Parlamento europeo
2019-2024

Commissione per gli affari esteri

2023/0109(COD)

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

PA_Legam

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 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	(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. ***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

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.	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 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[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***, come pure la sua abilità di reagire in modo proattivo e risoluto a tali minacce e incidenti***.

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

[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, 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[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 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 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).

---

[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).

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	(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").	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	(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***

informatiche.	***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 siano condivise e raccolte a livello nazionale in modo efficace e semplificato.	(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. ***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, 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.	(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 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	(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.	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 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	(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***, 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

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 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	(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***, alla comunità di ciberdifesa*** e alla

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.	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 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.	(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 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	(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

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).

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).

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 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	(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***[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

e nei paesi terzi.	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.	[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	(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

strumenti della diplomazia informatica.

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).

[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.

[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.

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	(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.	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	(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***[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.

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 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	(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.	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	(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.	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	(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.

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 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 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	(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 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

associati al programma Europa digitale.	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	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

infrastrutture, l'ECCC e il SOC nazionale concludono una convezione di accoglienza e di utilizzo che disciplina l'uso degli strumenti e delle infrastrutture.	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 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.	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 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	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**.**	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	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.	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	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.	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 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.	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 ***(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	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;	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 Commissione trasmette al Parlamento europeo e al Consiglio una relazione di valutazione e sul riesame del presente regolamento.	Entro [***tre*** anni dalla data di applicazione del presente regolamento ***e 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