COMMISSIONE
EUROPEA

Strasburgo, 18.4.2023
COM(2023) 209 final

2023/0109 (COD)

Proposta di

# REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

## che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi

# RELAZIONE

## 1. CONTESTO DELLA PROPOSTA

### • Motivi e obiettivi della proposta

La presente relazione accompagna la proposta di regolamento sulla cibersolidarietà. 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. Con una maggiore diffusione delle tecnologie digitali aumenta anche l'esposizione agli incidenti di cibersicurezza e alle loro potenziali conseguenze. Al contempo gli Stati membri si trovano ad affrontare crescenti rischi di cibersicurezza e un panorama di minacce globalmente complesso, con il chiaro rischio di una rapida propagazione degli incidenti informatici da uno Stato membro all'altro.

Inoltre le operazioni informatiche sono sempre più integrate nelle strategie ibride e di guerra, con effetti significativi sull'obiettivo. In particolare, l'aggressione militare della Russia contro l'Ucraina è stata preceduta ed è accompagnata da una strategia di operazioni informatiche ostili, il che segna una svolta nella percezione e nella valutazione della preparazione collettiva dell'UE alla gestione delle crisi di cibersicurezza e rende urgente un intervento. La minaccia di un possibile incidente su vasta scala in grado di provocare perturbazioni e danni significativi a infrastrutture critiche richiede una maggiore preparazione a tutti i livelli dell'ecosistema di cibersicurezza dell'UE. Tale minaccia va oltre l'aggressione militare della Russia nei confronti dell'Ucraina e include continue minacce informatiche da parte di soggetti statali e non statali destinate a persistere, data la molteplicità di soggetti allineati con le autorità di governo, criminali e hacktivisti coinvolti nelle attuali tensioni geopolitiche. Negli ultimi anni il numero di attacchi informatici è aumentato sensibilmente, compreso quello degli attacchi alle catene di approvvigionamento con finalità di ciberspionaggio, di ransomware o di perturbazione. Nel 2020 l'attacco SolarWinds alla catena di approvvigionamento ha interessato più di 18 000 organizzazioni a livello globale, tra cui agenzie governative e grandi imprese. Gli incidenti di cibersicurezza significativi possono comportare perturbazioni tali da impedire a uno o più Stati membri colpiti di gestirle autonomamente. Per tale ragione occorre dunque una solidarietà rafforzata a livello di Unione al fine di migliorare il rilevamento delle minacce e degli incidenti di cibersicurezza, nonché la preparazione e la risposta agli stessi.

Per quanto riguarda il rilevamento delle minacce e degli incidenti informatici, è urgente intensificare lo scambio di informazioni e migliorare le capacità collettive al fine di ridurre drasticamente il tempo necessario per rilevare le minacce informatiche, prima che possano provocare danni e comportare costi su vasta scala[1]. Sebbene un numero elevato di minacce e

[1] Secondo una relazione del Ponemon Institute e di IBM Security, il tempo medio necessario per identificare una violazione nel 2022 è stato di 207 giorni, a cui si aggiungono ulteriori 70 giorni per contenerla. Al contempo, nel 2022 le violazioni di dati con un ciclo di vita superiore a 200 giorni hanno avuto un costo medio di 4,86 milioni di EUR, rispetto ai 3,74 milioni di EUR per le violazioni con un ciclo di vita inferiore a 200 giorni. ("Cost of a data breach 2022", https://www.ibm.com/reports/data-breach).

incidenti di cibersicurezza abbia una potenziale dimensione transfrontaliera per via dell'interconnessione delle infrastrutture digitali, la condivisione di informazioni pertinenti tra gli Stati membri rimane limitata. L'istituzione di una rete di centri operativi di sicurezza (*Security Operations Centre*, SOC) transfrontalieri per migliorare le capacità di rilevamento e di risposta mira a far fronte a questo problema.

Per quanto riguarda la preparazione e la risposta agli incidenti di cibersicurezza, attualmente il sostegno a livello di Unione e la solidarietà tra gli Stati membri sono limitati. Nelle conclusioni dell'ottobre 2021 il Consiglio ha evidenziato la necessità di affrontare queste lacune, invitando la Commissione a presentare una proposta su un nuovo Fondo di risposta alle emergenze di cibersicurezza[2].

Il presente regolamento attua inoltre la strategia dell'UE in materia di cibersicurezza adottata nel dicembre 2020[3], che annunciava la creazione di un ciberscudo europeo per il rafforzamento delle capacità di rilevamento delle minacce informatiche e di condivisione delle informazioni nell'Unione europea tramite una federazione di SOC nazionali e transfrontalieri.

Il presente regolamento si basa sulle prime azioni già predisposte in stretta collaborazione con i principali portatori di interessi e sostenute dal programma Europa digitale. In particolare, per quanto riguarda i SOC, nell'ambito del programma di lavoro 2021-2022 sulla cibersicurezza del programma Europa digitale sono stati pubblicati un invito a manifestare interesse per l'appalto congiunto di strumenti e infrastrutture per l'istituzione di SOC transfrontalieri e un invito a presentare proposte per sovvenzioni al fine di consentire lo sviluppo delle capacità dei SOC al servizio di organizzazioni pubbliche e private. Per quanto concerne la preparazione e la risposta agli incidenti, la Commissione ha istituito un programma a breve termine per sostenere gli Stati membri, mediante un finanziamento aggiuntivo assegnato all'Agenzia dell'Unione europea per la cibersicurezza (ENISA), al fine di rafforzare immediatamente la preparazione e le capacità di risposta agli incidenti informatici gravi. Entrambe le azioni sono state preparate in stretto coordinamento con gli Stati membri. Il presente regolamento affronta le carenze e integra le indicazioni fornite da tali azioni.

Infine la presente proposta tiene fede all'impegno, in linea con la comunicazione congiunta sulla ciberdifesa[4] adottata il 10 novembre, di elaborare una proposta per un'iniziativa dell'UE per la cibersolidarietà con gli obiettivi seguenti: rafforzare le capacità comuni dell'UE in materia di rilevamento, conoscenza situazionale e risposta, sviluppare gradualmente una forza di riserva per la cibersicurezza a livello di UE, con servizi prestati da operatori privati di fiducia, e sostenere le prove presso soggetti critici.

---

2 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).

3 Comunicazione congiunta al Parlamento europeo e al Consiglio - "La strategia dell'UE in materia di cibersicurezza per il decennio digitale" (JOIN(2020) 18 final).

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

In questo contesto la Commissione propone il presente regolamento sulla cibersolidarietà inteso a rafforzare la solidarietà a livello di Unione per migliorare il rilevamento delle minacce e degli incidenti di cibersicurezza, nonché la preparazione e la risposta agli stessi, mediante gli obiettivi specifici seguenti:

- migliorare il rilevamento e la conoscenza situazionale comuni dell'UE in materia di minacce e incidenti informatici, contribuendo così alla sovranità tecnologica europea nel settore della cibersicurezza;
- rafforzare la preparazione dei soggetti critici in tutta l'UE e potenziare la solidarietà sviluppando capacità di risposta comuni contro incidenti di cibersicurezza significativi o su vasta scala, permettendo inoltre ai paesi terzi associati al programma Europa digitale di accedere al sostegno per la risposta agli incidenti;
- accrescere la resilienza dell'Unione e contribuire a una risposta efficace, riesaminando e valutando gli incidenti significativi o su vasta scala, traendone insegnamenti e, se del caso, formulando raccomandazioni.

Questi obiettivi saranno attuati mediante le azioni seguenti:

- la realizzazione di un'infrastruttura paneuropea di SOC (ciberscudo europeo) per sviluppare e potenziare capacità comuni in materia di rilevamento e conoscenza situazionale;
- la creazione di un meccanismo per le emergenze di cibersicurezza al fine di sostenere gli Stati membri nella preparazione e nella risposta agli incidenti di cibersicurezza significativi e su vasta scala e nella ripresa immediata dagli stessi. Il sostegno per la risposta agli incidenti sarà reso disponibile anche alle istituzioni, agli organi e agli organismi dell'Unione;
- l'istituzione di un meccanismo europeo di riesame degli incidenti di cibersicurezza finalizzato al riesame e alla valutazione di specifici incidenti significativi o su vasta scala.

Il ciberscudo europeo e il meccanismo per le emergenze di cibersicurezza saranno sostenuti dai finanziamenti del programma Europa digitale, che il presente strumento legislativo modificherà al fine di predisporre le suddette azioni, fornire un sostegno finanziario per il loro sviluppo e chiarire le condizioni per beneficiarne.

**•Coerenza con le disposizioni vigenti nel settore normativo interessato**

Il quadro dell'UE comprende diverse normative già in vigore o proposte a livello di Unione per ridurre le vulnerabilità, migliorare la resilienza dei soggetti critici contro i rischi di cibersicurezza e sostenere la gestione coordinata degli incidenti e delle crisi di cibersicurezza su vasta scala, in particolare la direttiva recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (NIS2)[5], il regolamento sulla

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

cibersicurezza[6], la direttiva sugli attacchi contro i sistemi di informazione[7] e la raccomandazione (UE) 2017/1584 della Commissione relativa alla risposta coordinata agli incidenti e alle crisi di cibersicurezza su vasta scala[8].

Le azioni proposte nell'ambito del regolamento sulla cibersolidarietà riguardano la conoscenza situazionale, la condivisione delle informazioni e il sostegno alla preparazione e alla risposta agli incidenti informatici. Tali azioni sono coerenti con gli obiettivi del quadro normativo in vigore a livello di Unione, segnatamente nell'ambito della direttiva (UE) 2022/2555 ("direttiva NIS2"), e li sostengono. In particolare il regolamento sulla cibersolidarietà si baserà sui quadri di cooperazione operativa e di gestione delle crisi esistenti in materia di cibersicurezza, specificamente sulla rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe) e sui gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), e ne sosterrà l'attuazione.

Le piattaforme SOC transfrontaliere 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 e strumenti all'avanguardia, e contribuendo allo sviluppo delle capacità e della sovranità tecnologica dell'Unione.

Infine la presente proposta è coerente con la raccomandazione del Consiglio su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche[9], che invita gli Stati membri ad adottare misure urgenti ed efficaci e a cooperare lealmente, efficacemente, in modo solidale e coordinato tra loro, con la Commissione e con le altre autorità pubbliche competenti, nonché con i soggetti interessati, al fine di migliorare la resilienza delle infrastrutture critiche utilizzate per fornire servizi essenziali nel mercato interno.

- **Coerenza con le altre normative dell'Unione**

La proposta è coerente con altri meccanismi e protocolli di emergenza per le crisi, come il dispositivo integrato per la riposta politica alle crisi (IPCR). Il regolamento sulla cibersolidarietà integrerà tali quadri e protocolli di gestione delle crisi, fornendo un sostegno specifico alla preparazione e alla risposta agli incidenti di cibersicurezza. La proposta sarà

[6] Regolamento (UE) 2019/881 del Parlamento Europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza").

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

[8] Proposta di regolamento del Parlamento europeo e del Consiglio relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica il regolamento (UE) 2019/1020 (COM(2022) 454 final).

[9] Raccomandazione del Consiglio, dell'8 dicembre 2022, su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche (Testo rilevante ai fini del SEE) 2023/C 20/01.

inoltre coerente con l'azione esterna dell'UE in risposta agli incidenti su vasta scala nel quadro della politica estera e di sicurezza comune (PESC), anche mediante il pacchetto di strumenti della diplomazia informatica dell'UE, e integrerà le azioni attuate nel contesto dell'articolo 42, paragrafo 7, del trattato sull'Unione europea o nelle situazioni definite nell'articolo 222 del trattato sul funzionamento dell'Unione europea.

Inoltre integra il meccanismo unionale di protezione civile (UCPM)[10] istituito nel dicembre 2013 e completato con una nuova normativa adottata nel maggio 2021[11], che rafforza i pilastri dell'UCPM, ovvero la prevenzione, la preparazione e la risposta, conferisce all'UE capacità aggiuntive per rispondere ai nuovi rischi in Europa e nel mondo e potenzia la riserva rescEU.

## 2. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

### • Base giuridica

La base giuridica della presente proposta è l'articolo 173, paragrafo 3, e l'articolo 322, paragrafo 1, lettera a), del trattato sul funzionamento dell'Unione europea (TFUE). L'articolo 173 TFUE dispone che l'Unione e gli Stati membri provvedano affinché siano assicurate le condizioni necessarie alla competitività dell'industria dell'Unione. Il presente regolamento mira a rafforzare la posizione competitiva del settore industriale e di quello dei servizi in Europa nell'ambito dell'economia digitalizzata e a sostenerne la trasformazione digitale, consolidando il livello di cibersicurezza nel mercato unico digitale. In particolare punta ad accrescere la resilienza dei cittadini, delle imprese e dei soggetti che operano in settori critici e altamente critici alle crescenti minacce alla cibersicurezza, che possono avere conseguenze sociali ed economiche devastanti.

La proposta si basa anche sull'articolo 322, paragrafo 1, lettera a), TFUE, in quanto contiene norme specifiche in materia di riporto che derogano al principio dell'annualità di cui al regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio (il "regolamento finanziario")[12]. Ai fini di una sana gestione finanziaria e considerando la natura imprevedibile, eccezionale e specifica del panorama della cibersicurezza e delle minacce informatiche, il meccanismo per le emergenze di cibersicurezza dovrebbe beneficiare di un certo grado di flessibilità in relazione alla gestione del bilancio, che consenta in particolare il riporto di diritto all'esercizio finanziario successivo degli stanziamenti di impegno e di pagamento non utilizzati per le azioni che perseguono gli obiettivi stabiliti nel regolamento. Poiché questa nuova norma crea problemi in relazione al regolamento finanziario, la questione potrebbe essere affrontata nel contesto dei negoziati in corso sulla rifusione del medesimo.

---

10 Decisione n. 1313/2013/UE del Parlamento europeo e del Consiglio, del 17 dicembre 2013, su un meccanismo unionale di protezione civile (Testo rilevante ai fini del SEE).

11 Regolamento (UE) 2021/836 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che modifica la decisione n. 1313/2013/UE su un meccanismo unionale di protezione civile (Testo rilevante ai fini del SEE).

12 Regolamento (UE, Euratom) 2018/1046 del Parlamento europeo e del Consiglio, del 18 luglio 2018, che stabilisce le regole finanziarie applicabili al bilancio generale dell'Unione (GU L 193 del 30.7.2018, pag. 1).

- **Sussidiarietà (per la competenza non esclusiva)**

La forte natura transfrontaliera delle minacce alla cibersicurezza e il numero crescente di rischi e incidenti, che hanno effetti di ricaduta a livello transfrontaliero e trasversalmente ai settori e ai prodotti, fanno sì che gli obiettivi del presente intervento non possano essere raggiunti efficacemente dai soli Stati membri e richiedano dunque un'azione comune e la solidarietà a livello di Unione.

L'esperienza di contrasto alle minacce informatiche derivanti dalla guerra contro l'Ucraina, unitamente agli insegnamenti tratti da un'esercitazione di cibersicurezza condotta nell'ambito della presidenza francese (EU CyCLES), ha dimostrato che è opportuno sviluppare meccanismi concreti di sostegno reciproco, in particolare la cooperazione con il settore privato, per realizzare la solidarietà a livello di UE. In questo contesto le conclusioni del Consiglio del 23 maggio 2022 sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica invitano la Commissione a presentare una proposta su un nuovo Fondo di risposta alle emergenze di cibersicurezza.

Il sostegno e le azioni a livello di Unione per migliorare il rilevamento delle minacce alla cibersicurezza nonché per accrescere la preparazione e le capacità di risposta apportano un valore aggiunto in quanto evitano la duplicazione degli sforzi nell'Unione e negli Stati membri. Ciò permetterebbe di sfruttare le risorse esistenti in modo più efficace e di intensificare il coordinamento e lo scambio di informazioni sugli insegnamenti tratti. Il meccanismo per le emergenze di cibersicurezza prevede inoltre la fornitura di sostegno ai paesi terzi associati al programma Europa digitale attingendo dalla riserva dell'UE per la cibersicurezza.

Il sostegno fornito tramite le varie iniziative che verranno attivate e finanziate a livello di Unione integrerà e non duplicherà le capacità nazionali per quanto riguarda il rilevamento, la conoscenza situazionale, la preparazione e la risposta alle minacce e agli incidenti informatici.

- **Proporzionalità**

Le azioni non vanno oltre quanto necessario per raggiungere gli obiettivi generali e specifici del regolamento. Le azioni previste dal presente regolamento lasciano impregiudicate le competenze degli Stati membri in materia di sicurezza nazionale, sicurezza pubblica, prevenzione, indagine, accertamento e perseguimento dei reati, così come gli obblighi giuridici dei soggetti che operano in settori critici e altamente critici di adottare misure di cibersicurezza, conformemente alla direttiva NIS 2.

Le azioni contemplate dal presente regolamento integrano tali sforzi e misure, sostenendo la creazione di infrastrutture per una migliore individuazione e analisi delle minacce e fornendo sostegno alle azioni di preparazione e di risposta in caso di incidenti significativi o su vasta scala.

- **Scelta dell'atto giuridico**

La proposta è presentata in forma di regolamento del Parlamento europeo e del Consiglio. Si tratta dello strumento giuridico più idoneo, in quanto solo un regolamento, con le sue disposizioni giuridiche direttamente applicabili, può fornire il grado di uniformità necessario per l'istituzione e il funzionamento di un ciberscudo europeo e di un meccanismo per le emergenze di cibersicurezza, garantendo il sostegno del programma Europa digitale per la loro istituzione nonché condizioni chiare per l'utilizzo e l'assegnazione di tale sostegno.

## 3. RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

- **Consultazioni dei portatori di interessi**

Le azioni del presente regolamento saranno sostenute dal programma Europa digitale, che è stato oggetto di un'ampia consultazione, e si baseranno sulle prime azioni già predisposte in stretta collaborazione con i principali portatori di interessi. Per quanto riguarda i SOC, la Commissione ha elaborato un documento di riflessione sulla messa a punto di piattaforme SOC transfrontaliere e un invito a manifestare interesse in stretta collaborazione con gli Stati membri nell'ambito del Centro europeo di competenza per la cibersicurezza (ECCC). In questo contesto è stata condotta un'indagine sulle capacità dei SOC nazionali e sono stati discussi approcci e requisiti tecnici comuni all'interno del gruppo di lavoro tecnico dell'ECCC che riunisce i rappresentanti degli Stati membri. Si sono inoltre svolti scambi con l'industria, in particolare mediante il gruppo di esperti sui SOC creato dall'ENISA e dall'Organizzazione europea per la sicurezza informatica (ECSO).

In secondo luogo, per quanto concerne la preparazione e la risposta agli incidenti, la Commissione ha istituito un programma a breve termine per sostenere gli Stati membri, mediante un finanziamento aggiuntivo assegnato all'ENISA dal programma Europa digitale, al fine di rafforzare immediatamente la preparazione e le capacità di risposta agli incidenti informatici gravi. Le osservazioni formulate dagli Stati membri e dall'industria, pervenute durante l'attuazione di tale programma a breve termine, hanno già fornito valide indicazioni che sono state tenute in considerazione nell'elaborazione della proposta di regolamento per risolvere le carenze individuate. Si è trattato di un primo passo in linea con le conclusioni del Consiglio sulla posizione in materia di deterrenza informatica che invitavano la Commissione a presentare una proposta su un nuovo Fondo di risposta alle emergenze di cibersicurezza.

Inoltre, sulla base di un documento di riflessione, il 16 febbraio 2023 si è tenuto un seminario con gli esperti degli Stati membri sul meccanismo per le emergenze di cibersicurezza. Tutti gli Stati membri hanno partecipato a tale seminario e undici hanno fornito ulteriori contributi per iscritto.

- **Valutazione d'impatto**

Vista l'urgenza della proposta, non è stata effettuata alcuna valutazione d'impatto. Le azioni del presente regolamento saranno sostenute dal programma Europa digitale e sono in linea

con quelle stabilite nel relativo regolamento, che è stato sottoposto a una specifica valutazione d'impatto. Il presente regolamento non comporterà alcun impatto amministrativo o ambientale significativo oltre a quelli già esaminati nella valutazione d'impatto del regolamento sul programma Europa digitale.

Si basa inoltre sulle prime azioni predisposte in stretta collaborazione con i principali portatori di interessi, come indicato sopra, e dà seguito all'invito rivolto dagli Stati membri alla Commissione di presentare una proposta su un nuovo Fondo di risposta alle emergenze di cibersicurezza entro la fine del terzo trimestre del 2022.

Nello specifico, per quanto riguarda la conoscenza situazionale e il rilevamento nell'ambito del ciberscudo europeo, nel contesto del programma di lavoro 2021-2022 sulla cibersicurezza del programma Europa digitale sono stati pubblicati un invito a manifestare interesse per l'appalto congiunto di strumenti e infrastrutture per l'istituzione di SOC transfrontalieri e un invito a presentare proposte per sovvenzioni al fine di consentire lo sviluppo delle capacità dei SOC al servizio di organizzazioni pubbliche e private.

Per quanto riguarda la preparazione e la risposta agli incidenti, come già menzionato, la Commissione ha istituito un programma a breve termine per sostenere gli Stati membri mediante il programma Europa digitale, attuato dall'ENISA. Tra i servizi forniti figurano azioni di preparazione, quali test di penetrazione dei soggetti critici al fine di individuare le vulnerabilità. Il programma rafforza inoltre le possibilità di assistere gli Stati membri in caso di incidenti gravi che colpiscano soggetti critici. L'attuazione da parte dell'ENISA di questo programma a breve termine è in corso e ha già fornito indicazioni pertinenti di cui si è tenuto conto nell'elaborazione del presente regolamento.

- **Diritti fondamentali**

Contribuendo alla sicurezza delle informazioni digitali, la presente proposta concorrerà a tutelare il diritto alla libertà e alla sicurezza, in conformità dell'articolo 6 della Carta dei diritti fondamentali dell'Unione europea, e il diritto al rispetto della vita privata e della vita familiare, in conformità dell'articolo 7 della stessa. Proteggendo le imprese dagli attacchi informatici che possono causare danni economici, la proposta contribuirà inoltre a garantire la libertà d'impresa in conformità dell'articolo 16 della Carta dei diritti fondamentali dell'UE e il diritto di proprietà in conformità dell'articolo 17 della stessa. Infine, proteggendo l'integrità delle infrastrutture critiche dagli attacchi informatici, la proposta contribuirà a garantire il diritto alla protezione della salute, in conformità dell'articolo 35 della Carta dei diritti fondamentali dell'Unione europea, e il diritto all'accesso ai servizi d'interesse economico generale, in conformità dell'articolo 36 della stessa.

## 4. INCIDENZA SUL BILANCIO

Le azioni del presente regolamento saranno sostenute da finanziamenti nel quadro dell'obiettivo strategico "Cibersicurezza" del programma Europa digitale.

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

Una parte dei 100 milioni di EUR aggiuntivi rafforzerà il bilancio gestito dall'ECCC per l'attuazione di azioni riguardanti i SOC e la preparazione nell'ambito dei loro programmi di lavoro. Il finanziamento aggiuntivo servirà inoltre a sostenere l'istituzione della riserva dell'UE per la cibersicurezza.

Integrando il bilancio già previsto per azioni analoghe nel quadro del programma di lavoro principale e del programma di lavoro sulla cibersicurezza del programma Europa digitale per il periodo 2023-2027, tale finanziamento potrebbe portare l'importo totale per il 2023-2027 a 551 milioni, mentre 115 milioni sono già stati stanziati per progetti pilota per il periodo 2021-2022. Includendo i contributi degli Stati membri, il bilancio complessivo potrebbe ammontare a 1,109 miliardi di EUR.

Una panoramica dei costi in questione è inclusa nella "scheda finanziaria legislativa" che accompagna la presente proposta.

## 5. ALTRI ELEMENTI

- **Piani attuativi e modalità di monitoraggio, valutazione e informazione**

La Commissione monitorerà l'attuazione, l'applicazione e il rispetto di queste nuove disposizioni al fine di valutarne l'efficacia. La Commissione presenterà al Parlamento europeo e al Consiglio una relazione sulla valutazione e sul riesame del presente regolamento entro quattro anni dalla data della sua applicazione.

- **Illustrazione dettagliata delle singole disposizioni della proposta**

Obiettivi generali, oggetto e definizioni (capo I)

Il capo I definisce gli obiettivi del regolamento di rafforzare la solidarietà a livello di Unione per migliorare il rilevamento delle minacce e degli incidenti di cibersicurezza, nonché la preparazione e la risposta agli stessi e, nello specifico, di migliorare il rilevamento e la conoscenza situazionale comuni dell'Unione in materia di minacce e incidenti informatici, 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, nonché accrescere la resilienza dell'Unione riesaminando e valutando tali incidenti. Questo capo definisce altresì le azioni tramite cui tali obiettivi saranno conseguiti: la realizzazione di un ciberscudo europeo, la creazione di un meccanismo per le emergenze di cibersicurezza e l'istituzione di un meccanismo di riesame degli incidenti di cibersicurezza. Stabilisce inoltre le definizioni utilizzate in tutto l'atto.

Il ciberscudo europeo (capo II)

Il capo II istituisce il ciberscudo europeo e ne definisce i vari elementi e le condizioni per parteciparvi. In primo luogo annuncia l'obiettivo generale del ciberscudo europeo, che consiste nello sviluppare capacità avanzate che permettano all'Unione di rilevare, analizzare ed elaborare i dati sulle minacce e sugli incidenti informatici nell'UE, nonché gli obiettivi operativi specifici. Specifica che il finanziamento dell'Unione per il ciberscudo europeo sarà attuato in conformità del regolamento sul programma Europa digitale.

Il capo descrive inoltre il tipo di soggetti che costituiscono il ciberscudo europeo, ossia i centri operativi di sicurezza nazionali ("SOC nazionali") e transfrontalieri ("SOC transfrontalieri"). Ogni Stato membro partecipante designa un SOC nazionale, che funge da punto di riferimento e da porta di accesso ad altre organizzazioni pubbliche e private a livello nazionale per raccogliere e analizzare informazioni sulle minacce e sugli incidenti di cibersicurezza e per contribuire a un SOC transfrontaliero. A seguito di un invito a manifestare interesse, un SOC nazionale può essere selezionato dall'ECCC per partecipare con quest'ultimo a un appalto congiunto di strumenti e infrastrutture e ricevere una sovvenzione per la gestione di tali strumenti e infrastrutture. Se diventa beneficiario del sostegno dell'Unione, un SOC nazionale si impegna a candidarsi per partecipare a un SOC transfrontaliero entro due anni.

I SOC transfrontalieri sono costituiti da un consorzio di almeno tre Stati membri, rappresentati dai SOC nazionali, che si impegnano a collaborare per coordinare le rispettive attività di rilevamento e monitoraggio delle minacce informatiche. A seguito di un invito iniziale a manifestare interesse, un consorzio ospitante può essere selezionato dall'ECCC per partecipare con quest'ultimo a un appalto congiunto di strumenti e infrastrutture e per ricevere una sovvenzione per la gestione di tali strumenti e infrastrutture. I membri del consorzio ospitante stipulano un accordo di consorzio scritto che definisce le disposizioni interne. Questo capo specifica inoltre le prescrizioni riguardanti la condivisione di informazioni tra i partecipanti a un SOC transfrontaliero e tra un SOC transfrontaliero e altri SOC transfrontalieri, nonché con i soggetti dell'UE pertinenti. I SOC nazionali che partecipano a un SOC transfrontaliero condividono tra loro informazioni pertinenti relative alle minacce informatiche; i dettagli, compreso l'impegno a condividere una quantità significativa di dati e le relative condizioni, dovrebbero essere definiti in un accordo di consorzio. I SOC transfrontalieri garantiscono un alto livello di interoperabilità tra di loro e dovrebbero altresì stipulare accordi di cooperazione con altri SOC transfrontalieri, specificando i principi di condivisione delle informazioni. Quando ottengono informazioni relative a un incidente di cibersicurezza su vasta scala, potenziale o in corso, i SOC transfrontalieri forniscono 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. Il capo II infine specifica le condizioni di sicurezza per partecipare al ciberscudo europeo.

Meccanismo per le emergenze di cibersicurezza (capo III)

Il capo III istituisce il 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 o delle crisi di cibersicurezza significativi e su vasta scala nonché attenuare tale impatto. Le azioni di attuazione del meccanismo per le emergenze di cibersicurezza sono sostenute da finanziamenti del programma Europa digitale. Il meccanismo prevede azioni per sostenere la preparazione, tra cui verifiche coordinate presso soggetti che operano in settori altamente critici, la risposta agli incidenti di cibersicurezza significativi o su vasta scala e la ripresa immediata dagli stessi, o l'attenuazione di minacce informatiche significative, e azioni di assistenza reciproca.

Le azioni di preparazione del meccanismo per le emergenze di cibersicurezza includono la verifica coordinata della preparazione dei soggetti che operano in settori altamente critici. La Commissione, previa consultazione dell'ENISA e del gruppo di cooperazione NIS, dovrebbe individuare periodicamente i settori o i sottosettori pertinenti 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 a livello di UE.

Ai fini dell'attuazione delle azioni di risposta agli incidenti proposte, il presente regolamento istituisce una riserva dell'UE per la cibersicurezza, che consiste in servizi di risposta agli incidenti erogati da fornitori di fiducia, selezionati in base ai criteri stabiliti nel presente regolamento. Tra gli utenti che usufruiscono dei servizi della riserva dell'UE per la cibersicurezza figurano le autorità di gestione delle crisi informatiche degli Stati membri e i CSIRT, nonché le istituzioni, gli organi e gli organismi dell'Unione. La Commissione ha la responsabilità generale dell'attuazione della riserva dell'UE per la cibersicurezza e può affidare all'ENISA, in tutto o in parte, il funzionamento e l'amministrazione della medesima.

Per ricevere il sostegno della riserva dell'UE per la cibersicurezza, gli utenti dovrebbero adottare misure volte ad attenuare gli effetti dell'incidente per il quale è richiesto il sostegno. Le richieste di sostegno a titolo della riserva dell'UE per la cibersicurezza dovrebbero includere le necessarie informazioni pertinenti sull'incidente e sulle misure già adottate dagli utenti. Il capo descrive inoltre le modalità di attuazione, compresa la valutazione delle richieste presentate alla riserva dell'UE per la cibersicurezza.

Il regolamento stabilisce inoltre i principi di aggiudicazione degli appalti e i criteri di selezione relativi ai fornitori di fiducia della riserva dell'UE per la cibersicurezza.

I paesi terzi possono richiedere il sostegno della riserva dell'UE per la cibersicurezza nei casi in cui è previsto dagli accordi di associazione conclusi in relazione alla loro partecipazione al programma Europa digitale. Questo capo descrive le ulteriori condizioni e modalità di tale partecipazione.

Meccanismo di riesame degli incidenti di cibersicurezza (capo IV)

Su richiesta della Commissione, di EU-CyCLONe o della rete di CSIRT, l'ENISA dovrebbe riesaminare e valutare le minacce, le vulnerabilità e le azioni di attenuazione in relazione a uno specifico incidente di cibersicurezza significativo o su vasta scala. Il riesame e la

valutazione dovrebbero essere presentati dall'ENISA sotto forma di una relazione di riesame dell'incidente alla rete di CSIRT, a EU-CyCLONe e alla Commissione, per sostenerli nello svolgimento dei loro compiti. Se l'incidente riguarda un paese terzo, la relazione dovrebbe essere condivisa dalla Commissione con l'alto rappresentante e includere gli insegnamenti tratti e, se del caso, le raccomandazioni formulate per migliorare la posizione dell'UE in materia di deterrenza informatica.

Disposizioni finali (capo V)

Il capo V contiene modifiche del regolamento sul programma Europa digitale e prevede l'obbligo per la Commissione di preparare relazioni periodiche per la valutazione e il riesame del regolamento, da presentare al Parlamento europeo e al Consiglio. Alla Commissione è conferito il potere di adottare atti di esecuzione secondo la procedura d'esame di cui all'articolo 21 al fine di: specificare le condizioni dell'interoperabilità tra i SOC transfrontalieri; determinare le modalità procedurali per la condivisione delle informazioni relative a un incidente di cibersicurezza su vasta scala, potenziale o in corso, tra i SOC transfrontalieri e i soggetti dell'Unione; stabilire i requisiti tecnici per garantire un elevato livello di sicurezza fisica e dei dati dell'infrastruttura e per proteggere gli interessi dell'Unione in materia di sicurezza in caso di condivisione delle informazioni con soggetti che non sono organismi pubblici degli Stati membri; specificare i tipi e il numero di servizi di risposta richiesti per la riserva dell'UE per la cibersicurezza; e specificare ulteriormente le modalità dettagliate di assegnazione dei servizi di sostegno della riserva dell'UE per la cibersicurezza.

2023/0109 (COD)

Proposta di

# REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

## che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

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

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere della Corte dei conti[1],

visto il parere del Comitato economico e sociale europeo[2],

visto il parere del Comitato delle regioni[3],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) L'utilizzo delle tecnologie dell'informazione e della comunicazione e la dipendenza dalle stesse sono diventati fondamentali 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.

(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

[1] GU C […] del […], pag. […].
[2] GU C , , pag. .
[3] GU C , , pag. .

brevi, non sono circoscritti a una determinata zona geografica e si verificano simultaneamente o si diffondono istantaneamente in numerosi paesi.

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

(4) L'Unione ha già adottato una serie di misure per ridurre le vulnerabilità e accrescere la resilienza delle infrastrutture e dei soggetti critici contro i rischi di cibersicurezza, in particolare la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[5], la raccomandazione (UE) 2017/1584 della Commissione[6], la direttiva 2013/40/UE del Parlamento europeo e del Consiglio[7] e il regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[8]. Inoltre la raccomandazione del Consiglio su un approccio coordinato a livello dell'Unione per rafforzare la resilienza delle infrastrutture critiche invita gli Stati membri ad adottare misure urgenti ed efficaci e a cooperare lealmente, efficacemente, in modo solidale e coordinato tra loro, con la Commissione e le altre autorità pubbliche competenti, nonché con i soggetti interessati, al fine di migliorare la resilienza delle infrastrutture critiche utilizzate per fornire servizi essenziali nel mercato interno.

(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 dell'UE in materia di deterrenza informatica[9] gli Stati

---

4 https://futureu.europa.eu/it/?locale=it.

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

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

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

8 Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza") (GU L 151 del 7.6.2019, pag. 15).

9 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).

membri hanno inoltre invitato la Commissione a presentare una proposta su un nuovo Fondo di risposta alle emergenze di cibersicurezza.

(6) La comunicazione congiunta sulla politica di ciberdifesa dell'UE[10], adottata il 10 novembre 2022, ha annunciato un'iniziativa dell'UE per la cibersolidarietà con gli obiettivi seguenti: rafforzare le capacità comuni dell'UE in materia di rilevamento, conoscenza situazionale e risposta, promuovendo la realizzazione di un'infrastruttura unionale dei centri operativi di sicurezza ("SOC"), sostenere la costituzione graduale di una forza di riserva per la cibersicurezza a livello di UE, con servizi prestati da operatori privati di fiducia, e le prove presso soggetti critici al fine di rilevare potenziali vulnerabilità basate sulle valutazioni del rischio effettuate a livello UE.

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

(8) Per conseguire questi obiettivi occorre inoltre modificare il regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio[11] in alcuni settori. In particolare il presente regolamento dovrebbe modificare il regolamento (UE) 2021/694 aggiungendo nuovi obiettivi operativi relativi al ciberscudo europeo e al meccanismo per le emergenze di cibersicurezza nell'ambito dell'obiettivo specifico 3 del programma Europa digitale, che mira a garantire la resilienza, l'integrità e l'affidabilità del mercato unico digitale, a rafforzare le capacità di monitoraggio delle minacce e degli attacchi informatici e di risposta agli stessi, nonché a rafforzare la cooperazione transfrontaliera in materia di cibersicurezza. È opportuno stabilire le condizioni specifiche in base alle quali può essere concesso il sostegno finanziario per queste azioni e definire i meccanismi di governance e di coordinamento necessari per raggiungere gli obiettivi previsti. Altre modifiche del regolamento (UE) 2021/694 dovrebbero includere descrizioni delle azioni proposte nell'ambito dei nuovi obiettivi operativi, nonché indicatori misurabili per monitorare l'attuazione di questi ultimi.

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

---

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

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

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

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

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

(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.

(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

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

vantaggi derivanti dal rilevamento delle minacce transfrontaliere e dalla gestione e condivisione delle informazioni. L'obiettivo generale dei SOC transfrontalieri dovrebbe essere quello di rafforzare le capacità di analisi, prevenzione e rilevamento delle minacce alla cibersicurezza e di favorire l'elaborazione di analisi di alta qualità sulle minacce alla cibersicurezza, in particolare mediante la condivisione di dati provenienti da varie fonti, pubbliche o private, nonché tramite la condivisione e l'uso congiunto di strumenti all'avanguardia e lo sviluppo congiunto di capacità di rilevamento, analisi e prevenzione in un contesto di fiducia. Tali SOC dovrebbero garantire nuove capacità aggiuntive, basandosi sui SOC e sui gruppi di intervento per la sicurezza informatica in caso di incidente ("CSIRT") esistenti nonché su altri soggetti pertinenti e integrandoli.

(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.

(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.

(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.

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

(19) Per consentire lo scambio di dati sulle minacce alla cibersicurezza provenienti da varie fonti, su vasta scala, in un contesto 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.

(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[13].

(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.

(22) La condivisione delle informazioni tra i partecipanti al ciberscudo europeo dovrebbe essere conforme alle prescrizioni giuridiche esistenti e in particolare al diritto nazionale e dell'Unione in materia di protezione dei dati, nonché alle norme

[13] 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).

dell'Unione sulla concorrenza che disciplinano lo scambio di informazioni. Il destinatario delle informazioni dovrebbe attuare, nella misura in cui il trattamento dei dati personali sia necessario, misure tecniche e organizzative a salvaguardia dei diritti e delle libertà degli interessati, distruggere i dati non appena non sono più necessari per la finalità dichiarata e comunicarne la distruzione all'organismo che li ha resi disponibili.

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

(24) Alla luce dell'aumento dei rischi e del numero di incidenti informatici che colpiscono gli Stati membri, occorre istituire uno strumento di sostegno alle crisi per migliorare la resilienza dell'Unione agli incidenti di cibersicurezza significativi e su vasta scala e integrare le azioni degli Stati membri mediante un sostegno finanziario di emergenza per la preparazione, la risposta e il ripristino immediato dei servizi essenziali. Tale strumento dovrebbe consentire una rapida 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").

(25) Il meccanismo per le emergenze di cibersicurezza dovrebbe fornire un sostegno agli Stati membri, integrando le loro misure e le loro risorse nonché altre opzioni di sostegno esistenti in caso di risposta agli incidenti di cibersicurezza significativi e su vasta scala e di ripresa immediata dagli stessi, come i servizi forniti dall'Agenzia dell'Unione europea per la cibersicurezza ("ENISA") conformemente al suo mandato, la risposta coordinata e l'assistenza della rete di CSIRT, il sostegno a strategie di attenuazione offerto da EU-CyCLONe, nonché l'assistenza reciproca tra gli Stati membri, anche nel contesto dell'articolo 42, paragrafo 7, TUE, i gruppi di risposta rapida agli incidenti informatici della PESCO[14] e i gruppi di risposta rapida alle minacce ibride. Tale meccanismo dovrebbe rispondere alla necessità di garantire la disponibilità di mezzi specializzati per sostenere la preparazione e la risposta agli incidenti di cibersicurezza in tutta l'Unione e nei paesi terzi.

(26) Il presente strumento non pregiudica le procedure e i quadri di coordinamento della risposta alle crisi a livello dell'Unione, in particolare l'UCPM[15], gli IPCR[16,] e la direttiva (UE) 2022/2555, e può contribuire alle azioni attuate nel contesto dell'articolo 42, paragrafo 7, TUE o nelle situazioni definite nell'articolo 222 TFUE oppure integrare tali azioni. L'utilizzo del presente strumento dovrebbe inoltre essere

---

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

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

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

coordinato, laddove opportuno, con l'attuazione delle misure del pacchetto di strumenti della diplomazia informatica.

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

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

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

elettroniche (BEREC), le valutazioni coordinate del rischio da condurre ai sensi dell'articolo 22 della direttiva (UE) 2022/2555 e i test di resilienza operativa digitale previsti dal regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio[17]. La selezione dei settori dovrebbe inoltre tenere conto della raccomandazione del Consiglio su un approccio coordinato a livello di Unione per rafforzare la resilienza delle infrastrutture critiche.

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

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

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

(33) È opportuno istituire gradualmente una riserva per la cibersicurezza a livello di Unione, costituita da servizi erogati da fornitori privati di servizi di sicurezza gestiti a sostegno di azioni di risposta e di ripresa immediata in caso di incidenti di cibersicurezza significativi o su vasta scala. La riserva dell'UE per la cibersicurezza dovrebbe garantire la disponibilità e la prontezza dei servizi. 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.

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

[17] Regolamento (UE) 2022/2554 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativo alla resilienza operativa digitale per il settore finanziario e che modifica i regolamenti (CE) n. 1060/2009, (UE) n. 648/2012, (UE) n. 600/2014, (UE) n. 909/2014 e (UE) 2016/1011.

(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.

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

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

(38) Al fine di garantire condizioni uniformi di attuazione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione per specificare le condizioni dell'interoperabilità tra i SOC transfrontalieri; determinare le modalità procedurali per la condivisione delle informazioni relative a un incidente di cibersicurezza su vasta scala, potenziale o in corso, tra i SOC transfrontalieri e i

soggetti dell'Unione; stabilire i requisiti tecnici al fine di garantire la sicurezza del ciberscudo europeo; specificare i tipi e il numero di servizi di risposta richiesti per la riserva dell'UE per la cibersicurezza; e specificare ulteriormente le modalità dettagliate di assegnazione dei servizi di sostegno della riserva dell'UE per la cibersicurezza. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio.

(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,

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

## *Capo I*

## *OBIETTIVI GENERALI, OGGETTO E DEFINIZIONI*

### *Articolo 1*

### **Oggetto e finalità**

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

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

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

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

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

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

b) rafforzare la preparazione dei soggetti che operano in settori critici e altamente critici in tutta l'Unione e potenziare la solidarietà sviluppando capacità di risposta comuni contro gli incidenti di cibersicurezza significativi o su vasta scala, permettendo

inoltre ai paesi terzi associati al programma Europa digitale di accedere al sostegno offerto dall'Unione per la risposta agli incidenti di cibersicurezza;

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

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

*Articolo 2*

**Definizioni**

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) **"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;

2) **"organismo pubblico"**: un organismo di diritto pubblico quale definito all'articolo 2, paragrafo 1, punto 4), della direttiva 2014/24/UE del Parlamento europeo e del Consiglio[18];

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;

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

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

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

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

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

9) **"preparazione"**: stato di prontezza e capacità in grado di garantire una risposta rapida ed efficace a un incidente di cibersicurezza significativo o su vasta scala,

[18] 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).

ottenuto a seguito di azioni di valutazione e monitoraggio del rischio intraprese in anticipo;

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

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.

## *Capo II*

## *IL CIBERSCUDO EUROPEO*

### *Articolo 3*

### Istituzione del ciberscudo europeo

1. 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").

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

2. Il ciberscudo europeo ha le funzioni seguenti:

a) mettere in comune e condividere, attraverso i SOC transfrontalieri, i dati sulle minacce e sugli incidenti informatici provenienti da varie fonti;

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

c) contribuire a una migliore protezione e risposta alle minacce informatiche;

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

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

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

*Articolo 4*

**Centri operativi di sicurezza nazionali**

1. Per partecipare al ciberscudo europeo, ogni Stato membro designa almeno un SOC nazionale. Il SOC nazionale è un organismo pubblico.

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.

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

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

*Articolo 5*

**Centri operativi di sicurezza transfrontalieri**

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

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

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

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

*Articolo 6*

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

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

a) miri a prevenire o rilevare gli incidenti, a rispondervi, a riprendersi dagli stessi o ad attenuarne l'impatto;

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

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

a) l'impegno a condividere una quantità significativa di dati di cui al paragrafo 1 e le condizioni di scambio di tali informazioni;

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

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

3. Per incoraggiare lo scambio di informazioni tra SOC transfrontalieri, 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.

4. I SOC transfrontalieri stipulano accordi di cooperazione tra di loro, specificando i principi di condivisione delle informazioni tra le piattaforme transfrontaliere.

*Articolo 7*

**Cooperazione e condivisione di informazioni con soggetti dell'Unione**

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.

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.

*Articolo 8*

**Sicurezza**

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

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

3. La Commissione può adottare atti di esecuzione che stabiliscono i requisiti tecnici che gli Stati membri devono rispettare per adempiere gli obblighi di cui ai paragrafi 1 e 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 21, paragrafo 2, del presente regolamento. 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.

## *Capo III*

## *MECCANISMO PER LE EMERGENZE DI CIBERSICUREZZA*

*Articolo 9*

**Istituzione del meccanismo per le emergenze di cibersicurezza**

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

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

*Articolo 10*

**Tipi di azioni**

1. Il meccanismo sostiene i tipi di azioni seguenti:

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

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

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

*Articolo 11*

**Verifica coordinata della preparazione dei soggetti**

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

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.

*Articolo 12*

**Istituzione della riserva dell'UE per la cibersicurezza**

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

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.

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

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

b) le istituzioni e gli organi e organismi dell'Unione.

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

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

6. La Commissione 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.

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.

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.

*Articolo 13*

**Richieste di sostegno della riserva dell'UE per la cibersicurezza**

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

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

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

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

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

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

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

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

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

7. 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.

*Articolo 14*

**Attuazione del sostegno della riserva dell'UE per la cibersicurezza**

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

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

a) la gravità dell'incidente di cibersicurezza;

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

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

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

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

3. I servizi della riserva dell'UE per la cibersicurezza sono forniti in conformità di accordi specifici stipulati tra il fornitore di servizi e l'utente a cui viene fornito il sostegno nell'ambito della riserva dell'UE per la cibersicurezza. Tali accordi includono condizioni di responsabilità.

4. Gli accordi di cui al paragrafo 3 possono essere basati su modelli preparati dall'ENISA, previa consultazione degli Stati membri.

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.

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.

7. La Commissione riferisce periodicamente al gruppo di cooperazione NIS in merito alle modalità di impiego e ai risultati del sostegno.

*Articolo 15*

**Coordinamento con i meccanismi di gestione delle crisi**

1. Nei casi in cui gli incidenti di cibersicurezza significativi o su vasta scala siano causati da catastrofi, quali definite nella decisione n. 1313/2013/UE[19], o vi diano luogo, il sostegno previsto dal presente regolamento per rispondere a tali incidenti integra le azioni di cui alla decisione n. 1313/2013/UE senza pregiudicare quest'ultima.

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

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

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

*Articolo 16*

**Fornitori di fiducia**

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

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

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

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

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.

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

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

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

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

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

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

f) il fornitore è dotato dell'attrezzatura tecnica hardware e software necessaria a supportare il servizio richiesto;

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

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

i) il fornitore è in grado di prestare il servizio nella lingua locale dello Stato membro o degli Stati membri in cui ciò è possibile;

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.

*Articolo 17*

**Sostegno ai paesi terzi**

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

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

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

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

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

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

## *Capo IV*

## *MECCANISMO DI RIESAME DEGLI INCIDENTI DI CIBERSICUREZZA*

### *Articolo 18*

### Meccanismo di riesame degli incidenti di cibersicurezza

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

2. Per preparare la relazione di riesame dell'incidente di cui al paragrafo 1, l'ENISA collabora con tutti i portatori di interessi, compresi i rappresentanti degli Stati membri, della Commissione, di altre istituzioni e di altri organi e organismi pertinenti dell'UE, dei fornitori di servizi di sicurezza gestiti 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.

## *Capo V*

## *DISPOSIZIONI FINALI*

### *Articolo 19*

### **Modifiche del regolamento (UE) 2021/694**

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

1) l'articolo 6 è così modificato:

a) il paragrafo 1 è così modificato:

1) è inserita la seguente lettera a bis):

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

2) è aggiunta la seguente lettera g):

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

a) il paragrafo 2 è sostituito dal seguente:

"2. Le azioni nell'ambito dell'obiettivo specifico 3 sono attuate principalmente mediante il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento in conformità del regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio[20], fatta eccezione per le azioni di attuazione della riserva dell'UE per la cibersicurezza, che sono attuate dalla Commissione e dall'ENISA.";

[20] Regolamento (UE) 2021/887 del Parlamento europeo e del Consiglio, del 20 maggio 2021, che istituisce il Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca e la rete dei centri nazionali di coordinamento (GU L 202 dell'8.6.2021, pag. 1).

2) l'articolo 9 è così modificato:

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

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

c) 1 629 566 000 EUR per l'obiettivo specifico 3 – Cibersicurezza e fiducia;

d) 482 347 000 EUR per l'obiettivo specifico 4 – Competenze digitali avanzate;";

b) è aggiunto il seguente paragrafo 8:

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

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

"2. 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.

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

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

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

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

Nell'attuazione delle procedure di appalto per la riserva dell'UE per la cibersicurezza istituita dall'articolo 12 del regolamento (UE) 2023/XX, la Commissione e l'ENISA possono fungere da centrale di committenza per condurre una procedura di appalto per conto o a nome di istituzioni, organi e organismi dell'Unione. La Commissione e l'ENISA possono anche agire in veste di grossisti, comprando, immagazzinando e rivendendo o donando forniture e servizi, comprese le locazioni, per le istituzioni, gli organi e gli organismi dell'Unione. In deroga all'articolo 169, paragrafo 3, del regolamento (UE) XXX/XXXX [rifusione del RF], la richiesta di una singola istituzione o di un singolo organo o organismo dell'Unione è sufficiente per conferire alla Commissione o all'ENISA il mandato di agire.

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

4) è aggiunto l'articolo 16 bis seguente:

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

5) l'articolo 19 è sostituito dal seguente:

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

Il sostegno erogato sotto forma di sovvenzioni può essere concesso direttamente dall'ECCC, senza invito a presentare proposte, ai SOC nazionali di cui all'articolo 4 del regolamento 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 per il meccanismo per le emergenze di cibersicurezza di cui all'articolo 10 del regolamento XXXX può essere concesso direttamente dall'ECCC agli Stati membri senza invito a presentare proposte, in conformità dell'articolo 195, primo comma, lettera d), del regolamento finanziario.

Per le azioni specificate nell'articolo 10, paragrafo 1, lettera c), del regolamento 202X/XXXX, l'ECCC informa la Commissione e l'ENISA sulle richieste di sovvenzioni dirette degli Stati membri senza invito a presentare proposte.

A sostegno dell'assistenza reciproca per la risposta a un incidente di cibersicurezza significativo o su vasta scala, come definito all'articolo 10, lettera c), del regolamento XXXX, e in conformità dell'articolo 193, paragrafo 2, secondo comma, lettera a), del regolamento finanziario, in casi debitamente giustificati i costi possono essere considerati

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

6) gli allegati I e II sono modificati conformemente all'allegato del presente regolamento.

*Articolo 20*

**Valutazione**

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.

*Articolo 21*

**Procedura di comitato**

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

*Articolo 22*

**Entrata in vigore**

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

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

Fatto a Strasburgo, il

*Per il Parlamento europeo*
*La presidente*

*Per il Consiglio*
*Il presidente*

# SCHEDA FINANZIARIA LEGISLATIVA

## 1. CONTESTO DELLA PROPOSTA/INIZIATIVA

### 1.1. Titolo della proposta/iniziativa

### 1.2. Settore/settori interessati

### 1.3. La proposta/iniziativa riguarda:

### 1.4. Obiettivi

*1.4.1. Obiettivi generali*

*1.4.2. Obiettivi specifici*

*1.4.3. Risultati e incidenza previsti*

*1.4.4. Indicatori di prestazione*

### 1.5. Motivazione della proposta/iniziativa

*1.5.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa*

*1.5.2. Valore aggiunto dell'intervento dell'Unione (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto o un'efficacia e una complementarità maggiori). Ai fini del presente punto, per "valore aggiunto dell'intervento dell'Unione" si intende il valore derivante dall'intervento dell'Unione, che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli.*

*1.5.3. Insegnamenti tratti da esperienze analoghe*

*1.5.4. Compatibilità con il quadro finanziario pluriennale ed eventuali sinergie con altri strumenti pertinenti*

*1.5.5. Valutazione delle varie opzioni di finanziamento disponibili, comprese le possibilità di riassegnazione*

### 1.6. Durata e incidenza finanziaria della proposta/iniziativa

### 1.7. Metodi di esecuzione del bilancio previsti

## 2. MISURE DI GESTIONE

### 2.1. Disposizioni in materia di monitoraggio e di relazioni

### 2.2. Sistema di gestione e di controllo

*2.2.1. Giustificazione della o delle modalità di gestione, del meccanismo o dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti*

*2.2.2. Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per ridurli*

*2.2.3. Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto "costi del controllo ÷ valore dei fondi gestiti") e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura)*

### 2.3. Misure di prevenzione delle frodi e delle irregolarità

**3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA**

**3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate**

**3.2. Incidenza finanziaria prevista della proposta sugli stanziamenti**

*3.2.1. Sintesi dell'incidenza prevista sugli stanziamenti operativi*

*3.2.2. Risultati previsti finanziati con gli stanziamenti operativi*

*3.2.3. Sintesi dell'incidenza prevista sugli stanziamenti amministrativi*

*3.2.3.1. Fabbisogno previsto di risorse umane*

*3.2.4. Compatibilità con il quadro finanziario pluriennale attuale*

*3.2.5. Partecipazione di terzi al finanziamento*

**3.3. Incidenza prevista sulle entrate**

## 1. CONTESTO DELLA PROPOSTA/INIZIATIVA

### 1.1. Titolo della proposta/iniziativa

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

### 1.2. Settore/settori interessati

Un'Europa pronta per l'era digitale

Investimenti strategici europei

Attività: plasmare il futuro digitale dell'Europa.

### 1.3. La proposta/iniziativa riguarda:

☒ **una nuova azione**

☐ **una nuova azione a seguito di un progetto pilota/un'azione preparatoria**[33]

☐ **la proroga di un'azione esistente**

☐ **la fusione o il riorientamento di una o più azioni verso un'altra/una nuova azione**

### 1.4. Obiettivi

*1.4.1. Obiettivi generali*

Il regolamento sulla cibersolidarietà rafforzerà la solidarietà a livello di Unione per migliorare il rilevamento delle minacce e degli incidenti di cibersicurezza, nonché la preparazione e la risposta agli stessi. Persegue gli obiettivi seguenti:

a) migliorare il rilevamento e la conoscenza situazionale comuni dell'UE in materia di minacce e incidenti informatici;

b) rafforzare la preparazione dei soggetti critici in tutta l'UE 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 per la risposta agli incidenti;

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.

*1.4.2. Obiettivi specifici*

Il regolamento sulla cibersolidarietà conseguirà i suoi obiettivi mediante:

[33] A norma dell'articolo 58, paragrafo 2, lettera a) o b), del regolamento finanziario.

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;

b) la creazione di un meccanismo per le emergenze di cibersicurezza al fine di sostenere gli Stati membri nella preparazione e nella risposta agli incidenti di cibersicurezza significativi e su vasta scala e nella ripresa immediata dagli stessi. Il sostegno per la risposta agli incidenti sarà reso disponibile anche alle istituzioni, agli organi e agli organismi dell'Unione.

Tali azioni saranno sostenute dai finanziamenti del programma Europa digitale, che il presente strumento legislativo modificherà al fine di predisporre le suddette azioni, fornire un sostegno finanziario per il loro sviluppo e chiarire le condizioni per beneficiarne;

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

*1.4.3. Risultati e incidenza previsti*

*Precisare gli effetti che la proposta/iniziativa dovrebbe avere sui beneficiari/gruppi interessati.*

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

Tali azioni rafforzeranno la posizione competitiva del settore industriale e imprenditoriale in Europa nell'ambito dell'economia digitalizzata e ne sosterranno la trasformazione digitale, consolidando il livello di cibersicurezza nel mercato unico digitale. L'obiettivo è, in particolare, di accrescere la resilienza dei cittadini, delle imprese e dei soggetti che operano in settori critici o altamente critici alle crescenti minacce alla cibersicurezza, che possono avere conseguenze sociali ed economiche devastanti. A tal fine si investirà in strumenti in grado di velocizzare il rilevamento delle minacce e degli incidenti di cibersicurezza e di assicurare una risposta più rapida; inoltre gli Stati membri saranno assistiti per garantire una migliore preparazione e capacità di risposta più adeguate agli incidenti di cibersicurezza significativi e su vasta scala. Ciò dovrebbe inoltre contribuire a dotare l'Europa di maggiori capacità in questi settori, in particolare per quanto riguarda la raccolta e l'analisi di dati sulle minacce e sugli incidenti di cibersicurezza.

*1.4.4. Indicatori di prestazione*

*Precisare gli indicatori con cui monitorare progressi e risultati*

Al fine di promuovere la solidarietà a livello di Unione, si potrebbero prendere in considerazione diversi indicatori, quali:

1) il numero di infrastrutture o strumenti di cibersicurezza, o di entrambi, acquisiti congiuntamente;

2) il numero di azioni a sostegno della preparazione e della risposta agli incidenti di cibersicurezza nell'ambito del meccanismo per le emergenze di cibersicurezza.

## 1.5. Motivazione della proposta/iniziativa

*1.5.1. Necessità nel breve e lungo termine, compreso un calendario dettagliato per fasi di attuazione dell'iniziativa*

È opportuno che il regolamento sia pienamente applicabile appena dopo la sua adozione, vale a dire il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

*1.5.2. Valore aggiunto dell'intervento dell'Unione (che può derivare da diversi fattori, ad es. un miglior coordinamento, la certezza del diritto o un'efficacia e una complementarità maggiori). Ai fini del presente punto, per "valore aggiunto dell'intervento dell'Unione" si intende il valore derivante dall'intervento dell'Unione, che va ad aggiungersi al valore che avrebbero altrimenti generato gli Stati membri se avessero agito da soli.*

La forte natura transfrontaliera delle minacce alla cibersicurezza in generale e il numero crescente di rischi e incidenti, che hanno effetti di ricaduta a livello transfrontaliero e trasversalmente ai settori e ai prodotti, fanno sì che gli obiettivi del presente intervento non possano essere raggiunti efficacemente dai soli Stati membri e richiedano un'azione comune e la solidarietà a livello di Unione. L'esperienza di contrasto alle minacce informatiche derivanti dalla guerra contro l'Ucraina, unitamente agli insegnamenti tratti da un'esercitazione di cibersicurezza condotta nell'ambito della presidenza francese (EU CyCLES), ha dimostrato che è opportuno sviluppare meccanismi concreti di sostegno reciproco, in particolare la cooperazione con il settore privato, per realizzare la solidarietà a livello di UE. In questo contesto le conclusioni del Consiglio del 23 maggio 2022 sullo sviluppo della posizione dell'Unione europea in materia di deterrenza informatica invitano la Commissione a presentare una proposta su un nuovo Fondo di risposta alle emergenze di cibersicurezza. Il sostegno e le azioni a livello di Unione per migliorare il rilevamento delle minacce alla cibersicurezza nonché per accrescere la preparazione e le capacità di risposta apportano un valore aggiunto in quanto evitano la duplicazione degli sforzi nell'Unione e negli Stati membri. Ciò permetterebbe di sfruttare le risorse esistenti in modo più efficace e di intensificare il coordinamento e lo scambio di informazioni sugli insegnamenti tratti.

*1.5.3. Insegnamenti tratti da esperienze analoghe*

Per quanto riguarda la conoscenza situazionale e il rilevamento nell'ambito del ciberscudo europeo, nel contesto del programma di lavoro 2021-2022 sulla cibersicurezza del programma Europa digitale sono stati pubblicati un invito a manifestare interesse per l'appalto congiunto di strumenti e infrastrutture per l'istituzione di SOC transfrontalieri e un invito a presentare proposte per sovvenzioni al fine di consentire lo sviluppo delle capacità dei SOC al servizio di organizzazioni pubbliche e private.

Per quanto concerne la preparazione e la risposta agli incidenti, la Commissione ha istituito un programma a breve termine per sostenere gli Stati membri, mediante un finanziamento aggiuntivo assegnato all'ENISA, al fine di rafforzare immediatamente la preparazione e le capacità di risposta agli incidenti informatici gravi. Tra i servizi forniti figurano azioni di preparazione, quali test di penetrazione dei soggetti critici al fine di individuare le vulnerabilità. Il programma rafforza inoltre le possibilità di assistere gli Stati membri in caso di incidenti gravi che colpiscano soggetti critici. L'attuazione da parte dell'ENISA di questo programma a breve termine è in corso e

ha già fornito valide indicazioni pertinenti di cui si è tenuto conto nell'elaborazione del presente regolamento.

*1.5.4. Compatibilità con il quadro finanziario pluriennale ed eventuali sinergie con altri strumenti pertinenti*

Il regolamento sulla cibersolidarietà si baserà sulle azioni attualmente sostenute dall'Unione e dagli Stati membri per migliorare la conoscenza situazionale e il rilevamento delle minacce informatiche e per rispondere agli incidenti di cibersicurezza su vasta scala e transfrontalieri. Lo strumento è inoltre coerente con altri quadri di gestione delle crisi, tra cui l'IPCR, la politica di sicurezza e di difesa comune, compresi i gruppi di risposta rapida agli incidenti informatici, e l'assistenza fornita da uno Stato membro ad un altro Stato membro nel contesto dell'articolo 42, paragrafo 7, del trattato sull'Unione europea. La nuova proposta integrerebbe e sosterrebbe anche le strutture sviluppate nell'ambito di altri strumenti in materia di cibersicurezza, come la direttiva (UE) 2022/2555 (direttiva NIS2) o il regolamento (UE) 2019/881 (regolamento sulla cibersicurezza).

*1.5.5. Valutazione delle varie opzioni di finanziamento disponibili, comprese le possibilità di riassegnazione*

La gestione dei settori d'intervento assegnati all'ENISA rientra nel suo mandato e nei suoi compiti generali. Tali settori d'intervento potrebbero richiedere profili specifici o nuovi incarichi, che tuttavia potrebbero essere assorbiti dalle risorse esistenti dell'ENISA e coperti mediante la riallocazione o il collegamento di vari incarichi. Attualmente l'ENISA sta attuando un programma a breve termine istituito dalla Commissione nel 2022 per rafforzare immediatamente la preparazione e le capacità di risposta agli incidenti informatici gravi. I servizi forniti includono possibilità per assistere gli Stati membri in caso di incidenti gravi che colpiscano soggetti critici. L'attuazione da parte dell'ENISA di tale programma a breve termine è in corso e ha già fornito valide indicazioni pertinenti di cui si è tenuto conto nell'elaborazione del presente regolamento. Le risorse assegnate al programma a breve termine potrebbero essere utilizzate anche nel contesto del presente regolamento.

## 1.6. Durata e incidenza finanziaria della proposta/iniziativa

☒ **durata limitata**

– ☒ in vigore dalla data di adozione della proposta di regolamento del Parlamento europeo e del Consiglio sul rafforzamento della solidarietà e delle capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi ("regolamento sulla cibersolidarietà")

– ☒ incidenza finanziaria dal 2023 al 2027 per gli stanziamenti di impegno e dal 2023 al 2031 per gli stanziamenti di pagamento[34]

☐ **durata illimitata**

– Attuazione con un periodo di avviamento dal AAAA al AAAA

– e successivo funzionamento a pieno ritmo.

## 1.7. Metodi di esecuzione del bilancio previsti[35]

☒ **Gestione diretta** a opera della Commissione

– ☒ a opera dei suoi servizi, compreso il suo personale presso le delegazioni dell'Unione

– ☐ a opera delle agenzie esecutive

☐ **Gestione concorrente** con gli Stati membri

☒ **Gestione indiretta** affidando compiti di esecuzione del bilancio:

– ☐ a paesi terzi o organismi da questi designati;

– ☐ a organizzazioni internazionali e loro agenzie (specificare);

– ☐ alla BEI e al Fondo europeo per gli investimenti;

– ☒ agli organismi di cui agli articoli 70 e 71 del regolamento finanziario;

– ☐ a organismi di diritto pubblico;

– ☐ a organismi di diritto privato investiti di attribuzioni di servizio pubblico nella misura in cui sono dotati di sufficienti garanzie finanziarie;

– ☐ a organismi di diritto privato di uno Stato membro preposti all'attuazione di un partenariato pubblico-privato e che sono dotati di sufficienti garanzie finanziarie;

– ☐ agli organismi o alle persone incaricati di attuare azioni specifiche della PESC a norma del titolo V del TUE e indicati nel pertinente atto di base.

– *Se è indicata più di una modalità, fornire ulteriori informazioni alla voce "Osservazioni".*

Osservazioni

| |
|---|
| Le azioni relative al ciberscudo europeo saranno attuate dall'ECCC. Fino a quando l'ECCC non avrà la capacità di eseguire il proprio bilancio, la Commissione europea attuerà le azioni in regime di gestione diretta per conto del Centro. L'ECCC può selezionare soggetti sulla base |

[34] Le azioni previste dal regolamento dovrebbero essere sostenute dal prossimo quadro finanziario pluriennale.

[35] Le spiegazioni dei metodi di esecuzione del bilancio e i riferimenti al regolamento finanziario sono disponibili sul sito BUDGpedia: https://myintracomm.ec.europa.eu/corp/budget/financial-rules/budget-implementation/Pages/implementation-methods.aspx

di inviti a manifestare interesse per partecipare all'appalto congiunto di strumenti e può attribuire sovvenzioni per il funzionamento di tali strumenti.

Inoltre l'ECCC può attribuire sovvenzioni per azioni di preparazione nell'ambito del meccanismo per le emergenze di cibersicurezza.

La Commissione ha la responsabilità generale dell'attuazione della riserva dell'UE per la cibersicurezza e può affidare all'ENISA, in tutto o in parte, mediante accordi di contributo, il funzionamento e l'amministrazione della stessa. Le azioni assegnate all'ENISA dal presente regolamento sono in linea con il suo attuale mandato. In particolare si tratta di: i) sostenere il gruppo di cooperazione NIS nella predisposizione delle azioni di preparazione in base alle valutazioni del rischio; ii) sostenere la Commissione nell'istituzione della riserva dell'UE per la cibersicurezza e nella supervisione della sua attuazione, compresi il ricevimento e il trattamento delle richieste di sostegno; iii) elaborare modelli per agevolare la presentazione di richieste di sostegno e accordi specifici da stipulare tra il fornitore di servizi e l'utente a cui viene fornito il sostegno nell'ambito della riserva dell'UE per la cibersicurezza; iv) riesaminare e valutare le minacce, le vulnerabilità e le azioni di attenuazione in relazione a specifici incidenti di cibersicurezza significativi o su vasta scala e preparare le relazioni corrispondenti.

Tali incarichi assorbiranno le risorse esistenti dell'ENISA per un totale stimato di circa 7 ETP, sulla base dell'esperienza già acquisita e del lavoro preliminare svolto attualmente dall'ENISA nell'ambito del progetto pilota relativo a un sostegno di emergenza per la preparazione e la risposta agli incidenti.

## 2. MISURE DI GESTIONE

### 2.1. Disposizioni in materia di monitoraggio e di relazioni

*Precisare frequenza e condizioni.*

La Commissione monitorerà l'attuazione, l'applicazione e il rispetto di queste nuove disposizioni al fine di valutarne l'efficacia. La Commissione presenterà al Parlamento europeo e al Consiglio una relazione sulla valutazione e sul riesame del presente regolamento entro quattro anni dalla data della sua applicazione.

### 2.2. Sistema di gestione e di controllo

*2.2.1. Giustificazione della o delle modalità di gestione, del meccanismo o dei meccanismi di attuazione del finanziamento, delle modalità di pagamento e della strategia di controllo proposti*

Il regolamento introduce un quadro per l'attuazione dei finanziamenti dell'UE al fine di incrementare la resilienza in materia di cibersicurezza mediante azioni volte a migliorare le capacità di rilevamento, risposta e ripresa in caso di incidenti di cibersicurezza significativi e su vasta scala. Le unità della DG CNECT incaricate del settore d'intervento gestiranno l'attuazione della direttiva.

Al fine di far fronte ai nuovi compiti, occorre fornire risorse adeguate ai servizi della Commissione. Si stima che l'applicazione del nuovo regolamento richieda 6 ETP (3 AD e 3 AC) che si occupino dei compiti seguenti:

- determinare le azioni di preparazione in base alle valutazioni del rischio;
- garantire l'interoperabilità tra le piattaforme SOC transfrontaliere;
- elaborare eventuali atti di esecuzione (due per i SOC e due per il meccanismo per le emergenze di cibersicurezza);
- gestire le convezioni di accoglienza e di utilizzo per i SOC;
- istituire e gestire la riserva dell'UE per la cibersicurezza, direttamente o tramite un accordo di contributo con l'ENISA. In caso di accordo, elaborare e supervisionare l'attuazione di tale accordo per i compiti assegnati all'ENISA;
- partecipare ai gruppi di consultazione convocati dall'ENISA per riesaminare e valutare gli incidenti di cibersicurezza significativi e su vasta scala e preparare le relazioni.

*2.2.2. Informazioni concernenti i rischi individuati e il sistema o i sistemi di controllo interno per ridurli*

Un rischio individuato in relazione al ciberscudo europeo è che gli Stati membri non condividano una quantità sufficiente di informazioni pertinenti sulle minacce informatiche all'interno delle piattaforme SOC transfrontaliere o tra le piattaforme transfrontaliere e altri soggetti pertinenti a livello di UE. Al fine di attenuare tali rischi, l'assegnazione dei finanziamenti seguirà un invito a manifestare interesse in cui gli Stati membri si impegnano a condividere una determinata quantità di informazioni a livello di UE. Tale impegno sarà poi formalizzato in una convezione di accoglienza e di utilizzo che conferirà all'ECCC la facoltà di condurre audit per garantire che le infrastrutture e gli strumenti acquisiti congiuntamente siano utilizzati in conformità di tale convenzione. Gli impegni per la condivisione di un numero

elevato di informazioni all'interno dei SOC transfrontalieri saranno formalizzati in un accordo di consorzio.

Un rischio individuato in relazione al meccanismo per le emergenze di cibersicurezza è che gli utenti che partecipano al meccanismo non adottino misure sufficienti a garantire la preparazione necessaria in caso di attacchi informatici. Per questo motivo, per poter ricevere il sostegno della riserva dell'UE per la cibersicurezza, gli utenti sono tenuti ad adottare tali misure di preparazione. Al momento di presentare le richieste di sostegno a titolo della riserva dell'UE per la cibersicurezza, gli utenti devono spiegare quali misure sono già state adottate per rispondere all'incidente e questo elemento sarà preso in considerazione durante la valutazione delle suddette richieste.

*2.2.3. Stima e giustificazione del rapporto costo/efficacia dei controlli (rapporto "costi del controllo ÷ valore dei fondi gestiti") e valutazione dei livelli di rischio di errore previsti (al pagamento e alla chiusura)*

Poiché le regole di partecipazione al programma Europea digitale applicabili al sostegno nell'ambito del regolamento sulla cibersolidarietà sono simili a quelle che la Commissione utilizzerà nei suoi programmi di lavoro e stante una popolazione di beneficiari che presenta un profilo di rischio simile a quello dei programmi in regime di gestione diretta, si prevede che il livello di errore sia simile a quello stabilito dalla Commissione per il programma Europa digitale, vale a dire un livello tale da offrire ragionevoli garanzie che il rischio di errore nel corso del periodo pluriennale di spesa si assesti, su base annua, tra il 2 % e il 5 %, allo scopo ultimo di arrivare a un livello di errore residuo il più possibile vicino al 2 % al termine dei programmi pluriennali, dopo aver tenuto conto dell'impatto finanziario di tutti gli audit e delle misure correttive e di recupero.

## 2.3. Misure di prevenzione delle frodi e delle irregolarità

*Precisare le misure di prevenzione e tutela in vigore o previste, ad esempio strategia antifrode.*

Nel caso del ciberscudo europeo, l'ECCC avrà il potere di verifica, esercitabile mediante l'accesso alle informazioni e ispezioni in loco, delle infrastrutture e degli strumenti acquisiti congiuntamente, in conformità della convezione di accoglienza e di utilizzo che sarà firmata tra il consorzio ospitante e il Centro.

Le vigenti misure di prevenzione delle frodi applicabili alle istituzioni, agli organi e agli organismi dell'Unione si applicheranno agli stanziamenti supplementari necessari per il presente regolamento.

## 3. INCIDENZA FINANZIARIA PREVISTA DELLA PROPOSTA/INIZIATIVA

### 3.1. Rubrica/rubriche del quadro finanziario pluriennale e linea/linee di bilancio di spesa interessate

- Linee di bilancio esistenti

*Secondo l'ordine delle rubriche del quadro finanziario pluriennale e delle linee di bilancio*

| Rubrica del quadro finanziario pluriennale | Linea di bilancio | Natura della spesa | Partecipazione | | | |
|---|---|---|---|---|---|---|
| | Numero | Diss./Non diss[36]. | di paesi EFTA[37] | di paesi candidati e potenziali candidati[38] | di altri paesi terzi | altre entrate con destinazione specifica |
| 1 | 02 04 01 10 - Programma Europa digitale - Cibersicurezza | Diss. | SÌ | SÌ | NO | NO |
| 1 | 02 04 01 11 - Programma Europa digitale - Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca | Diss. | SÌ | SÌ | NO | NO |
| 1 | 02 04 03 - Programma Europa digitale - Intelligenza artificiale | Diss. | SÌ | SÌ | NO | NO |
| 1 | 02 04 04 - Programma Europa digitale - Competenze | Diss. | SÌ | SÌ | NO | NO |
| 1 | 02 01 30 - Spese di supporto per il programma Europa digitale | Non diss. | SÌ | SÌ | NO | NO |

[36] Diss. = stanziamenti dissociati / Non diss. = stanziamenti non dissociati.
[37] EFTA: Associazione europea di libero scambio.
[38] Paesi candidati e, se del caso, potenziali candidati.

### 3.2. Incidenza finanziaria prevista della proposta sugli stanziamenti

*3.2.1. Sintesi dell'incidenza prevista sugli stanziamenti operativi*

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti operativi.

– ☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti operativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

| **Rubrica del quadro finanziario pluriennale** | Numero | 1 **Mercato unico, innovazione e agenda digitale** |
|---|---|---|

La proposta non accrescerà il livello totale degli impegni nell'ambito del programma Europa digitale. Il contributo per questa iniziativa consiste infatti in una ridistribuzione degli impegni dagli obiettivi specifici 2 e 4 a rafforzare il bilancio dell'obiettivo specifico 3 e dell'ECCC. Un eventuale aumento degli impegni nell'ambito del programma Europa digitale, derivante da una revisione del QFP, potrebbe essere utilizzato per la presente iniziativa.

| DG CONNECT | | | Anno **2025** | Anno **2026** | Anno **2027** | Anno **2028+** | Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6) | | | **TOTALE** |
|---|---|---|---|---|---|---|---|---|---|---|
| ○ Stanziamenti operativi | | | | | | | | | | |
| Linea di bilancio[39] 02.040110 (ridistribuzione da 02.0403 e 02.0404) | Impegni | (1a) | 15,000 | 15,000 | 6,000 | p.m. | | | | **36,000** |
| | Pagamenti | (2a) | 15,000 | 15,000 | 6,000 | | | | | **36,000** |
| Linea di bilancio 02.040111.02 (ridistribuzione da 02.0403 e 02.0404) | Impegni | (1b) | 13,000 | 23,000 | 28,000 | p.m. | | | | **64,000** |
| | Pagamenti | (2b) | 8,450 | 18,200 | 25,250 | 12,100 | | | | **64,000** |
| Stanziamenti amministrativi finanziati dalla dotazione di programmi specifici[40] | | | | | | | | | | |
| Linea di bilancio 02.0130 | | (3) | 0,150 | 0,150 | 0,150 | p.m. | | | | 0,450 |

[39] Secondo la nomenclatura di bilancio ufficiale.

[40] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **TOTALE stanziamenti per la DG CONNECT** | Impegni | =1a+1b +3 | **28,150** | **38,150** | **34,150** | **p.m.** | | | | **100,450** |
| | Pagamenti | =2a+2b +3 | **23,600** | **33,350** | **31,400** | **12,100** | | | | **100,450** |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ○TOTALE stanziamenti operativi | Impegni | (4) | 28,000 | 38,000 | 34,000 | p.m. | | | | **100,000** |
| | Pagamenti | (5) | 23,450 | 33,200 | 31,250 | 12,100 | | | | **100,000** |
| ○TOTALE stanziamenti amministrativi finanziati dalla dotazione di programmi specifici | | (6) | 0,150 | 0,150 | 0,150 | p.m. | | | | **0,450** |
| **TOTALE stanziamenti per la RUBRICA 1** del quadro finanziario pluriennale | Impegni | =4+ 6 | **28,150** | **38,150** | **34,150** | **p.m.** | | | | **100,450** |
| | Pagamenti | =5+ 6 | **23,600** | **33,350** | **31,400** | **12,100** | | | | **100,450** |

**Se la proposta/iniziativa incide su più rubriche operative, ricopiare nella sezione sotto:**

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ○ TOTALE stanziamenti operativi (tutte le rubriche operative) | Impegni | (4) | 28,000 | 38,000 | 34,000 | p.m. | | | | **100,000** |
| | Pagamenti | (5) | 23,450 | 33,200 | 31,250 | 12,100 | | | | **100,000** |
| TOTALE stanziamenti amministrativi finanziati dalla dotazione di programmi specifici (tutte le rubriche operative) | | (6) | 0,150 | 0,150 | 0,150 | | | | | **0,450** |
| **TOTALE stanziamenti per le RUBRICHE da 1 a 6** del quadro finanziario pluriennale (importo di riferimento) | Impegni | =4+ 6 | **28,150** | **38,150** | **34,150** | **p.m.** | | | | **100,450** |
| | Pagamenti | =5+ 6 | **23,600** | **33,350** | **31,400** | **12,100** | | | | **100,450** |

| | | |
|---|---|---|
| **Rubrica del quadro finanziario pluriennale** | **7** | "Spese amministrative" |

Sezione da compilare usando i "dati di bilancio di natura amministrativa", da introdursi *in primis* nell'allegato della scheda finanziaria legislativa (allegato 5 della decisione della Commissione sulle norme interne per l'esecuzione della sezione "Commissione europea" del bilancio generale dell'Unione europea), caricato su DECIDE a fini di consultazione interservizi.

Mio EUR (al terzo decimale)

| | | Anno **2025** | Anno **2026** | Anno **2027** | Anno **2028+** | Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6) | | | **TOTALE** |
|---|---|---|---|---|---|---|---|---|---|
| DG: CONNECT | | | | | | | | | |
| ○ Risorse umane | | 0,786 | 0,786 | 0,786 | p.m. | | | | **2,358** |
| ○ Altre spese amministrative | | 0,035 | 0,035 | 0,035 | p.m. | | | | **0,105** |
| **TOTALE DG CONNECT** | Stanziamenti | **0,821** | **0,821** | **0,821** | | | | | **2,463** |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **TOTALE stanziamenti per la RUBRICA 7** del quadro finanziario pluriennale | (Totale impegni = Totale pagamenti) | **0,821** | **0,821** | **0,821** | | | | | **2,463** |

Mio EUR (al terzo decimale)

| | | Anno **2025** | Anno **2026** | Anno **2027** | Anno **2028+** | Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6) | | | **TOTALE** |
|---|---|---|---|---|---|---|---|---|---|
| **TOTALE stanziamenti per le RUBRICHE da 1 a 7** del quadro finanziario pluriennale | Impegni | **28,971** | **38,971** | **34,971** | **p.m.** | | | | **102,913** |
| | Pagamenti | **24,421** | **34,171** | **32,221** | **12,100** | | | | **102,913** |

*3.2.2. Risultati previsti finanziati con gli stanziamenti operativi*

Stanziamenti di impegno in Mio EUR (al terzo decimale)

| **Specificare gli obiettivi e i risultati** | | | Anno **N** | | Anno **N+1** | | Anno **N+2** | | Anno **N+3** | | Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6) | | | | | | **TOTALE** | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **RISULTATI** | | | | | | | | | | | | | | | | | |
| ⇩ | Tipo[41] | Costo medio | N. | Costo | N. | Costo | N. | Costo | N. | Costo | N. | Costo | N. | Costo | N. | Costo | N. totale | Costo totale |
| OBIETTIVO SPECIFICO 1[42]… | | | | | | | | | | | | | | | | | | |
| - Risultato | | | | | | | | | | | | | | | | | | |
| - Risultato | | | | | | | | | | | | | | | | | | |
| - Risultato | | | | | | | | | | | | | | | | | | |
| Totale parziale obiettivo specifico 1 | | | | | | | | | | | | | | | | | | |
| OBIETTIVO SPECIFICO 2 … | | | | | | | | | | | | | | | | | | |
| - Risultato | | | | | | | | | | | | | | | | | | |
| Totale parziale obiettivo specifico 2 | | | | | | | | | | | | | | | | | | |
| **TOTALE** | | | | | | | | | | | | | | | | | | |

41 I risultati sono i prodotti e i servizi da fornire (ad es. numero di scambi di studenti finanziati, numero di km di strada costruiti ecc.).

42 Come descritto nella sezione 1.4.2. "Obiettivi specifici..."

*3.2.3. Sintesi dell'incidenza prevista sugli stanziamenti amministrativi*

– ☐ La proposta/iniziativa non comporta l'utilizzo di stanziamenti amministrativi.

– ☒ La proposta/iniziativa comporta l'utilizzo di stanziamenti amministrativi, come spiegato di seguito:

Mio EUR (al terzo decimale)

| | Anno 2025 | Anno 2026 | Anno 2027 | Anno N+3 | Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6) | | | **TOTALE** |
|---|---|---|---|---|---|---|---|---|
| **RUBRICA 7 del quadro finanziario pluriennale** | | | | | | | | |
| Risorse umane | 0,786 | 0,786 | 0,786 | | | | | **2,358** |
| Altre spese amministrative | 0,035 | 0,035 | 0,035 | | | | | **0,105** |
| **Totale parziale RUBRICA 7 del quadro finanziario pluriennale** | **0,821** | **0,821** | **0,821** | | | | | **2,463** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Esclusa la RUBRICA 7[43] del quadro finanziario pluriennale** | | | | | | | | |
| Risorse umane | | | | | | | | |
| Altre spese amministrative | 0,150 | 0,150 | 0,150 | | | | | **0,450** |
| **Totale parziale esclusa la RUBRICA 7 del quadro finanziario pluriennale** | **0,150** | **0,150** | **0,150** | | | | | **0,450** |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **TOTALE** | **0,971** | **0,971** | **0,971** | | | | | **2,913** |

Il fabbisogno di stanziamenti relativi alle risorse umane e alle altre spese amministrative è coperto dagli stanziamenti della DG già assegnati alla gestione dell'azione e/o riassegnati all'interno della stessa DG, integrati dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

[43] Assistenza tecnica e/o amministrativa e spese di sostegno all'attuazione di programmi e/o azioni dell'UE (ex linee "BA"), ricerca indiretta, ricerca diretta.

3.2.3.1. Fabbisogno previsto di risorse umane

– ☐ La proposta/iniziativa non comporta l'utilizzo di risorse umane.

– ☒ La proposta/iniziativa comporta l'utilizzo di risorse umane, come spiegato di seguito:

*Stima da esprimere in equivalenti a tempo pieno*

| | | Anno **2025** | Anno **2026** | Anno 2027 | Anno **N+3** | Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6) | | |
|---|---|---|---|---|---|---|---|---|
| **Posti della tabella dell'organico (funzionari e agenti temporanei)** | | | | | | | | |
| 20 01 02 01 (sede e uffici di rappresentanza della Commissione) | | 3 | 3 | 3 | | | | |
| 20 01 02 03 (delegazioni) | | | | | | | | |
| 01 01 01 01 (ricerca indiretta) | | | | | | | | |
| 01 01 01 11 (ricerca diretta) | | | | | | | | |
| Altre linee di bilancio (specificare) | | | | | | | | |
| **Personale esterno (in equivalenti a tempo pieno: ETP)**[44] | | | | | | | | |
| 20 02 01 (AC, END, INT della dotazione globale) | | 3 | 3 | 3 | | | | |
| 20 02 03 (AC, AL, END, INT e JPD nelle delegazioni) | | | | | | | | |
| **XX** 01 xx **yy zz** [45] | - in sede | | | | | | | |
| | - nelle delegazioni | | | | | | | |
| 01 01 01 02 (AC, END, INT - ricerca indiretta) | | | | | | | | |
| 01 01 01 12 (AC, END, INT - ricerca diretta) | | | | | | | | |
| Altre linee di bilancio (specificare) | | | | | | | | |
| **TOTALE** | | **6** | **6** | **6** | | | | |

**XX** è il settore o il titolo di bilancio interessato.

Il fabbisogno di risorse umane è coperto dal personale della DG già assegnato alla gestione dell'azione e/o riassegnato all'interno della stessa DG, integrato dall'eventuale dotazione supplementare concessa alla DG responsabile nell'ambito della procedura annuale di assegnazione, tenendo conto dei vincoli di bilancio.

Descrizione dei compiti da svolgere:

| | |
|---|---|
| Funzionari e agenti temporanei | - determinare le azioni di preparazione in base alle valutazioni del rischio (art. 11)<br>- elaborare eventuali atti di esecuzione (due per i SOC e due per il meccanismo per le emergenze di cibersicurezza)<br>- gestire le convezioni di accoglienza e di utilizzo per i SOC;<br>- istituire e gestire la riserva dell'UE per la cibersicurezza, direttamente o tramite un accordo di contributo con l'ENISA. |
| Personale esterno | Sotto la supervisione di un funzionario,<br>- determinare le azioni di preparazione in base alle valutazioni del rischio (art. 11)<br>- elaborare eventuali atti di esecuzione (due per i SOC e due per il meccanismo per le emergenze di cibersicurezza)<br>- gestire le convezioni di accoglienza e di utilizzo per i SOC;<br>- istituire e gestire la riserva dell'UE per la cibersicurezza, direttamente o |

44 AC = agente contrattuale; AL = agente locale; END = esperto nazionale distaccato; INT = personale interinale (intérimaire); JPD = giovane professionista in delegazione.

45 Sottomassimale per il personale esterno previsto dagli stanziamenti operativi (ex linee "BA").

| | |
|---|---|
| | tramite un accordo di contributo con l'ENISA. |

### 3.2.4. *Compatibilità con il quadro finanziario pluriennale attuale*

La proposta/iniziativa:

– [X] può essere interamente finanziata mediante riassegnazione all'interno della pertinente rubrica del quadro finanziario pluriennale (QFP).

| Spiegare la riprogrammazione richiesta, precisando le linee di bilancio interessate e gli importi corrispondenti. Allegare una tabella Excel in caso di riprogrammazione maggiore. |
|---|

| | 23 | 24 | 25 | 26 | 27 | totale |
|---|---|---|---|---|---|---|
| OS1 | 16 232 897 | 20 528 765 | 17 406 899 | 16 223 464 | 10 022 366 | 80 414 391 |
| | | | | | | |
| OS2 iniziale | 226 316 819 | 295 067 000 | 195 649 000 | 221 809 000 | 246 608 000 | 1 185 449 819 |
| All'iniziativa per la cibersolidarietà | | | 18 000 000 | 28 000 000 | 19 000 000 | 65 000 000 |
| **NUOVO OS2** | **226 316 819** | **295 067 000** | **177 649 000** | **193 809 000** | **227 608 000** | **1 120 449 819** |
| | | | | | | |
| OS3 PB 24 | 24 361 553 | 35 596 172 | 3 638 000 | 3 638 000 | 11 175 000 | 78 408 725 |
| Da OS2-OS4 | | | 15 000 000 | 15 000 000 | 6 000 000 | 36 000 000 |
| **Nuovo OS3** | **24 361 553** | **35 596 172** | **18 638 000** | **18 638 000** | **17 175 000** | **114 408 725** |
| | | | | | | |
| ECCC iniziale | 176 222 303 | 208 374 879 | 104 228 130 | 90 704 986 | 84 851 497 | 664 381 795 |
| Da OS2-OS4 | | | 13 000 000 | 23 000 000 | 28 000 000 | 64 000 000 |
| **Nuovo ECCC** | **176 222 303** | **208 374 879** | **117 228 130** | **113 704 986** | **112 851 497** | **728 381 795** |
| | | | | | | |
| OS4 iniziale | 66 902 708 | 64 892 032 | 56 577 977 | 70 477 245 | 72 107 201 | 330 957 163 |
| All'iniziativa per la cibersolidarietà | | | 10 000 000 | 10 000 000 | 15 000 000 | 35 000 000 |
| **NUOVO OS4** | **66 902 708** | **64 892 032** | **46 577 977** | **60 477 245** | **57 107 201** | **295 957 163** |

– [ ] comporta l'uso del margine non assegnato della pertinente rubrica del QFP e/o l'uso degli strumenti speciali definiti nel regolamento QFP.

| Spiegare la necessità, precisando le rubriche e le linee di bilancio interessate, gli importi corrispondenti e gli strumenti proposti. |
|---|

– [ ] comporta una revisione del QFP.

| Spiegare la necessità, precisando le rubriche e le linee di bilancio interessate e gli importi corrispondenti. |
|---|

### 3.2.5. *Partecipazione di terzi al finanziamento*

La proposta/iniziativa:

– [X] non prevede cofinanziamenti da terzi

– [ ] prevede il cofinanziamento da terzi indicato di seguito:

Stanziamenti in Mio EUR (al terzo decimale)

| | Anno **N**[46] | Anno **N+1** | Anno **N+2** | Anno **N+3** | Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6) | Totale |
|---|---|---|---|---|---|---|

[46] L'anno N è l'anno in cui inizia a essere attuata la proposta/iniziativa. Sostituire "N" con il primo anno di attuazione previsto (ad es. 2021) e così per gli anni a seguire.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Specificare l'organismo di cofinanziamento | | | | | | | | |
| TOTALE stanziamenti cofinanziati | | | | | | | | |

### 3.3. Incidenza prevista sulle entrate

– [X] La proposta/iniziativa non ha incidenza finanziaria sulle entrate.

– ☐ La proposta/iniziativa ha la seguente incidenza finanziaria:

  – ☐ sulle risorse proprie

  – ☐ su altre entrate

  – indicare se le entrate sono destinate a linee di spesa specifiche ☐

Mio EUR (al terzo decimale)

| Linea di bilancio delle entrate: | Stanziamenti disponibili per l'esercizio in corso | Incidenza della proposta/iniziativa[47] | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Anno **N** | Anno **N+1** | Anno **N+2** | Anno **N+3** | Inserire gli anni necessari per evidenziare la durata dell'incidenza (cfr. punto 1.6) | | |
| Articolo ……. | | | | | | | | |

Per quanto riguarda le entrate con destinazione specifica, precisare la o le linee di spesa interessate.

[…]

Altre osservazioni (ad es. formula/metodo per calcolare l'incidenza sulle entrate o altre informazioni).

[…]

[47] Per le risorse proprie tradizionali (dazi doganali, contributi zucchero), indicare gli importi netti, cioè gli importi lordi al netto del 20 % per spese di riscossione.