RELAZIONE SPECIALE 19/2026 **IT**

Individuazione degli incidenti di cibersicurezza e risposta agli stessi

Il quadro di cooperazione dell'UE è in evoluzione, ma la sua efficacia è solo parziale a causa di ritardi nell'attuazione e della limitata condivisione delle informazioni

CURIA RATIONUM
CORTE DEI CONTI EUROPEA

Indice

Paragrafo

01 Principali messaggi

Perché questo tema è importante

01 I rischi di attacchi informatici aumentano di pari passo con la progressiva digitalizzazione dell'economia e della nostra vita quotidiana. La cibersicurezza è definita come "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche"[1] e richiede un approccio olistico in grado di prevenire, individuare, rispondere alle minacce informatiche e riprendersi dalle stesse.

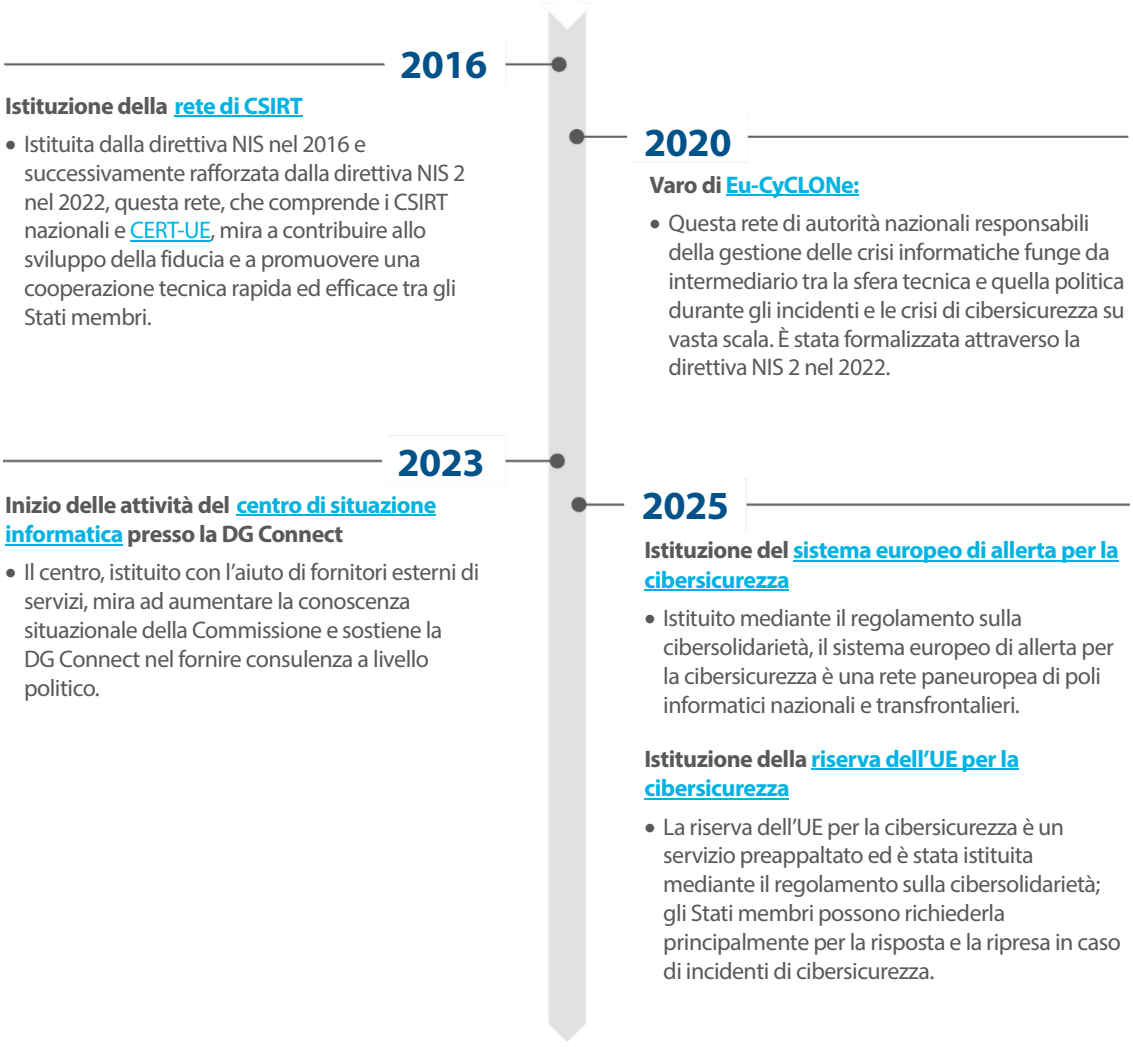
02 L'architettura di cibersicurezza dell'UE coinvolge numerosi soggetti pubblici e privati nella sfera civile, a livello regionale, nazionale e dell'UE. La cibersicurezza è inoltre un elemento essenziale della sicurezza e difesa nazionali.

03 La responsabilità primaria della prevenzione degli incidenti e delle crisi di cibersicurezza, nonché della preparazione e della risposta agli stessi, spetta agli Stati membri. Poiché questi incidenti possono incidere sul corretto funzionamento del mercato interno, anche l'UE svolge un ruolo importante in caso di incidenti o crisi significative. Negli ultimi anni, l'UE ha rafforzato il proprio quadro normativo in evoluzione in materia di cibersicurezza[2] e ha istituito reti e meccanismi, come illustrato nella ***figura 1*** e nell' ***allegato II***.

[1] Regolamento (UE) 2019/881 (regolamento sulla cibersicurezza).

[2] Ad esempio, la Commissione ha proposto il pacchetto omnibus nel settore digitale nel novembre 2025 e una revisione del regolamento dell'UE sulla cibersicurezza nel gennaio 2026.

Figura 1 | Reti e meccanismi di cibersicurezza dell'UE, 2016-2025



CSIRT: gruppo di intervento per la sicurezza informatica in caso di incidenti
DG Connect: direzione-generale delle Reti di comunicazione, dei contenuti e delle tecnologie
EU-CyCLONe: Rete europea delle organizzazioni di collegamento per le crisi informatiche
Direttiva NIS: direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
Direttiva NIS 2: direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione.

Fonte: Corte dei conti europea.

04 Nell'ambito dell'attuale quadro finanziario pluriennale 2021-2027, la principale fonte di finanziamenti per la cibersicurezza è il programma Europa digitale ("Europa digitale"), che dispone di una dotazione finanziaria totale di 8,1 miliardi di euro, di cui 1,4 miliardi destinati al rafforzamento della cibersicurezza.

05 L'obiettivo dell'audit della Corte è stato valutare se le azioni dell'UE siano efficaci nel facilitare l'individuazione di incidenti di cibersicurezza significativi o su vasta scala e la risposta agli stessi. La Corte ha valutato se ciò avvenisse per:

- le reti e i meccanismi a livello dell'UE, ossia il team di risposta agli incidenti di sicurezza informatica (CSIRT), la rete europea delle organizzazioni di collegamento per le crisi informatiche (EU-CyCLONe), il sistema europeo di allerta per la cibersicurezza, il centro di situazione e analisi informatiche e la riserva dell'UE per la cibersicurezza;
- le azioni finanziate nell'ambito di Europa digitale.

06 Con le proprie constatazioni, la Corte intende contribuire a rafforzare la ciberresilienza dell'UE, migliorando l'efficacia e l'efficienza delle reti e dei meccanismi dell'UE, nonché le modalità di selezione e monitoraggio delle azioni finanziate dall'UE.

07 L'audit riguarda il periodo dal 2022 al 2025 e si basa su un'analisi dei documenti pertinenti, su visite di audit in tre stati membri (Irlanda, Grecia e Italia) e su questionari scritti e colloqui con i portatori di interessi pertinenti. L'***allegato I*** riporta ulteriori informazioni sul contesto, nonché dettagli sull'estensione e sull'approccio dell'audit.

Constatazioni e raccomandazioni della Corte

08 In conclusione, la Corte ha appurato che le azioni dell'UE facilitano solo in parte l'individuazione degli incidenti di cibersicurezza significativi e su vasta scala e la risposta agli stessi. Sebbene sia stato gradualmente istituito un quadro di cooperazione, sono ancora in corso i lavori per conseguire la piena istituzione. La limitata condivisione delle informazioni, le carenze nella segnalazione e i notevoli ritardi nell'attuazione impediscono alle reti e ai meccanismi dell'UE di realizzare appieno il loro potenziale. I progetti finanziati da Europa digitale perseguono obiettivi pertinenti, ma diversi si trovano ad affrontare sfide e ritardi operativi e vi sono debolezze nel quadro generale di monitoraggio della performance.

09 L'attuale quadro delle reti e dei meccanismi dell'UE per semplificare l'individuazione degli incidenti di cibersicurezza significativi e la risposta agli stessi è stato costituito in modo graduale. Nel 2025, il Consiglio ha adottato il programma per la cibersicurezza che stabilisce il quadro dell'UE per la gestione delle crisi informatiche. La Corte ha riscontrato che nel programma vengono chiariti in gran parte i ruoli e le responsabilità nell'ambito della gestione delle crisi informatiche nell'UE, ma, ciononostante, le modalità procedurali riguardanti il modo in cui la rete CSIRT (istituita nel 2016) e EU-CyCLONe (formalizzata nel 2023) dovrebbero collaborare non sono ancora state formalizzate (paragrafi ***24***-***30***).

10 Gli auditor della Corte hanno constatato che la condivisione di informazioni attraverso queste reti è limitata: ciò è dovuto principalmente ai ritardi nel recepimento della direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (direttiva NIS 2), alle difficoltà nel determinare se un incidente abbia un impatto transnazionale e alla normativa in materia di sicurezza nazionale che osta alla condivisione delle informazioni. Il valore aggiunto delle reti diminuisce sensibilmente se gli Stati membri non sono disposti a condividere informazioni tempestive e fruibili (paragrafi ***31***-***44***).

Raccomandazione 1

Rafforzare la condivisione di informazioni tra gli Stati membri

Per migliorare l'individuazione degli incidenti di cibersicurezza e la risposta agli stessi, la Commissione, con il supporto dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA),dovrebbe:

a) proporre al gruppo di cooperazione in materia di sicurezza delle reti e dei sistemi informativi di effettuare un'analisi dettagliata delle restrizioni connesse alla sicurezza nazionale che limitano la condivisione delle informazioni e incidono negativamente sulla ciberesilienza dell'UE nonché di identificare soluzioni giuridiche e tecniche per aumentare la condivisione delle informazioni rispettando al contempo i limiti della sicurezza nazionale;

b) fatte salve le decisioni dei colegislatori, garantire, in collaborazione con gli Stati membri, che il punto di accesso unico per la segnalazione degli incidenti proposto dal pacchetto omnibus digitale possa individuare potenziali incidenti transfrontalieri;

c) lavorare a soluzioni che permettano la segnalazione di incidenti in tempo reale a ENISA.

Termine di attuazione: lettere a) e b): 2027; lettera c): 2028

11 Nel 2022 la Commissione ha istituito il settore "Centro di situazione informatica" per migliorare la propria conoscenza situazionale e sostenere l'esercizio delle proprie responsabilità istituzionali nellla gestione delle crisi. Il funzionamento del centro dipende in larga misura da un contratto con fornitori esterni di servizi. La Corte ha riscontrato che il lavoro svolto da tali fornitori replica in parte l'attività già svolta dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA) nell'ambito della conoscenza situazionale e del monitoraggio delle minacce. La Corte ritiene che, nell'istituire il centro di situazione e analisi informatiche, non siano state sfruttate a sufficienza le potenzialità di razionalizzazione, poiché non si è attinto alle informazioni già esistenti presso la Commissione e l'ENISA. Inoltre, l'assenza di un piano completo e dettagliato per il futuro dopo la scadenza del contratto rappresenta un rischio per il funzionamento del centro di situazione informatica dopo il 2026 (paragrafi ***45***-***51***).

Raccomandazione 2

Razionalizzare le capacità di conoscenza situazionale dell'UE nell'ambito della cibersicurezza e ottimizzare la diffusione delle informazioni

Per migliorare l'efficienza, la Commissione dovrebbe, insieme ad ENISA, valutare la fattibilità di un'acquisizione e analisi congiunta delle informazioni per la conoscenza situazionale. Tali informazioni e le relative relazioni sulle minacce informatiche dovrebbero essere messe a disposizione dei dipartimenti e delle agenzie dell'UE competenti.

Termine di attuazione: 2027

12 Il regolamento dell'UE sulla cibersolidarietà del 2024 istituisce la riserva dell'UE per la cibersicurezza, con l'obiettivo di assistere gli Stati membri nella risposta agli incidenti di cibersicurezza gravi e nella ripresa dagli stessi. La riserva è composta da fornitori di servizi selezionati per ciascuno Stato membro, in grado di rispondere agli incidenti 24 ore su 24. Sebbene questo approccio aiuti a rispondere ai requisiti specifici degli Stati membri e a rafforzarne la fiducia, la dotazione finanziaria disponibile è divisa ugualmente tra di loro e non prende in considerazione le esigenze specifiche di ciascuno Stato membro (paragrafi ***52***-***57***).

13 La Corte ritiene che avvalersi di fornitori con cui è già stato sottoscritto un contratto permette una rapida mobilitazione dei servizi di risposta agli incidenti. Nonostante la riserva dell'UE per la cibersicurezza abbia come principale obiettivo il sostegno alle attività di risposta e ripresa, quando non viene utilizzata per la risposta agli incidenti può essere utilizzata per la preparazione: questo approccio flessibile è in grado di evitare che servizi prepagati restino inutilizzati. Il rischio, tuttavia, è che la riserva venga utilizzata principalmente per la preparazione invece che per la risposta, in contrasto con la finalità che dovrebbe perseguire (paragrafi ***58***-***61***).

14 Il sistema europeo di allerta per la cibersicurezza è una rete di poli informatici nazionali e transfrontalieri che mirano a migliorare l'individuazione e l'analisi delle minacce informatiche nonché la risposta alle stesse. La Corte ha riscontrato che, al momento dell'audit, a causa di ritardi significativi nella fornitura di strumenti e di servizi, i due poli (ATHENA ed ENSOC) non erano ancora operativi e il sistema europeo di allerta per la cibersicurezza non era ancora in funzione (paragrafi ***62***-***70***).

15 Uno degli obiettivi principali del sistema europeo di allerta per la cibersicurezza è incoraggiare la condivisione di informazioni significative tra gruppi di Stati membri. Sebbene ciò potrebbe potenzialmente risolvere alcuni problemi relativi alla condivisione delle informazioni, l'integrazione dei poli informatici nella già complessa architettura di cibersicurezza è una sfida davvero ardua. La Corte ha riscontrato che gli accordi di cooperazione, la tassonomia comune e le norme di interoperabilità necessari per il pieno funzionamento del sistema europeo di allerta per la cibersicurezza non erano ancora operanti (paragrafi ***71***-***74***).

Raccomandazione 3

Integrare il sistema europeo di allerta per la cibersicurezza nel panorama della cibersicurezza dell'UE

La Commissione dovrebbe, insieme a ENISA e agli Stati membri, garantire che gli accordi di cooperazione e le norme di interoperabilità siano operanti per facilitare la condivisione di informazioni tra i poli transfrontalieri che fanno parte del sistema europeo di allerta per la cibersicurezza, la rete di CSIRT ed EU-CyCLONe.

Termine di attuazione: 2028

16 Nel 2018 la Commissione ha proposto la creazione di un Centro europeo di competenza per la cibersicurezza ("ECCC") per gestire la componente di cibersicurezza di Europa digitale a partire dal 2021. Il regolamento dell'ECCC ha chiesto la creazione di una comunità delle competenze in materia di cibersicurezza, che includa rappresentanti dell'industria, delle organizzazioni accademiche e di ricerca. Alcuni membri selezionati della comunità delle competenze in materia di cibersicurezza formeranno poi un gruppo consultivo strategico (SAG) (paragrafi ***75***-***76***).

17 La Corte ha rilevato ritardi nel raggiungimento dell'autonomia finanziaria dell'ECCC e nell'istituzione della comunità delle competenze in materia di cibersicurezza e del SAG. Ciò significa che la comunità delle competenze in materia di cibersicurezza e il SAG non hanno potuto apportare il loro contributo alla definizione dei programmi di lavoro di Europa digitale. La Corte ritiene che si sia trattato di un'occasione mancata (paragrafi ***77***-***81***).

18 Tutti i progetti esaminati dalla Corte perseguono obiettivi pertinenti che contribuiscono al conseguimento degli obiettivi di cibersicurezza di Europa digitale. In alcuni casi, tuttavia, la qualità dei risultati raggiunti non è stata soddisfacente, soprattutto a causa di ritardi nell'attuazione (paragrafi ***82***-***87***).

19 Il regolamento Europa digitale prevede che, per ragioni di sicurezza, i finanziamenti per la cibersicurezza siano limitati a soggetti con sede nell'UE e controllati da Stati membri o cittadini dell'UE. Il servizio centrale di convalida dell'Agenzia esecutiva europea per la ricerca effettua la valutazione della proprietà e del controllo per conto dell'ECCC (paragrafi ***88***-***91***).

20 Nel caso del sostegno finanziario a terzi, la valutazione della proprietà e del controllo è di competenza dei beneficiari dei progetti, sulla base del loro approccio e della loro metodologia. La Corte ha riscontrato che l'ECCC non convalida la propria metodologia, né effettua controlli per garantire che i terzi selezionati siano di proprietà dell'UE e siano controllati da quest'ultima. La Corte ritiene che vi sia un rischio significativo che i beneficiari non abbiano la capacità di eseguire correttamente tali controlli. Tale rischio non è stato sufficientemente ridotto e potrebbe comportare l'esposizione di infrastrutture sensibili, dati operativi e tecnologie critiche per la sicurezza (paragrafi ***92***-***96***)

Raccomandazione 4

Garantire una solida valutazione dell'assetto proprietario e del controllo dei soggetti che ricevono finanziamenti dell'UE nell'ambito del programma Europa digitale

Il Centro europeo di competenza per la cibersicurezza dovrebbe:

a) ottenere la ragionevole garanzia che i beneficiari responsabili della fornitura di sostegno finanziario a terzi dispongano della capacità amministrativa e tecnica necessaria per effettuare adeguate valutazioni della proprietà e del controllo, sulla base della metodologia esistente a disposizione dei beneficiari che attuano il sostegno finanziario a terzi;

b) verificare, a campione, se solo i soggetti ammissibili hanno ricevuto finanziamenti dell'UE.

Termine di attuazione: lettera a): 2026; lettera b): 2027

21 I beneficiari che gestiscono progetti finanziati dell'UE devono riferire all'ECCC in merito ai propri progressi, utilizzando traguardi intermedi e realizzazioni. Tali aspetti sono fondamentali per il monitoraggio dei progetti e dovrebbero essere definiti in modo adeguato. La Corte ha riscontrato che quasi nessuno dei progetti inclusi nel campione seguiva le istruzioni su come definire i traguardi intermedi e le realizzazioni e che molti di essi non erano utili per monitorare i progressi (paragrafi ***97***-***99***).

22 La Corte ha constatato che molti degli indicatori di performance utilizzati dai beneficiari non sono pertinenti o misurabili e mancano di un valore-obiettivo o di un valore di base. Inoltre, le informazioni ricavate da questi indicatori sono inadeguate e pertanto non possono fungere da base per valutare la performance dei progetti (paragrafi ***100***-***102***)

23 Per monitorare i risultati di Europa digitale nel suo complesso, tutti i progetti devono fornire relazioni sulla base di indicatori specifici del programma che confluiscono nelle dichiarazioni annuali sulla performance dei programmi della Commissione. L'ECCC è responsabile della raccolta dei dati forniti sugli indicatori e della verifica degli stessi. La Corte ha rilevato diversi problemi nel modo in cui i dati sono stati raccolti e nella loro qualità complessiva e non ha inoltre riscontrato alcun elemento attestante che l'ECCC abbia verificato l'accuratezza di tali dati. Sulla base di controlli a campione, la Corte ritiene che i dati comunicati non riflettano accuratamente i risultati conseguiti (paragrafi ***103***-***106***).

Raccomandazione 5

Rafforzare il quadro di monitoraggio della performance della componente relativa alla cibersicurezza del programma Europa digitale

Per consentire un adeguato monitoraggio dei progressi e della performance, il Centro europeo di competenza per la cibersicurezza dovrebbe:

a) garantire, prima della firma della sovvenzione, che tutti i progetti abbiano definito traguardi intermedi, realizzazioni e indicatori di performance conformi alle istruzioni fornite nel modulo di domanda;

b) progettare e attuare un solido sistema per la raccolta, la tracciabilità, la verifica e l'aggregazione dei dati per gli indicatori di performance della componente relativa alla cibersicurezza del programma Europa digitale, al fine di garantire che gli indicatori riflettano con precisione i risultati conseguiti.

Termine di attuazione: 2027

Le osservazioni della Corte in dettaglio

Nonostante le reti e i meccanismi dell'UE per la cibersicurezza sostengano la cooperazione e la risposta agli incidenti, la condivisione limitata delle informazioni e l'attuazione incompleta ne riducono l'efficacia

Le reti dell'UE consentono la cooperazione tra gli Stati membri, ma la condivisione limitata delle informazioni ne riduce il valore aggiunto

24 L'attuale quadro dell'UE di reti e meccanismi per facilitare l'individuazione degli incidenti di cibersicurezza significativi e la risposta agli stessi è stato istituito gradualmente, a partire dalla direttiva recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione[3] (direttiva NIS), entrata in vigore nell'agosto 2016. L'***allegato II*** illustra l'attuale panorama dell'UE.

[3] Direttiva (UE) 2016/1148.

Le reti dell'UE consentono la cooperazione tra gli Stati membri a livello tecnico e operativo

25 La direttiva NIS ha istituito la rete di CSIRT, che riunisce CERT-UE (il servizio per la cibersicurezza per tutte le istituzioni, gli organi e gli organismi dell'UE) e i CSIRT nominati dagli Stati membri. Questa rete mira a rafforzare la fiducia tra i CSIRT nazionali e a promuovere una cooperazione operativa rapida ed efficace tra gli Stati membri.

26 EU-CyCLONe è stata istituita nel 2020 come rete di cooperazione informale per le autorità nazionali responsabili della gestione delle crisi informatiche: funge infatti da ponte tra il livello tecnico, in cui opera la rete di CSIRT, e il livello politico, competenza del Consiglio dell'Unione europea e dei suoi dispositivi integrati per la risposta politica alle crisi. L'entrata in vigore della direttiva NIS 2 nel 2023 ha formalizzato il ruolo di EU-CyCLONe conferendole un mandato chiaro.

27 La Corte ha valutato se i ruoli e le responsabilità di queste reti a livello dell'UE siano ben definiti e se consentano la cooperazione degli Stati membri.

28 L'ENISA funge da segretariato della rete di CSIRT e di EU-CyCLONe e fornisce loro le risorse, le competenze, le infrastrutture e gli strumenti informatici necessari per la cooperazione e canali di comunicazione sicuri per la condivisione delle informazioni. Nella sua indagine sulla soddisfazione delle parti interessate[4] dell'inizio del 2025, l'ENISA ha ottenuto buoni punteggi per le sue prestazioni in qualità di segretariato di tali reti. Questo riscontro positivo è stato confermato durante le visite di audit della Corte, nel corso delle quali le autorità nazionali per la cibersicurezza hanno espresso il loro apprezzamento.

29 Nel 2025 il Consiglio ha adottato il programma per la cibersicurezza, che definisce i ruoli e le responsabilità degli attori chiave (tra cui la rete di CSIRT e EU-CyCLONe) e dei meccanismi coinvolti negli incidenti di cibersicurezza su vasta scala o nelle crisi informatiche. La Corte ha riscontrato che il programma per la cibersicurezza chiarisce ampiamente i ruoli e le responsabilità per quanto riguarda la gestione delle crisi informatiche dell'UE e tiene conto dei cambiamenti intervenuti nel panorama dopo il primo programma nel 2017. Il programma definisce tre livelli di cooperazione: tecnico, operativo e politico, illustrando nel dettaglio le nuove reti e strutture istituite dal 2017, come EU-CyCLONe, i gruppi di risposta rapida dell'UE alle minacce ibride e il sistema europeo di allerta per la cibersicurezza. Spiega inoltre in che modo la gestione delle crisi informatiche dovrebbe essere integrata nel più ampio quadro di risposta alle crisi dell'UE.

[4] Relazione annuale di attività consolidata per il 2024dell'ENISA, pagg. 33 e 36.

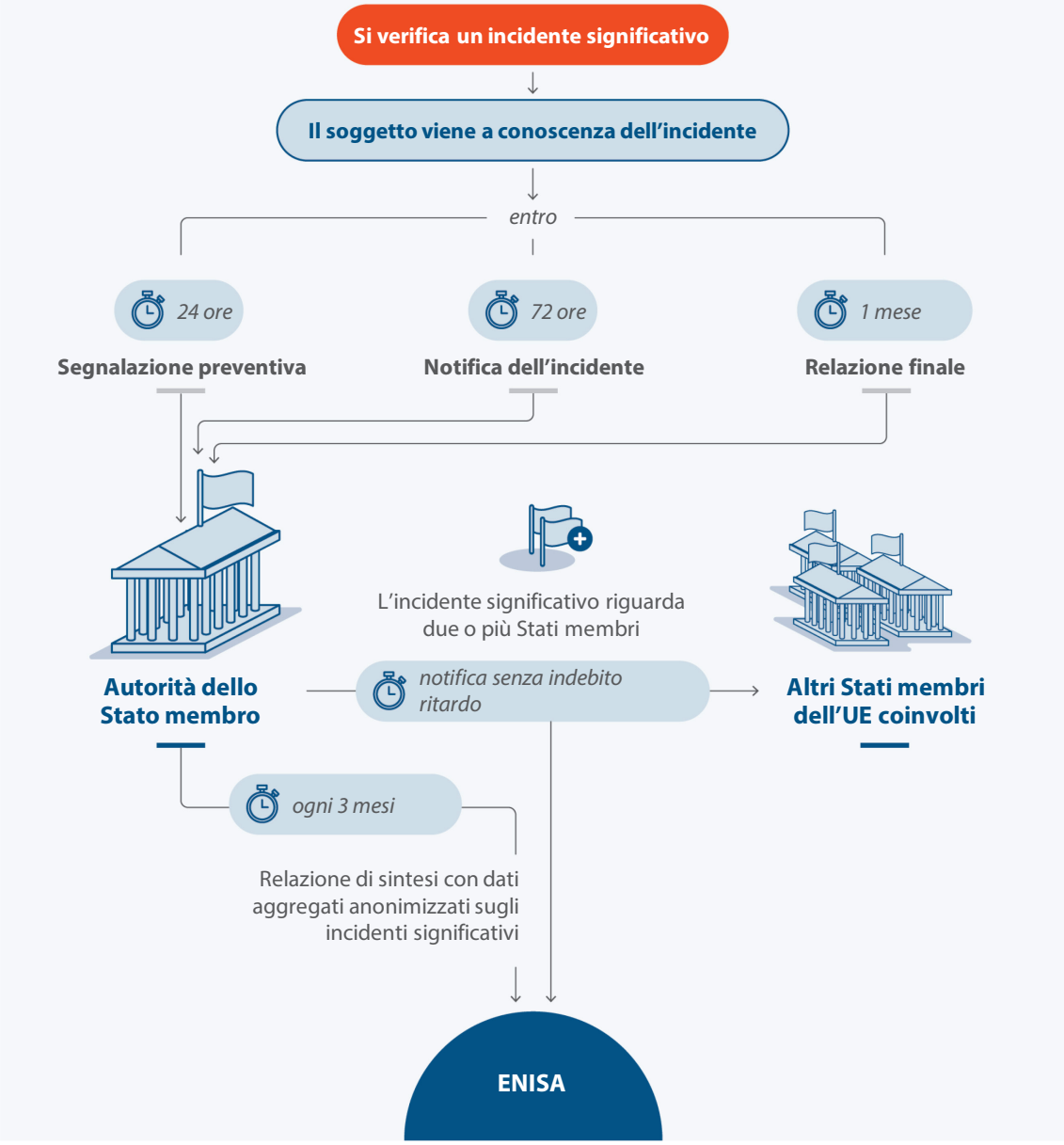
30 Tuttavia, nonostante l'istituzione ufficiale della rete di CSIRT nel 2016 e di EU-CyCLONe nel 2023, le due reti devono ancora formalizzare le procedure da seguire per la loro collaborazione. Inoltre, non hanno ancora stabilito i criteri in base ai quali la rete di CSIRT dovrebbe fornire consulenza a EU-CyCLONe in merito alla possibilità che un incidente di cibersicurezza osservato possa essere considerato un incidente di cibersicurezza su vasta scala potenziale o in corso. Le due reti devono inoltre concordare una tassonomia comune dei livelli di gravità degli incidenti e di concetti chiave – quali "minaccia", "autore della minaccia", "incidente" o "impatto" – che è necessaria per consentire lo scambio automatizzato di informazioni. Attualmente vi è margine di interpretazione per quanto riguarda i casi in cui un incidente sia da qualificare come significativo o su vasta scala. La mancanza di una tassonomia comune è stata menzionata dalle autorità di cibersicurezza di tutti e tre gli Stati membri visitati dagli auditor della Corte.

La mancanza di condivisione e comunicazione delle informazioni riduce notevolmente il valore aggiunto di tali reti

31 Le frontiere geografiche non impediscono il verificarsi e la diffusione di incidenti di cibersicurezza e attacchi informatici. La condivisione di informazioni tra gli Stati membri, ad esempio sulle tattiche e le tecniche utilizzate dagli autori delle minacce e sugli indizi digitali di violazione di una rete o di un sistema informativo ("indicatori di compromissione"), può contribuire in modo significativo ad aumentare la cibersicurezza.

32 La Corte ha riscontrato che una limitata condivisione delle informazioni ha ridotto significativamente il valore aggiunto di tali reti. I limiti osservati dalla Corte riguardano principalmente i ritardi nel recepimento della direttiva NIS 2, i problemi nel determinare se un incidente abbia un impatto transfrontaliero, la normativa nazionale in materia di sicurezza che limita la condivisione delle informazioni e la mancanza di fiducia. La direttiva NIS 2 introduce diversi obblighi di segnalazione per i soggetti che rientrano nel suo ambito di applicazione e per le autorità degli Stati membri, come illustrato nella ***figura 2***.

Figura 2 | Finestra temporale per la segnalazione degli incidenti, ai sensi della direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'UE (NIS 2)



Fonte: Corte dei conti europea, sulla base di documenti dell'ENISA.

33 Gli Stati membri hanno avuto tempo fino a ottobre 2024 per recepire la direttiva NIS 2 nel diritto nazionale, ma solo due hanno rispettato il termine. I ritardi nel recepimento hanno un impatto significativo sulla condivisione delle informazioni in quanto, nel frattempo, i soggetti contemplati dalla direttiva NIS 2 non sono giuridicamente tenuti a segnalare gli incidenti. La Commissione ha stimato[5] che 15 500 soggetti rientravano nell'ambito di applicazione della direttiva NIS, mentre oltre 110 000 rientrano nell'ambito di applicazione della direttiva NIS 2. Ad esempio, secondo la relazione 2025 dell'ENISA sul panorama delle minacce, la pubblica amministrazione, il settore più preso di mira nell'UE, non aveva l'obbligo di segnalare gli incidenti ai sensi della direttiva NIS.

34 La segnalazione dei dati relativi agli incidenti all'ENISA ogni tre mesi (ossia molto tempo dopo il verificarsi di un incidente) ne limita il valore aggiunto. Tali dati servono principalmente a fini statistici e di segnalazione storica delle tendenze, non per migliorare l'individuazione e la risposta. L'ENISA fornisce agli Stati membri uno strumento online per presentare le loro relazioni. Il modello di segnalazione contiene una serie minima di dati che devono essere forniti, quali il tipo di incidente e il settore coinvolto. Inoltre, l'ENISA suggerisce che gli Stati membri forniscano informazioni supplementari per consentire un'analisi più approfondita dei dati, ad esempio collegando gli incidenti a vulnerabilità specifiche. Tuttavia, non tutti gli Stati membri scelgono di fornire tali informazioni, riducendo in modo significativo la qualità e il valore aggiunto dei dati raccolti.

35 L'ENISA, nella sua relazione del 2024 sullo stato della cibersicurezza nell'UE, ha affermato che gli incidenti non sono probabilmente tutti segnalati, in quanto il numero di incidenti segnalati sembra essere basso. Negli anni dal 2018 al 2021 gli Stati membri hanno segnalato ogni anno all'ENISA tra 100 e 500 incidenti. Detto numero è aumentato gradualmente e nel 2024 è salito a 1 276[6].

---

[5] Commissione europea, relazione sulla valutazione d'impatto 2020.

[6] Dati CIRAS per il 2024.

36 Nella sua relazione del 2025 sul panorama delle minacce, che copre il periodo compreso tra giugno 2024 e giugno 2025, l'ENISA ha individuato circa 4 800 incidenti di cibersicurezza[7] attraverso intelligence da fonti aperte, come, ad esempio, articoli di giornale. Questi incidenti non sarebbero stati tutti da segnalare ai sensi della direttiva NIS 2 in quanto, al momento della raccolta dei dati, l'ENISA copriva una gamma più ampia di incidenti. Per contro, nell'intelligence da fonti aperte non sono segnalati molti incidenti significativi. Poiché i dati comunicati dagli Stati membri sono resi anonimi, l'ENISA non può correlare gli incidenti da essa individuati a quelli segnalati dagli Stati membri. Non è pertanto possibile determinare con precisione la portata della sottosegnalazione, ma la Corte ritiene che la differenza tra il numero di incidenti segnalati dagli Stati membri e quelli riportati nella relazione sul panorama delle minacce dimostri che non tutti gli incidenti significativi sono segnalati.

37 Un altro indice di sottosegnalazione è il numero di notifiche riguardanti incidenti transfrontalieri significativi inviate ad altri Stati membri coinvolti e all'ENISA. Un obbligo in questo senso esisteva nell'ambito della direttiva NIS, ma è stato ritenuto inefficace, in quanto [8]nel 2020 la Commissione ha concluso che, nonostante l'imposizione, le notifiche sono state inviate raramente. La mancata notifica è stata attribuita all'assenza di modalità chiare per la condivisione delle informazioni e l'assenza di obiettivi comuni che incentivino la condivisione.

38 Informare gli altri Stati membri è fondamentale per evitare la propagazione di incidenti: il mancato adempimento di tale obbligo incide negativamente sulla cibersicurezza dell'UE. Nel 2025 ci sono state solo 14 segnalazioni di incidenti transfrontalieri significativi da parte di sette Stati membri. Le segnalazioni di incidenti con un possibile impatto transfrontaliero sono state due nel 2024, nessuna nel 2023 e tre nel 2022. Ciò dimostra che la segnalazione di incidenti transfrontalieri significativi è molto bassa e non riflette la reale portata di tali attacchi. Per mettere le cose in prospettiva, nella sua relazione sul panorama delle minacce del 2024, l'ENISA ha individuato 322 incidenti che coinvolgevano specificamente due o più Stati membri. L'incidente di Collins Aerospace (cfr. ***riquadro 1***) è un esempio di mancata segnalazione di un incidente da parte degli Stati membri, nonostante avesse un impatto transfrontaliero significativo.

---

[7] Relazione 2025 dell'ENISA sul panorama delle minacce.

[8] Commissione europea, relazione sulla valutazione d'impatto 2020.

Riquadro 1

Incidente di cibersicurezza che perturba le operazioni aeroportuali

Nel settembre 2025 Collins Aerospace, un importante fornitore di tecnologie per il settore dell'aviazione, ha subìto un significativo attacco ransomware che ha preso di mira il suo software per il trattamento dei dati dei passeggeri. L'attacco ha costretto i principali aeroporti europei a tornare alle operazioni manuali, causando ritardi e cancellazioni dei voli su vasta scala. La perturbazione è stata più grave negli aeroporti di Londra Heathrow, Bruxelles, Berlino Brandeburgo e Dublino.

Ai sensi della direttiva NIS 2, un incidente è considerato "significativo" se, tra le altre cose, causa gravi perturbazioni operative dei servizi o perdite finanziarie per il soggetto coinvolto. Tuttavia, nessuno Stato membro ha trattato tale accaduto come un incidente transfrontaliero significativo o su vasta scala e, di conseguenza, nessuno di essi ha notificato formalmente l'incidente all'ENISA o ad altri Stati membri. La rete di CSIRT non ha fornito consulenza a EU-CyCLONe, che non ha quindi sostenuto la gestione coordinata dell'incidente.

Fonte: analisi della Corte dei conti europea, sulla base dei colloqui con ENISA.

39 Un altro motivo della limitata segnalazione di incidenti transfrontalieri è il fatto che spetta alle autorità di ciascuno Stato membro determinare se un incidente segnalato abbia un impatto transfrontaliero e individuare gli altri Stati membri colpiti. In base delle informazioni a loro disposizione, il soggetto segnalante o l'autorità dello Stato membro potrebbero non essere a conoscenza della natura transfrontaliera di alcuni attacchi. Attualmente non esiste una piattaforma a livello dell'UE che riceva segnalazioni di incidenti in tempo reale da tutti gli Stati membri e che possa correlare le informazioni sui settori o gli indicatori di compromissione per individuare gli incidenti transfrontalieri. Vi è pertanto un rischio significativo che alcuni incidenti transfrontalieri possano non essere identificati come tali e non venire segnalati.

40 Dal 2016 nessun incidente di cibersicurezza è stato classificato "su vasta scala" dagli Stati membri. In linea di principio, qualsiasi incidente che incida in modo significativo su almeno due Stati membri rientra in tale definizione. Tuttavia, anche gli incidenti di cibersicurezza che hanno causato interruzioni globali e danni significativi, come quelli illustrati nella ***figura 3***, non sono stati considerati su vasta scala: la procedura di escalation di EU-CyCLONe non è quindi mai stata pienamente attivata per un incidente di cibersicurezza su vasta scala.

Figura 3 | Esempi di gravi incidenti di cibersicurezza

WannaCry

2017

Un attacco ransomware a livello mondiale

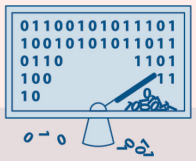
Ha infettato oltre 200 000 computer in più di 150 paesi, paralizzando i gestori delle infrastrutture critiche; ha criptato dati su dispositivi infetti e richiesto un riscatto per la decrittazione

NotPetya

2017

Un malware distruttivo camuffato da ransomware

Progettato per cancellare i dati in modo permanente, aveva come obiettivo principale l'Ucraina, ma si è diffuso rapidamente in tutto il mondo, paralizzando le multinazionali e causando danni globali



Indisponibilità dei sistemi informatici dovuta a CrowdStrike

Luglio 2024

Un'interruzione informatica massiccia a livello mondiale

Causato da un errato aggiornamento del software da parte della società di cibersicurezza CrowdStrike che ha comportato il malfunzionamento di milioni di computer

Fonte: Corte dei conti europea, adattato da Cloudflare, ENISA, Europol, Wired, IBM, CrowdStrike.

41 Oltre all'obbligo di segnalazione imposto a soggetti e Stati membri, al fine di facilitare la condivisione delle informazioni è stata creata la rete di CSIRT. La fiducia tra gli Stati membri è fondamentale per la rete di CSIRT, in cui le informazioni sono condivise su base volontaria: se gli Stati membri non sono disposti a condividere informazioni tempestive e fruibili, il valore aggiunto di detta rete diminuisce sensibilmente.

42 La condivisione delle informazioni a livello dell'UE è limitata dalla normativa in materia di sicurezza di ciascuno Stato membro. Se uno Stato membro ritiene che le informazioni relative ad attacchi informatici su un "soggetto critico" siano classificate o che la segnalazione di uno specifico incidente sia dannosa per la sua sicurezza nazionale, non è tenuto a condividerle. Durante le visite della Corte negli Stati membri, i rappresentanti della rete di CSIRT e di EU-CyCLONe hanno dichiarato che la condivisione può avvenire solo entro i limiti della normativa nazionale in materia di sicurezza. A livello dell'UE non è stata effettuata un'analisi dei quadri giuridici nazionali degli Stati membri e del loro impatto sulla condivisione delle informazioni.

43 Nel 2016 la rete di CSIRT comprendeva 28 CSIRT nazionali, con due rappresentanti per Stato membro. La mancanza di condivisione delle informazioni è stata un problema persistente e la valutazione della Commissione della direttiva NIS ha riconosciuto che gli Stati membri non condividono sistematicamente le informazioni tra loro, il che incide in particolare sull'efficacia delle misure di cibersicurezza e sul livello di conoscenza situazionale comune nell'UE. Nell'ambito dell'applicazione della direttiva NIS 2, molti Stati membri hanno nominato CSIRT settoriali in aggiunta ai loro CSIRT nazionali, per cui la rete si è notevolmente ampliata. Al momento dell'audit, vi erano 42 CSIRT e oltre 700 singoli partecipanti: ciò rende ancora più difficile instaurare un clima di fiducia, in quanto è difficile mantenere legami stretti tra tutti i membri.

44 La rete di CSIRT è consapevole del problema della condivisione delle informazioni e sta valutando varie azioni per aumentare la fiducia in una rete che cresce. La creazione di cluster più piccoli tra Stati membri, con l'obiettivo di formare poli transfrontalieri, come illustrato nei paragrafi ***62*-*74***, è una alternativa alla rete più ampia a livello dell'UE: tale approccio potrebbe contribuire a ovviare a questa problematica.

Il centro di situazione e di analisi informatiche duplica in parte le capacità esistenti e il suo futuro funzionamento non è chiaro

45 Ai sensi della direttiva NIS 2 e nei casi in cui un incidente di cibersicurezza su vasta scala, potenziale o in corso, abbia o possa avere un impatto significativo, la Commissione diventa membro di EU-CyCLONe[9]. Questo nuovo ruolo e l'evoluzione del panorama delle minacce hanno indotto la Commissione a istituire una task force di coordinamento informatico all'interno della DG Connect nel 2022. La task force comprende un centro di situazione e di analisi informatiche, che dovrebbe aiutare la Commissione ad aumentare la sua conoscenza situazionale con l'obiettivo di sostenere le proprie responsabilità istituzionali nella gestione delle crisi. Dovrebbe inoltre aiutare la DG Connect a fornire consulenza a livello politico.

[9] Articolo 16, paragrafo 2, della direttiva NIS 2.

46 Per istituire il centro di situazione e analisi informatiche, la Commissione si affida in larga misura a prestatori esterni di servizi, con cui nel dicembre 2022 sono stati stipulati contratti per quasi 18 milioni di euro per quattro anni. La Corte ha valutato l'istituzione del Centro, le sue realizzazioni e i piani della Commissione per il suo futuro funzionamento.

47 Nell'ambito dei servizi prestati, i fornitori esterni hanno istituito un quadro operativo basato su feed di intelligence commerciale sulle minacce informatiche, al fine di presentare e condividere informazioni su di esse. Si occupano inoltre di produrre varie relazioni di intelligence sulle minacce informatiche, tra cui relazioni giornaliere e settimanali, nonché relazioni tematiche su paesi o su settori dell'economia. Il centro di situazione e di analisi informatiche, costituito da una sala dotata di postazioni di lavoro collegate a distanza al quadro operativo gestito dai fornitori esterni, è stato fisicamente allestito in uno degli edifici della Commissione. Al momento dell'audit, il centro di situazione informatica comprendeva un numero limitato di membri del personale della Commissione, coadiuvati da numerosi analisti dei fornitori esterni e da esperti dell'ENISA.

48 La Corte ha riscontrato che il lavoro svolto dai fornitori esterni o da tale centro duplica in parte la capacità esistente dell'ENISA. Quest'ultima dispone di una capacità permanente di conoscenza situazionale e monitoraggio delle minacce e pubblica regolarmente relazioni sulle minacce informatiche, comprese relazioni flash su incidenti specifici, nonché relazioni settimanali che forniscono una panoramica delle minacce. Le relazioni si basano su informazioni *open source* e sono simili a quelle prodotte dai contraenti esterni. Inoltre, l'ENISA produce o contribuisce a produrre note informative di alto livello per i responsabili politici in tempi di crisi, anche queste simili a quanto prodotto dal centro di situazione e di analisi informatiche.

49 In aggiunta a ciò, i dati utilizzati dal centro di situazione e analisi informatiche per elaborare tali relazioni, basati su feed di intelligence commerciale sulle minacce informatiche, sono simili ai dati utilizzati da altri servizi della Commissione, quali la direzione generale dei Servizi digitali e CERT-UE. La Corte ritiene che, nell'istituire il centro di situazione e analisi informatiche, non siano state sfruttate a sufficienza le potenzialità di razionalizzazione, poiché non si è attinto alle informazioni già disponibili presso la Commissione e l'ENISA.

50 Il contratto scade a dicembre 2026, dopodiché i fornitori esterni non presteranno più i servizi per il centro. Fra questi servizi vi sono la fornitura dei dati disponibili nel quadro operativo, l'elaborazione delle relazioni sulle minacce e l'allestimento della maggior parte del centro. Il quadro operativo sarà consegnato alla Commissione, ma perderà il suo valore aggiunto se non sarà costantemente aggiornato con le informazioni sulle minacce informatiche.

51 Al momento dell'audit della Corte, la Commissione non aveva predisposto nessun piano riguardante il supporto da parte di fornitori esterni per il funzionamento del centro di situazione e di analisi informatiche dopo la scadenza del contratto Inoltre, l'assenza di un piano completo e dettagliato per il futuro dopo la scadenza del contratto rappresenta un rischio per il funzionamento del centro di situazione informatica dopo il 2026.

La riserva dell'UE per la cibersicurezza consente la rapida diffusione dei servizi di risposta agli incidenti

52 Nel 2022, dopo l'aggressione militare della Russia nei confronti dell'Ucraina, avendo riconosciuto che gli attacchi informatici su vasta scala erano diventati più diffusi, la Commissione ha fornito all'ENISA 15 milioni di euro di finanziamenti eccezionali per testare l'azione di sostegno alla cibersicurezza, varata nel 2023. Nel 2023 la Commissione ha fornito ulteriori finanziamenti (circa 20 milioni di euro) per prorogare il programma fino alla fine del 2026.

53 La Commissione ha inoltre proposto il regolamento sulla cibersolidarietà, adottato nel dicembre 2024, per prepararsi ad affrontare gli incidenti di cibersicurezza su vasta scala. Il regolamento istituisce una riserva dell'UE per la cibersicurezza che comprende servizi di risposta agli incidenti offerti da forniti da operatori di fiducia. Ha iniziato a funzionare gradualmente nel 2025, con una dotazione finanziaria di 36 milioni di euro per il periodo 2025-2027.

54 La Corte ha valutato il modo in cui è stato organizzato il programma d'azione di sostegno alla cibersicurezza, che costituisce la base della riserva dell'UE per la cibersicurezza, e ha inoltre verificato se quanto appreso a partire dal 2022 abbia contribuito alla progettazione di detta riserva.

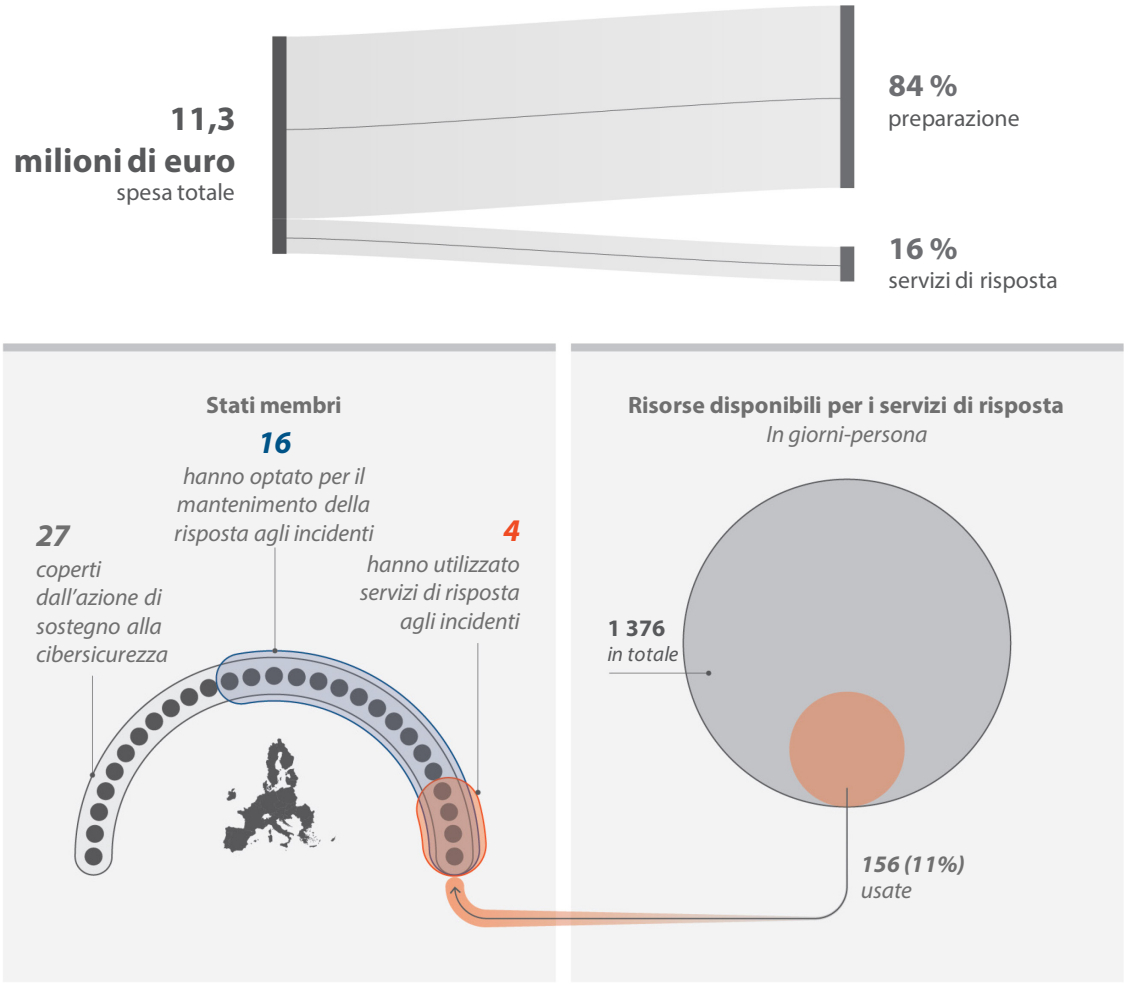
55 L'ENISA ha concepito l'azione di sostegno alla cibersicurezza come un meccanismo per fornire servizi a supporto della preparazione e della risposta degli Stati membri agli incidenti o alle crisi di cibersicurezza su vasta scala. Tutti i servizi sono preappaltati dall'ENISA: in altre parole, i prestatori di servizi possono iniziare a lavorare non appena gli Stati membri lo richiedono. Ciò è possibile anche grazie alla struttura dell'ENISA, che garantisce la presenza di un funzionario disponibile tutti i giorni 24 ore su 24 per trattare le richieste degli Stati membri.

56 L'ENISA ha scelto di ripartire equamente il bilancio disponibile tra gli Stati membri. In pratica, l'agenzia ha indetto una procedura di gara aperta suddivisa in 27 lotti, uno per Stato membro, per selezionare fino a tre fornitori privati di servizi di sicurezza che presteranno servizi fino alla fine del 2026. Inoltre, l'ENISA ha selezionato alcuni fornitori all'interno di un lotto paneuropeo per fornire servizi ai paesi non-UE che rispondono ai requisiti, alle istituzioni, agli organi e alle agenzie dell'UE, oppure per sostenere la risposta agli incidenti transfrontalieri.

57 Tale approccio ha consentito all'ENISA di tenere conto di specifiche necessità nazionali, tra cui la lingua, i nulla osta di sicurezza nazionali o la presenza consolidata negli Stati membri. D'altro canto, poiché i fornitori non sono stati selezionati per poter fornire servizi in tutta l'UE, uno dei principali inconvenienti di questo approccio consiste nel fatto che, se uno Stato membro non utilizza i servizi preappaltati, il bilancio destinato a questi servizi per uno specifico Stato membro non può essere utilizzato per assistere un altro Stato membro.

58 Per l'azione di sostegno alla cibersicurezza, gli Stati membri potevano scegliere tra servizi di preparazione o di risposta o una combinazione di entrambi: la maggior parte di loro ha scelto di utilizzare i finanziamenti disponibili per migliorare la propria preparazione (l'84 % della spesa nel 2023). Gli Stati membri che hanno scelto di disporre di un soggetto responsabile per la risposta agli incidenti (ossia di un accordo predefinito con un fornitore che garantisce allo Stato membro di poter accedere su richiesta ai servizi del fornitore per garantire una risposta rapida agli incidenti di cibersicurezza) vi hanno fatto ricorso sporadicamente, come illustrato nella ***figura 4***. Nei tre Stati membri visitati, le autorità hanno espresso apprezzamento per la gestione dell'azione di sostegno alla cibersicurezza da parte dell'ENISA.

Figura 4 | Azione di sostegno alla cibersicurezza dell'ENISA fino al 2023



Fonte: Corte dei conti europea sulla base dei dati dell'ENISA

59 Per il periodo 2024-2026, solo nove Stati membri hanno richiesto un soggetto responsabile per la risposta agli incidenti. I colloqui della Corte con l'ENISA e le autorità di tre Stati membri hanno confermato una forte preferenza per le attività di preparazione.

60 Nonostante la riserva dell'UE per la cibersicurezza miri principalmente a sostenere la risposta e la ripresa in caso di gravi incidenti di cibersicurezza, i servizi preimpegnati della riserva dell'UE per la cibersicurezza non utilizzati per la risposta agli incidenti possono essere convertiti in servizi di preparazione. Questo approccio flessibile mira a evitare che servizi prepagati restino inutilizzati.

61 La Corte ritiene che il modello scelto per la riserva dell'UE per la cibersicurezza si basi sugli insegnamenti tratti dal programma "Cybersecurity Support Action". Tuttavia, i dati sull'uso di tale programma indicano il rischio che la riserva dell'UE per la cibersicurezza possa essere utilizzata principalmente per la preparazione e non per la risposta, contrariamente allo scopo stabilito nel regolamento sulla cibersolidarietà.

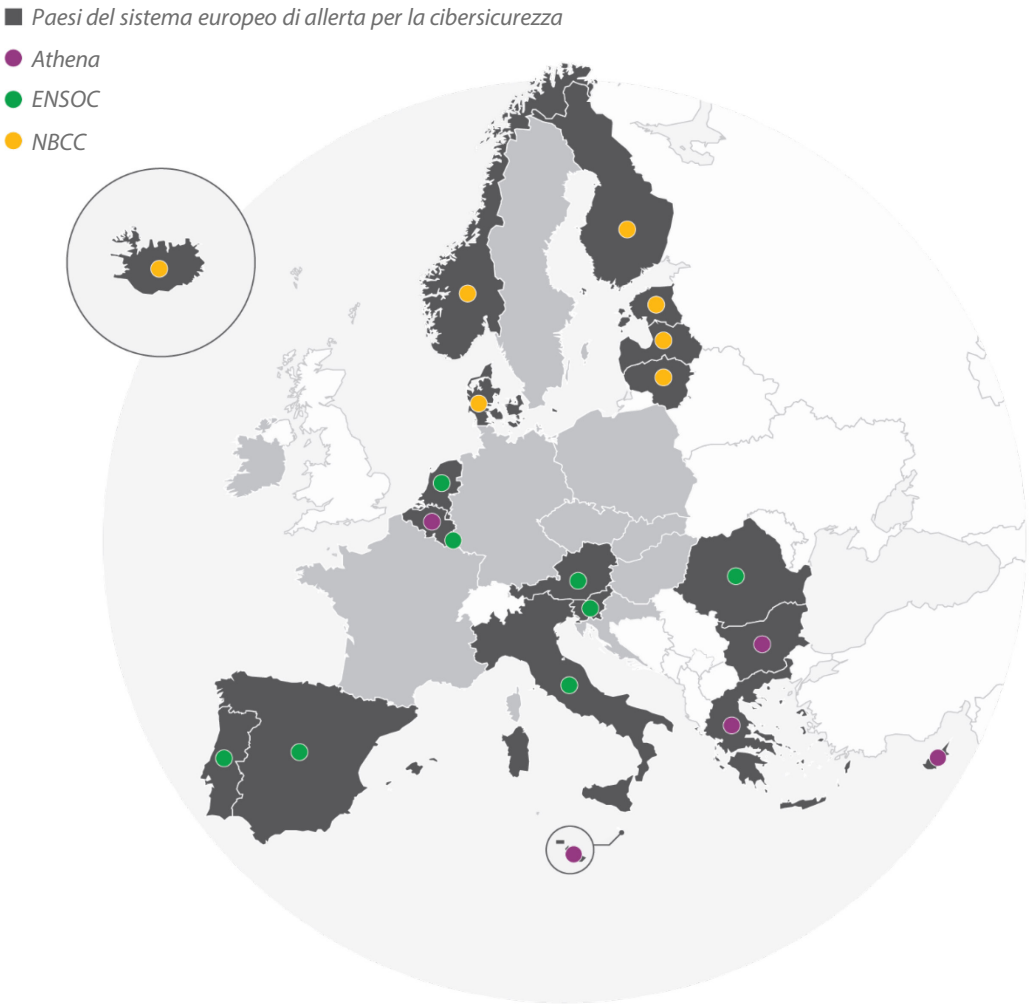
Il sistema europeo di allerta per la cibersicurezza mira a migliorare le capacità di individuazione delle minacce, ma non è operativo

62 Uno degli obiettivi principali del sistema europeo di allerta per la cibersicurezza è incoraggiare la condivisione di informazioni significative per migliorare l'individuazione, l'analisi e la risposta alle minacce informatiche. La partecipazione al sistema di allerta è volontaria, ma gli Stati membri che scelgono di aderire a un polo informatico transfrontaliero devono impegnarsi a condividere le informazioni pertinenti con gli altri membri. Lavorare insieme in cluster in un ambiente affidabile e sicuro permetterebbe agli Stati membri di evitare alcuni problemi relativi alla condivisione delle informazioni individuati nei paragrafi ***31***-***44***.

63 Al momento dell'audit, 13 Stati membri avevano scelto di far parte del sistema europeo di allerta per la cibersicurezza, istituendo due poli transfrontalieri: ATHENA ed ENSOC. Un terzo polo informatico transfrontaliero, l'NBCC, aveva ricevuto finanziamenti per la sua istituzione nel 2026, portando i membri della rete ad un totale di 20 paesi (18 Stati membri, più Islanda e Norvegia[10]), come illustrato nella ***figura 5***.

[10] Paesi non-UE associati conformemente all'articolo 10, paragrafo 1, lettera a, del regolamento (UE) 2021/694.

Figura 5 | Paesi del sistema europeo di allerta per la cibersicurezza



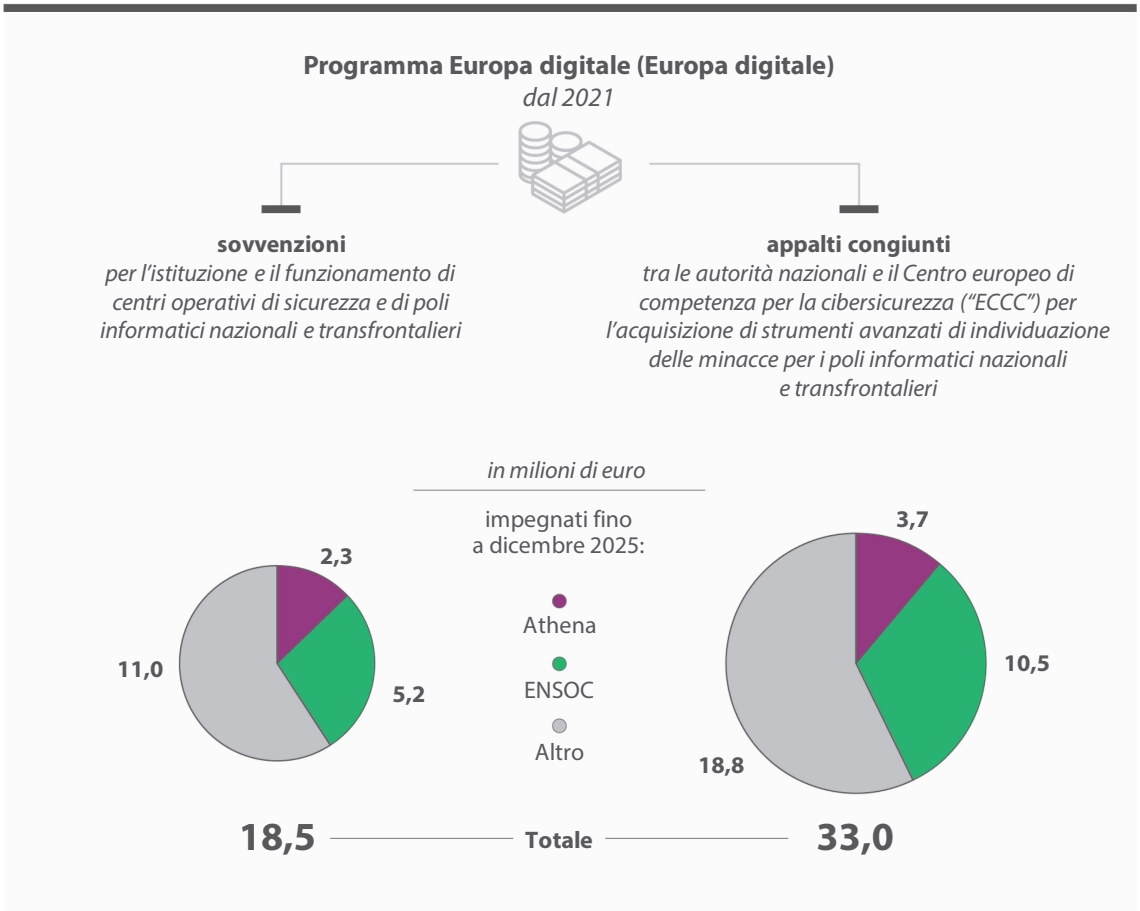
Fonte: Corte dei conti europea.

64 La Corte ha valutato come sono stati istituiti i primi due poli informatici transfrontalieri, nonché i progressi compiuti verso il conseguimento degli obiettivi del sistema europeo di allerta per la cibersicurezza. Ha inoltre esaminato come l'istituzione dei poli informatici transfrontalieri si inserisca nel più ampio panorama della cibersicurezza e interagisca con le reti e le strutture esistenti.

Finora non sono stati conseguiti risultati concreti a causa di ritardi considerevoli negli appalti

65 I finanziamenti a sostegno della creazione di poli informatici nazionali e transfrontalieri sono accessibili tramite Europa digitale dal 2021. Tali finanziamenti sono erogati attraverso una procedura complessa con due flussi paralleli: sovvenzioni tradizionali a sostegno dell'istituzione e del funzionamento dei poli e appalti congiunti per l'acquisizione di strumenti avanzati di individuazione delle minacce, come illustrato nella ***figura 6***. Dopo un invito a presentare proposte nel novembre 2022, ATHENA ed ENSOC hanno iniziato i loro lavori nel gennaio 2024.

Figura 6 | Finanziamenti di Europa digitale per i poli informatici



Fonte: Corte dei conti europea, sulla base dei dati dell'ECCC.

66 Le procedure di appalto ristrette in due fasi[11] sono state organizzate dai membri di ATHENA ed ENSOC, nonché dalla DG Connect (prima fase) e dall'ECCC di nuova istituzione (seconda fase). L'approccio in due fasi mira a limitare la circolazione di informazioni sensibili: le specifiche tecniche dettagliate vengono fornite infatti solo ai candidati selezionati nella prima fase.

67 La prima fase è stata avviata nel maggio 2024 per l'ENSOC e nel luglio 2024 per ATHENA. Le imprese interessate hanno avuto un mese di tempo per presentare domanda. Tuttavia, i candidati idonei sono stati notificati solo nell'aprile 2025, quasi un anno dopo l'avvio della procedura.

68 All'epoca né l'ENSOC né ATHENA potevano passare alla seconda fase delle procedure di appalto, in quanto i membri del polo e l'ECCC, non erano in grado di fornire alle società preselezionate le specifiche tecniche necessarie per presentare un'offerta, in quanto stavano ancora lavorando alla loro finalizzazione.

69 La seconda fase delle procedure di appalto è iniziata solo nell'agosto 2025 per alcuni lotti destinati all'ENSOC ed era prevista per l'inizio del 2026 per ATHENA. Al momento dell'audit, 18 mesi dopo l'avvio della procedura di appalto, non erano stati firmati contratti per nessuno dei lotti. La Corte ritiene che la mancanza di una preparazione adeguata e la complessità delle procedure di appalto abbiano pregiudicato il loro tempestivo completamento.

70 Pertanto, la Corte ha riscontrato che i poli transfrontalieri non sono sulla buona strada per conseguire i propri obiettivi: senza gli strumenti per rilevare le minacce e condividere le informazioni, sono in sospeso dal punto di vista operativo e il sistema europeo di allerta per la cibersicurezza non è ancora funzionante, il che ritarda l'efficace sviluppo di capacità avanzate per rilevare e prevenire le minacce e gli incidenti informatici. Sono state firmate modifiche per prorogare la durata della convenzione di sovvenzione, al fine di tenere conto dei ritardi nelle procedure di appalto (15 mesi per ATHENA e 18 mesi per ENSOC).

[11] Bando di gara ENSOC e bando di gara ATHENA.

I poli informatici transfrontalieri creano canali di comunicazione aggiuntivi che aumentano ulteriormente la complessità

71 Uno dei compiti principali dei poli informatici transfrontalieri è condividere informazioni pertinenti per migliorare l'individuazione delle minacce e la risposta alle stesse: ciò comprende informazioni sulle minacce informatiche, sulle vulnerabilità, sugli indicatori di compromissione e sugli autori delle minacce. I compiti dei poli informatici transfrontalieri si sovrappongono in parte a quelli dei CSIRT nazionali e della rete di CSIRT, in particolare per quanto riguarda la condivisione delle informazioni sulle minacce informatiche e sulle vulnerabilità. Non esiste un chiaro confine tra i ruoli dei poli informatici transfrontalieri e dei CSIRT: secondo il programma per la cibersicurezza del 2025 (paragrafo ***29***), i poli informatici transfrontalieri dovrebbero operare a livello sia tecnico (come i CSIRT nazionali e la rete di CSIRT) che operativo (come EU-CyCLONe).

72 Il regolamento sulla cibersolidarietà impone ai poli informatici transfrontalieri di firmare accordi di cooperazione tra loro per facilitare la condivisione delle informazioni. L'ENISA avrebbe dovuto pubblicare linee guida per l'interoperabilità tra i poli informatici transfrontalieri entro febbraio 2026, come previsto dal regolamento sulla cibersolidarietà. Nel frattempo, nel dicembre 2025 l'ECCC ha concesso una sovvenzione a un consorzio (comprendente alcuni membri dell'ENSOC e di ATHENA) per definire un quadro tecnico per l'interoperabilità tra i poli informatici transfrontalieri. Tuttavia, gli orientamenti e il quadro saranno completati solo quando i poli informatici transfrontalieri saranno già operativi. Come sottolineato nel parere del 2023 sulla proposta di regolamento sulla cibersolidarietà[12], vi è il rischio che, in assenza di un rapido accordo, si possano sviluppare sistemi incompatibili tra loro, con un conseguente aumento dei costi.

[12] Parere 02/2023 sulla proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce misure intese a rafforzare la solidarietà e le capacità dell'Unione di rilevamento delle minacce e degli incidenti di cibersicurezza, e di preparazione e risposta agli stessi, paragrafo 26.

73 I poli informatici transfrontalieri sono inoltre tenuti a condividere senza indebito ritardo le informazioni pertinenti sugli incidenti di cibersicurezza su vasta scala con EU-CyCLONe e la rete di CSIRT. A livello degli Stati membri, la creazione di poli informatici nazionali e la partecipazione a poli informatici transfrontalieri creano ulteriori livelli di comunicazione. Anche il coordinamento con gli stati non-UE[13], che non fanno parte della rete di CSIRT o di EU-CyCLONe, aumenta la complessità.

74 Sono necessari accordi di cooperazione chiari per concordare una tassonomia comune e una modalità di condivisione delle informazioni, nonché per garantire l'interoperabilità. Gli insegnamenti tratti dalla rete di CSIRT dimostrano che si tratta di una sfida significativa. La Corte ha riscontrato che, al momento dell'audit, non vi erano accordi procedurali in materia di cooperazione e condivisione delle informazioni. Si ritiene inoltre che l'istituzione di poli informatici nazionali e transfrontalieri potrebbe promuovere una condivisione più efficace delle informazioni. Tuttavia, l'integrazione dei poli transfrontalieri nel già complesso panorama della cibersicurezza sarà impegnativa e richiederà ulteriori canali di comunicazione e accordi di cooperazione.

[13] Islanda e Norvegia.

I progetti finanziati dall'UE nell'ambito di Europa digitale mirano a rafforzare la cibersicurezza, ma fanno fronte a sfide in materia di attuazione e comunicazione

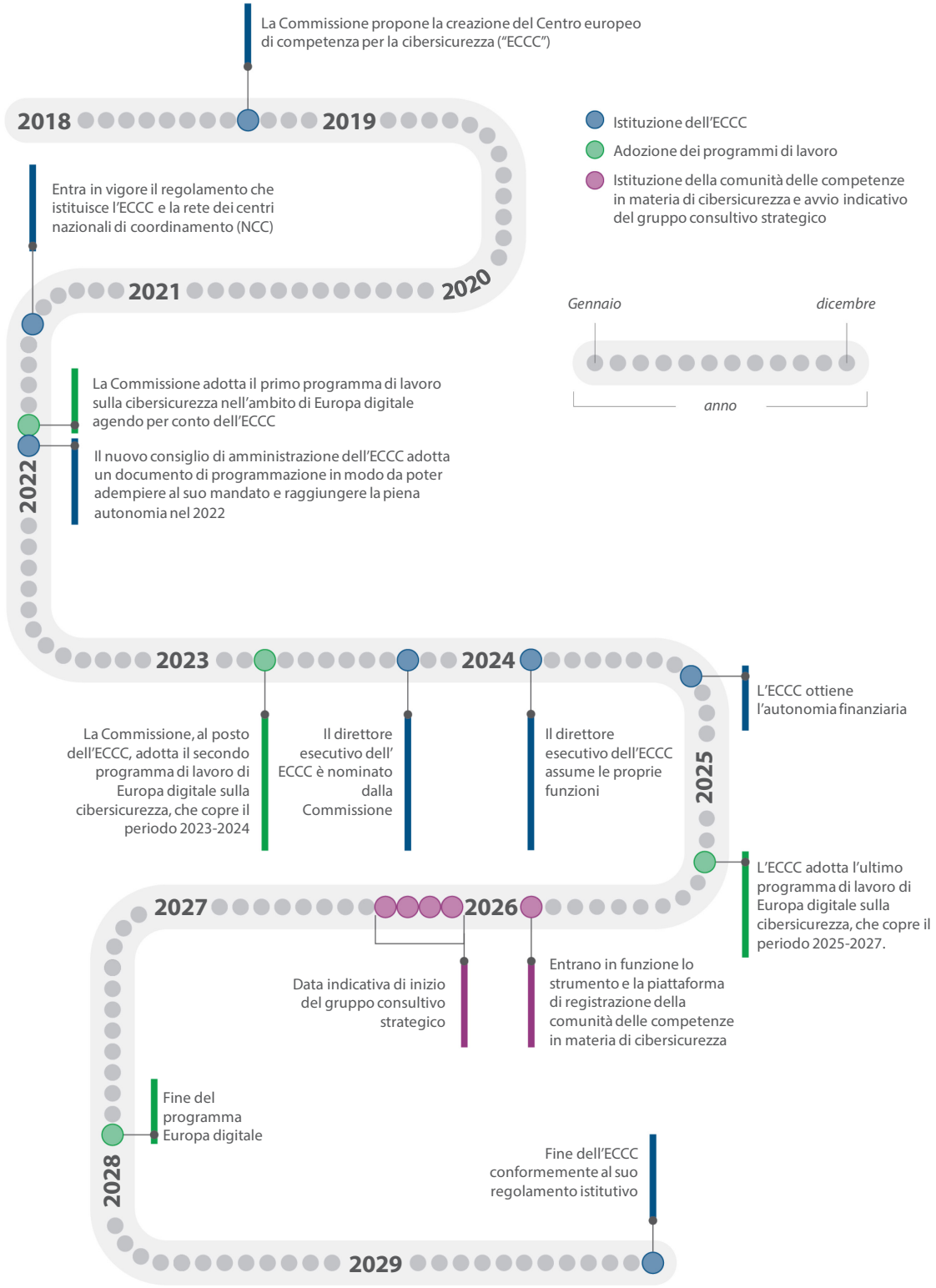
I ritardi nella sua istituzione hanno impedito alla comunità delle competenze in materia di cibersicurezza di configurare Europa digitale secondo le proprie esigenze

75 Per gestire la componente di cibersicurezza di Europa digitale, nel 2018 la Commissione ha proposto la creazione del Centro europeo di competenza per la cibersicurezza ("ECCC"). In base al suo regolamento, l'ECCC sarebbe dovuto essere sostenuto da una rete di 29 centri nazionali di coordinamento ("NCC"), uno per ciascuno Stato membro, nonché per l'Islanda e la Norvegia. Il regolamento prevedeva inoltre la creazione della comunità delle competenze in materia di cibersicurezza ("Comunità"), composta da rappresentanti dell'industria, del mondo accademico e delle organizzazioni di ricerca, nonché di altre associazioni pertinenti della società civile.

76 Fino a 20 membri della Comunità faranno parte del gruppo consultivo strategico ("SAG"), che è una delle tre componenti della struttura dell'ECCC. Fra i compiti principali del SAG vi è l'organizzazione di consultazioni pubbliche con il fine di alimentare l'agenda di Europa digitale e i programmi di lavoro dell'ECCC.

77 La Corte ha valutato se Europa digitale e i relativi programmi di lavoro siano stati adottati sulla base di una solida analisi delle esigenze e se l'ECCC, la rete dei centri nazionali di coordinamento, la Comunità e il SAG siano stati in grado di contribuire ai programmi di lavoro. Nella pratica, l'ECCC, la rete dei centri nazionali di coordinamento, la Comunità e il SAG sono stati istituiti gradualmente nel corso di diversi anni (cfr. ***figura 7***).

Figura 7 | Cronistoria dell'istituzione del Centro europeo di competenza per la cibersicurezza, della rete dei centri nazionali di coordinamento, della Comunità e del SAG



Fonte: Corte dei conti europea.

78 Poiché l'ECCC è diventato pienamente operativo solo nel settembre 2024, la Commissione, per conto dell'ECCC, ha adottato i programmi di lavoro per i periodi 2021-2022 e 2023-2024. I due programmi di lavoro adottati dalla Commissione non hanno potuto beneficiare del contributo della Comunità.

79 Nel frattempo gli Stati membri hanno iniziato a istituire i propri centri nazionali di coordinamento, che fungono da punti di contatto a livello nazionale per la Comunità. La loro istituzione e il loro funzionamento sono stati cofinanziati da Europa digitale, con oltre 90 milioni di euro di finanziamenti dell'UE concessi al momento dell'audit, di cui circa 44 milioni di euro saranno ulteriormente distribuiti con il sostegno finanziario a terzi. Altri 38 milioni di euro sono stati iscritti in bilancio fino al 2027 per sostenere i centri nazionali di coordinamento.

80 La Corte ha riscontrato che, nel dicembre 2025, quattro anni dopo l'istituzione dell'ECCC e della rete dei centri nazionali di coordinamento, la Comunità non era ancora stata istituita e il SAG non era ancora stato nominato. Il 14 marzo 2025 l'ECCC ha adottato l'ultimo programma di lavoro di Europa digitale sulla cibersicurezza, che copre il periodo 2025-2027. Pur avendo preparato e adottato il suo programma di lavoro a seguito di ampie consultazioni con gli Stati membri e la rete dei centri nazionali, l'ECCC non ha potuto beneficiare del contributo e della consulenza della Comunità o del gruppo consultivo strategico: ciò è in contrasto con le disposizioni del regolamento istitutivo e la Corte ritiene che si tratti di un'opportunità mancata.

81 Europa digitale scadrà nel 2027 e, se il mandato non sarà prorogato, l'ECCC dovrebbe essere liquidato nel 2029. Il sostegno della rete dei centri nazionali di coordinamento, della Comunità e del SAG, una volta istituito, potrebbe essere valido solo per un breve periodo.

I progetti finanziati dall'UE perseguono obiettivi pertinenti, ma molti si trovano ad affrontare problemi operativi

82 La Corte ha selezionato un campione di 11 progetti pertinenti per l'individuazione degli incidenti di cibersicurezza e la risposta agli stessi, finanziati nell'ambito di Europa digitale nel periodo 2022-2025 (cfr. ***figura 5*** degli ***allegati I*** e ***III***). La Corte ha verificato se:

- gli obiettivi dei progetti fossero in linea con gli effetti attesi elencati negli inviti a presentare proposte e con quelli di Europa digitale nel suo complesso;
- i progetti abbiano finora conseguito le realizzazioni e i risultati previsti;
- le realizzazioni dei progetti siano state portate a termine nei tempi previsti.

L'esito di tale valutazione è riportato nell'***allegato IV***.

Alcuni progetti mostrano i primi risultati, ma molti si trovano ad affrontare sfide operative e ritardi

83 La Corte ha riscontrato che tutti i progetti contribuiscono a perseguire gli obiettivi previsti da Europa digitale nell'ambito della cibersicurezza[14] e che perseguono la maggior parte degli obiettivi indicati negli inviti a presentare proposte[15].

84 Degli 11 progetti inclusi nel campione della Corte, due erano in una fase iniziale di attuazione: non è stato dunque possibile trarre conclusioni sulla loro performance. Per quanto riguarda i rimanenti, quattro sono stati giudicati soddisfacenti in termini di conseguimento delle realizzazioni e dei risultati previsti, due presentano alcune fragilità e tre sono stati giudicati insoddisfacenti (cfr. ***allegato IV***).

85 Europa digitale ha come obiettivo dichiarato l'aumento del livello di cibersicurezza delle piccole e medie imprese (PMI). In tal senso, diversi progetti offrono soluzioni concrete per le PMI (cfr. ***riquadro 2***).

---

[14] Articolo 6 del regolamento (UE) 2021/694 che istituisce il programma Europa digitale.

[15] Inviti a presentare proposte: Sviluppo delle capacità dei centri operativi di sicurezza; Dispiegamento della rete di centri nazionali di coordinamento con gli Stati membri; Sostegno alla preparazione e assistenza reciproca; Nuove applicazioni dell'IA e di altre tecnologie abilitanti per i centri operativi di sicurezza.

Riquadro 2

Esempi di progetti che producono risultati tangibili per le PMI

Il progetto GR-SME-SOC (progetto 6 nell'***allegato III***) mira a fornire strumenti e servizi di cibersicurezza alle PMI in Grecia istituendo un centro operativo di sicurezza (SOC) adeguato alle loro esigenze. Il progetto, avviato nel gennaio 2024, viene attuato da un consorzio di cinque organizzazioni greche. L'obiettivo è offrire servizi gratuiti di cibersicurezza a 120 PMI per un anno, dopo il quale i servizi diventeranno disponibili sul mercato. Alle PMI verranno offerti servizi avanzati quali il monitoraggio in tempo reale, l'individuazione delle minacce tramite l'IA e una risposta agile agli incidenti.

Tramite il progetto NCC-IE (progetto 3 nell'***allegato III***), il coordinatore del progetto ha fornito circa 1,8 milioni di euro in sovvenzioni a oltre 50 PMI irlandesi per migliorare la loro cibersicurezza. Il regime di sovvenzioni è andato a beneficio di imprese dai 2 ai 200 dipendenti circa, tra cui imprese a conduzione familiare, start-up ed esportatori mondiali in vari settori. Le sovvenzioni erano destinate esclusivamente a società che erano state precedentemente sottoposte a un esame della cibersicurezza gestita dall'ente pubblico Enterprise Ireland. La sovvenzione ha coperto l'80 % dei costi (fino a 60 000 euro) per attuare le raccomandazioni emerse da detto esame.

Fonte: Corte dei conti europea.

86 Molti progetti inclusi nel campione della Corte faticano a rispettare le scadenze o si trovano ad affrontare sfide operative (cfr. ***allegato IV***). La Corte ha riscontrato che quattro progetti stanno subendo notevoli ritardi. Ciò comprende ENSOC e ATHENA, come specificato ai paragrafi ***65***-***70***. Nel ***riquadro 3*** sono forniti alcuni esempi.

Riquadro 3

Esempi di progetti che affrontano sfide operative e ritardi

In Irlanda la "Local Government Management Authority" è l'unico beneficiario della sovvenzione per il progetto ILG-SOC (progetto 8 nell'***allegato III***). Tale progetto, inaugurato nell'ottobre 2023 per la durata di tre anni, ha l'obiettivo di istituire un centro operativo di sicurezza centrale grazie al quale 31 autorità locali potranno utilizzare strumenti avanzati per l'individuazione delle minacce e la risposta alle stesse. La revisione intermedia ha portato al rigetto di tutte le realizzazioni. Il progetto comprende diverse procedure di appalto che hanno avuto esito negativo o hanno subìto ritardi; la sua durata verrà quindi estesa (senza ulteriori finanziamenti), permettendogli forse di disporre di tempo sufficiente per concludersi con successo.

In Grecia, il progetto EL-SOC (progetto 5 nell'***allegato III***) mira a istituire un SOC consolidato a livello nazionale, che riunisca le informazioni provenienti dai SOC settoriali: al fine fornire una panoramica completa e in tempo reale della situazione della cibersicurezza. Il periodo di svolgimento del progetto va da gennaio 2024 a dicembre 2026. L'appalto previsto per hardware e servizi ha subìto ritardi a causa di problemi nella finalizzazione e nella pubblicazione delle specifiche tecniche del bando di gara. Tra i motivi del ritardo, il coordinatore del progetto ha menzionato anche problemi relativi alla garanzia del cofinanziamento nazionale e alla limitata disponibilità di personale addetto agli appalti

Fonte: Corte dei conti europea.

87 Tra gli altri progetti inclusi nel campione della Corte, due registrano ritardi moderati, tre hanno prodotto le loro realizzazioni nei tempi previsti e, infine, due sono in una fase iniziale di attuazione;non è pertanto ancora possibile trarre conclusioni.

Le restrizioni di sicurezza hanno comportato sfide operative e, quando i controlli sono effettuati dai beneficiari, vi sono rischi significativi

88 Il regolamento Europa digitale prevede che, per ragioni di sicurezza, i finanziamenti per la cibersicurezza siano limitati a soggetti con sede nell'UE e controllati da Stati membri o cittadini dell'UE. Tale restrizione mira ad attenuare il rischio di intrusione o influenza da parte di paesi non-UE e a impedire che informazioni sensibili in materia di sicurezza siano condivise con autorità di paesi terzi.

89 L'obbligo dell'UE in materia di proprietà e controllo si applica non solo ai beneficiari delle sovvenzioni, ma anche ai loro subappaltatori e a qualsiasi destinatario di sostegno finanziario a terzi. Fatta eccezione per quest'ultima categoria (cfr. paragrafi ***92***-***96***), la valutazione è effettuata dal Servizio centrale di convalida dell'Agenzia esecutiva europea per la ricerca. Tuttavia, la decisione finale sull'ammissibilità a partecipare agli inviti ristretti a presentare proposte spetta ancora all'autorità che concede l'aiuto, ossia la DG Connect o l'ECCC.

90 Nel corso del lavoro di audit della Corte, i beneficiari hanno ripetutamente menzionato le sfide pratiche poste dalle valutazioni dell'assetto proprietario e del controllo. Tali processi di valutazione nel contesto dell'UE possono essere lunghi e complessi: richiedono infatti l'analisi dell'intero assetto proprietario e della catena di controllo di ciascuna organizzazione, compresi tutti i livelli di proprietà fino ai proprietari finali. Il servizio centrale di convalida richiede che ciascun soggetto fornisca ampie prove documentali del proprio assetto proprietario e dei propri diritti specifici, del governo societario e di qualsiasi legame commerciale, finanziario o di altro tipo che conferisca il controllo.

91 In tre progetti finanziati dall'UE inclusi nel campione della Corte, almeno un beneficiario di un consorzio è stato successivamente escluso perché considerato di proprietà o controllato da paesi terzi. L'esclusione dei membri del consorzio dimostra che il concetto di proprietà e controllo dell'UE non è stato pienamente compreso da tutti i partecipanti di Europa digitale. Nel complesso, sulla base dei dati del Servizio centrale di convalida, il 7 % di tutti i richiedenti o subappaltatori di sovvenzioni di Europa digitale nell'ambito della cibersicurezza non ha superato la valutazione nel periodo 2022-2025. Le candidature agli inviti a presentare proposte da parte di partecipanti non ammissibili causano ritardi, come illustrato nel ***riquadro 4***.

Riquadro 4

Esempio di un caso in cui i beneficiari sono stati esclusi dopo il mancato superamento dei controlli di sicurezza

Due membri del consorzio del progetto NG-SOC (progetto 7 nell'***allegato III***) non hanno superato la valutazione dell'assetto proprietario e del controllo. L'esito è stato annunciato circa un mese prima del termine ultimo per la firma della convenzione di sovvenzione. Il coordinatore del progetto ha dovuto accettare di assumersi il lavoro assegnato ai due membri esclusi, in quanto non vi era tempo per trovare un nuovo partner. Uno dei membri esclusi apparteneva a un settore specifico in cui la soluzione sviluppata doveva essere sperimentata; pertanto, una parte significativa del progetto, che riguardava la sperimentazione pratica delle soluzioni, non ha potuto procedere come previsto. Successivamente si è giunti a una soluzione modificando la convenzione di sovvenzione per includere nuovi membri.

Fonte: Corte dei conti europea.

92 Due progetti esaminati dalla Corte (NCC-IE e CYberSynchrony) forniscono sostegno finanziario a terzi; tale meccanismo consente ai beneficiari di sovvenzioni di utilizzare parte di esse per finanziare altri soggetti attraverso inviti aperti, facilitando così l'accesso ai finanziamenti dell'UE. In questo caso, i beneficiari sono i soli responsabili della conduzione delle valutazioni dell'assetto proprietario e del controllo e il servizio centrale di convalida non è coinvolto.

93 Nel 2021 la Commissione ha pubblicato orientamenti pubblici generali per i candidati agli inviti ristretti a presentare proposte, aggiornati nel 2026. Nonostante il sostegno finanziario a terzi sia utilizzato dal 2021 per gli inviti di Europa digitale, né la Commissione né l'ECCC hanno fornito ai beneficiari una metodologia dettagliata su come effettuare le valutazioni dell'assetto proprietario e del controllo nei confronti dei paesi non-UE ai quali forniscono sostegno finanziario. Nel luglio 2025 l'ECCC ha condiviso orientamenti non obbligatori, fornendo alla rete dei centri nazionali di coordinamento un approccio strutturato per le valutazioni dell'assetto proprietario e del controllo. Il documento di orientamento illustra princìpi generali e misure che potrebbero essere adottate. Tuttavia, gli orientamenti non specificano le modalità di esecuzione dei controlli, lasciando ai beneficiari la responsabilità di sviluppare il proprio approccio.

94 La Corte ha riscontrato che l'ECCC non convalida la metodologia adottata dai beneficiari né effettua controlli a campione per garantire che la metodologia sia sufficientemente solida e che i destinatari selezionati del sostegno finanziario siano effettivamente di proprietà e sotto il controllo di entità UE.

95 Nel rapporto annuale del 2024 la Corte ha riscontrato che i beneficiari incaricati dalla Commissione di gestire il sostegno finanziario a terzi non sono tenuti a dimostrare che i controlli da loro effettuati consentano di garantire efficacemente la regolarità della spesa dell'UE. Analogamente, l'ECCC non valuta la capacità amministrativa e tecnica dei beneficiari di gestire correttamente le valutazioni dell'assetto proprietario e del controllo. Come specificato al paragrafo ***90***, tale valutazione può essere complessa ed è effettuata a livello dell'UE da un servizio dedicato con competenze specialistiche.

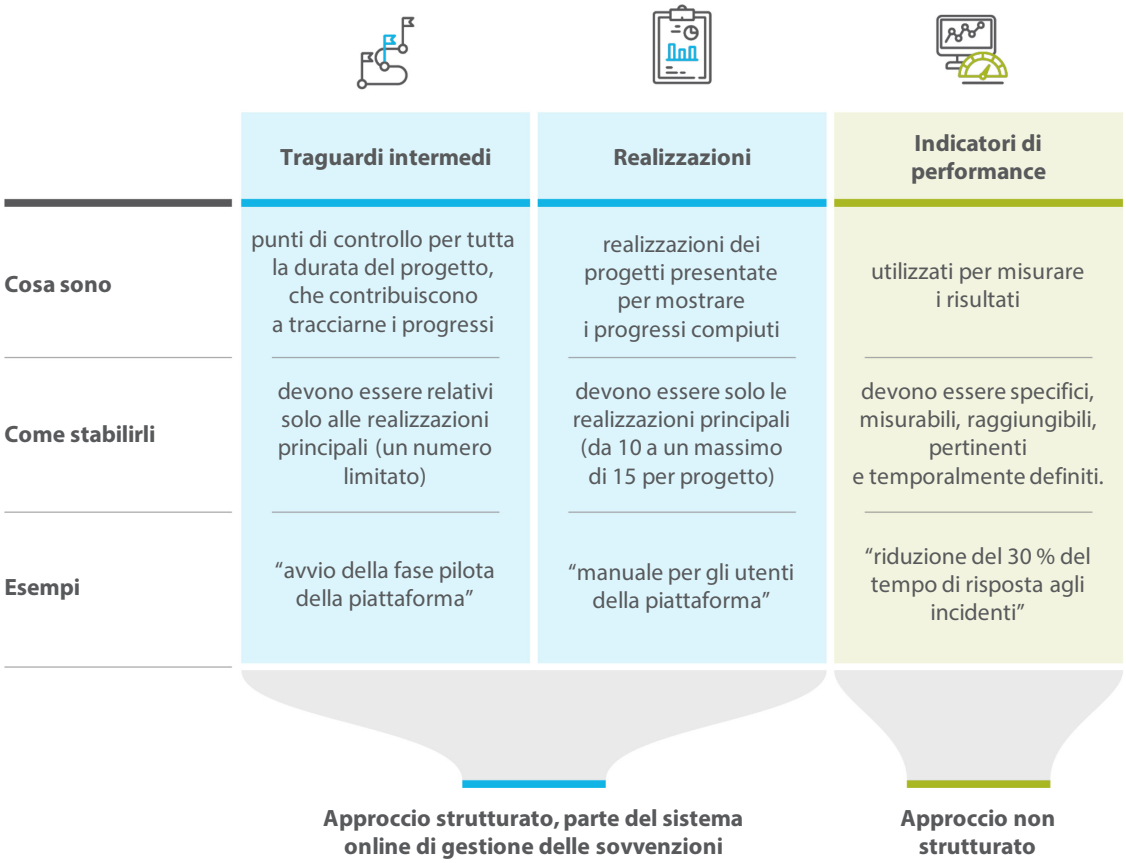
96 In tale contesto, la Corte ritiene che vi sia un rischio significativo che i beneficiari, responsabili dell'esecuzione delle valutazioni dell'assetto proprietario e del controllo, non abbiano la capacità di eseguirle correttamente. Data la natura delle attività finanziate, questa carenza potrebbe mettere a rischio infrastrutture sensibili, dati operativi e tecnologie critiche per la sicurezza.

La maggior parte dei progetti finanziati dall'UE dispone di quadri di performance inadeguati e i dati di Europa digitale sulla performance relativi alla cibersicurezza non sono precisi

La maggior parte dei progetti finanziati dall'UE dispone di quadri di performance inadeguati

97 I beneficiari che gestiscono progetti finanziati dall'UE devono riferire all'ECCC in merito ai loro progressi, utilizzando traguardi intermedi, realizzazioni ed indicatori, come illustrato nella ***figura 8***. La Corte ha valutato se i traguardi intermedi e le realizzazioni stabilite per ciascun progetto permettano di svolgere adeguatamente il monitoraggio dei progetti e se i relativi indicatori di performance siano pertinenti e misurabili, nonché abbiano un valore di base e un valore-obiettivo.

Figura 8 | Traguardi intermedi, realizzazioni e indicatori di performance nei progetti di Europa digitale



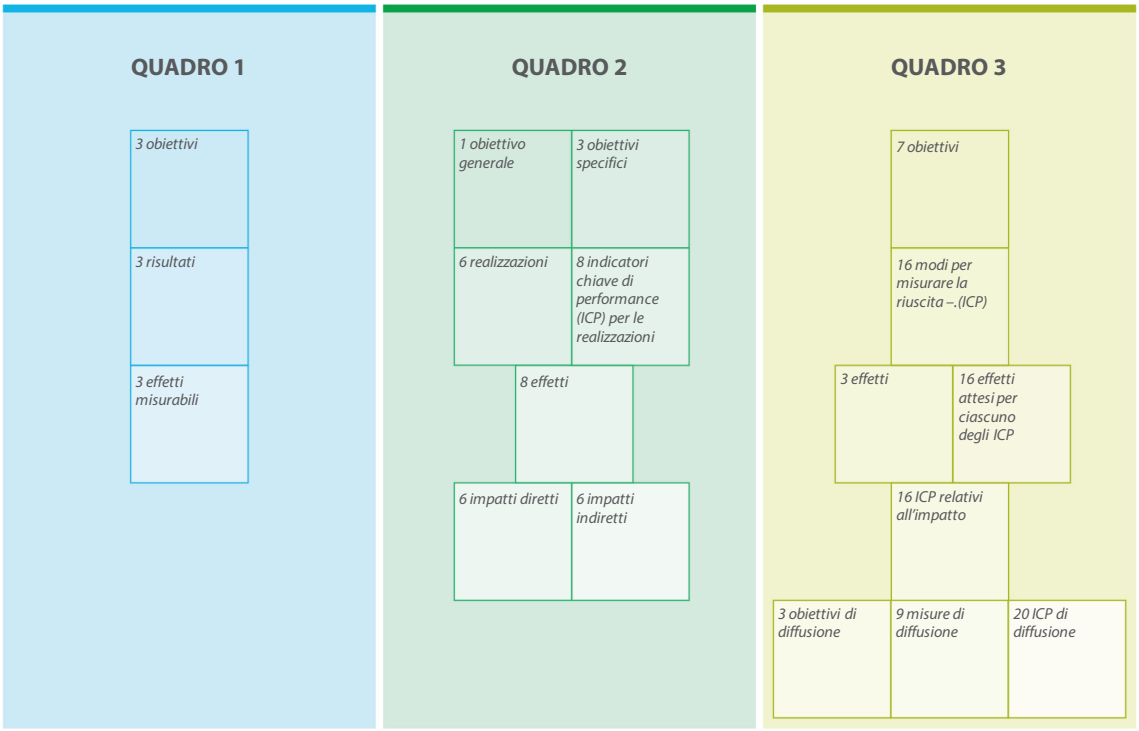
Fonte: Corte dei conti europea, sulla base della domanda di sovvenzione

98 Nella loro proposta di progetto, i beneficiari devono stabilire una serie di traguardi intermedi e di realizzazioni seguendo un approccio strutturato specificato nelle istruzioni per i candidati. Tutti i traguardi intermedi e le realizzazioni sono elencati nel sistema online di gestione delle sovvenzioni per facilitarne il follow-up. L'ECCC di solito esamina due volte ciascun progetto: una prima volta a metà del progetto e una seconda a progetto completato. Nel corso di tali esami, gli esperti esterni verificano il conseguimento dei traguardi intermedi e delle realizzazioni e l'ECCC li convalida: questi due elementi sono dunque essenziali per il monitoraggio dei progetti e dovrebbero essere definiti in modo adeguato.

99 La Corte ha riscontrato che quasi nessuno dei progetti inclusi nel campione ha seguito le istruzioni relative al numero di traguardi intermedi e realizzazioni: il numero di traguardi intermedi per progetto varia da 8 a 39, mentre il numero di realizzazioni varia da 8 a 45. Molti traguardi intermedi e realizzazionii non rispettano le istruzioni su come dovrebbero essere definiti e, pertanto, non sono utili per monitorare i progressi (ad esempio, "riunione per avviare la redazione dell'invito a presentare proposte di ricerca" o "verbale formale della riunione di progetto"). Per tre progetti, il comitato di valutazione aveva individuato tali problemi prima della firma della sovvenzione: in due casi, i beneficiari hanno proposto solo modifiche minori (ad esempio, ai termini ultimi) senza affrontare le questioni fondamentali, mentre nel terzo caso non è stata apportata alcuna modifica. Per altri sei progetti inclusi nel campione, dall'analisi della Corte emerge che i traguardi intermedi o le realizzazioni non sono in linea con le istruzioni e non sono sempre appropriati. La Corte conclude che, qualora i traguardi intermedi o le realizzazioni siano mal definiti o siano troppi, risulta difficile monitorare i progressi compiuti.

100 Contrariamente ai traguardi intermedi e alle realizzazioni, gli indicatori di performance non seguono un approccio strutturato e non sono raccolti in una tabella del sistema di gestione delle sovvenzioni, ma sono invece reperibili in diverse sezioni della proposta. Questo approccio ha portato a una molteplicità di quadri di riferimento per la verifica della performance proposti dai beneficiari: alcuni hanno fissato solo gli obiettivi del progetto con i connessi indicatori di performance, mentre altri hanno istituito quadri di riferimento per la performance molto più complessi. Nella ***figura 9*** sono forniti alcuni esempi.

Figura 9 | Esempio della molteplicità di quadri di riferimento della performance concepiti per i progetti



Fonte: Corte dei conti europea.

101 La Corte ha riscontrato che molti degli indicatori di performance utilizzati nei progetti non sono pertinenti o non sono misurabili e mancano di un valore-obiettivo o di un valore di base (cfr.***riquadro 5***). Inoltre, sette progetti hanno definito 20 o più indicatori, mentre un progetto ne ha definiti 52. L'esito di tale valutazione è riportato nell'***allegato IV***.

Riquadro 5

Esempi di indicatori di performance inadeguati

Non misurabili

- "L'indicatore di compromissione e altri servizi forniti rafforzano le capacità di cibersicurezza delle PMI"
- "La fornitura di strumenti e metodi di risposta agli incidenti che consentano l'integrazione con i canali di comunicazione EU-CyCLONe"

Senza valore di base o valore-obiettivo

- "Miglioramento ≥ 20 % nella preparazione del personale"
- "Riduzione ≥ 20 % degli sforzi necessari per allinearsi e conformarsi alle pertinenti iniziative dell'UE in materia di cibersicurezza"

Non legati alla performance

- "Relazione finale sul progetto al termine della fase di finanziamento"
- "Numero di tirocinanti che parteciperanno a tutte le sessioni di formazione"

Fonte: Corte dei conti europea, sulla base della documentazione dei progetti.

102 Nel complesso, la Corte ritiene che l'ampia varietà di quadri di riferimento della performance, la scarsa definizione degli indicatori e il loro numero eccessivo complichino notevolmente il monitoraggio della performance dei progetti, rendendone quindi impossibile la corretta valutazione. Quest'ultima è ulteriormente ostacolata dal fatto che il modello di rendicontazione non contiene una sezione dedicata agli indicatori di performance dei progetti e, di conseguenza, la maggior parte dei progetti inclusi nel campione della Corte non ha riferito su questi aspetti.

I dati sulla performance relativi alla componente di cibersicurezza di Europa digitale non sono precisi

103 Per monitorare quanto conseguito da Europa digitale, il regolamento prevede indicatori di programma sui quali tutti i progetti devono riferire, come illustrato nel ***riquadro 6***.

Riquadro 6

Indicatori di Europa digitale per la cibersicurezza

3.1 Numero di infrastrutture o strumenti di cibersicurezza, o di entrambi, acquisiti congiuntamente anche nell'ambito del sistema europeo di allerta per la cibersicurezza.

3.1.b. "*Cybersecurity infrastructure and/or tools deployed*" (Numero di infrastrutture e/o strumenti di cibersicurezza impiegati)

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

3.3 Numero di azioni a sostegno della preparazione e della risposta agli incidenti di cibersicurezza nell'ambito del meccanismo per le emergenze di cibersicurezza

Fonte: Allegato II del regolamento (UE) 2021/694 che istituisce il programma Europa digitale; quadro di monitoraggio e valutazione per il programma Europa digitale, SWD(2024) 37).

104 La Corte ha verificato se i progetti inclusi nel campione avessero riferito in merito a tali indicatori e ha esaminato il modo in cui l'ECCC raccoglie e verifica tali dati.

105 Tutti i progetti sono tenuti a riferire in merito agli indicatori di Europa digitale prima della loro revisione intermedia e finale nel sistema di gestione delle sovvenzioni. Dall'audit è emerso che, dei sette progetti che erano allora a metà del loro svolgimento, e che avrebbero dunque dovuto riferire in merito a tali indicatori, solo tre lo avevano fatto. Di questi tre, due non avevano comunicato informazioni precise: uno ha riferito in merito a un indicatore errato, l'altro ha fornito valori-obiettivo anziché risultati conseguiti.

106 Ogni anno la Commissione riferisce in merito a tali indicatori nelle dichiarazioni sulla performance dei programmi, le quali permettono ai portatori di interessi di valutare se il programma in questione stia conseguendo i propri obiettivi. Secondo le dichiarazioni sulla performance dei programmi del 2024, dagli indicatori di Europa digitale per la cibersicurezza risulta che si è sulla buona strada. L'ECCC ha spiegato alla Corte di aver utilizzato una serie di indagini mediante questionario inviate ai beneficiari dei progetti per compilare tali indicatori, invece di basarli sul sistema di gestione delle sovvenzioni. La Corte ha esaminato i dati disaggregati forniti dall'ECCC e ha riscontrato numerosi problemi nelle modalità di raccolta degli stessi e nella loro qualità complessiva: i dati raccolti, infatti, non corrispondono ai valori presentati nella dichiarazione sulla performance dei programmi; pertanto, non è chiaro come siano stati calcolati i valori comunicati. e non ha inoltre riscontrato alcun elemento attestante che l'ECCC abbia verificato l'accuratezza di tali dati. Sulla base dei controlli svolti sui progetti inclusi nel campione, poiché la maggior parte dei valori è mancante o imprecisa, la Corte ritiene che i dati comunicati non riflettano adeguatamente i risultati conseguiti.

La presente relazione è stata adottata dalla Sezione III, presieduta da George Marius Hyzler, Membro della Corte, a Lussemburgo nella riunione del 16 giugno 2026.

Per la Corte dei conti europea

Tony Murphy
Presidente

Allegati

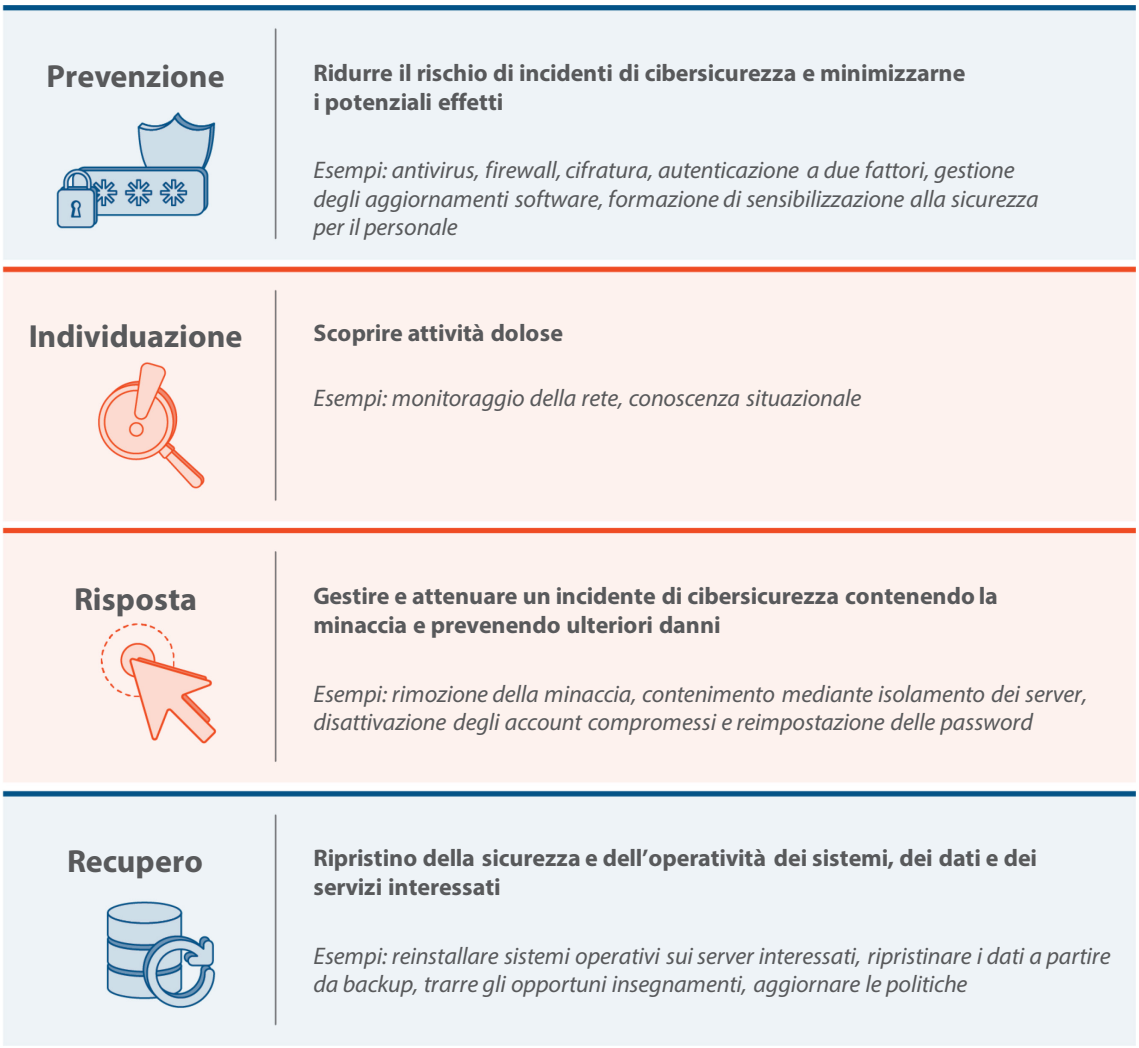
Allegato I – L'audit

01 La cibersicurezza è definita come "l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche"[1]. Per minaccia informatica si intende "qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo sui sistemi informativi e di rete, sugli utenti di tali sistemi e altre persone"[2]. La cibersicurezza richiede un approccio olistico, che consiste in una serie di attività interconnesse al fine di prevenire, monitorare, rispondere alla minacce informatiche e riprendersi dalle stesse, come illustrato nella ***figura 1***.

[1] Regolamento (UE) 2019/881 (regolamento sulla cibersicurezza).

[2] Articolo 2 del regolamento sulla cibersicurezza.

Figura 1 | Esempi di attività di cibersicurezza

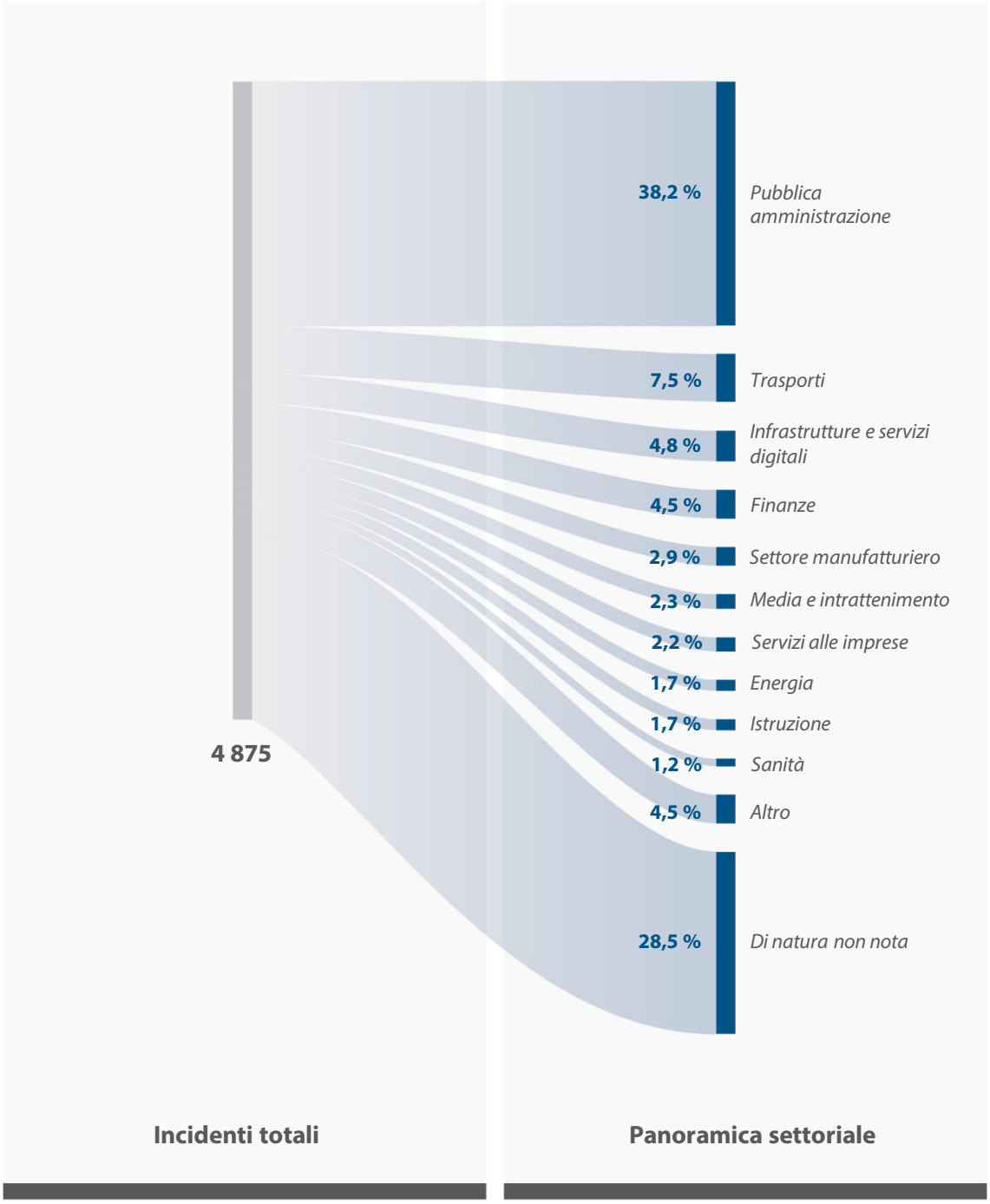


Fonte: Corte dei conti europea, sulla base del considerando 78 della direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza (direttiva NIS 2).

02 L'Agenzia dell'Unione europea per la cibersicurezza (ENISA) stima che l'entità delle minacce informatiche sia notevole e sottolinea come il panorama di tali minacce stia diventando sempre più complesso[3]. Queste minacce sottolineano l'importanza vitale della cibersicurezza in economie società sempre più digitalizzate. Nella relazione sul panorama delle minacce del 2025, l'ENISA ha identificato i *ransomware* come la minaccia più critica nell'UE. La ***figura 2*** illustra i settori presi di mira.

[3] ENISA, Relazione 2024 sullo stato della cibersicurezza nell'Unione.

Figura 2 | Settori presi di mira dagli attacchi informatici



Fonte: Corte dei conti europea, sulla base di documenti dell'ENISA.

Incidenti di cibersicurezza significativi e su vasta scala

03 Gli incidenti di cibersicurezza, tra cui sono incluse le minacce informatiche e gli eventi involontari (come quelli riportati nella ***figura 3*** e al paragrafo ***40***), "possono impedire la fornitura di servizi pubblici e l'esercizio delle attività economiche,[…] provocare ingenti perdite finanziarie, minare la fiducia degli utenti e causare gravi danni all'economia e ai sistemi democratici dell'Unione e potrebbero persino avere conseguenze sulla salute o essere potenzialmente letali".[4] Un incidente di cibersicurezza può essere classificato come[5]:

- **significativo**, se "ha causato o è in grado di causare una grave perturbazione operativa dei servizi o perdite finanziarie per il soggetto interessato", oppure se "si è ripercosso o è in grado di ripercuotersi su altre persone fisiche o giuridiche causando perdite materiali o immateriali considerevoli";

- **su vasta scala**, se "causa un livello di perturbazione superiore alla capacità di uno Stato membro di rispondervi o […] ha un impatto significativo su almeno due Stati membri".

04 Un incidente di cibersicurezza su vasta scala può degenerare in una vera e propria **crisi informatica dell'UE** se compromette il corretto funzionamento del mercato interno o comporta gravi rischi di pubblica sicurezza per soggetti o cittadini in diversi Stati membri o nell'intera Unione[6].

---

[4] Considerando 2 del regolamento (UE) 2025/38 (regolamento sulla cibersolidarietà).

[5] Articoli 6 e 23 della direttiva NIS 2, ulteriormente chiarito nel regolamento di esecuzione (UE) 2024/2690 della Commissioneper un numero di fornitori di servizi nel settore delle infrastrutture digitali.

[6] Considerando 69 della direttiva NIS 2.

Quadro strategico dell'UE

05 L'ecosistema della cibersicurezza dell'UE è complesso e stratificato, interessa trasversalmente vari ambiti d'intervento interni, come la giustizia e gli affari interni, il mercato unico digitale e le politiche in materia di ricerca[7]. In politica estera, la cibersicurezza svolge un ruolo di primo piano nella diplomazia ed è sempre più parte dell'emergente politica di difesa dell'UE[8].

06 Negli ultimi anni, l'UE ha potenziato il proprio quadro di regolamentazione della cibersicurezza. La seguente ***figura 3*** illustra le norme e gli strumenti strategici più pertinenti a livello dell'UE. In linea con il suo approccio di audit (cfr. paragrafi ***13***-***14***), la Corte ha posto la propria attenzione sugli strumenti che si occupano dell'individuazione di incidenti di cibersicurezza significativi o su vasta scala e della risposta agli stessi.

[7] Documento di riflessione della Corte dei conti europea sulle sfide insite in un'efficace politica dell'UE in materia di cibersicurezza", pag. 12.

[8] Per esempio, la posizione dell'UE in materia di deterrenza informatica (2022), il quadro per una risposta coordinata dell'UE alle campagne ibride (2022),la politica europea in materia di ciberdifesa (2023) e il pacchetto di strumenti della diplomazia informatica rivisto (2023).

Figura 3 | Strumenti strategici pertinenti dell'UE

Fonte: Corte dei conti europea.

Ruoli e responsabilità

07 Il panorama della cibersicurezza dell'UE coinvolge numerosi soggetti pubblici e privati, a livello regionale, nazionale e dell'UE, nella sfera civile, compresi gli organismi incaricati di far rispettare la legge. La cibersicurezza è inoltre un elemento essenziale della sicurezza e difesa nazionali[9]. L'***allegato II*** illustra l'attuale panorama dell'UE.

08 La responsabilità primaria della prevenzione degli incidenti e delle crisi di cibersicurezza, nonché della preparazione e della risposta agli stessi, spetta agli Stati membri. Secondo l'articolo 4, paragrafo 2, del trattato sull'Unione europea, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro. Poiché gli incidenti di cibersicurezza potrebbero perturbare e danneggiare le infrastrutture critiche informatizzate, da cui dipende il buon funzionamento del mercato interno, l'UE svolge un ruolo importante anche in caso di incidenti o crisi significativi[10]. I principali attori a livello dell'UE sono elencati nella ***figura 4***.

[9] Parere 02/2023 sulla proposta di regolamento sulla cibersolidarietà.

[10] Programma dell'UE per la gestione delle crisi informatiche.

Figura 4 | Attori a livello dell'UE con un ruolo chiave nella cibersicurezza

Fonte: Corte dei conti europea.

Finanziamenti dell'UE

09 Nell'ambito dell'attuale quadro finanziario pluriennale 2021-2027, la principale fonte di finanziamenti per la cibersicurezza è il programma Europa digitale (Europa digitale). Tale programma, avviato nel 2021, è il primo ad avere come obiettivo specifico la trasformazione digitale dell'UE, e dispone di una dotazione finanziaria complessiva di 8,1 miliardi di euro[11].

10 Europa digitale finanzia le azioni di cibersicurezza nell'ambito dell'obiettivo specifico 3 "Cibersicurezza e fiducia". Più precisamente, vi è una dotazione finanziaria di 1,4 miliardi di euro per:

- rafforzare la coordinazione in ambito di cibersicurezza fra gli strumenti e le infrastrutture di dati degli Stati membri.
- sostenere un'ampia diffusione di soluzioni di cibersicurezza in tutti i settori economici.

11 La maggior parte dei finanziamenti di Europa digitale per la cibersicurezza è erogata mediante inviti a presentare proposte: da novembre 2021 a dicembre 2025 sono stati indetti 12 inviti. I finanziamenti dell'UE per questi inviti ammontano a 825 milioni di euro. Sono previsti nuovi inviti a presentare proposte per il 2026 e il 2027, al fine di attribuire altri 212 milioni di euro in sovvenzioni.

12 Un altro importante programma dell'UE a sostegno della cibersicurezza è Orizzonte Europa. I progetti di cibersicurezza sono finanziati principalmente nel contesto del polo tematico 3 ("Sicurezza civile per la società") e sono in genere ancora in una fase preliminare, dal momento che Orizzonte Europa è incentrato principalmente sulla ricerca e l'innovazione. Anche il dispositivo per la ripresa e la resilienza fornisce finanziamenti per le misure di cibersicurezza.

[11] Programma Europa digitale.

Estensione e approccio dell'audit

13 L'aumento delle minacce alla cibersicurezza e il loro impatto potenziale hanno messo in luce la necessità di rafforzare la nostra ciberresilienza collettiva. L'obiettivo dell' audit della Corte è stato valutare se le azioni dell'UE siano efficaci nel facilitare l'individuazione di incidenti di cibersicurezza significativi o su vasta scala e la risposta agli stessi. In particolare, la Corte ha valutato se ciò avvenisse per:

- reti e meccanismi a livello dell'UE (come, ad esempio, la rete di CSIRT, EU-CyCLONe, il sistema europeo di allerta per la cibersicurezza, il centro di situazione e analisi informatiche e la riserva dell'UE per la cibersicurezza);
- le azioni finanziate nell'ambito di Europa digitale.

La Corte non si è occupata della cooperazione a livello dell'UE nel settore delle attività di contrasto, né delle azioni intraprese a livello dell'UE nel campo della deterrenza informatica attraverso misure diplomatiche e attività di difesa.

14 L'audit riguarda il periodo dal 2022 al 2025. e si basa su un'analisi dei documenti pertinenti, su visite di audit in tre stati membri (Irlanda, Grecia e Italia) e su questionari scritti e colloqui con i portatori di interessi pertinenti. La ***figura 5*** mostra in che modo la Corte ha ottenuto gli elementi probatori su cui ha basato le proprie osservazioni.

Figura 5 | Attività di audit espletate

Cosa è stato esaminato dalla Corte

- Il **quadro giuridico** applicabile all'individuazione degli incidenti di cibersicurezza significativi e su vasta scala e alla risposta agli stessi
- I **ruoli e le responsabilità** delle reti e delle strutture istituite a livello dell'UE

Cosa è stato analizzato

- Documenti sul funzionamento della **rete di CSIRT** e di **EU-CyCLONe**
- Documentazione sul **quadro di programmazione e monitoraggio della performance di Europa digitale**
- Documentazione su **13 azioni selezionate finanziate dall'UE** (11 sovvenzioni e 2 contratti – cfr.elenco dettagliato nell'allegato III)

* La Corte ha selezionato azioni finanziate dall'UE in tre paesi (Irlanda, Grecia e Italia) in cui i finanziamenti di Europa digitale pertinenti erano più rilevanti. Le 11 sovvenzioni sono state ricavate da un elenco di 137 progetti finanziati dall'UE pertinenti per l'individuazione delle minacce e la risposta alle stesse, al fine di coprire una combinazione diversificata di progetti.

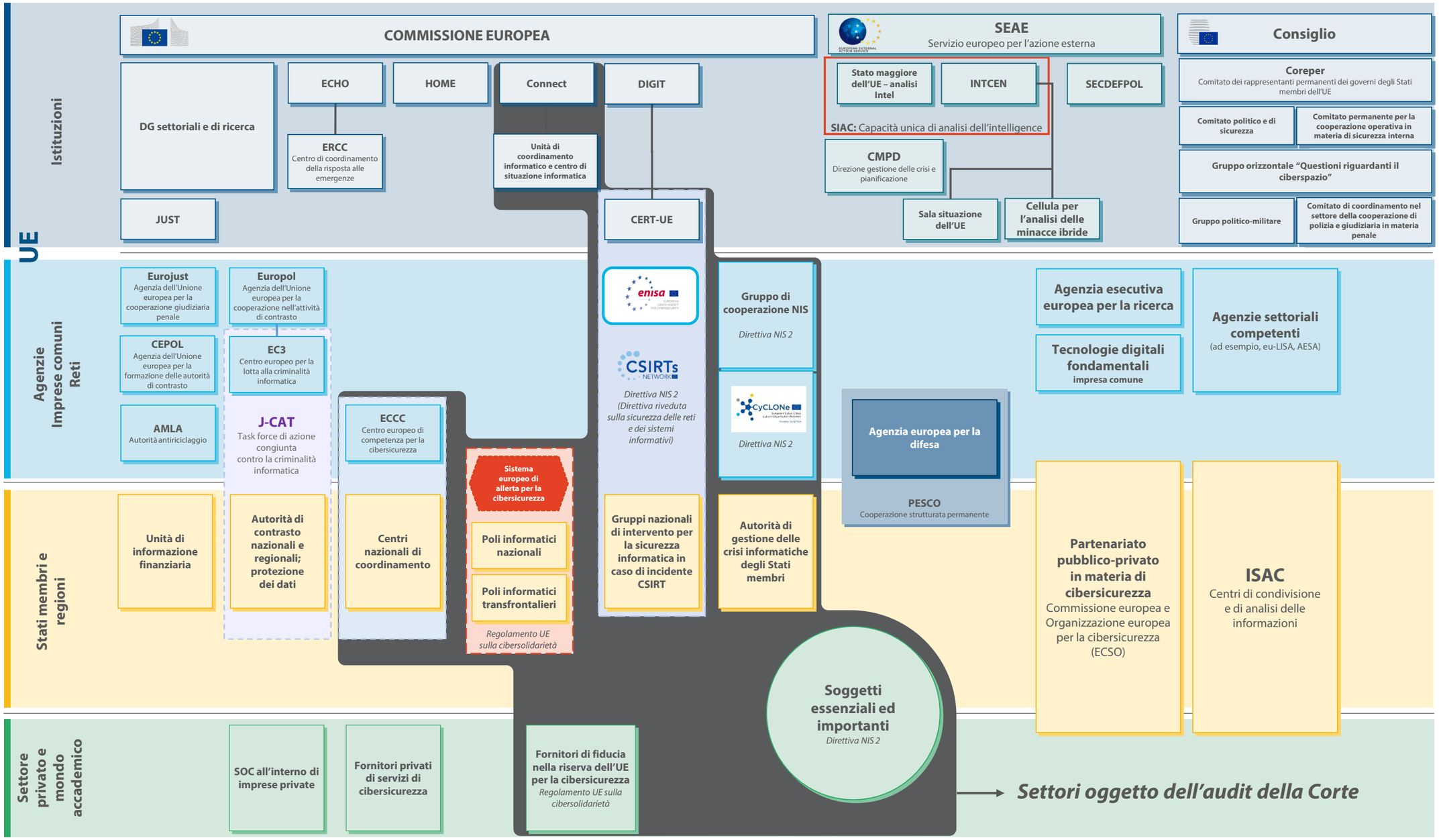
Con chi sono stati tenuti colloqui

- I beneficiari delle **11 sovvenzioni finanziate dall'UE incluse nel campione**
- I rappresentanti delle autorità nazionali per la cibersicurezza in **tre Stati membri** (Irlanda, Grecia e Italia)
- I rappresentanti della Commissione europea (**DG Connect**), dell'**ENISA** e dell'**ECCC**

Fonte: Corte dei conti europea.

15 La Corte ritiene che le proprie constatazioni possano contribuire a rendere più efficiente ed efficace l'individuazione e la risposta agli incidenti informatici significativi e su vasta scala e, al contempo, migliorare il modo in cui sono selezionate e monitorate le azioni finanziate dall'UE. La metodologia di audit della Corte rispetta i princìpi internazionali di audit dell'Organizzazione internazionale delle Istituzioni superiori di controllo (INTOSAI).

Allegato II – Il panorama della cibersicurezza dell'UE



DG Connect: direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie
DG ECHO: direzione generale per la Protezione civile e le operazioni di aiuto umanitario europee

DG HOME: direzione generale della Migrazione e degli affari interni
DG JUST: direzione generale della Giustizia e dei consumatori
DIGIT: direzione generale dei Servizi digitali
AESA: Agenzia dell'Unione europea per la sicurezza aerea

EU-CyCLONe: rete europea delle organizzazioni di collegamento per le crisi informatiche
eu-LISA: Agenzia dell'Unione europea per la gestione operativa dei sistemi IT su larga scala nello spazio di libertà, sicurezza e giustizia

INTCEN: Centro UE di situazione e di intelligence
SECDEFPOL: Politica di sicurezza e di difesa
SOC: *Security operations centre* (Centro operativo di sicurezza)

Allegato III – Azioni selezionate nell'ambito della cibersicurezza

Cod. identif.	Titolo	Paesi	Data di inizio	Data di fine	Costo totale (in milioni di euro) e contributo dell'UE (in percentuale)	Link al portale finanziamenti e gare d'appalto dell'UE.
Sovvenzioni per poli informatici transfrontalieri che fanno parte del sistema europeo di allerta per la cibersicurezza						
1	**Creazione di SOC transfrontalieri (ATHENA)**	Bulgaria, Grecia, Cipro; Malta	1.1.2024	31.3.2028	4,7 (50 %)	
2	**ENSOC-PIATTAFORMA TRANSFRONTALIERA (ENSOC)**	Spagna, Italia, Lussemburgo, Paesi Bassi, Austria, Portogallo, Romania	1.1.2024	30.6.2028	10,4 (50 %)	
Sovvenzioni per la realizzazione della rete di centri nazionali di coordinamento (NCC) negli Stati membri						
3	**Sviluppo e implementazione del centro nazionale di coordinamento e sviluppo per la cibersicurezza in Irlanda NCC-IE)**	Irlanda	2.10.2023	1.10.2026	4,2 (47 %)	
4	**Centro Nazionale di Coordinamento italiano (NCC-IT)**	Italia	1.11.2023	31.10.2025	2,0 (50 %)	

Cod. identif.	Titolo	Paesi	Data di inizio	Data di fine	Costo totale (in milioni di euro) e contributo dell'UE (in percentuale)	Link al portale finanziamenti e gare d'appalto dell'UE.
Sovvenzioni per sviluppare la capacità dei centri operativi di sicurezza (SOC), promuovere nuove applicazioni dell'IA e di altre tecnologie abilitanti per i SOC e fornire sostegno in materia di preparazione e assistenza reciproca.						
5	**Rafforzare la capacità del centro operativo di sicurezza ellenico consolidato (EL-SOC)**	Grecia, Cipro	1.1.2024	31.12.2026	9,7 (50 %)	
6	**Centro operativo di sicurezza greco per le piccole e medie imprese (GR-SME-SOC)**	Grecia	1.1.2024	31.12.2026	12,1 (50 %)	
7	**Centri operativi di sicurezza di prossima generazione (NG-SOC)**	Grecia, Spagna, Cipro, Lussemburgo, Slovenia, Norvegia	1.1.2024	31.12.2026	4,8 (50 %)	
8	**Centro operativo di sicurezza locale irlandese (ILG-SOC)**	Irlanda	1.10.2023	30.9.2026	8,3 (50 %)	
9	**Un ecosistema interconnesso di reti di coordinamento e risposta per la cibersicurezza**	Irlanda	1.1.2024	31.12.2026	3,6 (50 %)	
10	**Armonizzare persone, processi e tecnologie per una solida cibersicurezza (CYberSynchrony)**	Belgio, Grecia, Italia, Cipro, Paesi Bassi	1.6.2024	31.5.2027	7,0 (100 %)	
11	**Centri operativi di sicurezza cooperativi avanzati (ACSOC)**	Grecia, Italia, Romania	1.1.2025	31.12.2027	3,0 (50 %)	

Cod. identif.	Titolo	Paesi	Data di inizio	Data di fine	Costo totale (in milioni di euro) e contributo dell'UE (in percentuale)	Link al portale finanziamenti e gare d'appalto dell'UE.
Contratto quadro per l'azione di sostegno alla cibersicurezza di ENISA						
12	**Assistere ENISA nella fornitura di servizi nell'ambito dell'azione di sostegno alla cibersicurezza (28 lotti)**	27 lotti per gli Stati membri 1 lotto paneuropeo	1.12.2022[1]	31.12.2025	28,3 (100 %)	
Appalti di servizi per il centro di situazione e analisi informatiche della DG Connect						
13	**Servizio *ad hoc* per il supporto del centro di situazione e analisi informatiche della Commissione europea**	-	30.12.2022	30.12.2026	18,0 (100 %)	

Fonte: Corte dei conti europea.

[1] Vari contratti firmati nel corso del mese di Dicembre 2022

Allegato IV – Valutazione della Corte sui progetti in ambito di cibersicurezza finanziati dall'UE

Livello soddisfacente *Alcune criticità*
Livello insoddisfacente *Impossibile trarre conclusioni (troppo presto)*

Cod. identif.	Progetto	Il progetto risponde alla maggior parte delle esigenze individuate nell'invito	Il progetto ha finora conseguito le realizzazioni e i risultati previsti	Le realizzazioni del progetto sono state realizzate entro la data prevista	Gli indicatori di performance del progetto sono pertinenti, misurabili, hanno un valore di base e un valore-obiettivo.
1	Creazione di SOC transfrontalieri (ATHENA)				
2	ENSOC-PIATTAFORMA TRANSFRONTALIERA (ENSOC)				
3	Sviluppo e messa in opera del centro nazionale di coordinamento e sviluppo per la cibersicurezza in Irlanda (NCC-IE)				
4	Centro Nazionale di Coordinamento italiano (NCC-IT)				
5	Rafforzare la capacità del centro operativo di sicurezza ellenico consolidato (EL-SOC)				
6	Centro operativo di sicurezza greco per le piccole e medie imprese (GR-SME-SOC)				
7	Centri operativi di sicurezza di prossima generazione (NG-SOC)				
8	Centro operativo di sicurezza locale irlandese (ILG-SOC)				
9	Un ecosistema interconnesso di reti di coordinamento e risposta per la cibersicurezza (Cyber-CORE-Network)				
10	Armonizzare persone, processi e tecnologie per una solida cibersicurezza (CYberSynchrony)				
11	Centri operativi di sicurezza cooperativi avanzati (ACSOC)				

Acronimi

Acronimo	Definizione/Spiegazione
CSIRT	Gruppo di intervento per la sicurezza informatica in caso di incidente
DG Connect	direzione generale delle Reti di comunicazione, dei contenuti e delle tecnologie
ECCC	Centro europeo di competenza per la cibersicurezza
ENISA	Agenzia dell'Unione europea per la cibersicurezza
EU-CyCLONe	Rete europea delle organizzazioni di collegamento per le crisi informatiche
NCC	Centro nazionale di coordinamento
NIS	sicurezza delle reti e dell'informazione
PMI	piccola o media impresa
SAG	gruppo consultivo strategico
SOC	Centro operativo di sicurezza

Glossario

Lemma	Definizione/Spiegazione
Autori delle minacce	individui o gruppi che, intenzionalmente, causano danni, perturbano i servizi o rubano dati approfittando delle vulnerabilità dei sistemi, delle reti e dei dispositivi informatici.
Centro operativo di sicurezza	unità organizzativa che opera per prevenire minacce e incidenti informatici e raccoglie le relative informazioni di intelligence.
Ciberincidente	evento che compromette la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati o dei sistemi di informazione.
Incidente di cibersicurezza significativo	incidente di cibersicurezza che ha causato o può causare gravi perturbazioni o perdite finanziarie per un'organizzazione, o danni considerevoli ad altri soggetti o persone.
Incidente di cibersicurezza su vasta scala	incidente di cibersicurezza che è troppo grave perché uno Stato membro possa gestirlo da solo o che ha un impatto significativo su almeno due Stati membri.
Minaccia informatica	potenziale utilizzo del ciberspazio per compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati o dei sistemi di informazione.
Polo informatico	piattaforma centrale che riunisce vari servizi, strumenti e professionisti informatici per migliorare il monitoraggio, l'individuazione e l'analisi delle minacce informatiche, la prevenzione degli incidenti di cibersicurezza e il supporto all'elaborazione di analisi delle minacce informatiche.
Ransomware	malware che impedisce alle vittime di accedere a un sistema informatico o di leggere i file, costringendole a pagare un riscatto per ripristinare l'accesso.
Tassonomia	nell'ambito della cibersicurezza, uno schema di classificazione utilizzato per organizzare, categorizzare e strutturare le conoscenze su concetti chiave come minacce e incidenti.

Risposte della Commissione

https://www.eca.europa.eu/it/publications/sr-2026-19

Risposte del Centro europeo di competenza per la cibersicurezza (“ECCC”)

https://www.eca.europa.eu/it/publications/sr-2026-19

Risposte dell’Agenzia dell’Unione europea per la cibersicurezza (ENISA)

https://www.eca.europa.eu/it/publications/sr-2026-19

Cronologia

https://www.eca.europa.eu/it/publications/sr-2026-19

Team di audit

Le relazioni speciali della Corte dei conti europea illustrano le risultanze degli audit espletati su politiche e programmi dell'UE o su temi relativi alla gestione concernenti specifici settori di bilancio. La Corte seleziona e pianifica detti incarichi di audit in modo da massimizzarne l'impatto, tenendo conto dei rischi per la performance o la conformità, del livello delle entrate o delle spese, dei futuri sviluppi e dell'interesse pubblico e politico.

Il presente audit è stato espletato dalla Sezione di audit III della Corte, competente per l'audit della spesa per azioni esterne, sicurezza e giustizia, presieduta da George-Marius Hyzler, Membro della Corte. L'audit è stato diretto da George-Marius Hyzler, Membro della Corte, coadiuvato da: Romuald Kayibanda, capo di Gabinetto, e Annette Farrugia, attaché di Gabinetto; Cyril Messein, primo manager; Frédéric Soblet, capoincarico; Jurgen Manjé e Flavia Di Marco, auditor. Zoe Amador Martínez ha fornito assistenza linguistica. Dunja Weibel ha fornito supporto grafico.

Da sinistra a destra: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

DIRITTI D'AUTORE

HTML	ISBN 978-92-849-7875-5	ISSN 1977-5709	doi:10.2865/1878786	QJ-01-26-032-IT-Q
PDF	ISBN 978-92-849-7876-2	ISSN 1977-5709	doi:10.2865/0998018	QJ-01-26-032-IT-N

COME CITARE LA PRESENTE PUBBLICAZIONE:

Corte dei conti europea, relazione speciale 19/2026 “Individuare gli incidenti di cibersicurezza e risposta agli stessi – Il quadro di cooperazione dell’UE procede, ma è solo parzialmente efficace a causa dei ritardi nell’attuazione e della limitata condivisione delle informazioni”, Ufficio delle pubblicazioni dell’Unione europea, 2026.

Negli ultimi anni, l'UE ha rafforzato il proprio quadro normativo in materia di cibersicurezza e ha istituito reti e meccanismi per gestire gli incidenti informatici. L'UE finanzia anche progetti di cibersicurezza attraverso il programma Europa digitale

In conclusione, la Corte ha appurato che le azioni dell'UE facilitano solo in parte l'individuazione degli incidenti di cibersicurezza significativi e su vasta scala e la risposta agli stessi. Sebbene sia stato gradualmente posto in essere un quadro di cooperazione, sono ancora in corso i lavori per conseguirne la piena istituzione. La limitata condivisione delle informazioni, le carenze nella segnalazione e i notevoli ritardi nell'attuazione impediscono alle reti e ai meccanismi dell'UE di realizzare appieno il loro potenziale. I progetti perseguono obiettivi pertinenti, ma molti di essi si trovano ad affrontare sfide operative e ritardi. Inoltre, vi sono debolezze nel quadro generale di monitoraggio della performance della Commissione. La Corte formula raccomandazioni per ovviare a queste mancanze.

Relazione speciale della Corte dei conti europea presentata in virtù dell'articolo 287, paragrafo 4, secondo comma, del TFUE.

CURIA RATIONUM
CORTE DEI CONTI EUROPEA

Ufficio delle pubblicazioni dell'Unione europea

CORTE DEI CONTI EUROPEA
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1

Modulo di contatto: eca.europa.eu/it/contact
Sito Internet: eca.europa.eu
Social media: @EUauditors