorio dell'Unione, compresa la loro distribuzione geografica, l'interconnessione e gli effetti potenziali in caso di attacchi informatici contro tali infrastrutture. ***Tali risorse e infrastrutture critiche comprendono i sistemi di trasporto intelligenti, i quali, pur essendo essenziali per la mobilità automatizzata e multimodale, operano sulla base di scambi cruciali di dati sensibili.*** Dovrebbe essere realizzata un'infrastruttura di SOC dell'Unione su vasta scala ("ciberscudo europeo"), comprendente diverse piattaforme transfrontaliere interoperanti, ciascuna composta da diversi SOC nazionali. Tale infrastruttura dovrebbe essere al servizio degli interessi e delle esigenze di cibersicurezza nazionali e dell'Unione, sfruttando tecnologie all'avanguardia per strumenti di analisi e di raccolta di dati avanzati, migliorando le capacità di rilevamento e di gestione delle minacce informatiche e permettendo una conoscenza situazionale in tempo reale. Dovrebbe inoltre servire a incrementare le capacità di rilevamento delle minacce e degli incidenti di cibersicurezza e quindi a integrare e sostenere i soggetti e le reti dell'Unione responsabili della gestione delle crisi nell'UE, in particolare la rete europea delle organizzazioni di collegamento per le crisi informatiche ("EU-CyCLONe"), come definita nella direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[12].
[12] Direttiva (UE) 2022/2555 del	[12] 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).

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).

Emendamento 10

Proposta di regolamento
Considerando 14 bis (nuovo)

Testo della Commissione	*Emendamento*
	(14 bis) Il settore dei trasporti sta diventando sempre più uno degli ambiti di attività maggiormente redditizi per i criminali informatici, in quanto i dati dei clienti sono considerati un bene di grande valore e la catena di approvvigionamento dei trasporti è presa di mira in misura crescente. Per questo motivo, le infrastrutture di trasporto caratterizzate da una natura transfrontaliera o dallo scambio di dati attraverso tecnologie senza fili dovrebbero essere considerate un oggetto centrale di analisi e monitoraggio sia per i SOC nazionali che, in particolare, per i SOC transfrontalieri. Ad esempio, la recente proposta di revisione del regolamento TEN-T richiede una solidarietà e una cooperazione maggiori nella condivisione di informazioni sulle minacce informatiche transfrontaliere che questa rete transnazionale potrebbe trovarsi ad affrontare. Analogamente, i sistemi di trasporto intelligenti sono fondamentali per rendere i trasporti più sicuri, efficienti e sostenibili, ma aumentano la vulnerabilità dei sistemi di trasporto agli attacchi informatici che possono provocare incidenti e ingorghi stradali o causare perdite economiche agli operatori privati e pubblici. Al fine di salvaguardare la sicurezza dei passeggeri e la protezione

dei dati degli utenti e dei fornitori nonché di evitare danni finanziari, è essenziale che il programma di attuazione della direttiva riveduta sui sistemi di trasporto intelligenti comprenda disposizioni e strumenti intesi a rafforzare la collaborazione tra gli Stati membri nel rilevamento delle minacce e degli incidenti di cibersicurezza nonché nella preparazione e risposta agli stessi.

Emendamento 11

Proposta di regolamento
Considerando 15

Testo della Commissione	*Emendamento*
(15) A livello nazionale, il monitoraggio, il rilevamento e l'analisi delle minacce informatiche sono solitamente garantiti dai SOC di soggetti pubblici e privati, in combinazione con i CSIRT. Questi ultimi inoltre scambiano informazioni nel contesto della rete di CSIRT, conformemente a quanto disposto dalla direttiva (UE) 2022/2555. I SOC transfrontalieri dovrebbero costituire una nuova capacità complementare alla rete di CSIRT, mettendo in comune e condividendo i dati sulle minacce alla cibersicurezza provenienti da soggetti pubblici e privati, accrescendo il valore di tali dati mediante l'analisi di esperti, infrastrutture acquisite congiuntamente e strumenti all'avanguardia, e contribuendo allo sviluppo delle capacità e della sovranità tecnologica dell'Unione.	(15) A livello nazionale, il monitoraggio, il rilevamento e l'analisi delle minacce informatiche sono solitamente garantiti dai SOC di soggetti pubblici e privati, in combinazione con i CSIRT. Questi ultimi inoltre scambiano informazioni nel contesto della rete di CSIRT, conformemente a quanto disposto dalla direttiva (UE) 2022/2555. I SOC transfrontalieri dovrebbero costituire una nuova capacità complementare alla rete di CSIRT, mettendo in comune e condividendo i dati sulle minacce alla cibersicurezza provenienti da soggetti pubblici e privati, accrescendo il valore di tali dati mediante l'analisi di esperti, infrastrutture acquisite congiuntamente e strumenti all'avanguardia, e contribuendo allo sviluppo delle capacità e della sovranità tecnologica dell'Unione. ***A tal proposito, al fine di rafforzare l'autonomia dell'Unione in ambito informatico e in riferimento all'articolo 47, paragrafo 4, della proposta di regolamento sugli orientamenti per lo sviluppo della rete transeuropea dei trasporti (COM(2021)0812), è altresì necessario impedire l'accesso ai dati che comportano minacce informatiche applicando un solido quadro normativo***

	che disciplini la proprietà e gli investimenti esteri in infrastrutture critiche, come i trasporti.

Emendamento 12

Proposta di regolamento
Considerando 21

Testo della Commissione	*Emendamento*
(21) Sebbene il ciberscudo europeo sia un progetto civile, la comunità della ciberdifesa potrebbe trarre beneficio dalle maggiori capacità di rilevamento e di conoscenza situazionale sviluppate nel settore civile per la protezione delle infrastrutture critiche. I SOC transfrontalieri, con il sostegno della Commissione e del Centro europeo di competenza per la cibersicurezza ("ECCC"), e in collaborazione con l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza (l'"alto rappresentante"), dovrebbero gradualmente mettere a punto norme e protocolli specifici per consentire la cooperazione con la comunità di ciberdifesa, anche per quanto riguarda le indagini e le condizioni di sicurezza. Lo sviluppo del ciberscudo europeo dovrebbe essere accompagnato da una riflessione che consenta la futura collaborazione con le reti e le piattaforme responsabili della condivisione delle informazioni nella comunità di ciberdifesa, in stretta collaborazione con l'alto rappresentante.	(21) Sebbene il ciberscudo europeo sia un progetto civile, la comunità della ciberdifesa potrebbe trarre beneficio dalle maggiori capacità di rilevamento e di conoscenza situazionale sviluppate nel settore civile per la protezione delle infrastrutture critiche. I SOC transfrontalieri, con il sostegno della Commissione e del Centro europeo di competenza per la cibersicurezza ("ECCC"), e in collaborazione con l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza (l'"alto rappresentante"), dovrebbero gradualmente mettere a punto norme e protocolli specifici per consentire la cooperazione con la comunità di ciberdifesa, anche per quanto riguarda le indagini e le condizioni di sicurezza. Lo sviluppo del ciberscudo europeo dovrebbe essere accompagnato da una riflessione che consenta la futura collaborazione con le reti e le piattaforme responsabili della condivisione delle informazioni nella comunità di ciberdifesa, in stretta collaborazione con l'alto rappresentante. ***Dovrebbe inoltre favorire le sinergie con il piano d'azione sulla mobilità militare 2.0. Una rete di mobilità militare ben funzionante deve essere resiliente, anche nel contesto delle minacce informatiche e di altre minacce ibride che potrebbero colpire i nodi critici del sistema di trasporto a duplice uso. Ad esempio, un attacco informatico contro i sistemi utilizzati negli aeroporti, nei porti o nelle linee ferroviarie o un attacco informatico contro i mezzi militari***

potrebbe avere conseguenze importanti. Pertanto, la digitalizzazione dei processi e delle procedure, anche ai fini della necessaria cooperazione civile e militare, richiederà il rafforzamento dei sistemi informativi computerizzati contro le minacce informatiche.

Emendamento 13

Proposta di regolamento
Considerando 21 bis (nuovo)

Testo della Commissione	*Emendamento*
	(21 bis) In caso di crisi di cibersicurezza, un efficace scambio di informazioni è fondamentale per garantire la conoscenza situazionale nei settori del trasporto militare e civile. Tale scambio di informazioni dovrebbe inoltre stimolare la cooperazione tra le pertinenti autorità settoriali responsabili dei trasporti, le autorità competenti in materia di cibersicurezza, i SOC e i CSIRT.

Emendamento 14

Proposta di regolamento
Considerando 29

Testo della Commissione	*Emendamento*
(29) Nell'ambito delle azioni di preparazione, al fine di promuovere un approccio coerente e rafforzare la sicurezza in tutta l'Unione e nel suo mercato interno, è opportuno fornire un sostegno per verificare e valutare in modo coordinato il livello di cibersicurezza dei soggetti che operano nei settori altamente critici individuati ai sensi della direttiva (UE) 2022/2555. A tal fine la Commissione, con il sostegno dell'ENISA e in collaborazione con il gruppo di cooperazione NIS istituito dalla direttiva (UE) 2022/2555, dovrebbe	(29) Nell'ambito delle azioni di preparazione, al fine di promuovere un approccio coerente e rafforzare la sicurezza in tutta l'Unione e nel suo mercato interno, è opportuno fornire un sostegno per verificare e valutare in modo coordinato il livello di cibersicurezza dei soggetti che operano nei settori altamente critici individuati ai sensi della direttiva (UE) 2022/2555. A tal fine la Commissione, con il sostegno dell'ENISA e in collaborazione con il gruppo di cooperazione NIS istituito dalla direttiva (UE) 2022/2555, dovrebbe

individuare periodicamente i settori o i sottosettori pertinenti idonei a ricevere un sostegno finanziario per lo svolgimento di una verifica coordinata a livello dell'Unione. I settori o i sottosettori dovrebbero essere selezionati dall'allegato I della direttiva (UE) 2022/2555 ("Settori ad alta criticità"). Gli esercizi di verifica coordinata dovrebbero basarsi su scenari di rischio e metodologie comuni. La selezione dei settori e l'elaborazione degli scenari di rischio dovrebbero tenere conto delle valutazioni del rischio e degli scenari di rischio pertinenti a livello dell'Unione, compresa la necessità di evitare duplicazioni, come la valutazione del rischio e gli scenari di rischio previsti nelle conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, di cui devono occuparsi la Commissione, l'alto rappresentante e il gruppo di cooperazione NIS, in coordinamento con i pertinenti organismi e agenzie civili e militari e le pertinenti reti consolidate, compresa EU-CyCLONe. Dovrebbero inoltre essere prese in considerazione la valutazione del rischio delle reti e delle infrastrutture di comunicazione richiesta dall'invito ministeriale congiunto di Nevers e condotta dal gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA, e in collaborazione con l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC), le valutazioni coordinate del rischio da condurre ai sensi dell'articolo 22 della direttiva (UE) 2022/2555 e i test di resilienza operativa digitale previsti dal regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio[17]. La selezione dei settori dovrebbe inoltre tenere conto della raccomandazione del Consiglio su un approccio coordinato a livello di Unione per rafforzare la resilienza delle infrastrutture critiche.

individuare periodicamente i settori o i sottosettori pertinenti idonei a ricevere un sostegno finanziario per lo svolgimento di una verifica coordinata a livello dell'Unione. I settori o i sottosettori dovrebbero essere selezionati dall'allegato I della direttiva (UE) 2022/2555 ("Settori ad alta criticità"). ***Occorre prestare particolare attenzione al settore dei trasporti e ai suoi sottosettori (aereo, ferroviario, marittimo, stradale), in quanto comprendono infrastrutture critiche in cui gli incidenti e gli attacchi informatici potrebbero compromettere gravemente la sicurezza dei passeggeri e degli operatori.*** Gli esercizi di verifica coordinata dovrebbero basarsi su scenari di rischio e metodologie comuni. La selezione dei settori e l'elaborazione degli scenari di rischio dovrebbero tenere conto delle valutazioni del rischio e degli scenari di rischio pertinenti a livello dell'Unione, compresa la necessità di evitare duplicazioni, come la valutazione del rischio e gli scenari di rischio previsti nelle conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, di cui devono occuparsi la Commissione, l'alto rappresentante e il gruppo di cooperazione NIS, in coordinamento con i pertinenti organismi e agenzie civili e militari e le pertinenti reti consolidate, compresa EU-CyCLONe. Dovrebbero inoltre essere prese in considerazione la valutazione del rischio delle reti e delle infrastrutture di comunicazione richiesta dall'invito ministeriale congiunto di Nevers e condotta dal gruppo di cooperazione NIS, con il sostegno della Commissione e dell'ENISA, e in collaborazione con l'Organismo dei regolatori europei delle comunicazioni elettroniche (BEREC), le valutazioni coordinate del rischio da condurre ai sensi dell'articolo 22 della direttiva (UE) 2022/2555 e i test di resilienza operativa digitale previsti dal regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio[17]. La selezione dei settori

	dovrebbe inoltre tenere conto della raccomandazione del Consiglio su un approccio coordinato a livello di Unione per rafforzare la resilienza delle infrastrutture critiche.
[17] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, 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, (UE) n. 909/2014 e (UE) 2016/1011.	[17] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, 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, (UE) n. 909/2014 e (UE) 2016/1011.

Emendamento 15

Proposta di regolamento
Considerando 30 bis (nuovo)

Testo della Commissione	*Emendamento*
	(30 bis) Viste la criticità del settore e le implicazioni delle minacce informatiche per la mobilità e, di conseguenza, per le vite di passeggeri e pedoni, è opportuno dare priorità al settore dei trasporti per quanto riguarda la verifica coordinata della preparazione dei soggetti.

Emendamento 16

Proposta di regolamento
Considerando 35 bis (nuovo)

Testo della Commissione	*Emendamento*
	(35 bis) In considerazione dell'aumento dei compiti e delle responsabilità attribuiti all'ENISA dalla presente proposta e dalla proposta di legge sulla ciberresilienza, è necessaria l'adozione del bilancio rettificativo 1/2022 dell'ENISA per l'attuazione pilota di un'azione di sostegno alla cibersicurezza.

	Inoltre, alla luce degli interessi dell'Unione in gioco, occorre assegnare all'ENISA risorse finanziarie e umane supplementari.

Emendamento 17

Proposta di regolamento
Considerando 38 bis (nuovo)

Testo della Commissione	*Emendamento*
	(38 bis) Lo sviluppo di capacità e competenze dovrebbe pertanto assumere un ruolo centrale in tutti i settori, non da ultimo in quelli vulnerabili alle minacce di cibersicurezza, come il personale impiegato nel trasporto di massa o nelle infrastrutture critiche, compresi i sistemi di controllo dei treni e gli strumenti digitali di pianificazione dei trasporti per tutti i modi di trasporto. L'introduzione e l'ulteriore sviluppo della cultura della cibersicurezza sono dunque fondamentali per il successo dell'attuazione del presente regolamento, sia ai fini della sensibilizzazione dei cittadini che delle conoscenze degli specialisti in tutti i settori delle infrastrutture critiche.

Emendamento 18

Proposta di regolamento
Articolo 1 – paragrafo 2 – lettera a

Testo della Commissione	*Emendamento*
a) migliorare il rilevamento e la conoscenza situazionale comuni dell'Unione in materia di minacce e incidenti informatici, consentendo così di rafforzare la posizione competitiva dei settori dell'industria e dei servizi nell'Unione nell'ambito dell'economia digitale e di contribuire alla sovranità tecnologica dell'Unione nel settore della	a) migliorare il rilevamento e la conoscenza situazionale comuni dell'Unione in materia di minacce e incidenti informatici, consentendo così di rafforzare la posizione competitiva dei settori dell'industria***, delle infrastrutture di trasporto*** e dei servizi nell'Unione nell'ambito dell'economia digitale e di contribuire alla sovranità tecnologica

cibersicurezza;	dell'Unione nel settore della cibersicurezza;

Emendamento 19

Proposta di regolamento
Articolo 1 – paragrafo 2 – lettera b

Testo della Commissione	*Emendamento*
b) rafforzare la preparazione dei soggetti che operano in settori critici e altamente critici in tutta l'Unione e potenziare la solidarietà sviluppando capacità di risposta comuni contro gli incidenti di cibersicurezza significativi o su vasta scala, permettendo inoltre ai paesi terzi associati al programma Europa digitale di accedere al sostegno offerto dall'Unione per la risposta agli incidenti di cibersicurezza;	b) rafforzare la preparazione dei soggetti che operano in settori critici e altamente critici in tutta l'Unione e potenziare la solidarietà sviluppando capacità di risposta comuni contro gli incidenti di cibersicurezza significativi o su vasta scala, ***prestando particolare attenzione alle infrastrutture informatiche e fisiche critiche,*** permettendo inoltre ai paesi terzi associati al programma Europa digitale di accedere al sostegno offerto dall'Unione per la risposta agli incidenti di cibersicurezza;

Emendamento 20

Proposta di regolamento
Articolo 1 – paragrafo 2 – lettera c bis (nuova)

Testo della Commissione	*Emendamento*
	c bis) rafforzare la preparazione, la cooperazione e l'efficacia dell'Unione nel proteggere le infrastrutture e i servizi di trasporto negli Stati membri dagli incidenti di cibersicurezza, al fine di garantire il funzionamento continuo del settore dei trasporti, l'integrità delle catene di approvvigionamento e la mobilità a livello dell'Unione.

Emendamento 21

Proposta di regolamento
Articolo 3 – paragrafo 2 – comma 1 – lettera c

Testo della Commissione	*Emendamento*
c) contribuire a una migliore protezione e risposta alle minacce informatiche;	c) contribuire a una migliore protezione e risposta alle minacce informatiche***, anche per le infrastrutture di trasporto caratterizzate da una natura transfrontaliera, come la TEN-T, o dallo scambio di dati attraverso tecnologie senza fili, come i sistemi di trasporto intelligenti***;

Emendamento 22

Proposta di regolamento
Articolo 3 – paragrafo 2 – comma 2

Testo della Commissione	*Emendamento*
È messo a punto in collaborazione con l'infrastruttura paneuropea di calcolo ad alte prestazioni istituita ai sensi del regolamento (UE) 2021/1173.	È messo a punto in collaborazione con l'infrastruttura paneuropea di calcolo ad alte prestazioni istituita ai sensi del regolamento (UE) 2021/1173. ***Consente la collaborazione, attraverso protocolli e norme specifici, con la comunità della ciberdifesa al fine di garantire lo sviluppo di capacità civili di rilevamento e conoscenza situazionale più solide ai fini della protezione delle infrastrutture critiche. A tal proposito, sono sviluppate sinergie anche con il piano d'azione sulla mobilità militare 2.0 ed è assicurato un efficace scambio di informazioni per fornire una conoscenza situazionale ai settori del trasporto militare e civile.***

Emendamento 23

Proposta di regolamento
Articolo 8 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. La Commissione coinvolge il ciberscudo europeo, in particolare i SOC transfrontalieri, nel suo parere destinato agli Stati membri nel quadro della proposta di regolamento sulla rete

	transeuropea dei trasporti (COM(2021)0812) ogniqualvolta la partecipazione o un contributo di qualsiasi tipo da parte di una persona fisica di un paese terzo o di un'impresa di un paese terzo possa incidere sulla cibersicurezza di infrastrutture critiche transfrontaliere, come la TEN-T.

Emendamento 24

Proposta di regolamento
Articolo 10 – paragrafo 1 – lettera a

Testo della Commissione	*Emendamento*
a) azioni di preparazione, compresa la verifica coordinata della preparazione dei soggetti che operano in settori altamente critici in tutta l'Unione;	a) azioni di preparazione, compresa la verifica coordinata della preparazione dei soggetti che operano in settori altamente critici in tutta l'Unione***, prestando particolare attenzione alle infrastrutture di trasporto e ai relativi sottosettori elencati all'allegato I della direttiva (UE) 2022/2555***;

Emendamento 25

Proposta di regolamento
Articolo 18 – paragrafo 2

Testo della Commissione	*Emendamento*
2. Per preparare la relazione di riesame dell'incidente di cui al paragrafo 1, l'ENISA collabora con tutti i portatori di interessi, compresi i rappresentanti degli Stati membri, della Commissione, di altre istituzioni e di altri organi e organismi pertinenti dell'UE, dei fornitori di servizi di sicurezza gestiti e degli utenti di servizi di cibersicurezza. Ove opportuno, l'ENISA collabora anche con i soggetti interessati da incidenti di cibersicurezza significativi o su vasta scala. A sostegno del riesame l'ENISA può anche consultare altri tipi di portatori di interessi. I rappresentanti consultati dichiarano eventuali potenziali	2. Per preparare la relazione di riesame dell'incidente di cui al paragrafo 1, l'ENISA collabora con tutti i portatori di interessi, compresi i rappresentanti degli Stati membri, della Commissione, di altre istituzioni e di altri organi e organismi pertinenti dell'UE, dei fornitori di servizi di sicurezza gestiti e degli utenti di servizi di cibersicurezza. Ove opportuno, l'ENISA collabora anche con i soggetti interessati da incidenti di cibersicurezza significativi o su vasta scala***, compresi gli operatori di trasporto***. A sostegno del riesame l'ENISA può anche consultare altri tipi di portatori di interessi. I rappresentanti consultati

conflitti di interessi.	dichiarano eventuali potenziali conflitti di interessi.

Emendamento 26

Proposta di regolamento
Articolo 19 – punto 1 – lettera b
Regolamento (UE) 2021/694
Articolo 6 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. Alla luce degli interessi dell'Unione in gioco, in considerazione delle sua responsabilità di elaborare proposte di sistemi di certificazione a norma del regolamento (UE) 2019/881, di esaminare e valutare le minacce informatiche, le vulnerabilità e le azioni di attenuazione, di preparare una relazione di riesame degli incidenti per il meccanismo di riesame degli incidenti di cibersicurezza nonché di fornire formazione agli operatori delle infrastrutture critiche contro gli attacchi e gli incidenti informatici, e alla luce delle nuove responsabilità attribuitele nel quadro della proposta di regolamento sulla ciberresilienza, l'ENISA è dotata delle risorse necessarie a titolo del bilancio dell'Unione conformemente alla legislazione applicabile.

Emendamento 27

Proposta di regolamento
Articolo 19 – punto 1 bis (nuovo)
Regolamento (UE) 2021/694
Articolo 7 – paragrafo 1 – lettera c bis (nuova)

Testo della Commissione	*Emendamento*
	1 bis) l'articolo 7 è così modificato:
	a) il paragrafo 1 è così modificato:
	1) è inserita la seguente lettera c bis):

"c bis) sostenere una formazione di alta qualità per gli operatori di trasporto e per i gestori e la forza lavoro delle infrastrutture di trasporto critiche, anche al fine di condividere e attuare efficacemente pratiche di attenuazione in caso di attacchi o incidenti informatici alle infrastrutture critiche, come quelle fornite dal kit di strumenti per la cibersicurezza nel settore dei trasporti.";

PROCEDURA DELLA COMMISSIONE COMPETENTE PER PARERE

Titolo	Proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi
Riferimenti	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Commissione competente per il merito Annuncio in Aula	ITRE 1.6.2023
Parere espresso da Annuncio in Aula	TRAN 1.6.2023
Relatore per parere Nomina	Gheorghe Falcă 7.7.2023
Approvazione	25.10.2023
Esito della votazione finale	+: 38 –: 0 0: 0
Membri titolari presenti al momento della votazione finale	Magdalena Adamowicz, Andris Ameriks, José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Karolin Braunsberger-Reinhold, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Carlo Fidanza, Jens Gieseke, Elsi Katainen, Elena Kountoura, Bogusław Liberadzki, Peter Lundgren, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Rovana Plumb, Thomas Rudner, Massimiliano Salini, Vera Tax, Barbara Thaler, István Ujhelyi, Achille Variati, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Supplenti presenti al momento della votazione finale	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

VOTAZIONE FINALE PER APPELLO NOMINALE IN SEDE DI COMMISSIONE COMPETENTE PER PARERE

38	+
ECR	Carlo Fidanza, Peter Lundgren, Dorien Rookmaker
ID	Roman Haider
PPE	Magdalena Adamowicz, Karolin Braunsberger-Reinhold, Gheorghe Falcă, Jens Gieseke, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Colm Markey, Cláudia Monteiro de Aguiar, Ljudmila Novak, Massimiliano Salini, Barbara Thaler, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Renew	José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Pierre Karleskind, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen
S&D	Andris Ameriks, Sara Cerdas, Josianne Cutajar, Bogusław Liberadzki, Rovana Plumb, Thomas Rudner, Vera Tax, István Ujhelyi, Achille Variati, Petar Vitanov
The Left	Elena Kountoura
Verts/ALE	Karima Delli, Anna Deparnay-Grunenberg, Pär Holmgren, Tilly Metz

0	-

0	0

Significato dei simboli utilizzati:
+ : favorevoli
- : contrari
0 : astenuti

PROCEDURA DELLA COMMISSIONE COMPETENTE PER IL MERITO

Titolo	Istituzione di misure intese a rafforzare la solidarietà e la capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi			
Riferimenti	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)			
Presentazione della proposta al PE	19.4.2023			
Commissione competente per il merito Annuncio in Aula	ITRE 1.6.2023			
Commissioni competenti per parere Annuncio in Aula	AFET 1.6.2023	BUDG 1.6.2023	CONT 1.6.2023	IMCO 1.6.2023
	TRAN 1.6.2023	LIBE 1.6.2023		
Pareri non espressi Decisione	BUDG 26.4.2023	CONT 24.5.2023	IMCO 23.5.2023	LIBE 30.5.2023
Relatori Nomina	Lina Gálvez Muñoz 2.5.2023			
Esame in commissione	19.9.2023			
Approvazione	7.12.2023			
Esito della votazione finale	+: –: 0:	43 10 1		
Membri titolari presenti al momento della votazione finale	Nicola Beer, Hildegard Bentele, Vasile Blaga, Michael Bloss, Marc Botenga, Martin Buschmann, Jerzy Buzek, Maria da Graça Carvalho, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Martina Dlabajová, Christian Ehler, Valter Flego, Niels Fuglsang, Nicolás González Casares, Henrike Hahn, Ivo Hristov, Ivars Ijabs, Romana Jerković, Seán Kelly, Izabela-Helena Kloc, Andrius Kubilius, Miapetra Kumpula-Natri, Iskra Mihaylova, Angelika Niebler, Niklas Nienaß, Johan Nissinen, Mikuláš Peksa, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Manuela Ripa, Robert Roos, Sara Skyttedal, Riho Terras, Pernille Weiss, Carlos Zorrinho			
Supplenti presenti al momento della votazione finale	Andrus Ansip, Laura Ballarín Cereza, Cornelia Ernst, Alexis Georgoulis, Ladislav Ilčić, Elena Kountoura, Alin Mituța, Günther Sidl, Jordi Solé, Susana Solís Pérez			
Supplenti (art. 209, par. 7) presenti al momento della votazione finale	Alexander Alexandrov Yordanov, Jonás Fernández, Virginie Joron, Radan Kanev, Karin Karlsbro			
Deposito	8.12.2023			

VOTAZIONE FINALE PER APPELLO NOMINALE
IN SEDE DI COMMISSIONE COMPETENTE PER IL MERITO

43	+
ECR	Ladislav Ilčić, Izabela-Helena Kloc
ID	Marie Dauchy, Virginie Joron
NI	Alexis Georgoulis
PPE	Alexander Alexandrov Yordanov, Hildegard Bentele, Vasile Blaga, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Radan Kanev, Seán Kelly, Andrius Kubilius, Angelika Niebler, Markus Pieper, Sara Skyttedal, Riho Terras, Pernille Weiss
Renew	Andrus Ansip, Nicola Beer, Nicola Danti, Martina Dlabajová, Valter Flego, Ivars Ijabs, Karin Karlsbro, Iskra Mihaylova, Alin Mituța, Morten Petersen, Susana Solís Pérez
S&D	Laura Ballarín Cereza, Josianne Cutajar, Jonás Fernández, Niels Fuglsang, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Tsvetelina Penkova, Günther Sidl, Carlos Zorrinho
The Left	Elena Kountoura

10	-
ECR	Johan Nissinen, Robert Roos
The Left	Marc Botenga, Cornelia Ernst
Verts/ALE	Michael Bloss, Henrike Hahn, Niklas Nienaß, Mikuláš Peksa, Manuela Ripa, Jordi Solé

1	0
NI	Martin Buschmann

Significato dei simboli utilizzati:
+ : favorevoli
- : contrari
0 : astenuti