Parlamento europeo
2019-2024

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

2023/0109(COD)

22.9.2023

EMENDAMENTI
46 - 216

Progetto di relazione
Lina Gálvez Muñoz
(PE752.795v01-00)

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

Proposta di regolamento
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Emendamento 46
Evžen Tošenovský

Proposta di regolamento
Titolo 1

Testo della Commissione	*Emendamento*
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	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 ***(regolamento sulla cibersolidarietà)***

Or. en

Emendamento 47
Ville Niinistö
a nome del gruppo Verts/ALE

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 ***e vulnerabili*** 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.

Or. en

Motivazione

La necessità del presente testo giuridico nasce dal fatto che dalle dipendenze fondamentali derivano anche le vulnerabilità.

Emendamento 48
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Considerando 2

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

cooperazione stretta e coordinata tra il settore pubblico, il settore privato, gli Stati membri, le istituzioni o agenzie dell'Unione e il mondo accademico al fine di migliorare la posizione dell'Unione in materia di cibersicurezza. La risposta dell'Unione dovrebbe essere basata sulla collaborazione con istituzioni e partner internazionali di fiducia e che condividono gli stessi principi, in linea con i quadri e gli accordi di cooperazione internazionale.

Or. en

Emendamento 49
Ville Niinistö
a nome del gruppo Verts/ALE

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. Tale minaccia va oltre l'aggressione militare della Russia nei confronti dell'Ucraina ed è destinata a persistere, data la molteplicità di soggetti allineati con le autorità di governo ***e*** criminali coinvolti nelle attuali tensioni geopolitiche. Tali incidenti possono ostacolare l'erogazione di servizi

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.

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.

Or. en

Motivazione

L'inclusione generale dell'hacktivismo tra le attività criminali non riflette la varietà di tali attività, comprese le proteste legittime e la denuncia di irregolarità. Evitare ambiguità e tutelare le attività legittime rappresenterebbe un vantaggio per il testo.

Emendamento 50
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Ioan-Rareş Bogdan, Cristian-Silviu Buşoi

Proposta di regolamento
Considerando 3

Testo della Commissione

(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

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***[1]***, è necessario accrescere la resilienza dei cittadini, delle imprese***, comprese le microimprese e le piccole e medie imprese (PMI),*** e dei soggetti che gestiscono infrastrutture critiche***, tra cui le autorità locali o regionali,*** contro le

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.

crescenti minacce alla cibersicurezza, che possono avere conseguenze devastanti a livello sociale ed economico. Occorre quindi investire in infrastrutture***,*** servizi ***e personale altamente qualificato dotato delle competenze necessarie*** 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***, anche attraverso la raccolta proattiva di informazioni***. 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. ***[1] https://futureu.europa.eu/it/?locale=it.***

---

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

Or. en

Emendamento 51
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Considerando 5

Testo della Commissione	*Emendamento*
(5) I crescenti rischi di cibersicurezza e un panorama di minacce globalmente complesso, con il chiaro rischio di rapida propagazione di incidenti informatici da uno Stato membro all'altro e da un paese terzo all'Unione, richiedono una solidarietà rafforzata a livello di Unione per migliorare il rilevamento delle minacce e degli incidenti di cibersicurezza, nonché la preparazione e la risposta agli stessi. Nelle conclusioni del Consiglio su una posizione	(5) I crescenti rischi di cibersicurezza e un panorama di minacce globalmente complesso, con il chiaro rischio di rapida propagazione di incidenti informatici da uno Stato membro all'altro e da un paese terzo all'Unione, richiedono una solidarietà rafforzata a livello di Unione per migliorare il rilevamento delle minacce e degli incidenti di cibersicurezza, nonché la preparazione e la risposta agli stessi***, come pure la ripresa dai medesimi***. Nelle

dell'UE in materia di deterrenza informatica gli Stati membri hanno inoltre invitato la Commissione a presentare una proposta su un nuovo Fondo di risposta alle emergenze di cibersicurezza[21].	conclusioni del Consiglio su una posizione dell'UE in materia di deterrenza informatica gli Stati membri hanno inoltre invitato la Commissione a presentare una proposta su un nuovo Fondo di risposta alle emergenze di cibersicurezza[21].
[21] Conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, approvate dal Consiglio nella sessione del 23 maggio 2022 (9364/22).	[21] Conclusioni del Consiglio sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica, approvate dal Consiglio nella sessione del 23 maggio 2022 (9364/22).

Or. en

Emendamento 52
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Considerando 9 bis (nuovo)

Testo della Commissione	*Emendamento*
	(9 bis) Alla luce degli sviluppi geopolitici e del crescente panorama delle minacce informatiche, sono importanti la continuità e l'ulteriore sviluppo delle misure previste dal presente regolamento, in particolare del ciberscudo europeo e del meccanismo europeo per le emergenze. Pertanto, occorre garantire una linea di bilancio specifica nel quadro finanziario pluriennale per il periodo 2028-2034. Gli Stati membri dovrebbero inoltre impegnarsi a sostenere tutte le misure necessarie per rafforzare la solidarietà all'interno dell'Unione e ridurre le minacce e gli incidenti informatici in tutta l'Unione.

Or. en

Emendamento 53

Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Considerando 12

Testo della Commissione	*Emendamento*
(12) Al fine di rendere più efficaci la prevenzione e la valutazione delle minacce e degli incidenti informatici, nonché la risposta agli stessi, occorre sviluppare una conoscenza più completa delle minacce alle risorse e alle infrastrutture critiche sul territorio dell'Unione, compresa la loro distribuzione geografica, l'interconnessione e gli effetti potenziali in caso di attacchi informatici contro tali infrastrutture. Dovrebbe essere realizzata un'infrastruttura di SOC dell'Unione su vasta scala ("ciberscudo europeo"), comprendente diverse piattaforme transfrontaliere interoperanti, ciascuna composta da diversi SOC nazionali. Tale infrastruttura dovrebbe essere al servizio degli interessi e delle esigenze di cibersicurezza nazionali e dell'Unione, sfruttando tecnologie all'avanguardia per strumenti di analisi e di raccolta di dati avanzati, migliorando le capacità di rilevamento e di gestione delle minacce informatiche e permettendo una conoscenza situazionale in tempo reale. Dovrebbe inoltre servire a incrementare le capacità di rilevamento delle minacce e degli incidenti di cibersicurezza e quindi a integrare e sostenere i soggetti e le reti dell'Unione responsabili della gestione delle crisi nell'UE, in particolare la rete europea delle organizzazioni di collegamento per le crisi informatiche ("EU-CyCLONe"), come definita nella direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[24].	(12) Al fine di rendere più efficaci la prevenzione e la valutazione delle minacce e degli incidenti informatici, nonché la risposta agli stessi ***e la ripresa dai medesimi***, occorre sviluppare una conoscenza più completa delle minacce alle risorse e alle infrastrutture critiche sul territorio dell'Unione, compresa la loro distribuzione geografica, l'interconnessione e gli effetti potenziali in caso di attacchi informatici contro tali infrastrutture***, tra cui la raccolta proattiva di informazioni***. Dovrebbe essere realizzata un'infrastruttura di SOC dell'Unione su vasta scala ("ciberscudo europeo"), comprendente diverse piattaforme transfrontaliere interoperanti, ciascuna composta da diversi SOC nazionali***. Un SOC nazionale è una memoria centralizzata responsabile della raccolta continua di informazioni relative ai dati sulle minacce e del miglioramento costante della posizione in materia di cibersicurezza di soggetti rientranti nella giurisdizione nazionale attraverso la prevenzione, il rilevamento e l'analisi delle minacce alla cibersicurezza***. Tale infrastruttura dovrebbe essere al servizio degli interessi e delle esigenze di cibersicurezza nazionali e dell'Unione, sfruttando tecnologie all'avanguardia per strumenti di analisi e di raccolta di dati avanzati, migliorando le capacità di rilevamento e di gestione delle minacce informatiche e permettendo una conoscenza situazionale in tempo reale. Dovrebbe inoltre servire a incrementare le capacità di rilevamento delle minacce e degli incidenti di cibersicurezza e quindi a integrare e sostenere i soggetti e le reti dell'Unione responsabili della gestione delle crisi nell'UE, in particolare la rete

europea delle organizzazioni di collegamento per le crisi informatiche ("EU-CyCLONe"), come definita nella direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[24].

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

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

Or. en

Emendamento 54
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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) ***Per partecipare al ciberscudo europeo,*** ogni Stato membro dovrebbe designare un organismo pubblico a livello nazionale, incaricato di coordinare le attività di rilevamento delle minacce informatiche ***e di condivisione delle informazioni*** in tale Stato membro***. Gli Stati membri sono fortemente incoraggiati a integrare la memoria del SOC nazionale nella struttura e nella governance informatiche già esistenti per non creare ulteriori livelli di governance e per allineare il regolamento sulla cibersolidarietà alla legislazione già esistente, inclusa la direttiva (UE) 2022/2555***. Questi SOC nazionali dovrebbero fungere da punto di riferimento e porta di accesso a livello nazionale per la partecipazione ***di soggetti pubblici e***

privati, in particolare dei rispettivi SOC, al ciberscudo europeo e garantire che le informazioni sulle minacce informatiche provenienti da soggetti pubblici e privati siano condivise e raccolte a livello nazionale in modo efficace e semplificato. ***I SOC nazionali dovrebbero rafforzare la collaborazione e la condivisione delle informazioni tra soggetti pubblici e privati al fine di smantellare i silos di comunicazione attualmente esistenti. In tal modo, potrebbero sostenere la creazione di modelli di scambio di dati e dovrebbero facilitare e incoraggiare la condivisione delle informazioni in un ambiente affidabile e sicuro. Una cooperazione stretta e coordinata tra soggetti pubblici e privati è fondamentale per rafforzare la resilienza dell'Unione nel campo della cibersicurezza.***

Or. en

Emendamento 55
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	(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 ***proattive e*** di alta

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***.	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. ***I SOC transfrontalieri dovrebbero agevolare e incoraggiare la condivisione delle informazioni in un ambiente affidabile e sicuro. L'ENISA dovrebbe sostenere i SOC transfrontalieri nelle questioni relative alla cooperazione operativa.*** Tali SOC dovrebbero garantire nuove capacità aggiuntive, ***pur essendo integrati nell'infrastruttura di cibersicurezza già esistente, che comprende i*** SOC e ***i*** gruppi di intervento per la sicurezza informatica in caso di incidente ("CSIRT") nonché altri soggetti pertinenti.

Or. en

Emendamento 56
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Considerando 15

Testo della Commissione	*Emendamento*
(15) A livello nazionale, il monitoraggio, il rilevamento e l'analisi delle minacce informatiche sono solitamente garantiti dai SOC di soggetti pubblici e privati, in combinazione con i CSIRT. Questi ultimi inoltre scambiano informazioni nel contesto della rete di CSIRT, conformemente a quanto disposto dalla direttiva (UE) 2022/2555. I SOC transfrontalieri dovrebbero costituire una nuova capacità ***complementare alla*** rete di CSIRT, mettendo in comune e condividendo i dati sulle minacce alla cibersicurezza provenienti da soggetti	(15) A livello nazionale, il monitoraggio, il rilevamento e l'analisi delle minacce informatiche sono solitamente garantiti dai SOC di soggetti pubblici e privati, in combinazione con i CSIRT. Questi ultimi inoltre scambiano informazioni nel contesto della rete di CSIRT, conformemente a quanto disposto dalla direttiva (UE) 2022/2555. I SOC transfrontalieri dovrebbero costituire una nuova capacità ***integrata nell'infrastruttura di cibersicurezza già esistente, specialmente nella*** rete di CSIRT, mettendo in comune e

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.	condividendo i dati sulle minacce alla cibersicurezza provenienti da soggetti pubblici e privati***, in particolare dai relativi SOC***, accrescendo il valore di tali dati mediante l'analisi di esperti, infrastrutture acquisite congiuntamente e strumenti all'avanguardia, e contribuendo allo sviluppo delle capacità e della sovranità tecnologica dell'Unione***, al fine di potenziarne la resilienza***.

Or. en

Emendamento 57
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Considerando 15

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

Or. en

Emendamento 58
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 transfrontalieri.	(16) I SOC transfrontalieri dovrebbero fungere da punto centrale in grado di consentire un'ampia condivisione di dati pertinenti e di analisi delle minacce informatiche e permettere la diffusione di informazioni sulle minacce tra più soggetti di diversa natura (ad esempio, squadre di pronto intervento informatico ("CERT"), CSIRT, centri di analisi e condivisione delle informazioni ("ISAC"), operatori di infrastrutture critiche) ***per facilitare lo smantellamento dei silos di comunicazione attualmente esistenti. In tal modo, i SOC transfrontalieri potrebbero anche sostenere la creazione di modelli di scambio di dati in tutta l'Unione***. Le informazioni scambiate tra i partecipanti a un SOC transfrontaliero potrebbero includere dati provenienti da reti e sensori, feed di analisi delle minacce***, compresa la raccolta proattiva di informazioni***, indicatori di compromissione e informazioni contestualizzate su incidenti, minacce e vulnerabilità. I SOC transfrontalieri dovrebbero inoltre stipulare accordi di cooperazione con altri SOC transfrontalieri.

Or. en

Emendamento 59
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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 transfrontalieri.	(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 ***analizzati*** provenienti da reti***,*** sensori***, registrazioni e telemetria***, feed di analisi delle minacce, indicatori di compromissione e informazioni contestualizzate su ***tattiche, tecniche e procedure (TTP),*** incidenti***, campioni di malware***, minacce e vulnerabilità. I SOC transfrontalieri dovrebbero inoltre stipulare accordi di cooperazione con altri SOC transfrontalieri.

Or. en

Emendamento 60
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	(17) La condivisione della conoscenza situazionale tra le autorità competenti è un prerequisito indispensabile per la preparazione e il coordinamento a livello dell'Unione in caso di incidenti di cibersicurezza significativi e su vasta scala. La direttiva (UE) 2022/2555 istituisce EU-CyCLONe al fine di sostenere la gestione coordinata a livello operativo degli

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

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 linea con le disposizioni già esistenti stabilite nella direttiva (UE) 2022/2555***. In particolare, a seconda della situazione, le informazioni da condividere potrebbero includere informazioni tecniche, informazioni sulla natura e sulle motivazioni dell'autore di un attacco informatico o di un potenziale autore nonché informazioni non tecniche di livello superiore su un incidente di cibersicurezza potenziale o in corso su vasta scala. In questo contesto è opportuno prestare la dovuta attenzione al principio della necessità di conoscere e alla natura potenzialmente sensibile delle informazioni condivise.

Or. en

Emendamento 61
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş

Bogdan

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 ***nonché di personale altamente qualificato***. Ciò dovrebbe consentire di migliorare le capacità collettive di rilevamento e di avvertire tempestivamente le autorità e i soggetti competenti, in particolare utilizzando le più recenti tecnologie di intelligenza artificiale e di analisi dei dati.

Or. en

Emendamento 62
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Considerando 20

Testo della Commissione	*Emendamento*
(20) Mediante la raccolta, la condivisione e lo scambio di dati, il ciberscudo europeo dovrebbe rafforzare la sovranità tecnologica dell'Unione. La condivisione di dati selezionati di alta qualità dovrebbe inoltre contribuire allo sviluppo di tecnologie avanzate di intelligenza artificiale e di analisi dei dati ***e*** dovrebbe essere facilitata dal collegamento del ciberscudo europeo con l'infrastruttura paneuropea di calcolo ad alte prestazioni istituita dal regolamento (UE) 2021/1173 del Consiglio[25].	(20) Mediante la raccolta, la condivisione e lo scambio di dati, il ciberscudo europeo dovrebbe rafforzare la sovranità tecnologica dell'Unione. La condivisione di dati selezionati di alta qualità dovrebbe inoltre contribuire allo sviluppo di tecnologie avanzate di intelligenza artificiale e di analisi dei dati***, tenendo tuttavia conto che l'intelligenza artificiale è più efficace se abbinata all'analisi umana. Pertanto, resta cruciale la presenza di personale altamente qualificato per la condivisione di dati di***

	alta qualità e la raccolta di informazioni proattive sulle minacce. Tale condivisione dovrebbe essere facilitata dal collegamento del ciberscudo europeo con l'infrastruttura paneuropea di calcolo ad alte prestazioni istituita dal regolamento (UE) 2021/1173 del Consiglio[25].
[25] Regolamento (UE) 2021/1173 del Consiglio, del 13 luglio 2021, relativo all'istituzione dell'impresa comune per il calcolo ad alte prestazioni europeo e che abroga il regolamento (UE) 2018/1488 (GU L 256 del 19.7.2021, pag. 3).	[25] Regolamento (UE) 2021/1173 del Consiglio, del 13 luglio 2021, relativo all'istituzione dell'impresa comune per il calcolo ad alte prestazioni europeo e che abroga il regolamento (UE) 2018/1488 (GU L 256 del 19.7.2021, pag. 3).

Or. en

Emendamento 63
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Considerando 20

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

Or. en

Emendamento 64
Ville Niinistö
a nome del gruppo Verts/ALE

Proposta di regolamento
Considerando 21

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

Or. en

Motivazione

Nell'ottica di evitare duplicazioni e salvaguardare i diritti e le libertà, la collaborazione tra il lato civile e quello di difesa della cibersicurezza deve basarsi su garanzie, evitando di cambiare la destinazione dei finanziamenti civili.

Emendamento 65
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Considerando 24

Testo della Commissione	*Emendamento*
(24) Alla luce dell'aumento dei rischi e del numero di incidenti informatici che colpiscono gli Stati membri, occorre istituire uno strumento di sostegno alle crisi per migliorare la resilienza dell'Unione agli incidenti di cibersicurezza significativi e su vasta scala e integrare le azioni degli Stati membri mediante un sostegno finanziario di emergenza per la preparazione, la risposta e il ripristino immediato dei servizi essenziali. Tale strumento dovrebbe consentire una rapida mobilitazione dell'assistenza in circostanze definite e nel rispetto di condizioni ben precise, e permettere un monitoraggio e una valutazione accurati delle modalità di utilizzo delle risorse. Sebbene agli Stati membri spetti la responsabilità primaria della prevenzione degli incidenti e delle crisi di cibersicurezza, nonché della preparazione e della risposta agli stessi, il meccanismo per le emergenze di cibersicurezza promuove la solidarietà tra gli Stati membri conformemente all'articolo 3, paragrafo 3, del trattato sull'Unione europea ("TUE").	(24) Alla luce dell'aumento dei rischi e del numero di incidenti informatici che colpiscono gli Stati membri, occorre istituire uno strumento di sostegno alle crisi per migliorare la resilienza dell'Unione agli incidenti di cibersicurezza significativi e su vasta scala e integrare le azioni degli Stati membri mediante un sostegno finanziario di emergenza per la preparazione, la risposta e il ripristino immediato dei servizi essenziali. Tale strumento dovrebbe consentire una rapida ***ed efficace*** mobilitazione dell'assistenza in circostanze definite e nel rispetto di condizioni ben precise, e permettere un monitoraggio e una valutazione accurati delle modalità di utilizzo delle risorse. Sebbene agli Stati membri spetti la responsabilità primaria della prevenzione degli incidenti e delle crisi di cibersicurezza, nonché della preparazione e della risposta agli stessi, il meccanismo per le emergenze di cibersicurezza promuove la solidarietà tra gli Stati membri conformemente all'articolo 3, paragrafo 3, del trattato sull'Unione europea ("TUE").

Or. en

Emendamento 66

Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Considerando 27

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

Or. en

Emendamento 67
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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	(33) È opportuno istituire gradualmente una riserva per la cibersicurezza a livello di Unione, costituita da servizi erogati da fornitori privati di servizi di sicurezza gestiti a sostegno di azioni di risposta e di ripresa immediata in caso di incidenti di cibersicurezza significativi o su vasta scala. La riserva dell'UE per la cibersicurezza dovrebbe garantire la disponibilità e la prontezza dei servizi***, rafforzando la resilienza e la competitività dell'Unione, inclusa la partecipazione dei fornitori europei di servizi di sicurezza gestiti che sono PMI. I fornitori di fiducia, comprese le PMI, dovrebbero essere in grado di***

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.	***collaborare tra loro al fine di soddisfare i criteri di cui sopra***. I servizi della riserva dell'UE per la cibersicurezza dovrebbero servire a sostenere le autorità nazionali nel fornire assistenza ai soggetti colpiti che operano in settori critici o altamente critici, a integrazione delle azioni da esse svolte a livello nazionale***. Ove possibile, i servizi dovrebbero essere basati su tecnologie all'avanguardia, tra cui il cloud e l'intelligenza artificiale. Pertanto, la riserva per la cibersicurezza dovrebbe incentivare gli investimenti nella ricerca e nell'innovazione per promuovere lo sviluppo di tali tecnologie. Ove opportuno, potrebbero essere condotti esercizi comuni con i fornitori di fiducia e i potenziali utenti della riserva per la cibersicurezza al fine di garantire il funzionamento efficiente della riserva stessa***. Nel richiedere il sostegno della riserva dell'UE per la cibersicurezza, gli Stati membri dovrebbero specificare il sostegno fornito al soggetto interessato a livello nazionale, che è opportuno prendere in considerazione nella valutazione della richiesta dello Stato membro. I servizi di tale riserva possono inoltre servire a sostenere le istituzioni, gli organi e gli organismi dell'Unione, in condizioni analoghe.

Or. en

Emendamento 68
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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	(33) È opportuno istituire gradualmente una riserva per la cibersicurezza a livello di Unione, ***con un finanziamento iniziale di 10 milioni di EUR a titolo del presente regolamento fino alla valutazione. La riserva è*** costituita da servizi erogati da

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.	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. ***La Commissione garantisce che non vi siano duplicazioni di iniziative simili all'interno della NATO.***

Or. en

Motivazione

The Commission foresees a "gradual set up" of the Reserve but this is not reflected in the rest of the proposed Regulation. This amendment therefore proposes to reduce the initial budget for the Reserve from 36 million to 10 million euro until the evaluation of this Regulation. This would return 26 million euro to the Digital Europe Program - Special Objective 4 on Advanced Digital Skills (of the 35 million taken from it). Developing a EU Cybersecurity Reserve next to an existing NATO cyber reserve comes with a high risk of duplication and should not be at the expense of investing more in developing and attracting cybersecurity talent in Europe.

Emendamento 69
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Considerando 35

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

Or. en

Emendamento 70
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti

Proposta di regolamento
Considerando 35 bis (nuovo)

Testo della Commissione	*Emendamento*
	(35 bis) Alla luce dei compiti aggiuntivi previsti dal presente regolamento e dalla [proposta relativa a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali], all'ENISA dovrebbero essere fornite le risorse umane e finanziarie necessarie a titolo del bilancio dell'Unione.

Or. en

Emendamento 71
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Considerando 37 bis (nuovo)

Testo della Commissione	*Emendamento*
	(37 bis) Ai fini della fornitura di servizi specifici nell'ambito della riserva

dell'UE per la cibersicurezza potrebbero occorrere fornitori di servizi di risposta agli incidenti di paesi terzi, compresi paesi terzi associati al programma Europa digitale o membri della NATO o altri paesi partner internazionali che condividono gli stessi principi. Per rafforzare la resilienza e la sovranità dell'Unione e salvaguardarne le risorse strategiche, gli interessi o la sicurezza, potrebbe essere necessario limitare o escludere la partecipazione di soggetti giuridici con sede in paesi non associati o controllati da tali paesi.

Or. en

Emendamento 72
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Considerando 38 bis (nuovo)

Testo della Commissione	*Emendamento*
	(38 bis) Per attuare efficacemente il ciberscudo europeo e il meccanismo per le emergenze di cibersicurezza è fondamentale disporre di personale altamente qualificato, in grado di fornire i pertinenti servizi di cibersicurezza in modo affidabile e secondo gli standard più elevati. Pertanto, è preoccupante che l'Unione si trovi ad affrontare, da un lato, un divario di talenti caratterizzato da una carenza di professionisti qualificati e, dall'altro, un panorama delle minacce in rapida evoluzione, come riconosciuto nella comunicazione della Commissione del 18 aprile 2023 sull'Accademia per le competenze in materia di cibersicurezza. È importante colmare tale divario di talenti rafforzando la cooperazione e il coordinamento tra i diversi portatori di interessi, compresi il settore privato, il mondo accademico, gli Stati membri, la

Commissione e l'ENISA, al fine di aumentare e creare sinergie per gli investimenti nell'istruzione e nella formazione, lo sviluppo di partenariati pubblico-privati, il sostegno a iniziative di ricerca e innovazione, lo sviluppo e il riconoscimento reciproco di norme comuni e la certificazione delle competenze in materia di cibersicurezza, anche attraverso il quadro europeo delle competenze in materia di cibersicurezza. Ciò dovrebbe agevolare anche la mobilità dei professionisti della cibersicurezza all'interno dell'Unione. Il presente regolamento dovrebbe mirare a promuovere una forza lavoro più diversificata nel settore della cibersicurezza.

Or. en

Emendamento 73
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Considerando 38 ter (nuovo)

Testo della Commissione	*Emendamento*
	(38 ter) Lo sviluppo delle capacità degli Stati membri è essenziale per un approccio coordinato a livello di Unione volto a rafforzare la resilienza della posizione dell'Unione in materia di cibersicurezza. Come sottolineato nella comunicazione della Commissione del 18 aprile 2023 sull'Accademia per le competenze in materia di cibersicurezza, la sicurezza dell'UE non può essere garantita senza il bene più prezioso dell'UE: la sua popolazione. Il quadro europeo delle competenze in materia di cibersicurezza può aiutare a comprendere meglio la composizione della forza lavoro dell'Unione, comprese le competenze attuali e richieste all'interno dei soggetti

partecipanti.

Or. en

Emendamento 74
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Considerando 39

Testo della Commissione	*Emendamento*
(39) L'obiettivo del presente regolamento può essere conseguito meglio a livello di Unione piuttosto che dagli Stati membri. L'Unione può quindi intervenire in base ai principi di sussidiarietà e proporzionalità sanciti dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per il conseguimento di tale obiettivo.	(39) L'obiettivo del presente regolamento***, ossia smantellare i silos di comunicazione e rafforzare le capacità dell'Unione in materia di prevenzione, rilevamento, risposta e ripresa in caso di minacce informatiche,*** può essere conseguito meglio a livello di Unione piuttosto che dagli Stati membri. L'Unione può quindi intervenire in base ai principi di sussidiarietà e proporzionalità sanciti dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per il conseguimento di tale obiettivo.

Or. en

Emendamento 75
Nicola Danti

Proposta di regolamento
Considerando 39 bis (nuovo)

Testo della Commissione	*Emendamento*
	(39 bis) Alla luce dei compiti aggiuntivi previsti dal presente regolamento e dalla [proposta relativa a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali], all'ENISA dovrebbero essere fornite le risorse umane e finanziarie necessarie a titolo del

bilancio dell'Unione.

Or. en

Emendamento 76
Johan Nissinen

Proposta di regolamento
Articolo 1 – paragrafo 1 – parte introduttiva

Testo della Commissione	*Emendamento*
1. Il presente regolamento stabilisce misure volte a rafforzare le capacità dell'Unione in materia di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi, in particolare mediante:	1. Il presente regolamento stabilisce misure volte a rafforzare le capacità dell'Unione in materia di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi, ***nel rispetto del fatto che la sicurezza nazionale, anche nel settore informatico, resta di esclusiva competenza di ciascuno Stato membro, come indicato all'articolo 4, paragrafo 2, TUE,*** in particolare mediante:

Or. en

Emendamento 77
Evžen Tošenovský

Proposta di regolamento
Articolo 1 – paragrafo 1 – lettera a

Testo della Commissione	*Emendamento*
a) la realizzazione ***di un'infrastruttura paneuropea*** di centri operativi di sicurezza (***"ciberscudo europeo"***) per sviluppare e potenziare capacità comuni in materia di rilevamento e conoscenza situazionale;	a) ***il rafforzamento di gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), di cui all'articolo 10 della direttiva (UE) 2022/2555, e della rete di CSIRT di cui all'articolo 15 della direttiva (UE) 2022/2555 e*** la realizzazione di centri operativi di sicurezza (***SOC***) per sviluppare e potenziare capacità ***nazionali e*** comuni in materia di rilevamento e conoscenza situazionale ***("ciberscudo europeo")***;

Or. en

Emendamento 78
Evžen Tošenovský

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.	***soppresso***

Or. en

Emendamento 79
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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***, incluse le PMI,*** e dei servizi nell'Unione nell'ambito dell'economia digitale e di contribuire alla sovranità tecnologica dell'Unione nel settore della cibersicurezza;

Or. en

Emendamento 80
Johan Nissinen

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 ***volontari e*** 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;

Or. en

Emendamento 81
Johan Nissinen

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 ***collaborazione volontaria*** 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;

Or. en

Emendamento 82
Evžen Tošenovský

Proposta di regolamento
Articolo 1 – paragrafo 2 – lettera c

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

Or. en

Emendamento 83
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Testo della Commissione	*Emendamento*
	c bis) sviluppare e migliorare le capacità e le competenze della forza lavoro nel settore della cibersicurezza in modo coordinato, collaborando con l'Accademia per le competenze in materia di cibersicurezza per offrire formazione e opportunità con l'obiettivo di colmare il divario di talenti nel settore della cibersicurezza.

Or. en

Emendamento 84
Johan Nissinen

Proposta di regolamento
Articolo 1 – paragrafo 3

Testo della Commissione	*Emendamento*
3. Il presente regolamento lascia impregiudicata la responsabilità primaria degli Stati membri in materia di sicurezza nazionale, sicurezza pubblica e	3. Il presente regolamento lascia impregiudicata la responsabilità primaria degli Stati membri in materia di sicurezza nazionale, sicurezza pubblica e

prevenzione, indagine, accertamento e perseguimento dei reati.	prevenzione, indagine, accertamento e perseguimento dei reati ***ed evita inutili duplicazioni con le iniziative esistenti***.

Or. en

Emendamento 85
Evžen Tošenovský

Proposta di regolamento
Articolo 1 – paragrafo 3

Testo della Commissione	*Emendamento*
3. Il presente regolamento lascia impregiudicata la ***responsabilità primaria*** degli Stati membri in materia di sicurezza nazionale, sicurezza pubblica e prevenzione, indagine, accertamento e perseguimento dei reati.	3. Il presente regolamento lascia impregiudicata la ***competenza esclusiva*** degli Stati membri in materia di sicurezza nazionale, sicurezza pubblica e prevenzione, indagine, accertamento e perseguimento dei reati.

Or. en

Emendamento 86
Nicola Danti

Proposta di regolamento
Articolo 1 – paragrafo 3 bis (nuovo)

Testo della Commissione	*Emendamento*
	3 bis. Ogni anno, in occasione della presentazione del progetto di bilancio per l'anno successivo, la Commissione presenta una valutazione dettagliata dei compiti dell'ENISA ai sensi del presente regolamento nonché della [proposta di regolamento relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali] e di altre normative dell'Unione e specifica le risorse finanziarie e umane necessarie allo svolgimento di tali compiti.

Or. en

Emendamento 87
Evžen Tošenovský

Proposta di regolamento
Articolo 2 – punto 1

Testo della Commissione	*Emendamento*
1) "centro operativo di sicurezza transfrontaliero" ("SOC transfrontaliero"): una piattaforma multinazionale che riunisce in una struttura di rete coordinata i SOC nazionali di almeno tre Stati membri che formano un consorzio ospitante e che è concepita per prevenire le minacce e gli incidenti informatici e per favorire l'elaborazione di analisi di alta qualità, in particolare mediante lo scambio di dati provenienti da varie fonti, pubbliche e private, nonché tramite la condivisione di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi, prevenzione e protezione nel settore informatico in un contesto di fiducia;	***soppresso***

Or. en

Emendamento 88
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 2 – punto 1

Testo della Commissione	*Emendamento*
1) "centro operativo di sicurezza transfrontaliero" ("SOC transfrontaliero"): una piattaforma multinazionale che riunisce in una struttura di rete coordinata i SOC nazionali di almeno tre Stati membri che formano un consorzio ospitante e che è concepita per ***prevenire*** le minacce e gli incidenti informatici e per favorire	1) "centro operativo di sicurezza transfrontaliero" ("SOC transfrontaliero"): una piattaforma multinazionale che riunisce in una struttura di rete coordinata i SOC nazionali di almeno tre Stati membri che formano un consorzio ospitante e che è concepita per ***rilevare e analizzare*** le minacce e ***prevenire*** gli incidenti

l'elaborazione di analisi di alta qualità, in particolare mediante lo scambio di dati provenienti da varie fonti, pubbliche e private, nonché tramite la condivisione di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi, prevenzione e protezione nel settore informatico in un contesto di fiducia;	informatici e per favorire l'elaborazione di analisi di alta qualità, in particolare mediante lo scambio di dati provenienti da varie fonti, pubbliche e private, nonché tramite la condivisione di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi, prevenzione e protezione nel settore informatico in un contesto di fiducia;

Or. en

Emendamento 89
Johan Nissinen

Proposta di regolamento
Articolo 2 – punto 1

Testo della Commissione	*Emendamento*
1) "centro operativo di sicurezza transfrontaliero" ("SOC transfrontaliero"): una piattaforma multinazionale che riunisce in una struttura di rete coordinata i SOC nazionali di almeno tre Stati membri che formano un consorzio ospitante e che è concepita per prevenire le minacce e gli incidenti informatici e per favorire l'elaborazione di analisi di alta qualità, in particolare mediante lo scambio di dati provenienti da varie fonti, pubbliche e private, nonché tramite la condivisione di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi, prevenzione e protezione nel settore informatico in un contesto di fiducia;	1) "centro operativo di sicurezza transfrontaliero" ("SOC transfrontaliero"): una piattaforma multinazionale che riunisce in una struttura di rete coordinata i SOC nazionali di almeno tre Stati membri che formano un consorzio ospitante e che è concepita per prevenire le minacce e gli incidenti informatici e per favorire l'elaborazione di analisi di alta qualità, in particolare mediante lo scambio ***volontario*** di dati provenienti da varie fonti, pubbliche e private, nonché tramite la condivisione di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi, prevenzione e protezione nel settore informatico in un contesto di fiducia;

Or. en

Emendamento 90
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento

Articolo 2 – punto 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	1 bis) "centro operativo di sicurezza" ("SOC"): memoria centralizzata, che può essere interna o esterna, responsabile del monitoraggio e del miglioramento continuo della posizione di cibersicurezza di un soggetto per prevenire, rilevare e analizzare le minacce di cibersicurezza nonché rispondere alle stesse;

Or. en

Emendamento 91
Evžen Tošenovský

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

Testo della Commissione	*Emendamento*
	1 bis) "centro operativo di sicurezza" ("SOC"): centro, istituito da soggetti privati e pubblici o autorità nazionali, che monitora e analizza costantemente le reti di comunicazione e i sistemi informatici per rilevare intrusioni e anomalie in tempo reale;

Or. en

Emendamento 92
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 2 – punto 1 ter (nuovo)

Testo della Commissione	*Emendamento*
	1 ter) "centro operativo di sicurezza nazionale" ("SOC nazionale"): una memoria centralizzata responsabile della

	raccolta continua di informazioni sulle minacce e del miglioramento costante della posizione in materia di cibersicurezza di soggetti rientranti nella giurisdizione nazionale attraverso la prevenzione, il rilevamento e l'analisi delle minacce alla cibersicurezza, con l'obiettivo di poter rispondere meglio a tali minacce. Ove applicabile, tale memoria è integrata nelle strutture nazionali già esistenti come i CSIRT istituiti a norma della direttiva (UE) 2022/2555;

Or. en

Emendamento 93
Evžen Tošenovský

Proposta di regolamento
Articolo 2 – punto 2

Testo della Commissione	*Emendamento*
2) "***organismo di diritto pubblico***": soggetto quale definito all'articolo ***2, paragrafo 1***, punto ***4***), della direttiva ***2014/24/UE del Parlamento europeo e del Consiglio***[30];	2) "***ente della pubblica amministrazione***": soggetto ***della pubblica amministrazione*** quale definito all'articolo ***6***, punto ***35***), della direttiva ***(UE) 2022/2555***;
[30] Direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65).	

Or. en

Emendamento 94
Evžen Tošenovský

Proposta di regolamento
Articolo 2 – punto 3

Testo della Commissione	*Emendamento*
3) "consorzio ospitante": un consorzio composto da Stati partecipanti, rappresentati da SOC nazionali, che hanno concordato di stabilire e sostenere l'acquisizione di strumenti e infrastrutture per un SOC transfrontaliero e il suo funzionamento;	***soppresso***

Or. en

Emendamento 95
Evžen Tošenovský

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

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

Or. en

Emendamento 96
Evžen Tošenovský

Proposta di regolamento
Articolo 2 – punto 5 ter (nuovo)

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

Or. en

Emendamento 97
Evžen Tošenovský

Proposta di regolamento
Articolo 2 – punto 6 bis (nuovo)

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

Or. en

Emendamento 98
Evžen Tošenovský

Proposta di regolamento
Articolo 2 – punto 9

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

Or. en

Emendamento 99
Evžen Tošenovský

Proposta di regolamento
Articolo 2 – punto 10

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

generate;

Or. en

Emendamento 100
Evžen Tošenovský

Proposta di regolamento
Articolo 2 – punto 11

Testo della Commissione	*Emendamento*
11) "fornitori di fiducia": fornitori di servizi di sicurezza gestiti quali definiti all'articolo 6, punto 40), della direttiva (UE) 2022/2555, selezionati in conformità dell'articolo 16 del presente regolamento.	11) "fornitori di fiducia ***di servizi di sicurezza gestiti***": fornitori di servizi di sicurezza gestiti quali definiti all'articolo 6, punto 40), della direttiva (UE) 2022/2555, selezionati ***per essere inclusi nella riserva dell'UE per la cibersicurezza*** in conformità dell'articolo 16 del presente regolamento.

Or. en

Emendamento 101
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 3 – paragrafo 1 – comma 1

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

Or. en

Emendamento 102
Johan Nissinen

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

Testo della Commissione	*Emendamento*
a) mettere in comune e condividere, attraverso ***i*** SOC transfrontalieri, i dati sulle minacce e sugli incidenti informatici provenienti da varie fonti;	a) mettere in comune e condividere, attraverso ***la condivisione volontaria di informazioni dai*** SOC transfrontalieri, i dati sulle minacce e sugli incidenti informatici provenienti da varie fonti;

Or. en

Emendamento 103
Evžen Tošenovský

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

Testo della Commissione	*Emendamento*
a) mettere in comune e condividere, attraverso i SOC transfrontalieri, i dati sulle minacce e sugli incidenti informatici provenienti da varie fonti;	a) mettere in comune e condividere, attraverso i SOC transfrontalieri, i dati sulle minacce e sugli incidenti informatici provenienti da varie fonti ***sia a livello nazionale che dell'UE***;

Or. en

Emendamento 104
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Testo della Commissione	*Emendamento*
c) contribuire a una migliore protezione e risposta alle minacce	c) contribuire a una migliore protezione e risposta alle minacce informatiche***, anche fornendo***

informatiche;	***raccomandazioni concrete ai soggetti***;

Or. en

Emendamento 105
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Testo della Commissione	*Emendamento*
d) contribuire a un più rapido rilevamento delle minacce informatiche e alla conoscenza situazionale in tutta l'Unione;	d) contribuire a un più rapido rilevamento delle minacce informatiche e alla conoscenza situazionale in tutta l'Unione***, compresa la raccolta proattiva di informazioni***;

Or. en

Emendamento 106
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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

Testo della Commissione	*Emendamento*
e) fornire servizi e attività per la comunità di cibersicurezza nell'Unione, compreso il contributo allo sviluppo di strumenti avanzati di intelligenza artificiale e di analisi dei dati.	*(Non concerne la versione italiana)*

Or. en

Emendamento 107
Evžen Tošenovský

Proposta di regolamento
Articolo 4 – titolo

Testo della Commissione	*Emendamento*
Centri operativi di sicurezza nazionali	***Rafforzamento della cooperazione e della condivisione delle informazioni a livello nazionale***

Or. en

Emendamento 108
Evžen Tošenovský

Proposta di regolamento
Articolo 4 – paragrafo 1 – comma 1

Testo della Commissione	*Emendamento*
Per ***partecipare*** al ciberscudo europeo, ogni Stato membro designa ***almeno un SOC nazionale. Il SOC nazionale è un organismo pubblico***.	Per ***contribuire*** al ciberscudo europeo, ogni Stato membro designa ***uno dei suoi gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), di cui all'articolo 10 della direttiva (UE) 2022/2555, in qualità di centro di analisi e condivisione delle informazioni (ISAC)***.

Or. en

Emendamento 109
Evžen Tošenovský

Proposta di regolamento
Articolo 4 – paragrafo 1 – comma 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	Le organizzazioni pubbliche e private o le autorità nazionali, in particolare i soggetti operanti in settori critici o altamente critici, sono incoraggiate a istituire e gestire i propri SOC autonomi o condivisi.

Or. en

Emendamento 110

Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 4 – 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 a livello nazionale per la raccolta e l'analisi di informazioni sulle minacce 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 o il CSIRT nazionale possono richiedere a fornitori di fiducia o fornitori di servizi di sicurezza gestiti i dati raccolti mediante telemetria, sensori o registrazioni relativi a settori ad alta criticità come definiti nella direttiva (UE) 2022/2555. Tali dati possono essere condivisi esclusivamente per supportare i compiti e le responsabilità del SOC o del CSIRT nazionale nel rilevare e prevenire gli incidenti di cibersicurezza.***

Or. en

Emendamento 111
Evžen Tošenovský

Proposta di regolamento
Articolo 4 – 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	Il SOC ha la capacità di fungere da punto di riferimento e da porta di accesso ***principalmente ai SOC istituiti da soggetti privati e pubblici o autorità nazionali, ad altri CSIRT dello stesso Stato membro, al coordinatore per la gestione di incidenti e crisi di cibersicurezza su vasta scala, nonché*** ad altre organizzazioni pubbliche e

grado di rilevare, aggregare e analizzare dati relativi alle minacce e agli incidenti di cibersicurezza**.**	private a livello nazionale per la raccolta e l'analisi di informazioni sulle minacce e sugli incidenti di cibersicurezza e***, ove opportuno, per la condivisione di tali informazioni con altri membri della rete di CSIRT***. È dotato di tecnologie all'avanguardia in grado di rilevare, aggregare e analizzare dati relativi alle minacce e agli incidenti di cibersicurezza

Or. en

Emendamento 112
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 4 – 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 a livello nazionale***, in particolare ai rispettivi SOC,*** 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.

Or. en

Emendamento 113
Evžen Tošenovský

Proposta di regolamento
Articolo 4 – paragrafo 2

Testo della Commissione	*Emendamento*
2. A seguito di un invito a manifestare interesse, i SOC nazionali	***soppresso***

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

Or. en

Emendamento 114
Ville Niinistö
a nome del gruppo Verts/ALE

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

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.	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.

Or. en

Motivazione

L'inderogabilità del termine "sono" esclude il concetto di invito a manifestare interesse e i processi di selezione. Naturalmente i SOC possono partecipare e possono essere selezionati.

Emendamento 115
Evžen Tošenovský

Proposta di regolamento
Articolo 4 – paragrafo 3

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

Or. en

Emendamento 116
Evžen Tošenovský

Proposta di regolamento
Articolo 5 – titolo

Testo della Commissione	*Emendamento*

Centri operativi di sicurezza transfrontalieri

Appalto congiunto di strumenti e infrastrutture

Or. en

Emendamento 117
Evžen Tošenovský

Proposta di regolamento
Articolo 5 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Un consorzio ospitante composto da almeno tre Stati membri, rappresentati da SOC nazionali, impegnati a collaborare per coordinare le loro attività di rilevamento e di monitoraggio delle minacce informatiche, è ammesso a partecipare alle azioni volte all'istituzione di un SOC transfrontaliero.	***soppresso***

Or. en

Emendamento 118
Evžen Tošenovský

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	2. A seguito di un invito a manifestare interesse, un ***CSIRT-ISAC può essere*** selezionato dall'ECCC per partecipare con quest'ultimo a un appalto congiunto di strumenti e infrastrutture. L'ECCC può attribuire al ***CSIRT-ISAC*** 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 ***CSIRT-***

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 convenzione di accoglienza e di utilizzo che disciplina l'uso degli strumenti e delle infrastrutture.

ISAC. Prima di avviare la procedura di acquisizione degli strumenti e delle infrastrutture, l'ECCC e il ***CSIRT-ISAC partecipante*** concludono una convenzione di accoglienza e di utilizzo che disciplina l'uso degli strumenti e delle infrastrutture***, compreso l'utilizzo degli stessi da parte di altri CSIRT e SOC in tale Stato membro***.

Or. en

Emendamento 119
Ville Niinistö
a nome del gruppo Verts/ALE

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

Or. en

Motivazione

Sebbene il presente regolamento non preveda criteri espliciti, altre normative applicabili potrebbero ridurre la certezza che un/ogni richiedente abbia successo.

Emendamento 120
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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

Testo della Commissione	*Emendamento*
	2 bis. Gli appalti e la partecipazione di un soggetto privato con sede in un paese terzo che condivide gli stessi principi devono essere consentiti qualora non violino gli interessi di sicurezza e di difesa dell'Unione e degli Stati membri come stabilito nel quadro della politica estera e di sicurezza comune ai sensi del titolo V del TUE o degli obiettivi delineati nel presente regolamento. Tali soggetti privati non devono essere controllati da un paese terzo non associato o essere stati sottoposti a controllo ai sensi del regolamento (UE) 2019/452 del Parlamento europeo e del Consiglio.

Or. en

Emendamento 121
Evžen Tošenovský

Proposta di regolamento
Articolo 5 – paragrafo 3

Testo della Commissione	*Emendamento*
3. I membri del consorzio ospitante stipulano un accordo di consorzio scritto che definisce le disposizioni interne per l'attuazione della convenzione di accoglienza e di utilizzo.	***soppresso***

Or. en

Emendamento 122

Evžen Tošenovský

Proposta di regolamento
Articolo 5 – paragrafo 4

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

Or. en

Emendamento 123
Evžen Tošenovský

Proposta di regolamento
Articolo 6 – titolo

Testo della Commissione	*Emendamento*
Cooperazione e condivisione di informazioni ***tra SOC transfrontalieri e al loro interno***	***Rafforzamento della*** cooperazione e ***della*** condivisione di informazioni ***a livello dell'UE***

Or. en

Emendamento 124
Johan Nissinen

Proposta di regolamento
Articolo 6 – paragrafo 1 – parte introduttiva

Testo della Commissione	*Emendamento*
1. I membri di un consorzio ospitante ***scambiano*** tra loro, all'interno del SOC transfrontaliero, informazioni pertinenti, comprese informazioni relative a minacce	1. I membri di un consorzio ospitante ***possono scambiare*** tra loro, all'interno del SOC transfrontaliero, informazioni pertinenti, comprese informazioni relative

informatiche, quasi incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli autori delle minacce, allarmi di cibersicurezza e raccomandazioni relative alla configurazione degli strumenti di cibersicurezza per rilevare gli attacchi informatici, laddove tale condivisione di informazioni:	a minacce informatiche, quasi incidenti, vulnerabilità, tecniche e procedure, indicatori di compromissione, tattiche avversarie, informazioni specifiche sugli autori delle minacce, allarmi di cibersicurezza e raccomandazioni relative alla configurazione degli strumenti di cibersicurezza per rilevare gli attacchi informatici, laddove tale condivisione di informazioni:

Or. en

Emendamento 125
Evžen Tošenovský

Proposta di regolamento
Articolo 6 – paragrafo 1 – parte introduttiva

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

Or. en

Emendamento 126
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 6 – paragrafo 1 – lettera a

Testo della Commissione	*Emendamento*
a) ***miri a*** prevenire ***o*** rilevare gli incidenti***, a rispondervi, a riprendersi dagli stessi o ad attenuarne l'impatto***;	a) ***migliori lo scambio di informazioni sulle minacce informatiche tra SOC e ISAC dell'industria allo scopo di*** prevenire***,*** rilevare ***o attenuare*** gli incidenti;

Or. en

Emendamento 127
Evžen Tošenovský

Proposta di regolamento
Articolo 6 – paragrafo 2 – parte introduttiva

Testo della Commissione	*Emendamento*
2. L'accordo ***di consorzio scritto di cui all'articolo 5, paragrafo 3, stabilisce***:	2. L'accordo ***sulla condivisione di informazioni e di intelligence tra CSIRT-ISAC o, se del caso, altri CSIRT, può stabilire***:

Or. en

Emendamento 128
Johan Nissinen

Proposta di regolamento
Articolo 6 – paragrafo 2 – lettera a

Testo della Commissione	*Emendamento*
a) l'impegno a condividere ***una quantità significativa di*** dati di cui al paragrafo 1 e le condizioni di scambio di tali informazioni;	a) l'impegno a condividere ***su base volontaria i*** dati di cui al paragrafo 1 e le condizioni di scambio di tali informazioni;

Or. en

Emendamento 129
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 6 – paragrafo 2 – lettera a

Testo della Commissione	*Emendamento*
a) l'impegno a condividere ***una quantità significativa di*** dati di cui al paragrafo 1 e le condizioni di scambio di tali informazioni;	a) l'impegno a condividere ***i*** dati ***significativi*** di cui al paragrafo 1 e le condizioni di scambio di tali informazioni;

Or. en

Emendamento 130
Evžen Tošenovský

Proposta di regolamento
Articolo 6 – paragrafo 3

Testo della Commissione	*Emendamento*
3. Per incoraggiare lo scambio di informazioni tra SOC transfrontalieri, questi ultimi garantiscono un elevato livello di interoperabilità tra di loro. Per facilitare l'interoperabilità tra i SOC transfrontalieri, la Commissione può, mediante atti di esecuzione, previa consultazione dell'ECCC, specificare le condizioni di tale interoperabilità. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2, del presente regolamento.	***soppresso***

Or. en

Emendamento 131
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 6 – paragrafo 3

Testo della Commissione	*Emendamento*
3. Per incoraggiare lo scambio di informazioni tra SOC transfrontalieri,	3. Per incoraggiare lo scambio di informazioni tra ***ISAC dell'industria e***

questi ultimi garantiscono un elevato livello di interoperabilità tra di loro. Per facilitare l'interoperabilità tra i SOC transfrontalieri, ***la*** Commissione ***può***, mediante atti ***di esecuzione, previa consultazione dell'ECCC***, ***specificare*** le condizioni di tale interoperabilità. Tali atti ***di esecuzione*** sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2, del presente regolamento.	SOC transfrontalieri, questi ultimi garantiscono un elevato livello di interoperabilità tra di loro ***e, ove possibile, con gli ISAC dell'industria***. Per facilitare l'interoperabilità tra i SOC transfrontalieri ***e gli ISAC dell'industria***, ***le norme e i protocolli di condivisione delle informazioni devono essere armonizzati con le norme internazionali e le migliori pratiche del settore. L'ECCC può anche richiedere alla*** Commissione ***di proporre***, mediante atti ***delegati***, le condizioni di tale interoperabilità ***in stretta collaborazione con i SOC regionali e sulla base delle norme internazionali e delle migliori pratiche del settore***. Tali atti ***delegati*** sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2, del presente regolamento.

Or. en

Emendamento 132
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 6 – paragrafo 3

Testo della Commissione	*Emendamento*
3. Per incoraggiare lo scambio di informazioni tra SOC transfrontalieri, questi ultimi garantiscono un elevato livello di interoperabilità tra di loro. ***Per*** facilitare l'interoperabilità tra i SOC transfrontalieri, la Commissione può, mediante atti di esecuzione, previa consultazione dell'ECCC, specificare le condizioni di tale interoperabilità. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2, del presente regolamento.	3. Per incoraggiare lo scambio di informazioni tra SOC transfrontalieri, questi ultimi garantiscono un elevato livello di interoperabilità tra di loro. ***L'appalto congiunto di infrastrutture, servizi e strumenti informatici può*** facilitare l'interoperabilità tra i SOC transfrontalieri***. Al fine di specificare le condizioni per l'interoperabilità dei SOC transfrontalieri***, la Commissione può, mediante atti di esecuzione, previa consultazione dell'ECCC ***e dell'ENISA***, specificare le condizioni di tale interoperabilità. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2, del

presente regolamento.

Or. en

Emendamento 133
Evžen Tošenovský

Proposta di regolamento
Articolo 6 – paragrafo 4

Testo della Commissione	*Emendamento*
4. I SOC transfrontalieri stipulano accordi di cooperazione tra di loro, specificando i principi di condivisione delle informazioni tra le piattaforme transfrontaliere.	***soppresso***

Or. en

Emendamento 134
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 6 – paragrafo 4

Testo della Commissione	*Emendamento*
4. I SOC transfrontalieri stipulano accordi di cooperazione tra di loro, specificando i principi di condivisione delle informazioni tra le piattaforme transfrontaliere.	4. I SOC transfrontalieri stipulano accordi di cooperazione tra di loro, specificando i principi di condivisione delle informazioni tra le piattaforme transfrontaliere***, tenendo conto dei meccanismi di condivisione delle informazioni pertinenti già esistenti a norma della direttiva (UE) 2022/2555. Nel contesto di un incidente di cibersicurezza su vasta scala, potenziale o in corso, i meccanismi di condivisione delle informazioni sono conformi alle pertinenti disposizioni della direttiva (UE) 2022/2555.***

Or. en

Emendamento 135
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 6 – paragrafo 4

Testo della Commissione	*Emendamento*
4. I SOC transfrontalieri stipulano accordi di cooperazione tra di loro, specificando i principi di condivisione delle informazioni tra le piattaforme transfrontaliere.	4. I SOC transfrontalieri stipulano accordi di cooperazione tra di loro ***e con gli ISAC dell'industria***, specificando i principi di condivisione delle informazioni ***e di interoperabilità*** tra le piattaforme transfrontaliere.

Or. en

Emendamento 136
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 7 – titolo

Testo della Commissione	*Emendamento*
Cooperazione e condivisione di informazioni con ***soggetti dell'Unione***	Cooperazione e condivisione di informazioni con ***la rete di CSIRT***

Or. en

Emendamento 137
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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	1. Quando ***i SOC transfrontalieri*** ottengono informazioni relative a un incidente di cibersicurezza su vasta scala, potenziale o in corso, ***ai fini della condivisione della conoscenza situazionale, il*** SOC ***coordinatore fornisce***

Commissione, in considerazione dei rispettivi ruoli di gestione delle crisi conformemente alla direttiva (UE) 2022/2555.	senza indebito ritardo le informazioni pertinenti ***al CSIRT o all'autorità competente, che ne darà notifica*** a EU-CyCLONe, alla rete di CSIRT e alla Commissione, in considerazione dei rispettivi ruoli ***e procedimenti*** di gestione delle crisi conformemente alla direttiva (UE) 2022/2555.

Or. en

Motivazione

Suggeriamo di attenersi alla procedura NIS2 per incidenti su vasta scala.

Emendamento 138
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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***,*** alla Commissione ***e all'ENISA***, in ***linea con i*** rispettivi ruoli di gestione delle crisi conformemente alla direttiva (UE) 2022/2555.

Or. en

Emendamento 139
Evžen Tošenovský

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 ***CSIRT-ISAC*** forniscono senza indebito ritardo le informazioni pertinenti a EU-CyCLONe ***e*** alla rete di CSIRT, in considerazione dei rispettivi ruoli di gestione delle crisi conformemente alla direttiva (UE) 2022/2555.

Or. en

Emendamento 140
Evžen Tošenovský

Proposta di regolamento
Articolo 7 – paragrafo 2

Testo della Commissione	*Emendamento*
2. La Commissione può, mediante atti di esecuzione, determinare le modalità procedurali per la condivisione delle informazioni di cui al paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2, del presente regolamento.	***soppresso***

Or. en

Emendamento 141
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 7 – paragrafo 2

Testo della Commissione	*Emendamento*
2. La Commissione può, mediante atti di esecuzione, determinare le modalità procedurali per la condivisione delle informazioni di cui al paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21,	2. La Commissione può, mediante atti di esecuzione, ***previa consultazione delle piattaforme transfrontaliere e della rete di CSIRT,*** determinare le modalità procedurali per la condivisione delle informazioni di cui al paragrafo 1. Tali atti

paragrafo 2, del presente regolamento.	di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2, del presente regolamento ***e conformemente alla direttiva (UE) 2022/2555***.

Or. en

Motivazione

Suggeriamo di attenersi alla procedura NIS2 per incidenti su vasta scala e pertanto di consultare prima la rete di CSIRT.

Emendamento 142
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 7 – paragrafo 2

Testo della Commissione	*Emendamento*
2. La Commissione può, mediante atti di esecuzione, determinare le modalità procedurali per la condivisione delle informazioni di cui al paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2, del presente regolamento.	2. La Commissione può***, previa consultazione dell'ENISA***, mediante atti di esecuzione, determinare le modalità procedurali per la condivisione delle informazioni di cui al paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2, del presente regolamento.

Or. en

Emendamento 143
Johan Nissinen

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	1. Gli Stati membri che partecipano al ciberscudo europeo garantiscono un elevato livello ***di riservatezza,*** di sicurezza dei dati e di sicurezza fisica

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.	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.

Or. en

Emendamento 144
Evžen Tošenovský

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.	***soppresso***

Or. en

Emendamento 145
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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	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.	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 ***e conformemente alla direttiva (UE) 2022/2555 e alla direttiva (UE) 2022/2557***. 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.

Or. en

Emendamento 146
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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***, previa consultazione dell'ENISA,*** 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.

Or. en

Emendamento 147
Johan Nissinen

Proposta di regolamento

Articolo 9 – paragrafo 1

Testo della Commissione	*Emendamento*
1. È istituito un meccanismo per le emergenze di cibersicurezza al fine di migliorare la resilienza dell'Unione alle minacce gravi alla cibersicurezza e, in uno spirito di solidarietà, prepararsi all'impatto a breve termine degli incidenti di cibersicurezza significativi e su vasta scala nonché attenuare tale impatto (il "meccanismo").	1. È istituito un meccanismo per le emergenze di cibersicurezza al fine di migliorare la resilienza dell'Unione alle minacce gravi alla cibersicurezza e, in uno spirito di solidarietà, prepararsi all'impatto a breve termine degli incidenti di cibersicurezza significativi e su vasta scala nonché attenuare tale impatto (il "meccanismo")***, su esplicita richiesta dello Stato membro o degli Stati membri interessati***.

Or. en

Emendamento 148
Evžen Tošenovský

Proposta di regolamento
Articolo 9 – paragrafo 1

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

Or. en

Emendamento 149
Johan Nissinen

Proposta di regolamento
Articolo 10 – paragrafo 1 – lettera b

Testo della Commissione	*Emendamento*
b) azioni di risposta, a sostegno della risposta agli incidenti di cibersicurezza significativi e su vasta scala e della ripresa immediata dagli stessi, che devono essere condotte da fornitori di fiducia che partecipano alla riserva dell'UE per la cibersicurezza istituita ai sensi dell'articolo 12;	b) azioni di risposta, a sostegno della risposta agli incidenti di cibersicurezza significativi e su vasta scala e della ripresa immediata dagli stessi, che devono essere condotte da fornitori di fiducia che partecipano alla riserva dell'UE per la cibersicurezza istituita ai sensi dell'articolo 12***, su esplicita richiesta dello Stato membro o degli Stati membri interessati***;

Or. en

Emendamento 150
Evžen Tošenovský

Proposta di regolamento
Articolo 10 – paragrafo 1 – lettera b

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

Or. en

Emendamento 151
Ville Niinistö
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 10 – paragrafo 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	1 bis. A seguito dell'attivazione del meccanismo per le emergenze di

	cibersicurezza, la Commissione riferisce ogni anno in merito alla valutazione del funzionamento sia positivo che negativo del meccanismo, compresa l'eventuale necessità di ulteriori requisiti di cooperazione o formazione.

Or. en

Emendamento 152
Evžen Tošenovský

Proposta di regolamento
Articolo 11 – paragrafo 1

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

Or. en

Emendamento 153
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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	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.	scenari di rischio e metodologie comuni per ***la*** verifica coordinata ***della preparazione. Ciò consentirà di individuare i settori o i sottosettori interessati in cui i soggetti possono essere sottoposti alla verifica coordinata della preparazione come descritto al paragrafo 1***.

Or. en

Emendamento 154
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 ***e i soggetti che possono essere sottoposti alla verifica della preparazione***, elabora scenari di rischio e metodologie comuni per gli esercizi di verifica coordinata.

Or. en

Emendamento 155
Johan Nissinen

Proposta di regolamento
Articolo 12 – paragrafo 1

Testo della Commissione	*Emendamento*
1. È istituita una riserva dell'UE per la cibersicurezza al fine di assistere gli utenti di cui al paragrafo 3 nella risposta o nella fornitura di sostegno per la risposta agli incidenti di cibersicurezza significativi o su vasta scala e nella ripresa immediata da tali incidenti.	1. È istituita una riserva dell'UE per la cibersicurezza al fine di assistere gli utenti di cui al paragrafo 3 nella risposta o nella fornitura di sostegno per la risposta agli incidenti di cibersicurezza significativi o su vasta scala e nella ripresa immediata da tali incidenti***, su esplicita richiesta dello Stato***

	membro o degli Stati membri interessati e fatto salvo il carattere specifico della politica di sicurezza e di difesa di taluni Stati membri.

Or. en

Emendamento 156
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 12 – paragrafo 2

Testo della Commissione	*Emendamento*
2. La riserva dell'UE per la cibersicurezza consiste in servizi di risposta agli incidenti erogati da fornitori di fiducia selezionati in base ai criteri di cui all'articolo 16. La riserva include servizi preimpegnati. I servizi sono realizzabili in tutti gli Stati membri.	2. La riserva dell'UE per la cibersicurezza consiste in servizi di risposta agli incidenti erogati da fornitori di fiducia selezionati in base ai criteri di cui all'articolo 16. La riserva include servizi preimpegnati. I servizi sono realizzabili in tutti gli Stati membri***, rafforzano la resilienza e la sovranità dell'Unione e ne migliorano la competitività***. ***I nomi dei fornitori di fiducia selezionati e i loro servizi sono mantenuti riservati.***

Or. en

Emendamento 157
Johan Nissinen

Proposta di regolamento
Articolo 12 – paragrafo 2

Testo della Commissione	*Emendamento*
2. La riserva dell'UE per la cibersicurezza consiste in servizi di risposta agli incidenti erogati da fornitori di fiducia selezionati in base ai criteri di cui all'articolo 16. La riserva include servizi preimpegnati. I servizi sono realizzabili in tutti gli Stati membri.	2. La riserva dell'UE per la cibersicurezza consiste in servizi di risposta agli incidenti erogati da fornitori di fiducia selezionati in base ai criteri di cui all'articolo 16. La riserva include servizi preimpegnati. I servizi sono realizzabili in tutti gli Stati membri. ***La riserva dell'UE***

	per la cibersicurezza non limita la necessità di consentire ai paesi di monitorare e valutare le proprie esigenze.

Or. en

Emendamento 158
Evžen Tošenovský

Proposta di regolamento
Articolo 12 – paragrafo 2

Testo della Commissione	*Emendamento*
2. La riserva dell'UE per la cibersicurezza consiste in servizi di risposta agli incidenti erogati da fornitori di fiducia selezionati in base ai criteri di cui all'articolo 16. La riserva include servizi preimpegnati. I servizi ***sono*** realizzabili in tutti gli Stati membri.	2. La riserva dell'UE per la cibersicurezza consiste in servizi di risposta agli incidenti erogati da fornitori di fiducia ***di servizi di sicurezza gestiti*** selezionati in base ai criteri di cui all'articolo 16. La riserva include servizi preimpegnati. I servizi ***possono essere, su richiesta,*** realizzabili in tutti gli Stati membri.

Or. en

Emendamento 159
Evžen Tošenovský

Proposta di regolamento
Articolo 12 – paragrafo 3 – lettera b

Testo della Commissione	*Emendamento*
b) ***le istituzioni e gli organi e organismi dell'Unione***.	b) ***paesi terzi di cui all'articolo 17 del presente regolamento***.

Or. en

Emendamento 160
Evžen Tošenovský

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), ***possono, su richiesta, utilizzare*** 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.

Or. en

Emendamento 161
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 12 – paragrafo 5

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

Or. en

Emendamento 162
Evžen Tošenovský

Proposta di regolamento

Articolo 12 – paragrafo 5

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

Or. en

Emendamento 163
Evžen Tošenovský

Proposta di regolamento
Articolo 12 – paragrafo 6

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

Or. en

Emendamento 164
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 12 – paragrafo 6

Testo della Commissione	*Emendamento*

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

Or. en

Emendamento 165
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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, ***comprensiva delle competenze e delle capacità necessarie alla forza lavoro impegnata nel settore della cibersicurezza,*** previa consultazione con gli Stati membri e la Commissione. L'ENISA prepara inoltre una mappatura analoga, previa consultazione con la Commissione ***e in collaborazione con il settore privato***, 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.

Or. en

Emendamento 166
Evžen Tošenovský

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 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 ***e informa il Consiglio riguardo alle esigenze dei paesi terzi***.

Or. en

Emendamento 167
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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***,*** la Commissione***, i fornitori di servizi di sicurezza gestiti e i rappresentanti dell'industria***. 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.

Or. en

Emendamento 168

Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 12 – paragrafo 8

Testo della Commissione	*Emendamento*
8. La Commissione può***, mediante atti di esecuzione,*** specificare i tipi e il numero di servizi di risposta richiesti per la riserva dell'UE per la cibersicurezza. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2.	8. La Commissione può ***adottare un atto delegato conformemente all'articolo 20 bis del presente regolamento al fine di*** specificare i tipi e il numero di servizi di risposta richiesti per la riserva dell'UE per la cibersicurezza. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2.

Or. en

Emendamento 169
Evžen Tošenovský

Proposta di regolamento
Articolo 13 – paragrafo 5 – lettera a

Testo della Commissione	*Emendamento*
a) ***adeguate informazioni sul*** soggetto interessato e ***sugli*** impatti potenziali dell'incidente nonché ***sull'***uso previsto del sostegno richiesto, compresa un'indicazione delle esigenze stimate;	a) ***il tipo di*** soggetto interessato e ***gli*** impatti potenziali dell'incidente nonché ***l'***uso previsto del sostegno richiesto, compresa un'indicazione delle esigenze stimate;

Or. en

Emendamento 170
Evžen Tošenovský

Proposta di regolamento
Articolo 13 – paragrafo 5 – lettera b

Testo della Commissione	*Emendamento*
b) ***informazioni*** sulle misure adottate	b) ***notizie generali*** sulle misure

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

Or. en

Emendamento 171
Evžen Tošenovský

Proposta di regolamento
Articolo 13 – paragrafo 5 – lettera c

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

Or. en

Emendamento 172
Evžen Tošenovský

Proposta di regolamento
Articolo 13 – paragrafo 7

Testo della Commissione	*Emendamento*
7. La Commissione può, mediante atti di esecuzione, specificare ulteriormente le modalità dettagliate di assegnazione dei servizi di sostegno della riserva dell'UE per la cibersicurezza. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2.	***soppresso***

Or. en

Emendamento 173
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 13 – paragrafo 7

Testo della Commissione	*Emendamento*
7. La Commissione può***, mediante atti di esecuzione,*** specificare ulteriormente le modalità dettagliate di assegnazione dei servizi di sostegno della riserva dell'UE per la cibersicurezza. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2.	7. La Commissione può ***adottare atti delegati conformemente all'articolo 20 bis del presente regolamento al fine di*** specificare ulteriormente le modalità dettagliate di assegnazione dei servizi di sostegno della riserva dell'UE per la cibersicurezza. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2.

Or. en

Emendamento 174
Evžen Tošenovský

Proposta di regolamento
Articolo 14 – paragrafo 1

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

Or. en

Emendamento 175
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 14 – paragrafo 2 – lettera d

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

Or. en

Emendamento 176
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 14 – paragrafo 3

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

Or. en

Emendamento 177
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 14 – paragrafo 3

Testo della Commissione	*Emendamento*
3. I servizi della riserva dell'UE per la cibersicurezza sono forniti in conformità di accordi specifici stipulati tra il fornitore di servizi e l'utente a cui viene fornito il sostegno nell'ambito della riserva dell'UE	3. I servizi della riserva dell'UE per la cibersicurezza sono forniti ***previa approvazione dell'utente e*** in conformità di accordi specifici stipulati tra il fornitore di servizi e l'utente a cui viene fornito il

per la cibersicurezza. Tali accordi includono condizioni di responsabilità.

sostegno nell'ambito della riserva dell'UE per la cibersicurezza. Tali accordi includono condizioni di responsabilità.

Or. en

Emendamento 178
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 14 – paragrafo 4

Testo della Commissione	*Emendamento*
4. Gli accordi di cui al paragrafo 3 ***possono essere*** basati su modelli preparati dall'ENISA, previa consultazione degli Stati membri.	4. Gli accordi di cui al paragrafo 3 ***sono*** basati su modelli preparati dall'ENISA, previa consultazione degli Stati membri ***e di altri utenti della riserva***.

Or. en

Emendamento 179
Evžen Tošenovský

Proposta di regolamento
Articolo 14 – paragrafo 5

Testo della Commissione	*Emendamento*
5. La Commissione e l'ENISA non si assumono alcuna responsabilità contrattuale per i danni causati a terzi dai servizi forniti nel quadro dell'attuazione della riserva dell'UE per la cibersicurezza.	***soppresso***

Or. en

Emendamento 180
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 14 – paragrafo 5

Testo della Commissione	*Emendamento*
5. La Commissione e l'ENISA non si assumono alcuna responsabilità contrattuale per i danni causati a terzi dai servizi forniti nel quadro dell'attuazione della riserva dell'UE per la cibersicurezza.	5. La Commissione e l'ENISA non si assumono alcuna responsabilità contrattuale per i danni causati a terzi dai servizi forniti nel quadro dell'attuazione della riserva dell'UE per la cibersicurezza***, salvo nei casi di negligenza nella valutazione dell'applicazione del fornitore di servizi, o nei casi in cui la Commissione o l'ENISA siano utenti e siano ritenute responsabili dei danni***.

Or. en

Emendamento 181
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 14 – paragrafo 5

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

Or. en

Emendamento 182
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 14 – paragrafo 6

Testo della Commissione	*Emendamento*
6. Entro un mese dalla fine dell'azione	6. Entro un mese dalla fine dell'azione

di sostegno, gli utenti forniscono alla Commissione e all'ENISA una relazione sintetica sul servizio fornito, sui risultati ottenuti e sugli insegnamenti tratti. Quando l'utente proviene da un paese terzo, come indicato nell'articolo 17, tale relazione è condivisa con l'alto rappresentante.

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

Or. en

Emendamento 183
Evžen Tošenovský

Proposta di regolamento
Articolo 14 – paragrafo 6

Testo della Commissione	*Emendamento*
6. Entro un mese dalla fine dell'azione di sostegno, gli utenti forniscono alla Commissione ***e*** all'ENISA una relazione sintetica sul servizio fornito, sui risultati ottenuti e sugli insegnamenti tratti. Quando l'utente proviene da un paese terzo, come indicato nell'articolo 17, tale relazione è condivisa con l'alto rappresentante.	6. Entro un mese dalla fine dell'azione di sostegno, gli utenti forniscono alla Commissione***,*** all'ENISA***, alla rete di CSIRT e, ove opportuno, a EU-CyCLONe*** una relazione sintetica sul servizio fornito, sui risultati ottenuti e sugli insegnamenti tratti. Quando l'utente proviene da un paese terzo, come indicato nell'articolo 17, tale relazione è condivisa con l'alto rappresentante.

Or. en

Emendamento 184
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 14 – paragrafo 7

Testo della Commissione	*Emendamento*
7. La Commissione riferisce periodicamente al gruppo di cooperazione NIS in merito alle modalità di impiego e ai	7. La Commissione riferisce periodicamente al gruppo di cooperazione NIS in merito alle modalità di impiego e ai

risultati del sostegno.	risultati del sostegno. ***La relazione tutela la riservatezza delle informazioni, conformemente al diritto nazionale o dell'Unione in materia di protezione delle informazioni sensibili o classificate.***

Or. en

Emendamento 185
Evžen Tošenovský

Proposta di regolamento
Articolo 14 – paragrafo 7

Testo della Commissione	*Emendamento*
7. La Commissione riferisce ***periodicamente*** al gruppo di cooperazione NIS in merito alle modalità di impiego e ai risultati del sostegno.	7. La Commissione riferisce ***almeno due volte all'anno*** al gruppo di cooperazione NIS in merito alle modalità di impiego e ai risultati del sostegno.

Or. en

Emendamento 186
Evžen Tošenovský

Proposta di regolamento
Articolo 15 – titolo

Testo della Commissione	*Emendamento*
Coordinamento con i meccanismi di gestione delle crisi	Coordinamento ***del meccanismo per le emergenze di cibersicurezza*** con i meccanismi di gestione delle crisi

Or. en

Emendamento 187
Evžen Tošenovský

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.

Or. en

Emendamento 188
Evžen Tošenovský

Proposta di regolamento
Articolo 16 – titolo

Testo della Commissione	*Emendamento*
Fornitori di fiducia	Fornitori di fiducia ***di servizi di sicurezza gestiti***

Or. en

Emendamento 189
Johan Nissinen

Proposta di regolamento
Articolo 16 – paragrafo 1 – parte introduttiva

Testo della Commissione	*Emendamento*
1. Nelle procedure di appalto per l'istituzione della riserva dell'UE per la cibersicurezza, l'amministrazione aggiudicatrice agisce in conformità dei principi stabiliti nel regolamento (UE,	1. Nelle procedure di appalto per l'istituzione della riserva dell'UE per la cibersicurezza, l'amministrazione aggiudicatrice agisce in conformità dei principi stabiliti nel regolamento (UE,

Euratom) 2018/1046 e conformemente ai principi seguenti:	Euratom) 2018/1046***, fatta salva la responsabilità primaria degli Stati membri in materia di sicurezza nazionale,*** e conformemente ai principi seguenti:

Or. en

Emendamento 190
Evžen Tošenovský

Proposta di regolamento
Articolo 16 – paragrafo 1 – lettera a

Testo della Commissione	*Emendamento*
a) garantire che la riserva dell'UE per la cibersicurezza includa servizi che possano essere realizzabili in tutti gli Stati membri, tenendo conto in particolare dei requisiti nazionali per la fornitura di tali servizi, compresa la certificazione o l'accreditamento;	a) garantire che la riserva dell'UE per la cibersicurezza includa servizi che possano essere realizzabili in tutti gli Stati membri ***e paesi terzi conformemente all'articolo 17 del presente regolamento***, tenendo conto in particolare dei requisiti nazionali per la fornitura di tali servizi, compresa la certificazione o l'accreditamento;

Or. en

Emendamento 191
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 16 – paragrafo 1 – lettera c

Testo della Commissione	*Emendamento*
c) garantire che la riserva dell'UE per la cibersicurezza apporti valore aggiunto dell'UE, contribuendo agli obiettivi di cui all'articolo 3 del regolamento (UE) 2021/694, tra cui la promozione dello sviluppo delle competenze in materia di cibersicurezza nell'UE.	c) garantire che la riserva dell'UE per la cibersicurezza apporti valore aggiunto dell'UE, contribuendo agli obiettivi di cui all'articolo 3 del regolamento (UE) 2021/694, tra cui la promozione dello sviluppo delle competenze in materia di cibersicurezza nell'UE***, il rafforzamento della resilienza e della sovranità dell'Unione e il miglioramento della sua***

competitività.

Or. en

Emendamento 192
Evžen Tošenovský

Proposta di regolamento
Articolo 16 – paragrafo 1 – lettera c

Testo della Commissione	*Emendamento*
c) garantire che la riserva dell'UE per la cibersicurezza ***apporti valore aggiunto dell'UE, contribuendo*** agli obiettivi di cui all'articolo 3 del regolamento (UE) 2021/694, tra cui la promozione dello sviluppo delle competenze in materia di cibersicurezza nell'UE.	c) garantire che la riserva dell'UE per la cibersicurezza ***contribuisca*** agli obiettivi di cui all'articolo 3 del regolamento (UE) 2021/694, tra cui la promozione dello sviluppo delle competenze in materia di cibersicurezza nell'UE.

Or. en

Emendamento 193
Angelika Niebler, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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 ***aggiornata*** necessaria a supportare il servizio richiesto ***e soddisfa i requisiti stabiliti nel regolamento XX/XXXX (legge sulla ciberresilienza), ove applicabile***;

Or. en

Emendamento 194
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

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

Testo della Commissione	*Emendamento*
	f bis) il fornitore dimostra che le proprie strutture decisionali e gestionali sono scevre da qualsiasi influenza indebita da parte dei governi di Stati classificati come rivali sistemici dell'Unione;

Or. en

Emendamento 195
Evžen Tošenovský

Proposta di regolamento
Articolo 16 – paragrafo 2 – lettera h

Testo della Commissione	*Emendamento*
h) il fornitore è in grado di prestare il servizio in tempi brevi nello Stato membro o negli Stati membri in cui ciò è possibile;	h) il fornitore è in grado di prestare il servizio in tempi brevi nello Stato membro o negli Stati membri ***o nei paesi terzi*** in cui ciò è possibile;

Or. en

Emendamento 196
Evžen Tošenovský

Proposta di regolamento
Articolo 16 – paragrafo 2 – lettera i

Testo della Commissione	*Emendamento*
i) il fornitore è in grado di prestare il servizio nella lingua locale dello Stato membro o degli Stati membri in cui ciò è possibile;	i) il fornitore è in grado di prestare il servizio nella lingua locale dello Stato membro o degli Stati membri ***o dei paesi terzi*** in cui ciò è possibile ***o in una delle lingue di lavoro delle istituzioni dell'UE***;

Or. en

Emendamento 197
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 16 – paragrafo 2 – lettera j

Testo della Commissione	*Emendamento*
j) una volta posto in essere un sistema di certificazione UE per il servizio di sicurezza gestito a norma del regolamento (UE) 2019/881, il fornitore è certificato conformemente a tale sistema.	j) una volta posto in essere un sistema di certificazione UE per il servizio di sicurezza gestito a norma del regolamento (UE) 2019/881, il fornitore è certificato conformemente a tale sistema ***entro un periodo di due anni dall'adozione del sistema***.

Or. en

Emendamento 198
Evžen Tošenovský

Proposta di regolamento
Articolo 16 – paragrafo 2 – lettera j

Testo della Commissione	*Emendamento*
j) una volta posto in essere un sistema di certificazione ***UE*** per il servizio di sicurezza gestito a norma del regolamento (UE) 2019/881, il fornitore è certificato conformemente a tale sistema.	j) una volta posto in essere un sistema di certificazione ***europeo in materia di cibersicurezza*** per il servizio di sicurezza gestito a norma del regolamento (UE) 2019/881, il fornitore è certificato conformemente a tale sistema.

Or. en

Emendamento 199
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 16 – paragrafo 2 – lettera j

Testo della Commissione	*Emendamento*

j) una volta posto in essere un sistema di certificazione UE per il servizio di sicurezza gestito a norma del regolamento (UE) 2019/881, il fornitore è certificato conformemente a tale sistema.	j) una volta posto in essere un sistema di certificazione UE per il servizio di sicurezza gestito a norma del regolamento (UE) 2019/881, il fornitore è certificato conformemente a tale sistema ***entro due anni***.

Or. en

Motivazione

La proposta della Commissione prevede di sostituire i requisiti tecnici elencati nel presente regolamento con un sistema di certificazione. Il presente emendamento concede più tempo alle imprese, in particolare alle PMI, per passare a tale sistema, incoraggiando condizioni più paritarie in tutta l'Unione. Fino ad allora sarà necessario attenersi ai requisiti tecnici del presente regolamento.

Emendamento 200
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

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

Testo della Commissione	*Emendamento*
	j bis) il fornitore è in grado di dissociare i propri servizi dal contratto più ampio in modo che l'utente possa passare a un altro fornitore di servizi;

Or. en

Emendamento 201
Evžen Tošenovský

Proposta di regolamento
Articolo 17 – paragrafo 6

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

riserva dell'UE per la cibersicurezza.

Or. en

Emendamento 202
Evžen Tošenovský

Proposta di regolamento
Articolo 18

Testo della Commissione	*Emendamento*
Articolo 18	***soppresso***
Meccanismo di riesame degli incidenti di cibersicurezza	
1. Su richiesta della Commissione, di EU-CyCLONe o della rete di CSIRT, l'ENISA riesamina e valuta le minacce, le vulnerabilità e le azioni di attenuazione in relazione a uno specifico incidente di cibersicurezza significativo o su vasta scala. Al termine del riesame e della valutazione di un incidente, l'ENISA presenta una relazione di riesame dell'incidente alla rete di CSIRT, a EU-CyCLONe e alla Commissione per sostenerli nello svolgimento dei loro compiti, in particolare alla luce di quelli stabiliti negli articoli 15 e 16 della direttiva (UE) 2022/2555. Laddove opportuno, la Commissione condivide la relazione con l'alto rappresentante.	
2. Per preparare la relazione di riesame dell'incidente di cui al paragrafo 1, l'ENISA collabora con tutti i portatori di interessi, compresi i rappresentanti degli Stati membri, della Commissione, di altre istituzioni e di altri organi e organismi pertinenti dell'UE, dei fornitori di servizi di sicurezza gestiti e degli utenti di servizi di cibersicurezza. Ove opportuno, l'ENISA collabora anche con i soggetti interessati da incidenti di cibersicurezza significativi o su vasta scala. A sostegno del riesame l'ENISA può anche consultare altri tipi di portatori di	

interessi. I rappresentanti consultati dichiarano eventuali potenziali conflitti di interessi.

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

4. Ove opportuno, la relazione formula raccomandazioni per migliorare la posizione dell'Unione in materia di deterrenza informatica.

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

Or. en

Emendamento 203
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 18 – paragrafo 2

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

portatori di interessi. I rappresentanti consultati dichiarano eventuali potenziali conflitti di interessi.	l'ENISA può anche consultare altri tipi di portatori di interessi. I rappresentanti consultati dichiarano eventuali potenziali conflitti di interessi.

Or. en

Emendamento 204
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen

Proposta di regolamento
Articolo 18 – paragrafo 3

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

Or. en

Emendamento 205
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 18 – paragrafo 4

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

Or. en

Emendamento 206
Johan Nissinen

Proposta di regolamento
Articolo 18 – paragrafo 4

Testo della Commissione	*Emendamento*
4. Ove opportuno, la relazione formula raccomandazioni per migliorare la posizione dell'Unione in materia di deterrenza informatica.	4. Ove opportuno, la relazione formula raccomandazioni ***volontarie e non giuridicamente vincolanti*** per migliorare la posizione dell'Unione in materia di deterrenza informatica.

Or. en

Emendamento 207
Evžen Tošenovský

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

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

Or. en

Emendamento 208
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 19 – punto 3
Regolamento (UE) 2021/694
Articolo 14 – paragrafo 2 – comma 1

Testo della Commissione	*Emendamento*
Il Programma può concedere finanziamenti in tutte le forme previste dal regolamento finanziario, anche, in particolare, sotto forma di appalti, quale forma principale, o di sovvenzioni e premi.	Il Programma può concedere finanziamenti in tutte le forme previste dal regolamento finanziario, anche, in particolare, sotto forma di appalti, quale forma principale, o di sovvenzioni e premi. ***L'ENISA riceve risorse aggiuntive per svolgere i suoi compiti aggiuntivi stabiliti nel regolamento XX/XXX (regolamento sulla cibersolidarietà). Tali finanziamenti aggiuntivi non compromettono il conseguimento degli obiettivi del Programma.***

Or. en

Emendamento 209
Evžen Tošenovský

Proposta di regolamento
Articolo 19 – punto 5
Regolamento (UE) 2021/694
Articolo 19 – comma 2

Testo della Commissione	*Emendamento*
Il sostegno erogato sotto forma di sovvenzioni può essere concesso direttamente dall'ECCC, senza invito a presentare proposte, ai ***SOC nazionali*** di cui all'articolo 4 del regolamento XXXX e ***al consorzio ospitante*** di cui all'articolo 5 del regolamento XXXX, in conformità dell'articolo 195, primo comma, lettera d), del regolamento finanziario.	Il sostegno erogato sotto forma di sovvenzioni può essere concesso direttamente dall'ECCC, senza invito a presentare proposte, ai ***CSIRT-ISAC*** di cui all'articolo 4 del regolamento XXXX e di cui all'articolo 5 del regolamento XXXX, in conformità dell'articolo 195, primo comma, lettera d), del regolamento finanziario.

Or. en

Emendamento 210
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 20 – titolo

Testo della Commissione	*Emendamento*
Valutazione	Valutazione ***e riesame***

Or. en

Emendamento 211
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 20 – comma 1

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 [***due*** anni dalla data di applicazione del presente regolamento] ***e successivamente ogni due anni***, la Commissione ***conduce*** una valutazione sul ***funzionamento delle misure*** del presente regolamento ***e presenta una relazione al Parlamento europeo e al Consiglio***. ***La valutazione verte in particolare sui seguenti elementi:*** ***a) la partecipazione degli Stati membri al ciberscudo europeo, compreso il numero di SOC nazionali e transfrontalieri istituiti nell'ambito del regolamento e l'efficacia dello scambio di informazioni;*** ***b) il contributo del presente regolamento al rafforzamento della resilienza e della sovranità dell'Unione, al miglioramento della competitività dei settori industriali interessati, comprese le PMI, e allo sviluppo delle competenze in materia di cibersicurezza nell'UE;*** ***c) l'uso della riserva per la cibersicurezza, compresa l'opportunità di ampliare***

	l'ambito della riserva ai servizi di preparazione agli incidenti o ad esercizi comuni con i fornitori di fiducia e i potenziali utenti della riserva per la cibersicurezza al fine di garantire il funzionamento efficiente della riserva quando necessario;
	d) il contributo del presente regolamento allo sviluppo e al miglioramento delle capacità e delle competenze della forza lavoro nel settore della cibersicurezza, necessari per rafforzare la capacità dell'Unione di individuare e prevenire le minacce e gli incidenti di cibersicurezza, di rispondervi e di riprendersi dagli stessi;
	e) il contributo del presente regolamento alla diffusione e allo sviluppo di tecnologie all'avanguardia nell'Unione;
	Sulla base di tale relazione la Commissione presenta, se del caso, una proposta legislativa al Parlamento europeo e al Consiglio al fine di modificare il presente regolamento.

Or. en

Emendamento 212
Evžen Tošenovský

Proposta di regolamento
Articolo 20 – comma 1

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 [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. ***La relazione è corredata, se del caso, di una proposta legislativa.***

Or. en

Emendamento 213
Bart Groothuis, Klemen Grošelj, Ivars Ijabs, Mauri Pekkarinen, Nicola Danti

Proposta di regolamento
Articolo 20 – comma 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	Ogni anno, in occasione della presentazione del progetto di bilancio per l'anno successivo, la Commissione presenta una valutazione dettagliata dei compiti dell'ENISA ai sensi del presente regolamento nonché della [proposta di regolamento relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali] e di altre normative dell'Unione e specifica le risorse finanziarie e umane necessarie allo svolgimento di tali compiti.

Or. en

Emendamento 214
Angelika Niebler, Sara Skyttedal, Angelika Winzig, Gheorghe Falcă, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Proposta di regolamento
Articolo 20 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 20 bis
	Esercizio della delega
	1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.
	2. Il potere di adottare atti delegati di cui all'articolo 12, paragrafo 8, e all'articolo 13, paragrafo 7, è conferito alla Commissione per un periodo di cinque anni dal ... [data di entrata in vigore dell'atto legislativo di base o qualsiasi altra data fissata dai co-legislatori]. La Commissione elabora una relazione sulla delega di potere al più tardi nove mesi

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

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

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

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

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

Or. en

Emendamento 215
Evžen Tošenovský

Proposta di regolamento
Allegato – punto 1
Regolamento (UE) 2021/694
Allegato I – sezione "Obiettivo specifico 3 – Cibersicurezza e fiducia" – comma 2 – punto 1

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

Or. en

Emendamento 216
Evžen Tošenovský

Proposta di regolamento
Allegato – punto 1
Regolamento (UE) 2021/694
Allegato I – sezione "Obiettivo specifico 3 – Cibersicurezza e fiducia" – comma 2 – punto 5

Testo della Commissione	*Emendamento*
5. la promozione della solidarietà tra gli Stati membri nella preparazione e nella risposta agli incidenti di cibersicurezza significativi tramite l'introduzione di servizi di cibersicurezza a livello transfrontaliero, tra cui il sostegno all'assistenza reciproca tra le autorità	5. la promozione della solidarietà tra gli Stati membri nella preparazione e nella risposta agli incidenti di cibersicurezza significativi tramite l'introduzione di servizi di cibersicurezza a livello transfrontaliero, tra cui il sostegno all'assistenza reciproca tra le autorità

pubbliche e l'istituzione di una riserva di fornitori ***di cibersicurezza*** di fiducia a livello dell'Unione.	pubbliche e l'istituzione di una riserva di fornitori di fiducia ***di servizi di sicurezza gestiti*** a livello dell'Unione.

Or. en